The Correlations and the Power Characteristics of Special Classes of Binary Sequences for Multicarrier Communications

Xin Gao

A thesis presented to Lakehead University

In partial fulfillment of the requirement for the degree of

Master of Science in Electrical and Computer Engineering

Thunder Bay, Ontario, Canada, 2009

Contents

List of Figures

List of Tables

Abstract

In recent years, multicarrier communication has attracted considerable attention as a promising technology that enables transmission of high data rates. One of major drawbacks of multicarrier communications is the high peak-to-average power ratio (PAPR) of transmitted signals. Sequences and codes can be used as a solution to handle this problem.

This thesis focuses on the correlations and the power characteristics of special classes of binary sequences with ideal two-level autocorrelation. The aperiodic autocorrelations of the four classes of sequences with length $n = 2^m - 1$ are calculated and analyzed via merit factors, peak sidelobe levels (PSL), and average sidelobe levels (ASL). It is shown that merit factors of 3-term, 5-term and Welch-Gong sequences asymptotically approach to 3.0. Moreover, new growth rates of PSLs and ASLs of these sequences are conjectured. The power characteristics are calculated and discussed via peak-to-mean-envelope-power ratios (PMEPR) of the four classes of sequences with short length $n = 2^m - 1$ $(5 \leq m \leq 8)$, where PMEPRs give the upper bounds of PAPRs. Also, the PMEPRs of orthogonal codes generated by the sequences are calculated. Compared to the PMEPRs of Walsh code sets, it is claimed that the orthogonal codes generated by binary sequences can replace Walsh codes to obtain small PAPRs in multicarrier communications.

Chapter 1

Introduction

1.1 Multicarrier Communications

Multicarrier communications including orthogonal frequency division multiplexing (OFDM) and multicarrier code division multiple access (MC-CDMA) are of interest in many wireless applications. In practice, IEEE 802.11 [1] and 802.16 [2] are employing OFDM for wireless local area network (LAN) applications. Also, it has been adopted for digital video broadcastings [3]. MC-CDMA is a scheme of multicarrier systems, which combines the advantages of both OFDM and code division multiplexing access (CDMA) [4]. Since it has high capacity and flexibility, MC-CDMA is promising for next generation wireless communications. The main benefits of multicarrier communications are the following:

- Multicarrier communications convert a frequency selective channel into a set of frequency flat subchannels, which allow simple strategies to combat against fading channels.

- Data symbol constellation size and/or power allocation to each subcar-

rier can be independently adjusted according to the respective signal to noise (SNR). This leads to a better usage of bandwidth and allows near-capacity performance.

- Multicarrier communications can be efficiently implemented using simple and cheap hardwares of the fast discrete Fourier transform.

A major drawback of multicarrier communication schemes is the high peak-to-average power ratio (PAPR) of the transmitted signals. Since signals of multicarrier communications consist of a number of independently modulated subcarriers, they will give high peak-to-average power ratios when added up coherently. The high PAPR brings disadvantages such as an increased complexity of the analog-to-digital and digital-to-analog converters and a reduced efficiency of the power amplifier [5],[6].

1.2 Motivation

Many approaches have been proposed to solve the PAPR problem in multicarrier systems [7]. Using codes or sequences is one of the techniques for PAPR reduction. A simple idea introduced in [8] is to select good codes that minimize or reduce the PAPR for multicarrier transmissions. In [9] and [10], the results reported are the length 7 or 8 codes with a PAPR around 3 dB. In [11] and [12], m-sequences have been used for OFDM block coding to provide a low PAPR of the OFDM signals. The results suggest that m-sequences with length $n = 2^m - 1$, $3 \leq m \leq 10$, can yield PAPR values in the range 5-8 dB. However, designing coding schemes with a low PAPR, error-correcting capability, and simple implementation, is a challenging problem. Moreover, the search for good codes is still at its initial stage. In this thesis, we tried to find good codes or sequences for PAPR reduction in multicarrier

communications, starting from the known binary sequences with ideal two-level autocorrelation. For this purpose, we examined aperiodic and power characteristics of some candidate sequences.

1.3 Original Contributions

In our experiments, we focused on the four classes of binary sequences with idea two-level autocorrelation, i.e. m-sequences, 3-term, 5-term and Welch-Gong sequences. The main contributions of this thesis are summarized in the following.

- We calculated and analyzed aperiodic autocorrelations of four classes of binary sequences with ideal two-level autocorrelation, i.e., m-sequences, 3-term, 5-term and Welch-Gong (WG) sequences with length $n = 2^m - 1$, $5 \leq m \leq 21$, via merit factor, peak sidelobe level (PSL), and average sidelobe level (ASL). For merit factor, we found 3-term, 5-term and WG sequences have the similar properties with m-sequences, where the MFs asymptotically approach to 3.0. For peak sidelobe level, it is conjectured that

  $$PSL \approx c\sqrt{n}(\ln m)^2$$

  where for m-sequences, $c = 0.15$, and for 3-term, 5-term, and WG sequences, $c = 0.26$. For average sidelobe level, it is conjectured that

  $$ASL \approx c\sqrt{n}$$

  where for m-sequences, $c = 0.33$, and for 3-term, 5-term, and WG sequences, $c = 0.31$.

- We calculated and analyzed peak-to-mean-envelope-power ratios (PMEPR) of the four classes of sequences with short lengths $n = 2^m - 1$, $5 \leq m \leq$

8. The results suggest that most of PMEPRs and PAPRs produced by the four classes of sequences are below 8 dB. Moreover, the numerical results show that the distributions of PMEPR of 3-term sequences with length 31 and 5-term sequences with length 255 are better than that of m-sequences.

- We calculated and analyzed PMEPRs of the orthogonal codes generated by the four classes of sequences with short length $n = 2^m$, $5 \leq m \leq 8$. The highest value of PMEPRs of the orthogonal codes is 8.04 dB. The orthogonal code sets provide lower PMEPRs than conventional Walsh code sets . Moreover, the binary sequences generate the various orthogonal code sets depending on the primitive polynomials, which can be efficiently implemented using linear feedback shift registers (LFSR). In conclusion, the orthogonal codes can replace Walsh codes to obtain low PAPR in the multicarrier communications.

1.4 Thesis Outline

Chapter 2 introduces principles of multicarrier communications and basic concepts for sequences. Chapter 3 introduces special classes of binary sequences with ideal two-level autocorrelation, which will be examined in this thesis. Chapter 4 calculates and presents aperiodic autocorrelations of m-sequences, 3-term, 5-term and WG sequences with length $n = 2^m - 1$, $5 \leq m \leq 21$, via merit factor, peak sidelobe level, and average sidelobe level. Chapter 5 calculates and discusses the PMEPRs of the four classes of sequences and orthogonal codes generated by the sequences, and compares them to PMEPRs of Walsh code sets. Chapter 6 concludes the thesis, provides a summary of the work and proposes potential research work regarding

this issue.

Chapter 2

Preliminaries

2.1 Principles of Multicarrier Communication

The basic idea of multicarrier communications is to divide the transmitted bitstream into many different substreams and send them over many different narrowband subchannels [13]. The number of the subcarriers is chosen to ensure that each subchannel experiences flat fading, where the intersymbol interference (ISI) on each subchannel is negligible.

Consider a linearly modulated system with data rate R and bandwidth B . The coherence bandwidth for the channel is assumed to be $B_C < B$, so the signal experiences frequency-selective fading. The basic premise of multicarrier modulations is to break this wideband system into N linearly modulated subsystems in parallel, each with subchannel bandwidth $B_N = B/N$ and data rate $R_N \approx R/N$. The power spectrum of transmitted signals is shown in Figure 2.1. For sufficiently large N , the subchannel bandwidth $B_N \ll B_C$, which ensures relatively flat fading on each subchannel. In the time domain, the symbol time T_N of the modulated signals in each subchannel is approximate to $1/B_N$. So $B_N \ll B_C$ implies that $T_N \approx 1/B_N \gg 1/B_C \approx T_C$, where

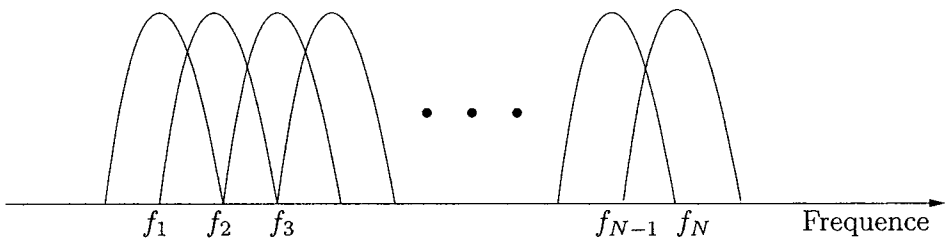


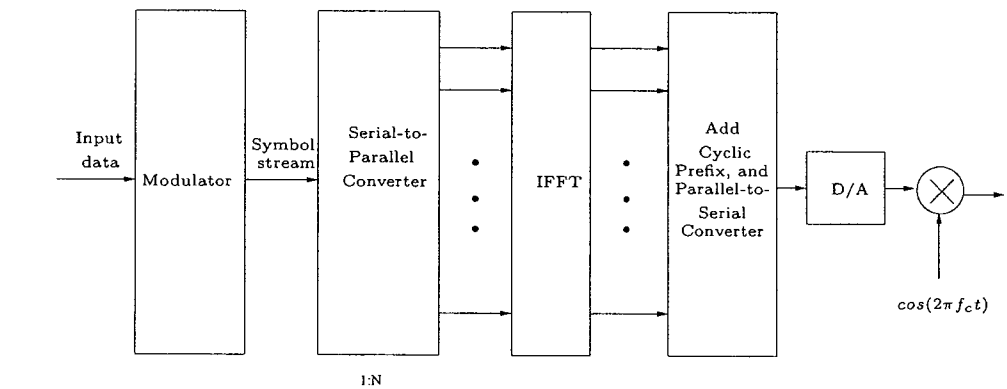
Figure 2.1: The power spectrum of transmitted signals of multicarrier systems

T_C denotes the delay spread of the channel. Thus, if N is sufficiently large, the symbol time is much greater than the delay spread. So each subchannel experiences little ISI degradation.

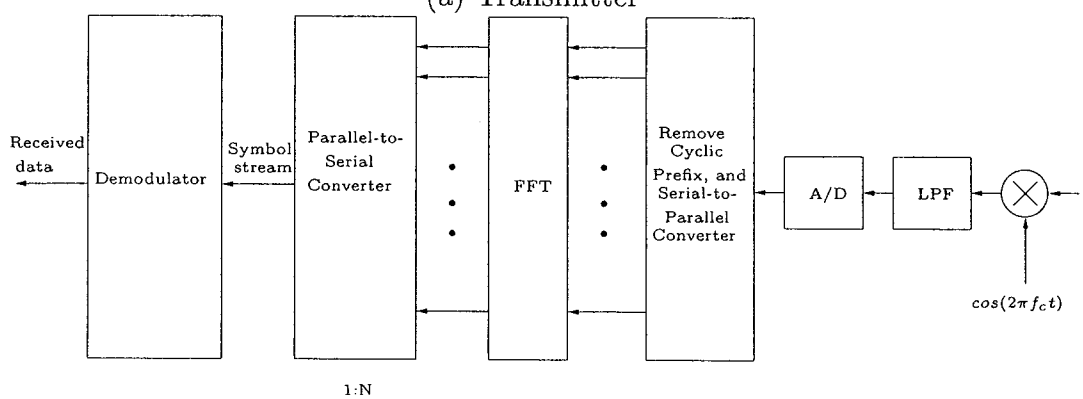
According to the structure of multicarrier communications, it requires separate modulators and demodulators on each subchannel, which was too complex to implement in the early years. However, the development of simple and cheap implementations of the discrete Fourier transform (DFT) and its inverse ignited its widespread use. The DFT and its inverse are performed using the fast Fourier transform (FFT) and inverse fast Fourier transform (IFFT) techniques.

2.1.1 Orthogonal frequency division multiplexing (OFDM) and orthogonal frequency division multiple access (OFDMA)

OFDM is a popular scheme for many existing and future wideband digital communication systems, whether wireless or over wirelines, such as asymmetric digital subscriber line (ADSL) broadband internet access system [14], digital video and audio broadcasting systems [3], IEEE 802.11 Wi-Fi systems [1], IEEE 802.16 WiMAX systems [2], etc.



(a) Transmitter



(b) Receiver

Figure 2.2: Block diagram of an OFDM system

The block diagram of an OFDM system is shown in Figure 2.2. From this figure, it can be seen that the high data rate stream of symbols is passed through serial to parallel converter resulting in a block of N low rate parallel data streams. This serial to parallel conversion increases the symbol duration by a factor of N. Each one of the low rate streams is then loaded onto a different subcarrier. The baseband transmitted signal implemented by IFFT for a single OFDM block corresponds to[1]

$$s(t) = \sum_{i=0}^{N-1} b_i e^{j2\pi i \Delta f t} p(t) \tag{2.1}$$

where b_i is the ith data symbol of the OFDM block, $p(t)$ is a pulse shaping function existing in one OFDM symbol duration, and Δf is the frequency spacing between adjacent subcarriers [13]. To minimize the effects of inter-symbol interference caused by the multipath nature of the channel, the cyclic prefix is appended to the beginning of each OFDM symbol.

At the receiver side, the received signal in one OFDM block corresponds to

$$r(t) = \sum_{i=0}^{N-1} h_i b_i e^{j2\pi i \Delta f t} p(t) + n(t) \tag{2.2}$$

where h_i denotes the channel fading coefficients for the ith subchannel which is assumed to be a flat fading, and $n(t)$ is additive white Gaussian noise. After the OFDM baseband signal is recovered, the cyclic prefix is removed. A fast Fourier transform (FFT) is then applied to recover the original transmitted data in parallel. Finally, the parallel data substreams are aggregated into the serial data stream and demodulated to recover the original high speed information data stream.

Compared with single-carrier modulation schemes, OFDM can cope with severe channel conditions including narrowband interference, attenuation of

[1]In this thesis, $j = \sqrt{-1}$.

high frequencies in a long copper wire, and frequency-selective fading due to multipath environments.

Recently, orthogonal frequency division multiple access (OFDMA), which is a multi-user version of OFDM, has emerged as one of the prime multiple-access schemes for broadband wireless network, e.g., IEEE 802.16a/d/e Mobile WiMAX [2], IEEE 802.20 [15], and 3G-LTE [16], etc. The OFDMA scheme allows multiple access to the same wideband channel, which is divided into narrowband subchannels. Each subchannel can be considered independently so that multiple users can transmit and receive at the same time. According to the feedback information about the channel conditions, the system can adaptively assign the subcarriers to multiple users, and the modulation and coding schemes on each subcarrier can be adapted to provide improved coverage and throughput [17].

2.1.2 Multicarrier code division multiple access (MC-CDMA)

Multicarrier code division multiple access (MC-CDMA) inherits the benefits of both multicarrier communications and code division multiple access (CDMA) [4]. Hence the scheme is promising for next generation wireless communications, which have rigid demands on system capacity and flexibility.

In MC-CDMA, each data symbol is spread over multiple subcarriers with a user specific code. Each data modulated by a spreading code is transmitted on different subcarriers. Consequently, all users share the same frequency band at the same time. Figure 2.3(a) illustrates the MC-CDMA transmitter of the k-th user. Here, the data symbols b^k of kth user is multiplied by $\mathbf{C}^k = [c_1^k, c_2^k, c_3^k, \ldots, c_N^k]$, where c_i^k is the spreading code element for the kth

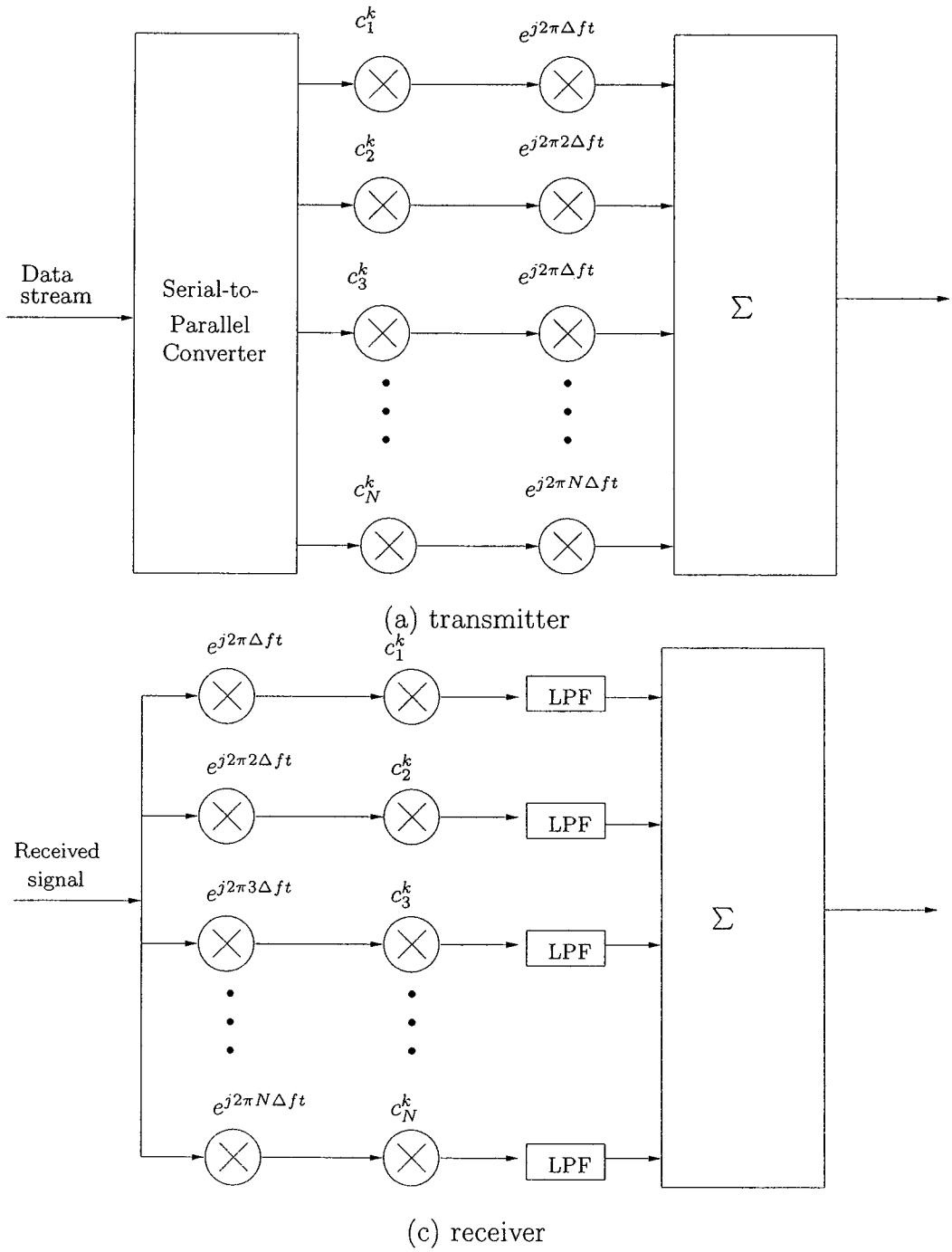


Figure 2.3: A Block diagram of MC-CDMA scheme

user, and then transmitted on all N orthogonal subcarriers. The N signal components are summed and converted to passband prior to transmission. The baseband transmitted signal implemented by IFFT corresponding to the kth user is

$$s^k(t) = \sum_{i=1}^{N} b^k c_i^k e^{j2\pi i \Delta f t} p(t) \tag{2.3}$$

where Δf is the frequency spacing between adjacent subcarriers, and $p(t)$ is a pulse shaping function existing in one MC-CDMA symbol duration.

The receiver reverses the operation of the transmitter as shown in Figure 2.3(b). The received signal can be represented as

$$r(t) = \sum_{i=1}^{N} \sum_{k=1}^{K} h^k b^k c_i^k e^{j2\pi i \Delta f t} p(t) + n(t). \tag{2.4}$$

where h^k denotes the channel fading coefficients for the kth user, which is assumed to be a flat fading, K is the number of users, and $n(t)$ is additive white Gaussian noise. The first step is to perform the FFT operation to transform the received signal to the frequency domain. To detect the kth user data symbol, the N subcarrier components are despread using the kth user spreading code $C^k = [c_1^k, c_2^k, \ldots, c_N^k]$. As the MC-CDMA received signal is combined in the frequency domain, the receiver can always employ all the received signal energy scattered in the frequency domain. That is the main advantage of the MC-CDMA schemes over other schemes.

2.2 Sequences for Communications

2.2.1 Sequences for code division multiple access systems (CDMA)

In code division multiple access (CDMA) systems, multiple access capability is primarily achieved by means of spreading codes or sequences. Orthogonal codes are assigned to different users in a CDMA system, known as spreading codes. Moreover, sequences in the CDMA are used for data scrambling, separation and identification of cells and users.

The binary valued Walsh codes are widely used as spreading codes in wireless CDMA system. The Walsh codes are perfectly orthogonal codes and are ideal for synchronous CDMA communications. The IS-95 wireless communication standard uses orthogonal 64-length Walsh codes as spreading codes. Also, it employs m-sequence of length $(2^{42} - 1)$ as scrambling codes, and de Bruijn sequences of length 2^{15} for the cell identification in the forward and reverse transmission [18]. The Wideband CDMA (WCDMA) employs variable length orthogonal Walsh codes as spreading codes and Gold and Z_4 sequences as scrambling codes [16].

2.2.2 Sequences for multicarrier communications

The Baker sequences [19] are binary sequences with optimal aperiodic autocorrelation, where all out-of-phase aperiodic autocorrelation magnitudes are at most 1. The 11 bit Barker sequences are employed as spreading sequences of direct sequence spread spectrum physical layer of IEEE 802.11 wireless local area network (WLAN) standard [1].

Golay complementary sequences [20] are adopted as the sets of synchro-

nization codes in the third generation cellular standard [16]. Recently, Golay complementary sequences are considered to be an option for reducing the high peak-to-mean-envelope-power ratio (PMEPR)of the OFDM systems [21], [10], [22].

2.3 Basic Concepts for Sequences

In this section, we review the definitions and basic concepts of sequences.

2.3.1 Finite fields and primitive polynomials

Let m be a positive integer. To construct the finite field $GF(2^m)$ of order 2^m, we choose that $f(x)$ is an irreducible polynomial over $GF(p)$ of degree m. α is an element that satisfies $f(\alpha) = 0$. Then

$$GF(2^m) = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} | a_i \in GF(2)\}, \tag{2.5}$$

where α is the primitive element of $GF(2^m)$. $GF(2^m)$ also can be presented as $GF(2^m) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$. The polynomials having primitive elements as a zero is called *primitive polynomials*.

2.3.2 Periodic sequences

The sequences $a_0, a_1, \ldots$ is denoted as $\mathbf{a} = \{a_u\}$. If there exist any integer $n > 0$ such that

$$a_{u+n} = a_u, \tag{2.6}$$

then the sequence is said to be *periodic*, and the smallest integer n is called a *period* of the sequence.

2.3.3 Trace function

Note that $GF(q)$ is a finite field with q elements. Let n and m be positive integers, and m be a divisor of n. For $x \in GF(2^m)$, a trace function from $GF(2^n)$ to $GF(2^m)$, $Tr_m^n(x)$ is defined by

$$Tr_m^n(x) = x + x^{2^m} + \cdots + x^{2^{m(\frac{n}{m}-1)}}, \tag{2.7}$$

where x is an element of $GF(2^n)$, and the addition is computed modulo 2^m. If $m = 1$ and the context is clear, $Tr_m^n(x)$ can be simply denoted as $Tr(x)$.

Example 1 [23] Consider a finite field $GF(2^3)$ generated by a primitive polynomial $f(x) = x^3 + x + 1$. The primitive element α is a root of the primitive polynomial, i.e., $\alpha^7 = 1$, $\alpha^3 + \alpha + 1 = 0$. Then,

$$Tr(1) = 1 + 1 + 1 = 1,$$

$$Tr(\alpha) = \alpha + \alpha^2 + \alpha^4 = 0,$$

$$Tr(\alpha^2) = Tr(\alpha^4) = Tr(\alpha) = 0,$$

$$Tr(\alpha^3) = \alpha^3 + \alpha^6 + \alpha^5 = 1,$$

$$Tr(\alpha^6) = Tr(\alpha^5) = Tr(\alpha^3) = 1,$$

Hence, a binary sequence $a_u = Tr(\alpha^u)$, $u = 0, 1, \ldots, 6$, is $\mathbf{a} = (1, 0, 0, 1, 0, 1, 1)$. The sequence $\mathbf{a}$ is called a binary m-sequence of period 7, and $Tr(x)$ is a trace representation of a binary m-sequence of period 7.

2.3.4 Cyclic equivalence and distinctness

Let $\mathbf{a} = \{a_u\}$ and $\mathbf{b} = \{b_u\}$ be two periodic sequences. Then, they are called *cyclically equivalent* if there exists an integer k such that

$$a_u = b_{u+k} \text{ for all } u \geq 0$$

denoted by $\mathbf{a} = L^k(\mathbf{b})$. Otherwise, they are called *cyclically distinct*.

2.3.5 Decimation of sequences

Let $\mathbf{a}$ be a binary sequence of period n. Let $0 < s < n$ be a positive integer. If the elements of a sequence $\mathbf{b} = \{b_u\}$ are defined by

$$b_u = a_{su}, \quad u = 0, 1, \cdots,$$

where the indices are computed modulo n, then $\mathbf{b}$ is called an s-decimation sequence of $\mathbf{a}$, denoted by $\mathbf{b} = \mathbf{a}^{(s)}$. Moreover, if $\gcd(s, n) = 1$, then $\mathbf{a}^{(s)}$ is also a binary sequence of period n. In particular, if the $\mathbf{a} = \{a_u\}$ is binary sequence of period $n = 2^m - 1$ generated by $a_u = Tr(\alpha^u), \quad u = 0, 1, \cdots, 2^m - 2$, where α is the primitive element of GF(2^m), then the $\mathbf{a}^{(s)} = \{a_u^{(s)}\}$ is also a binary sequence generated by $a_u^{(s)} = Tr(\alpha^{us}), \quad u = 0, 1, \cdots, 2^m - 2$.

Example 2 In Example 1, $\mathbf{a}^{(s)}$, a 3-decimation of $\mathbf{a}$, is given by

$$\mathbf{a}^{(3)} = (1, 1, 1, 0, 1, 0, 0)$$

We also can check that $\mathbf{a}^{(3)}$ can be generated by $Tr(\alpha^{3u})$, $u = 0, 1, \cdots, 6$.

2.3.6 Periodic autocorrelation of binary sequences

A periodic autocorrelation function of a binary sequence $\mathbf{a} = \{a_u\}$ of period n, denoted by $C_{\mathbf{a}}(\tau)$, is defined as

$$C_{\mathbf{a}}(\tau) = \sum_{u=0}^{n-1} (-1)^{a_{u+\tau} + a_u}, \ 0 \leq \tau \leq n - 1 \tag{2.8}$$

where τ is a phase shift of $\mathbf{a}$, and the indices are computed modulo n. $C_{\mathbf{a}}(\tau)$ measures the amount of similarity between the sequence and its phase shift. For $\tau = 0$, $C_{\mathbf{a}}(0) = \sum_{u=0}^{n-1} (-1)^{a_u + a_u} = n$ is always the highest value.

The sequence $\mathbf{a}$ of period n is said to have the *ideal two-level autocorrelation function*, if $C_{\mathbf{a}}(\tau)$ is given by

$$C_{\mathbf{a}}(\tau) = \begin{cases} n & \text{if } \tau \equiv 0 \pmod{n} \\ -1 & \text{if } \tau \not\equiv 0 \pmod{n} \end{cases}$$

2.3.7 Orthogonal codes

A periodic crosscorrelation function of binary sequences $\mathbf{a}$ and $\mathbf{b}$ of period n is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{u=0}^{n-1} (-1)^{a_{u+\tau}+b_u}, \quad 0 \leq \tau \leq n-1$$

where τ is a phase shift of the sequence $\mathbf{a}$, and the indices are computed modulo n. In particular, if $\tau = 0$,

$$C_{\mathbf{a},\mathbf{b}}(0) = \sum_{u=0}^{n-1} (-1)^{a_u+b_u} = \langle \mathbf{a}, \mathbf{b} \rangle$$

is the *inner product* of the sequences $\mathbf{a}$ and $\mathbf{b}$. Let $\mathbf{a}_i$ be a binary sequence of period n, $i = 1, 2, \ldots, N$, and $A = \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_N\}$ be a set of the binary sequences of size N. Then a pair of sequences $(\mathbf{a}_i, \mathbf{a}_k)$ in the set A is called *mutually orthogonal* if and only if

$$\langle \mathbf{a}_i, \mathbf{a}_k \rangle = 0 \text{ for all } 1 \leq i \neq k \leq N.$$

If any pair of A is mutually orthogonal, then A is called an *orthogonal code set.*

A Hadamard matrix H_n is a square matrix of dimension $n \times n$ with two kinds of elements $+1$ and -1 satisfying

$$H_n H_n^T = H_n^T H_n = nI_n, \tag{2.9}$$

where H_n^T stands for transpose of H_n, and I_n is the identity matrix of order n [24]. If we consider the rows of H_n as N sequences $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$, then $\langle \mathbf{a}_i, \mathbf{a}_k \rangle = 0$ for all $1 \leq i \neq k \leq n$. Therefore, any pair of rows of the $n \times n$ Hadamard matrix is orthogonal, and each row constitutes an orthogonal code set of size n.

A method to generate Hadamard matrices with $n = 2^m$ $(n \geq 0)$ is using a simple recursive procedure

$$H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}, \tag{2.10}$$

with a given H_n. Starting from $H_1 = [1]$, we can generate Hadamard matrices by the recursive procedure.

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \cdots$$

Then, we can consider all row sequences in this matrix as a code set named the Walsh code. The Walsh code contains one row of all 1s and the other rows of equal number of -1s and $+1$s.

An alternative method to generate Hadamard matrices of size $n = 2^m$ is using binary sequences with two-level autocorrelation. Let $\mathbf{a}$ be a binary sequence of length $2^m - 1$ with two-level autocorrelation. Consider the set

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & & L^0(\mathbf{a}) & \\ 0 & & L^1(\mathbf{a}) & \\ \vdots & & \vdots & \\ 0 & & L^{2^m-2}(\mathbf{a}) & \end{bmatrix}, \tag{2.11}$$

where $L^i(\mathbf{a})$, $i = 0, 1, \ldots, 2^m - 2$, is the i phase shift of $\mathbf{a}$. Denote that $\mathbf{a}_i, \mathbf{a}_k$ are the rows of set A, then,

$$\langle \mathbf{a}_i, \mathbf{a}_k \rangle = \sum_{u=0}^{n} (-1)^{a_{iu}+a_{ku}} = 0 \text{ for all } 1 \leq i \neq k \leq n.$$

Mapping the elements $\{0, 1\}$ onto $\{+1, -1\}$, respectively, then the set A of size 2^m becomes the orthogonal code set $\tilde{A}$. More details on Hadamard matrices and their constructions are presented in [24].

Example 3 In Example 1, all the cyclic shifts of $\mathbf{a}$ are

$$L^0(\mathbf{a}) = \{1, 0, 0, 1, 0, 1, 1\};$$

$$L^1(\mathbf{a}) = \{0, 0, 1, 0, 1, 1, 1\};$$

$$L^2(\mathbf{a}) = \{0, 1, 0, 1, 1, 1, 0\};$$

$$L^3(\mathbf{a}) = \{1, 0, 1, 1, 1, 0, 0\};$$

$$L^4(\mathbf{a}) = \{0, 1, 1, 1, 0, 0, 1\};$$

$$L^5(\mathbf{a}) = \{1, 1, 1, 0, 0, 1, 0\};$$

$$L^6(\mathbf{a}) = \{1, 1, 0, 0, 1, 0, 1\};$$

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

$$\tilde{A} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \end{bmatrix}$$

Chapter 3

Binary Sequences With Ideal Two-level Autocorrelation

The high PAPR of transmitted signals, which is a major disadvantage of multicarrier communications, can be handled by good sequences or codes. In this chapter, we introduced the classes of binary sequences examined in our experiments, which can be used to solve the PAPR problem.

3.1 Development of Binary Pseudorandom Sequences

Binary sequences with ideal autocorrelation properties are widely used in spread spectrum communication systems, ranging, stream cipher cryptosystems, code division multiple access (CDMA) systems, etc. The well-known classes of binary sequences of period $n = 2^m - 1$ with two-level autocorrelation include m-sequences [25], Gordon-Mills-Welch (GMW) sequences [26], generalized GMW sequences [27], Legendre sequences [28], and Hall's sextic residue sequences [29], [30]. Recently, several new classes of binary sequences

have been constructed and discovered. In 1998, Maschietti [31] constructed hyperoval sequences. Multiple trace term sequences, including 3-term sequences, 5-term sequences, and WG sequences are conjectured to be two-level autocorrelation sequences in [32]. In [33], Dillon and Dobbertin constructed the Kasami-power function sequences (or B_k sequences). A complete summary of classes of all known binary sequences of period $n = 2^m - 1$ with two-level autocorrelation is listed in [33].

3.2 Binary m-sequences

A maximal length shift register sequence, also called an m-sequence, ML-sequence, or pseudoniose sequence, is a binary sequence $\mathbf{a} = (a_0, a_1, \ldots, a_{2^m-2})$ of period $2^m - 1$ for which

$$a_u = Tr(\beta\alpha^u) \quad \text{for all } 0 \leq u \leq 2^m - 1 \tag{3.1}$$

where α is a primitive element of the finite field $GF(2^m)$, β is a fixed nonzero element from the same field. A binary m-sequence of a given period $2^m - 1$ is not unique, since the choice of α and β is arbitrary.

Alternatively, we can define a binary m-sequence $\mathbf{a}$ using a linear recurrence relation. Let $f(x) = 1 + \sum_{i=1}^{m} c_i x^i$ be the primitive polynomial of degree m over $GF(2)$. Let $(a_0, a_1, \ldots, a_{2^m-2})$ be a 0/1 sequence of period $2^m - 1$ whose first m elements take arbitrary values (not all zeros), and whose subsequent elements satisfy the linear recurrence relation, i.e.,

$$a_{u+m} = \sum_{i=0}^{m-1} c_i a_{u+i} \mod 2 \quad \text{for } 0 \leq u \leq 2^m - 1 - m. \tag{3.2}$$

This also gives an m-sequence. This alternative definition can be physically implemented using a linear feedback shift register (LFSR) with m stages.

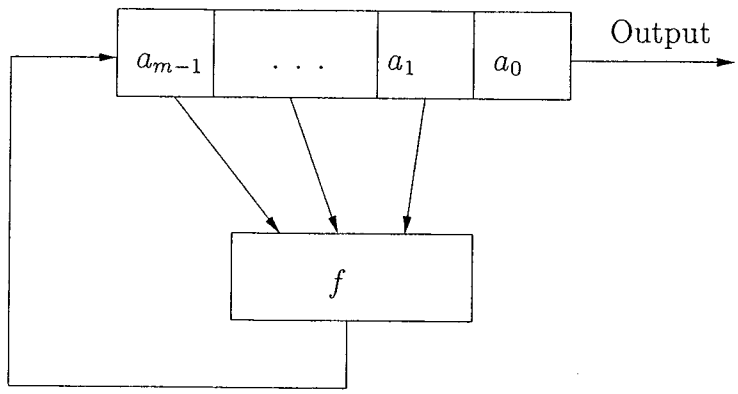


Figure 3.1: A block diagram of a m-stage LFSR for a binary m-sequence of period $2^m - 1$

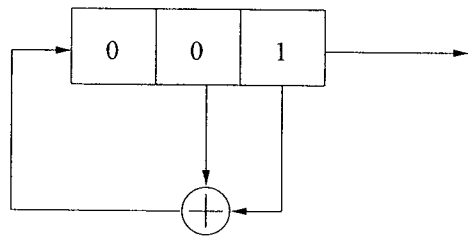


Figure 3.2: A 3-stage LFSR for Example 4

In this case, the primitive polynomial $f(x) = 1 + \sum_{i=1}^{m} c_i x^i$ is also called a characteristic polynomial of sequence **a**. A block diagram of a LFSR is shown in Figure 3.1.

Example 4 In Example 1, the sequence **a** is an m-sequence, and it can be generated by a 3-stage linear feedback shift register (LFSR) shown in Figure 3.2. The linear recurrence function is $a_{u+3} = a_u + a_{u+1}$, $0 \leq u \leq 4$. The output sequence with the initial state $(a_0, a_1 a_2) = (1, 0, 0)$ is

$$10010111001011\ldots.$$

which is identical to **a** in Example 1.

If the $\mathbf{a} = \{a_u\}$ is an m-sequence of period $2^m - 1$ generated by $a_u =$

$Tr(\alpha^u), \quad u = 0, 1, \cdots, n-1$, where α is the primitive element of $GF(2^m)$, the number of all different primitive polynomials is

$$\frac{\phi(2^m - 1)}{m},$$

where $\phi(x)$ is the Euler phi function that denotes the number of integers in the range from 1 to x that are coprime to x. Considering the cyclical equivalence, there are total $\frac{\phi(2^m-1)}{m} \times (2^m - 1)$ m-sequences of length $n = 2^m - 1$. Similarly, the numbers of all 3-term, 5-term, and WG sequences are $\frac{\phi(2^m-1)}{m} \times (2^m - 1)$ [23].

3.3 Three-term and Five-term Sequences

Three-term and five-term sequences are two classes of sequences with two-level autocorrelation, which are represented by multiple trace terms.

The construction of 3-term sequences is given in [23]. For odd $m \geq 5$, and $m = 2l + 1$, with period $n = 2^m - 1$, the binary sequence

$$a_u = Tr(\alpha^u) + Tr(\alpha^{q_1 u}) + Tr(\alpha^{q_2 u}), u = 0, 1, \ldots, 2^m - 2 \qquad (3.3)$$

has two-level autocorrelation, where α is a primitive element of $GF(2^m)$ and

$$q_1 = 2^l + 1, q_2 = 2^l + 2^{l-1} + 1. \qquad (3.4)$$

According to the construction, the 3-term sequences are considered as the sum of three distinct binary m-sequences, i.e.,

$$\mathbf{a} = \mathbf{a}_0 + \mathbf{a}_0^{(q_1)} + \mathbf{a}_0^{(q_2)},$$

where $\mathbf{a}_0 = \{a_u = Tr(\alpha^u)\}$, $u = 0, 1, \ldots, 2^m - 2\}$, therefore it can be implemented by three LFSRs, where each LFSR generates $\mathbf{a}_0^{(q_i)}$, $i = 0, 1,$ and 2 (set $q_0 = 1$), and the feedback configuration of $\mathbf{a}_0^{(q_i)}$ is defined by the minimal

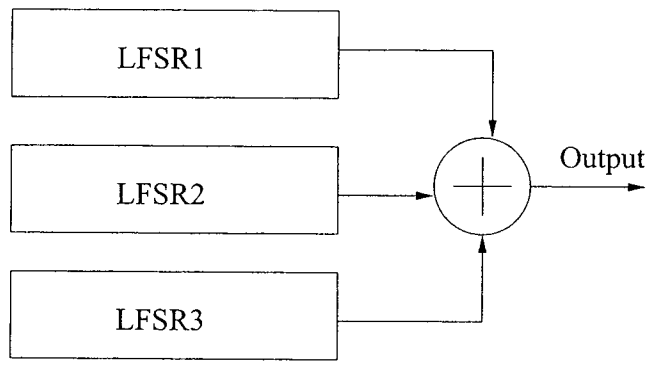


Figure 3.3: LFSR implementation of 3-term sequences

polynomials of α^{q_i}, $i = 0, 1, \text{and } 2$. The minimal polynomial $m(x)$ can be calculated by

$$m(x) = (x - \alpha^{q_i})(x - \alpha^{2q_i})(x - \alpha^{2^2 q_i}) \cdots (x - \alpha^{2^{m_s-1} q_i})$$

where m_s is the smallest positive integer such that $q_i = 2^{m_s} q_i \pmod{2^m - 1}$. The block diagram of LFSR of 3-term sequences is shown in Figure 3.3.

Example 5 Let $m = 5$ and $l = 2$. Let $f_0(x) = x^5 + x^3 + 1$ and α be a root of $f_0(x)$. Then $q_1 = 1 + 2^2 = 5$, $q_2 = 1 + 2 + 2^2 = 7 \bmod 31$. Therefore, we have

$$\mathbf{a} = Tr(x + x^5 + x^9) = Tr(x) + Tr(x^5) + Tr(x^7) = \mathbf{a}_0 + \mathbf{a}_0^{(5)} + \mathbf{a}_0^{(7)}$$

The minimal polynomials of α^5 and α^7 are $f_1(x) = x^5 + x^4 + x^3 + x + 1$ and $f_2(x) = x^5 + x^4 + x^3 + x^2 + 1$, respectively. The LFSR implementation of $\mathbf{a}$ is shown in Figure 3.4.

$\mathbf{a}_0 = Tr(\alpha^u)$	10000101011101100011111100110100
$\mathbf{a}_0^{(5)} = Tr(\alpha^{5u})$	11101100111000011010100100011011
$\mathbf{a}_0^{(7)} = Tr(\alpha^{7u})$	11111011100010101101000011001000
$\mathbf{a} = \mathbf{a}_0 + \mathbf{a}_0^{(5)} + \mathbf{a}_0^{(7)}$	10010010000111010100011111011011

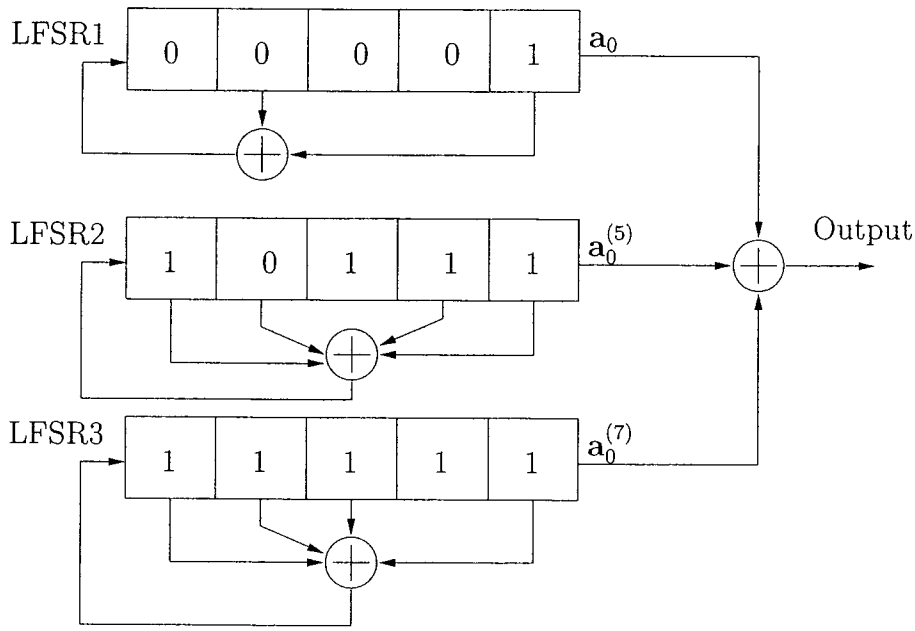


Figure 3.4: LFSR implementation of 3-term sequences of period 31

The definition of 5-term sequences is given in [23]. Let $m \neq 0 \bmod 3$, α be a primitive element of $GF(2^m)$, and $t(x) = x + x^{q_1} + x^{q_2} + x^{q_3} + x^{q_4}, x \in GF(2^m)$, where the q_i's are given by Table 3.1. Let $\mathbf{a} = \{a_u\}$ whose elements are given by

$$a_u = Tr(t(\alpha^u)),\ u = 0, 1, \ldots, 2^m - 2 \tag{3.5}$$

Then, $\mathbf{a}$ is called five-term sequence, which is a class of sequences with two-level autocorrelation. Five-term sequences can be implemented as the sum of five LFSRs, i.e.,

$$\mathbf{a} = \mathbf{a}_0 + \mathbf{a}_0^{(q_1)} + \mathbf{a}_0^{(q_2)} + \mathbf{a}_0^{(q_3)} + \mathbf{a}_0^{(q_4)},$$

where each $\mathbf{a}_0^{(q_i)} = \{a_u = Tr(\alpha^u)\}$, $i = 0, 1, 2, 3$, and 4 (set $q_0 = 1$) is generated by LFSR with the minimal polynomial $f_{\alpha^{q_i}}(x)$, which is illustrated in Figure 3.5.

Table 3.1: Power exponents of 5-term sequences

$m = 3l - 1$	$q_1 = 2^l + 1$ $q_2 = 2^{2l-1} + 2^{l-1} + 1$ $q_3 = 2^{2l-1} - 2^{l-1} + 1$ $q_4 = 2^{2l-1} + 2^l - 1$
$m = 3l - 2$	$q_1 = 2^{l-1} + 1$ $q_2 = 2^{2l-2} + 2^{l-1} + 1$ $q_3 = 2^{2l-2} - 2^{l-1} + 1$ $q_4 = 2^{2l-1} + 2^{l-1} + 1$

Example 6 A 5-term sequence of period 127 For $m = 7$ and $l = 3$, let $f(x) = x^7 + x + 1$, and let α be a root of $f(x)$ in $GF(2^7)$. Then

$$q_1 = 2^2 + 1 = 5,\ q_2 = 2^4 + 2^2 + 1 = 21,$$

$$q_3 = 2^4 - 2^2 + 1 = 13, \text{ and } q_4 = 2^5 - 2^2 + 1 = 29. \pmod{127}$$

$$\mathbf{a} = Tr(x + x^5 + x^{21} + x^{13} + x^{29}) = \mathbf{a}_0 + \mathbf{a}_0^{(5)} + \mathbf{a}_0^{(21)} + \mathbf{a}_0^{(13)} + \mathbf{a}_0^{(29)}$$

The minimal polynomials $f_{\alpha^{q_i}}(x)$ of LFSRs which generate $\mathbf{a}_0^{(q_i)}$, $i = 0, 1, \ldots, 4$ are

$$\begin{aligned} f_{\alpha^5}(x) &= (x - \alpha^5)(x - \alpha^{10})(x - \alpha^{20})(x - \alpha^{40})(x - \alpha^{80})(x - \alpha^{33})(x - \alpha^{66}) \\ &= x^7 + x^3 + x^2 + x + 1 \end{aligned}$$

$$\begin{aligned} f_{\alpha^{21}}(x) &= (x - \alpha^{21})(x - \alpha^{42})(x - \alpha^{84})(x - \alpha^{42})(x - \alpha^{82})(x - \alpha^{37})(x - \alpha^{74}) \\ &= x^7 + x^6 + x^3 + x + 1 \end{aligned}$$

$$\begin{aligned} f_{\alpha^{13}}(x) &= (x - \alpha^{13})(x - \alpha^{26})(x - \alpha^{52})(x - \alpha^{104})(x - \alpha^{81})(x - \alpha^{35})(x - \alpha^{70}) \\ &= x^7 + x^6 + x^5 + x^2 + 1 \end{aligned}$$

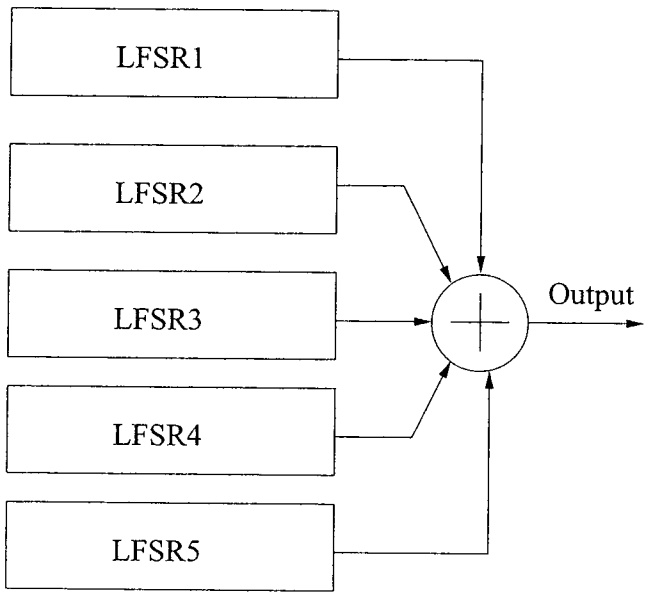


Figure 3.5: LFSR implementation of 5-term sequences

$$f_{\alpha^{29}}(x) = (x-\alpha^{29})(x-\alpha^{58})(x-\alpha^{116})(x-\alpha^{105})(x-\alpha^{83})(x-\alpha^{39})(x-\alpha^{78})$$
$$= x^7 + x^4 + 1$$

The LFSR implementation of the 5-term sequence **a** is shown in Figure 3.6.

3.4 Welch-Gong Sequences

The construction of Welch-Gong sequences is given in [32]. Let $m \neq 0 \bmod 3$, α be a primitive element of $GF(2^m)$, the trace representation of Welch-Gong transformation sequences or WG sequence $\mathbf{a} = \{a_u\}$, is given by

$$a_u = \sum_{u \in I} Tr(x^u) \tag{3.6}$$

where $I = I_1 \bigcup I_2$ for $m = 3l - 1$, where

$$I_1 = \{2^{2l-1} + 2^{l-1} + 2 + u | 0 \leq u \leq 2^{l-1} - 3\} \tag{3.7}$$

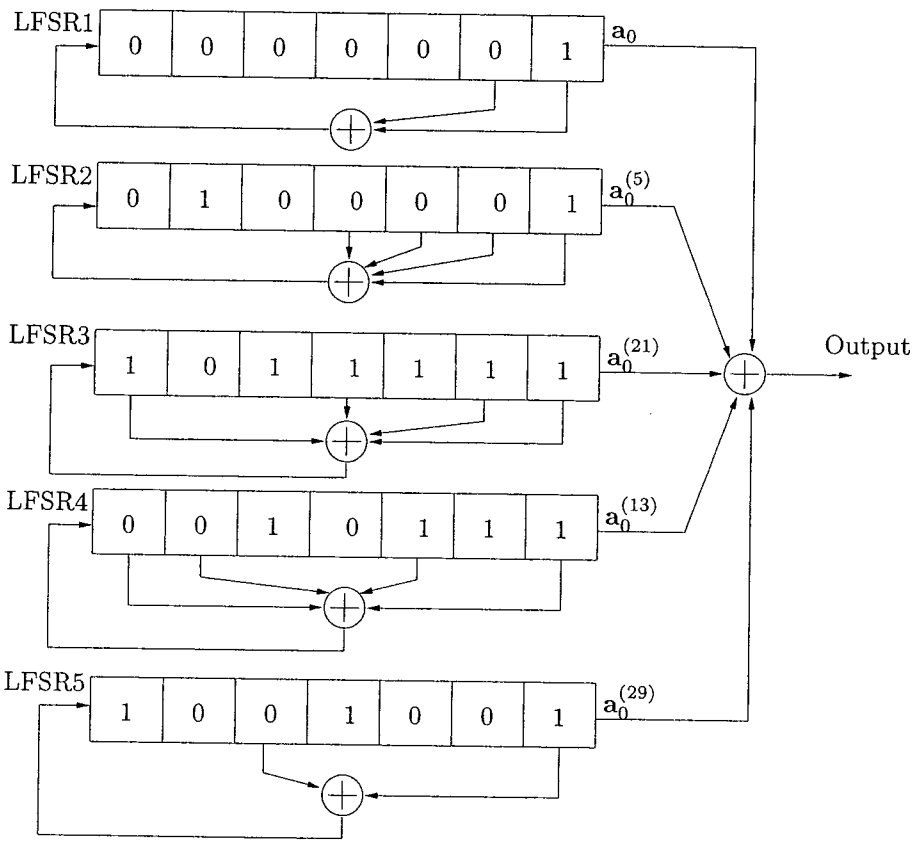


Figure 3.6: LFSR implementation of 5-term sequence of period 127

$$I_2 = \{2^{2l} + 3 + 2u | 0 \leq u \leq 2^{l-1} - 2\} \tag{3.8}$$

and where $I = \{1\} \bigcup I_3 \bigcup I_4$ for $m = 3l - 2$, where

$$I_3 = \{2^{l-1} + 2 + u | 0 \leq u \leq 2^{l-1} - 3\} \tag{3.9}$$

$$I_4 = \{2^{2l-1} + 2^{l-1} + 2 + u | 0 \leq u \leq 2^{l-1} - 3\} \tag{3.10}$$

Example 7 A WG sequence of period 127 For $m = 7$ and $l = 3$, let $f(x) = x^7 + x + 1$, and let α be a root of $f(x)$ in $GF(2^7)$. Then the WG sequences are

$$\mathbf{a} = Tr(x + x^3 + x^7 + x^{19} + x^{29}) = \mathbf{a}_0 + \mathbf{a}_0^{(3)} + \mathbf{a}_0^{(7)} + \mathbf{a}_0^{(19)} + \mathbf{a}_0^{(29)}$$

The minimal polynomials are

$$f_{\alpha^3}(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^{24})(x-\alpha^{48})(x-\alpha^{96})(x-\alpha^{65})$$
$$= x^7 + x^3 + x + 1$$

$$f_{\alpha^7}(x) = (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{28})(x-\alpha^{56})(x-\alpha^{112})(x-\alpha^{97})(x-\alpha^{67})$$
$$= x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$$

$$f_{\alpha^{19}}(x) = (x-\alpha^{19})(x-\alpha^{38})(x-\alpha^{76})(x-\alpha^{25})(x-\alpha^{50})(x-\alpha^{100})(x-\alpha^{73})$$
$$= x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$$

$$f_{\alpha^{29}}(x) = (x-\alpha^{29})(x-\alpha^{58})(x-\alpha^{116})(x-\alpha^{105})(x-\alpha^{83})(x-\alpha^{39})(x-\alpha^{78})$$
$$= x^7 + x^4 + 1$$

The LFSR implementation of the WG sequence **a** is shown in Figure 3.7.

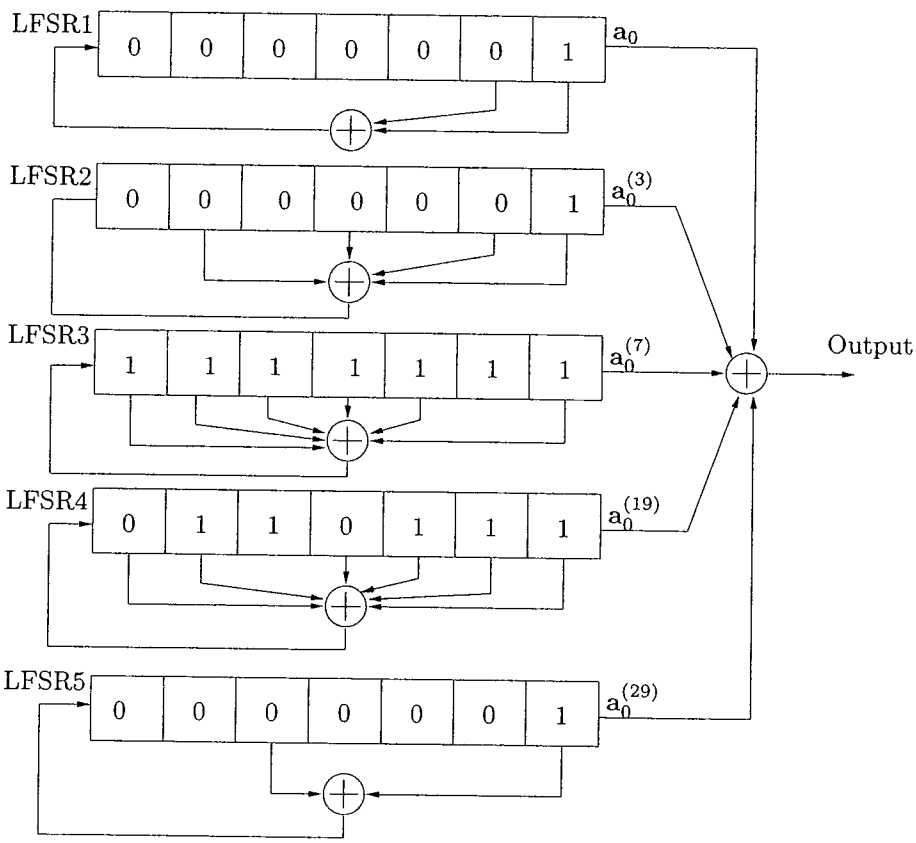


Figure 3.7: LFSR implementation of WG sequence of period 127

Chapter 4

Aperiodic Autocorrelation Properties of Binary Sequences

In order to search for good codes or sequences to solve the high PAPR problem in multicarrier communications, we need to examine the aperiodic and the power characteristics of candidate sequences. Since aperiodic autocorrelation properties of binary sequences have intimate connection with PAPRs, we calculated and discussed them over the special classes of sequences.

4.1 Aperiodic Autocorrelation of Binary Sequences

4.1.1 Definition of aperiodic autocorrelations

The aperiodic autocorrelation of $\mathbf{a}$ at shift τ is defined as

$$\rho_{\mathbf{a}}(\tau) = \sum_{u=0}^{n-\tau-1} (-1)^{a_{u+\tau}+a_u} \tag{4.1}$$

where $\mathbf{a} = \{a_0, a_1, \cdots, a_{n-1}\}$ is a binary sequences of length n. It has been of interest in the study of sequence design to find binary sequences whose aperiodic autocorrelations are, in some suitable sense, collectively small.

In 1953 Barker [19] proposed a strict condition for an ideal sequence. Later, Subsequent authors relaxed Barker's condition to

$$|\rho_{\mathbf{a}}(\tau)| \leq 1 \quad \text{for } 0 < \tau < n, \tag{4.2}$$

and binary sequences satisfying (4.2) became known as Barker sequences. We only can find 9 Barker sequences with lengths 2,3,4,5,7,11,13 respectively. Furthermore, it has been conjectured that no other Barker sequence with lengths $n > 13$ is possible [34].

In 1961, Golay introduced Golay complementary sequences [20]. Let $\mathbf{a}$ and $\mathbf{b}$ be binary sequences of length n. Let $\rho_{\mathbf{a}}(\tau)$ and $\rho_{\mathbf{b}}(\tau)$ be the aperiodic correlations of these sequences. The sequences constitute a complementary pair if, for all $\tau \neq 0$,

$$\rho_{\mathbf{a}}(\tau) + \rho_{\mathbf{b}}(\tau) = 0. \tag{4.3}$$

Each member of a complementary pair is called a Golay complementary sequence.

4.1.2 Measures of good aperiodic autocorrelation

The Barker condition in (4.2) is still too strict to find good sequences. Therefore, in 1972, Golay [35] gave an alternative measure of small aperiodic autocorrelation – the merit factor $F(\mathbf{a})$, i.e.,

$$F(\mathbf{a}) = \frac{n^2}{2\sum_{\tau=1}^{n-1} |\rho_{\mathbf{a}}|^2} \text{ for } n > 1. \tag{4.4}$$

where n is the length of sequence $\mathbf{a}$. In 1989 Jensen and Høholdt [36] used the method introduced in [37] to show that for any m-sequence, $\lim_{n\to\infty} F(\mathbf{a}) = 3$.

Another measure of small aperiodic autocorrelations is the peak sidelobe level (PSL), i.e.,

$$M(\mathbf{a}) = \max_{1 \leq \tau \leq n-1} |\rho_{\mathbf{a}}(\tau)|. \tag{4.5}$$

The PSL of m-sequences $\mathbf{a}$ of length n has been discussed in the literatures [38], [39] and [40]. In 1980, McEliece [41] showed that $\sqrt{n+1}\ln(en)$ is an upper bound for $M(\mathbf{a})$, where e is the base of the Natural Logarithms. In 1984, Sarwate improved this bound [42]. Let $\mathbf{a}$ be an m-sequences of length n. Then $M(\mathbf{A}) < 1 + \frac{2}{\pi}\sqrt{n+1}\ln(\frac{4n}{\pi})$. In [43], it is proposed that if $F(\mathbf{a})$ is bounded, then $\sqrt{n} \leq cM(\mathbf{a})$, for all sufficiently large n, where c is a constant. That means the PSL of m-sequences grows like $\sqrt{n}$. Jebwab and Yoshida tested the growth rate of PSL of m-sequences against the bounding function $\sqrt{n \ln n}$, and found that the mean value of the PSL of m-sequences of length $n = 2^m - 1$ seems to have an upper bound $c\sqrt{n \ln n}$, where c is a constant [43].

Furthermore, we are also interested in the average sidelobe level (ASL), i.e.,

$$A(\mathbf{a}) = \frac{1}{n}\sum_{\tau=1}^{n-1} |\rho_{\mathbf{a}}(\tau)|. \tag{4.6}$$

These three measures of aperiodic autocorrelations (MF, PSL and ASL) involved in this thesis give the upper bounds of PAPRs in multicarrier communications which will be discussed in Chapter 5.

Table 4.1: The values of m

the family of sequences	m
m-sequences	5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
3-term sequences	5,7,9,11,13,15,17,19,21
5-term sequences	7,8,10,11,13,14,16,17,19,20
WG sequences	7,8,10,11,13,14,16,17,19,20

4.2 Aperiodic Autocorrelations for Binary Sequences with Ideal Two-level Autocorrelations

We calculated the merit factors, PSLs and ASLs of m-sequences, 3-term, 5-term and WG sequences. To the best of our knowledge, MF, PSL and ASL of these classes of binary sequences except m-sequences have never been studied. In our experiments, we considered all possible primitive polynomials of the sequences via decimations, and for each cyclically distinct sequence we involved all possible phase shifts. In other words, the numerical experiments have been accomplished for all possible m-sequences, 3-term, 5-term and WG sequences of a given length $n = 2^m - 1$, for $5 \leq m \leq 21$, where m is an integer. Table 5.1 gives the values of m taken in our experiments. The basic primitive polynomials generating sequences and the trace exponents of each basic 3-term, 5-term and WG sequence are listed in Appendix B.

4.2.1 Merit factors

Figures 4.1, 4.2 and 4.3 show the merit factors of 3-term, 5-term, and WG sequences, respectively.

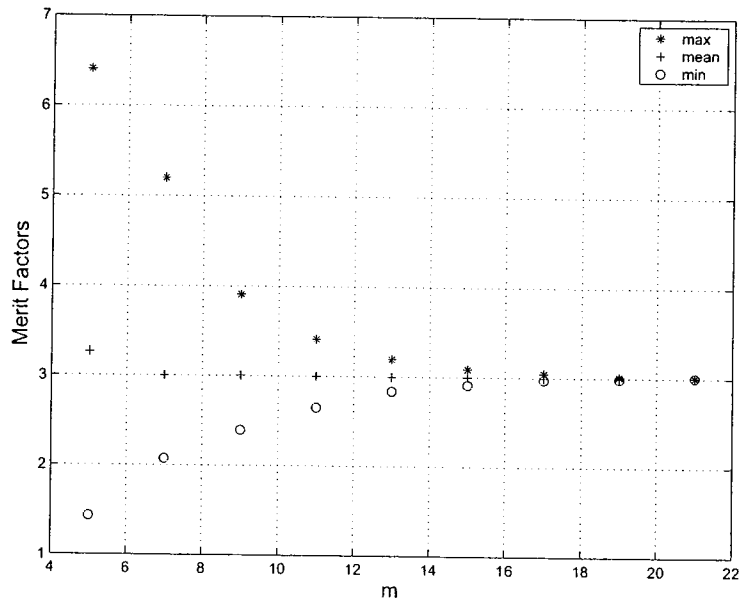


Figure 4.1: Min/mean/max values of merit factor of 3-term sequences

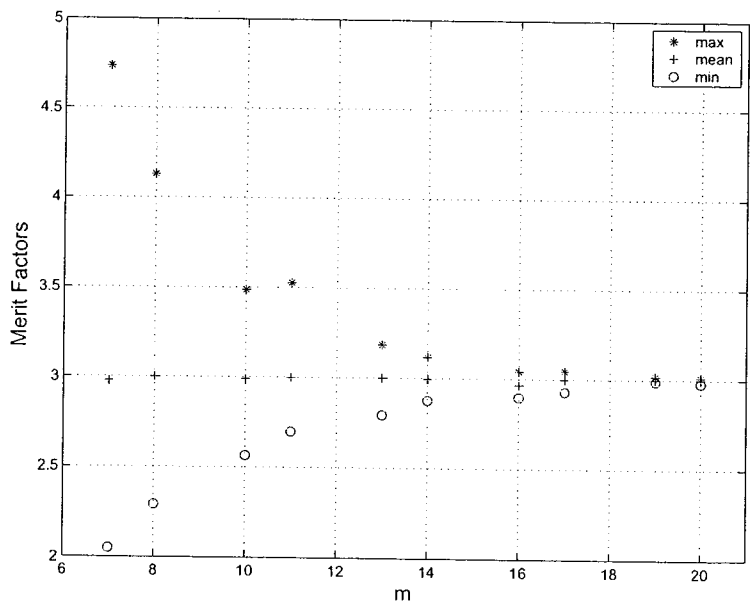


Figure 4.2: Min/mean/max values of merit factor of 5-term sequences

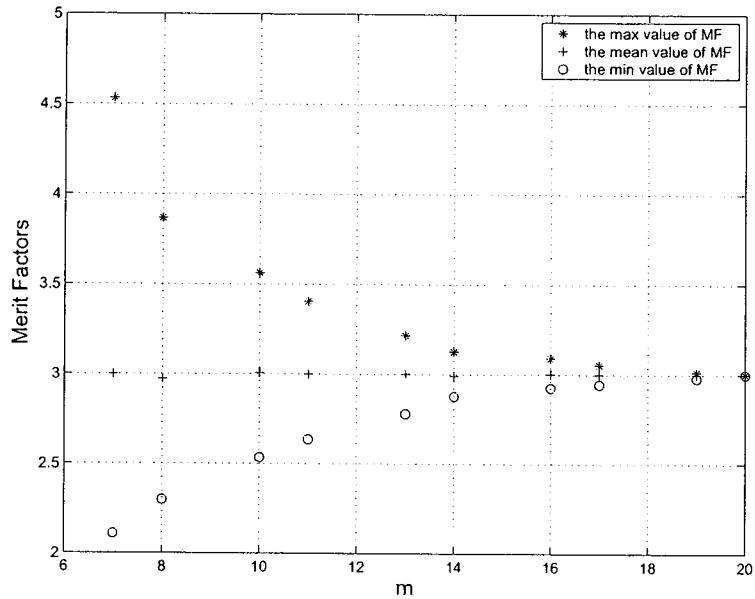


Figure 4.3: Min/mean/max values of merit factor of WG sequences

In Section 4.1.2, it is known that $\lim_{n\to\infty} F(\mathbf{a}) = 3$ for m-sequences of length n. From the figures, the merit factors over 3-term, 5-term, and WG sequences have similar results. Thus, we can establish the following conjecture.

Conjecture 1 For 3-term, 5-term, and WG sequences of length n, the merit factors $\lim_{n\to\infty} F(\mathbf{a}) = 3$.

4.2.2 Peak sidelobe levels

Figure 4.4 presents the maximum PSLs of the four classes of binary sequences. From this figure, it is obvious that when the sequence length n goes to infinity, the PSLs of the four classes of sequences approach to infinity, i.e., $\lim_{n\to\infty} M(\mathbf{a}) = \infty$. Figures 4.5, 4.6, 4.7 and 4.8 show the normalized peak sidelobe levels of m-sequences, 3-term, 5-term, and WG sequences of length

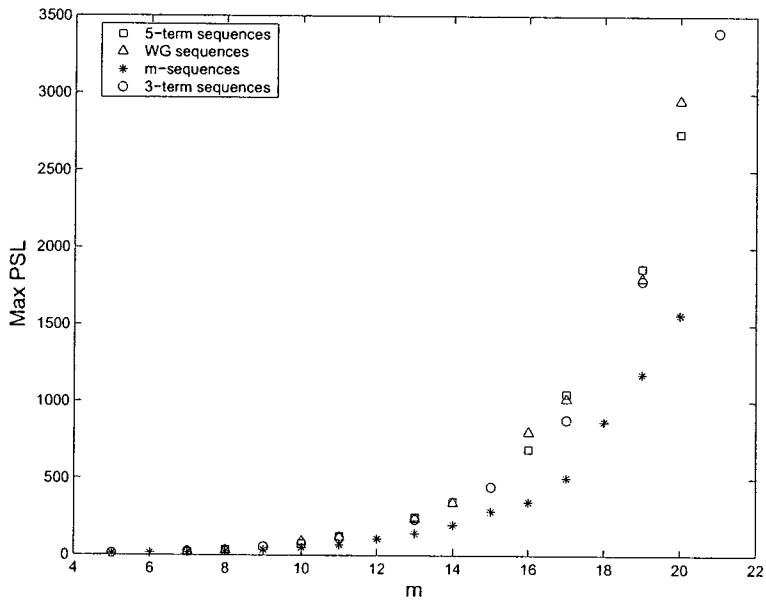


Figure 4.4: Max values of PSL of the four classes of binary sequences

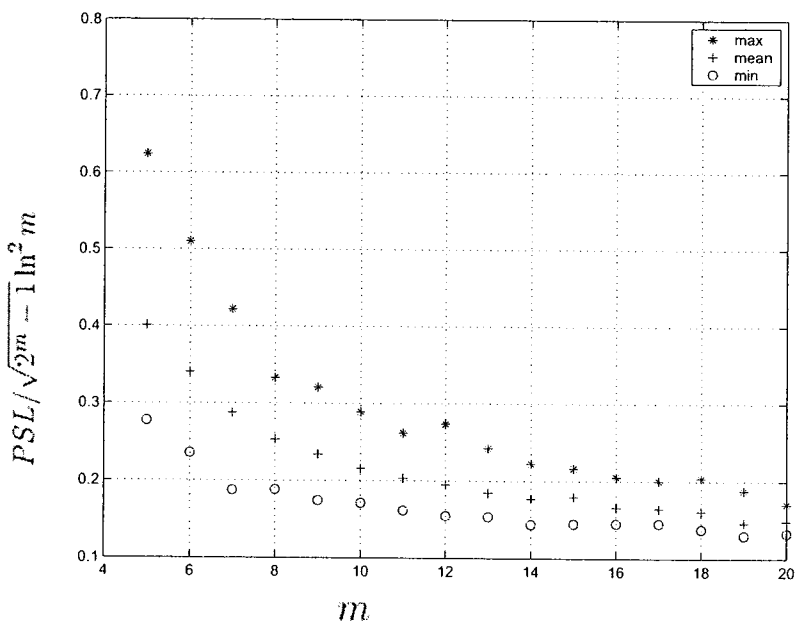


Figure 4.5: Min/mean/max values of PSL of m-sequences normalized by $\sqrt{n}(\ln m)^2$

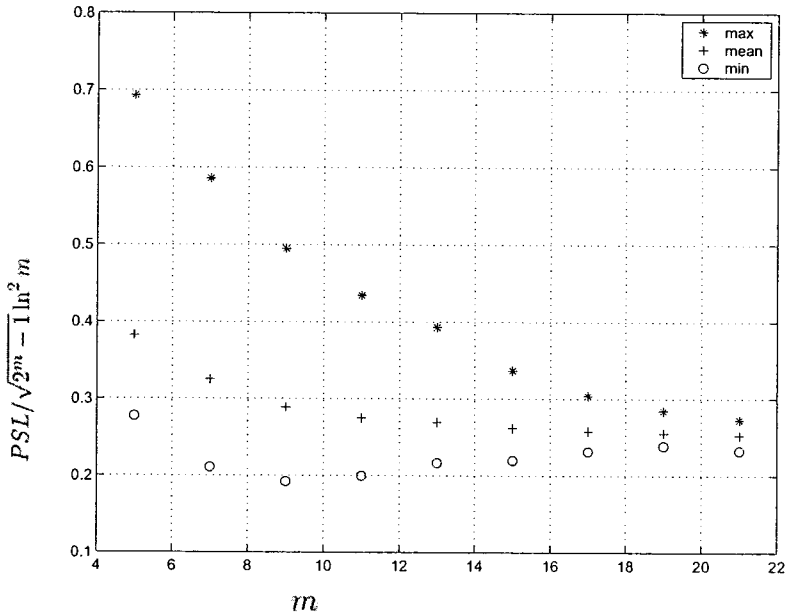


Figure 4.6: Min/mean/max values of PSL of 3-term sequences normalized by $\sqrt{n}(\ln m)^2$

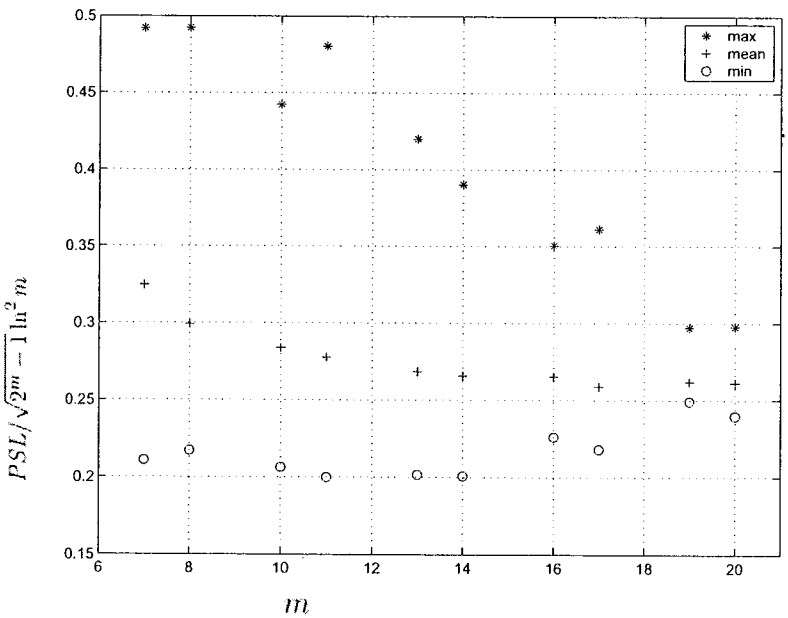


Figure 4.7: Min/mean/max values of PSL of 5-term sequences normalized by $\sqrt{n}(\ln m)^2$

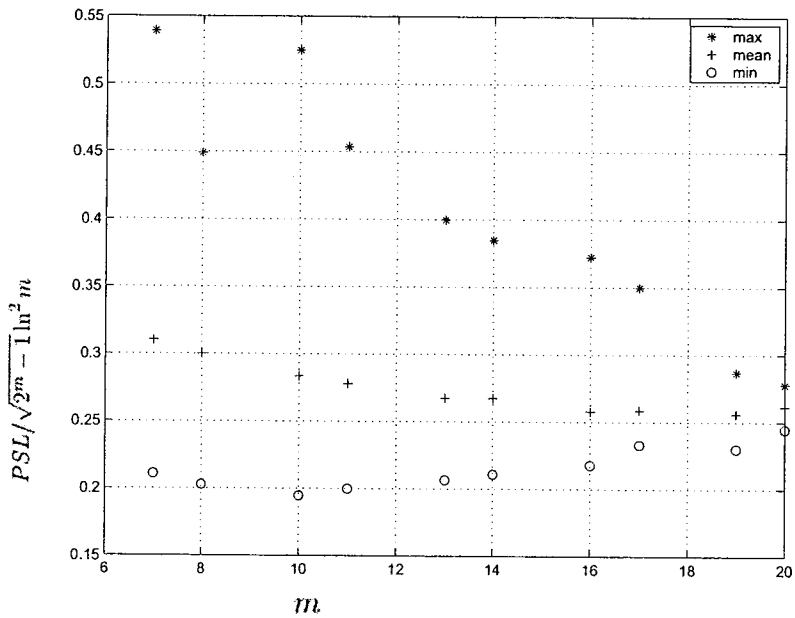


Figure 4.8: Min/mean/max values of PSL of WG sequences normalized by $\sqrt{n}(\ln m)^2$

$n = 2^m - 1$, $5 \leq m \leq 21$. What we tried to do is to find out the growth rates of the PSLs of the four classes of sequences. Jebwab and Yoshida in [43] gave the lower bound of PSLs of m-sequences ($\sqrt{n}$), and in [41] McEliece gave the upper bound of PSL of m-sequences ($\sqrt{n+1}\ln(en)$). Therefore, we test their growth against some parameters between $\sqrt{n}$ and $\sqrt{n+1}\ln(en)$. From the figures, the PSLs of the four classes of sequences grow almost like $\sqrt{n}(\ln m)^2$, i.e., $\lim_{n\to\infty} \frac{M(\mathbf{a})}{\sqrt{n}(\ln m)^2} \to c$, where c is a constant. The values of c are slightly different for each class of sequences . For m-sequences, $c < 0.2$, while for 3-term, 5-term, and WG sequences, $0.2 < c < 0.3$. That hints m-sequences has better performance of PSL than the other 3 classes of binary sequences.

Conjecture 2 In terms of PSL, for m-sequences of length $n = 2^m - 1$, $\lim_{n\to\infty} \frac{M(\mathbf{a})}{\sqrt{n}(\ln m)^2} \to 0.15$, and for 3-term, 5-term, and WG sequences of length $n = 2^m - 1$, $\lim_{n\to\infty} \frac{M(\mathbf{a})}{\sqrt{n}(\ln m)^2} \to 0.26$.

4.2.3 Average sidelobe levels

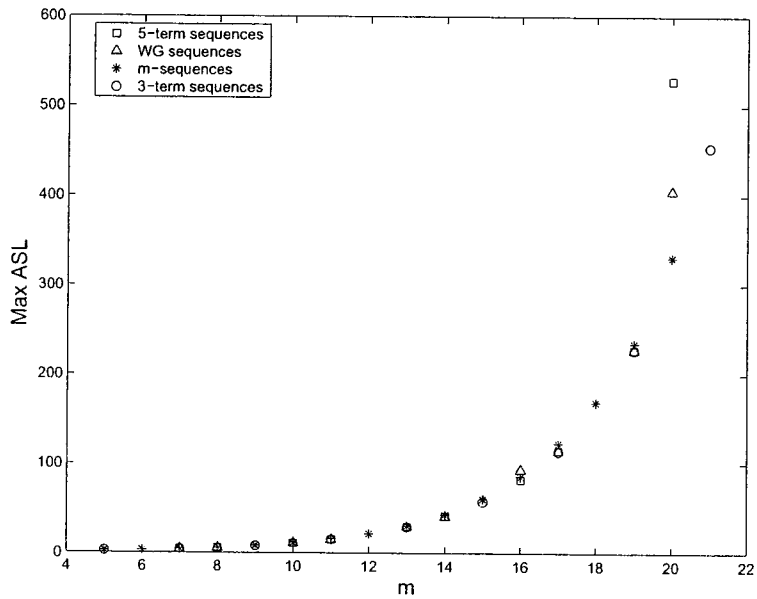


Figure 4.9: Max values of ASL of the four classes of binary sequences

Figure 4.9 presents the maximum ASLs of the four classes of binary sequences. Similarly, the ASLs approach to infinity when n goes to infinity. Figures 4.10, 4.11, 4.12 and 4.13 display the normalized average sidelobe levels of the four classes of binary sequences over the length $n = 2^m - 1$, respectively. By the definitions of ASL and PSL, $A(\mathbf{a}) = \frac{1}{n}\sum_{\tau=1}^{n-1} |\rho_{\mathbf{a}}(\tau)| \leq M(\mathbf{a}) = \max_{1\leq\tau\leq n-1} |\rho_{\mathbf{a}}(\tau)|$. Therefore, we tried smaller normalize factors than the ones of PSLs to find out the growth rates of the ASLs of the four classes of sequences. We found that the approximate growth rates of ASLs of the sequences are $\sqrt{n}$, i.e., $\lim_{n\to\infty} \frac{A(\mathbf{a})}{\sqrt{n}} \to c$. For m-sequences, $c \approx 0.33$, while

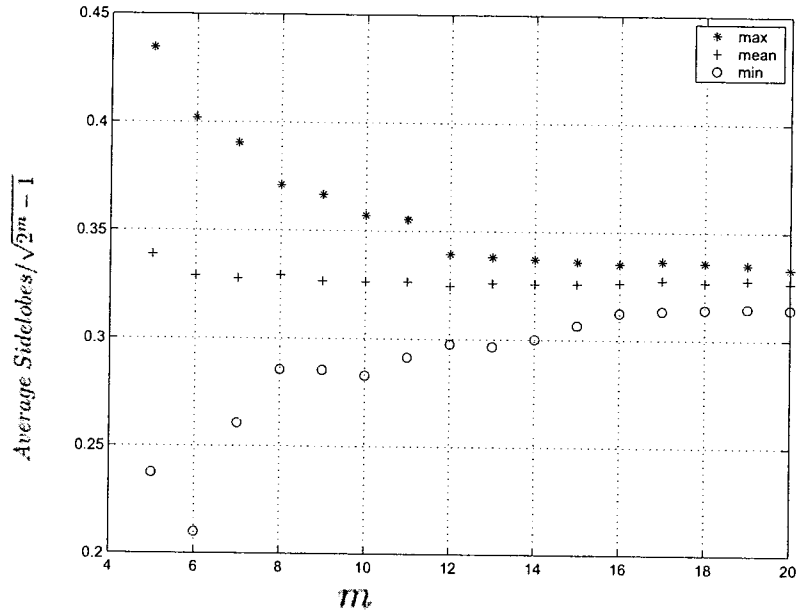


Figure 4.10: Min/mean/max values of ASL of m-sequences normalized by $\sqrt{n}$

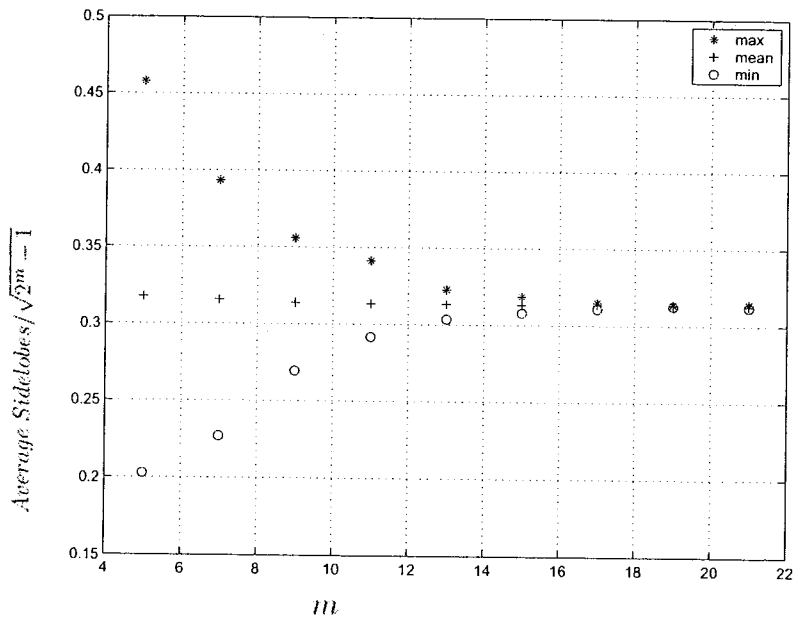


Figure 4.11: Min/mean/max values of ASL of 3-term sequences normalized by $\sqrt{n}$

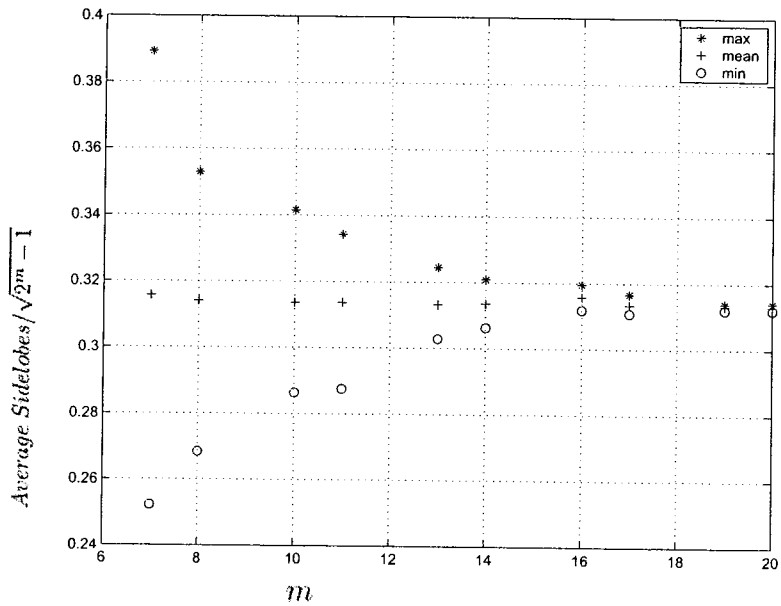


Figure 4.12: Min/mean/max values of ASL of 5-term sequences normalized by $\sqrt{n}$

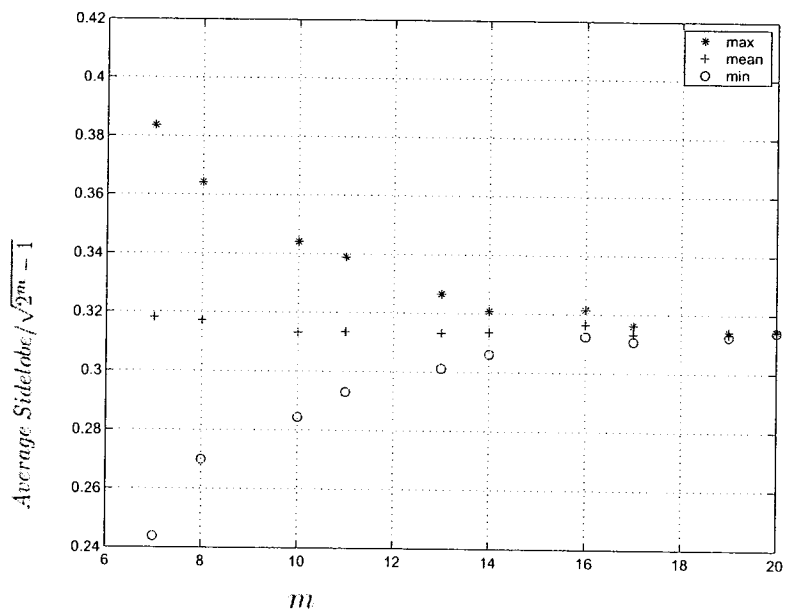


Figure 4.13: Min/mean/max values of ASL of WG sequences normalized by $\sqrt{n}$

for 3-term, 5-term, and WG sequences, $0.3 < c < 0.32$. Thus, m-sequences perform the worst property of ASL in these four classes of sequences.

Conjecture 3 For m-sequences of length $n = 2^m - 1$, $\lim_{n\to\infty} \frac{A(\mathbf{a})}{\sqrt{n}} \to 0.33$, and for 3-term, 5-term, and WG sequences of length $n = 2^m - 1$, $\lim_{n\to\infty} \frac{A(\mathbf{a})}{\sqrt{n}} \to 0.31$.

Chapter 5

Power Characteristics of Binary Sequences

5.1 Peak Power Control of Multicarrier Communications

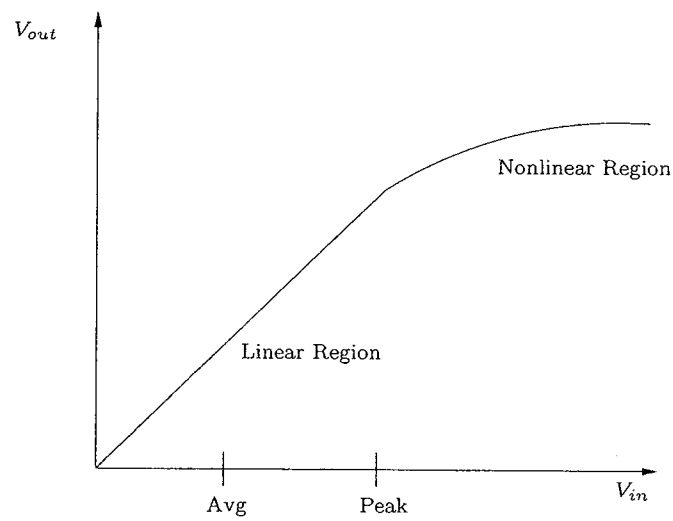


Figure 5.1: A typical power amplifier response

Figure 5.1 shows a typical power amplifier response. Operating in the linear region of this response is generally required to avoid signal distortion. Furthermore, it would be desirable to have the average and peak value be as close together as possible in order for the power amplifier to operate at maximum efficiency, which is measured by the peak-to-average power ratio (PAPR). A high PAPR forces the transmit power amplifier to have a large backoff in order to ensure linear amplification of signal, and requires high resolution for the receiver A/D converter. In multicarrier communication systems, if the number of subcarriers N is large enough, the maximum PAPR will approach to N. So the high PAPR is an important penalty that must be paid by multicarrier communication systems for large N.

A multicarrier signal is the sum of many independent signals modulated onto subchannels of equal bandwidth. Denote that N is the number of subcarriers, and $\mathbf{a} = \{a_u\}$, $u = 0, \ldots, N-1$ is a collection of N data symbols. Let f_c be the carrier frequency and Δf be the bandwidth of each subcarrier. The transmitted signal on the interval $t = [0, \frac{1}{\Delta f})$ is represented by the real part of

$$S_{\mathbf{a}}(t) = \sum_{u=0}^{N-1} a_u e^{j2\pi(f_c + u\Delta f)t} \tag{5.1}$$

The instantaneous power of the transmit signal is $\Big(\Re\big(S_{\mathbf{a}}(t)\big)\Big)^2$, where $\Re(\cdot)$ denotes the real part of the variable, while $|S_{\mathbf{a}}(t)|^2$ is called the envelope power. Denoting $\hat{f} = \frac{f_c}{\Delta f}$, we have the following definition for the peak-to-average power ratio of $S_{\mathbf{a}}(t)$

$$\mathrm{PAPR}(\mathbf{a}) = \frac{1}{\sum_{u=0}^{N-1} |a_u|^2} \cdot \max_{t\in[0,1)} \left| \Re\Big(\sum_{u=0}^{N-1} a_u e^{j2\pi(\hat{f}+u)t} \Big) \right|^2. \tag{5.2}$$

It is straightforward that

$$\mathrm{PAPR}(\mathbf{a}) \leq \mathrm{PMEPR}(\mathbf{a}) = \frac{1}{\sum_{u=0}^{N-1} |a_u|^2} \cdot \max_{t\in[0,1)} |\mu_{\mathbf{a}}(t)|^2, \tag{5.3}$$

where

$$\mu_{\mathbf{a}}(t) = \sum_{u=0}^{N-1} a_u e^{j2\pi ut}, \tag{5.4}$$

and PMEPR stands for the peak-to-mean-envelope-power ratio [44].

5.2 Peak Power Control and Aperiodic Autocorrelation

The intimate connection between the PAPR of multicarrier signals and the measures of their aperiodic autocorrelations, i.e., MF, PSL, and ASL, is described in the following. In our experiments, assume that $\mathbf{a} = \{a_u\}$, $u = 0, \ldots, n-1$ is a binary $\{\pm 1\}$ sequence of length n, transmitted by multicarrier communication systems, and the number of subcarriers N equals to the sequence length n. Therefore, we have $\sum_{u=0}^{n-1} |a_u|^2 = n$ for the binary sequence $\mathbf{a}$.

Theorem 1 [45]

$$\text{PMEPR}(\mathbf{a}) \leq \frac{\sum_{u=0}^{n-1} |a_u|^2}{n} + \frac{2}{n} \sum_{\tau=1}^{n-1} |\rho(\tau)| = 1 + 2A(\mathbf{a}). \tag{5.5}$$

where $A(\mathbf{a}) = \frac{1}{n} \sum_{\tau=1}^{n-1} |\rho_{\mathbf{a}}(\tau)|$ is the ASL.

Theorem 2 [44]

$$\text{PMEPR}(\mathbf{a}) \leq 1 + \frac{2(n-1)}{n} \max_{\tau=1,\ldots,n-1} |\rho(\tau)| = 1 + \frac{2(n-1)}{n} \text{PSL}(\mathbf{a}). \tag{5.6}$$

where $\max_{\tau=1,\ldots,n-1} |\rho(\tau)|$ is PSL of $\mathbf{a}$.

Theorem 3 [44]

$$\text{PMEPR}(\mathbf{a}) \leq \frac{\sum_{u=0}^{n-1} |a_u|^2}{n} + \sqrt{\frac{2(n-1)}{F(\mathbf{a})}} = 1 + \sqrt{\frac{2(n-1)}{F(\mathbf{a})}}. \tag{5.7}$$

The above equations hint that it might be beneficial to expect a low PMEPR from sequences with small aperiodic autocorrelations. That is an important motivation of our researching on aperiodic autocorrelation properties of binary sequences in Chapter 4.

5.3 PMEPR of Binary Sequences with Ideal Two-level Autocorrelation

A block coding scheme has previously been proposed in [11] and [12] using m-sequences to reduce the PAPR for OFDM systems. The results suggest that m-sequences with length $n = 2^m - 1$, $3 \leq m \leq 10$, can yield PAPR values in the range 5–8 dB. But the results only included the m-sequences generated by special primitive polynomials. In this thesis, we try to investigate power characteristics of all m-sequences by all possible primitive polynomials and all possible phase shifts. Furthermore, we examined the PMEPRs of the other classes of binary sequences with two-level autocorrelation, which have never been studied. We obtained all possible sequences with different primitive polynomials by applying all possible decimations to a basic sequence with the basic primitive polynomial. The basic primitive polynomials are listed in Appendix A, and the trace exponents of each basic 3-term, 5-term and WG sequence are listed in Appendix B.

The numerical results of PMEPRs of the four classes of binary sequences are presented in the following. We calculated the PMEPRs of all m-sequences, 3-term, 5-term and WG sequences with short length $n = 2^m - 1$, $5 \leq m \leq 8$,

Table 5.1: The values of m

The classes of binary sequences	m
m-sequences	5,6,7,8
3-term sequences	5,7
5-term sequences	7,8
WG sequences	7,8

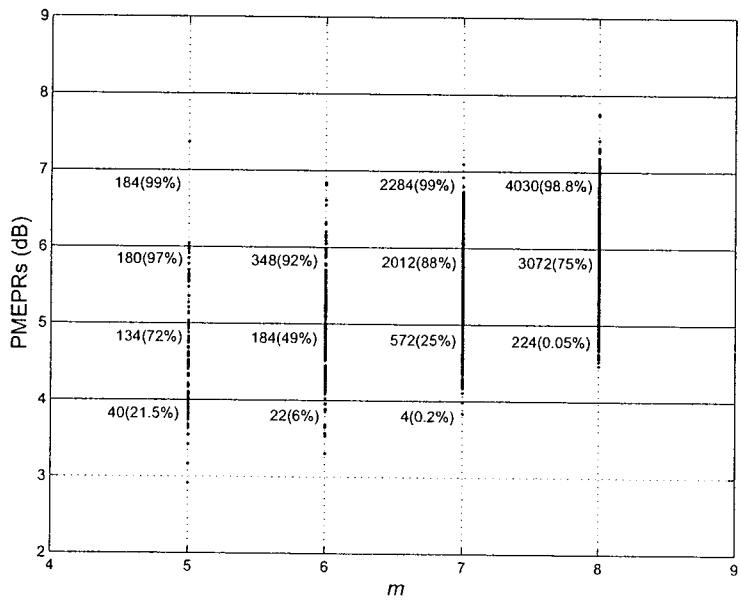


Figure 5.2: PMEPRs (dB) of m-sequences

where m is an integer. Table 5.1 gives the values of m taken in our experiments.

Figures 5.2, 5.3, 5.4 and 5.5 show the PMEPRs of the four classes of binary sequences. Each class of sequences contains all possible binary sequences considering cyclic shifts and different primitive polynomials. The numbers below the lines PMEPRs=4, 5, 6, 7, 8 dB, present the numbers of sequences of length $2^m - 1$ with PMEPRs <4, 5, 6, 7, 8 dB, respectively. We also displayed the percentages corresponding to the numbers.

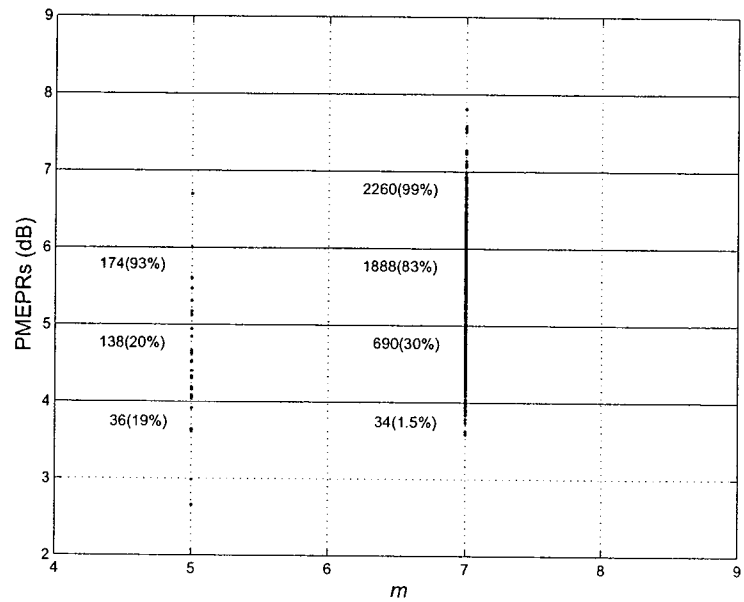


Figure 5.3: PMEPRs (dB) of 3-term sequences

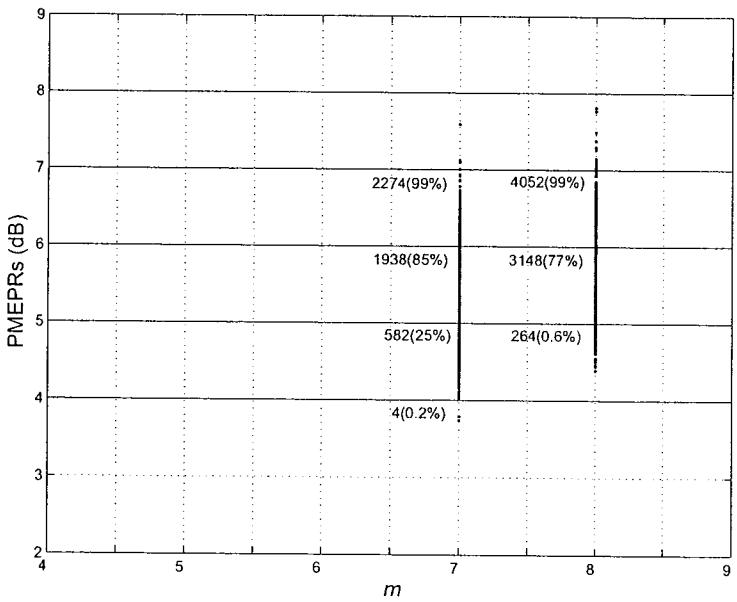


Figure 5.4: PMEPRs (dB) of 5-term sequences

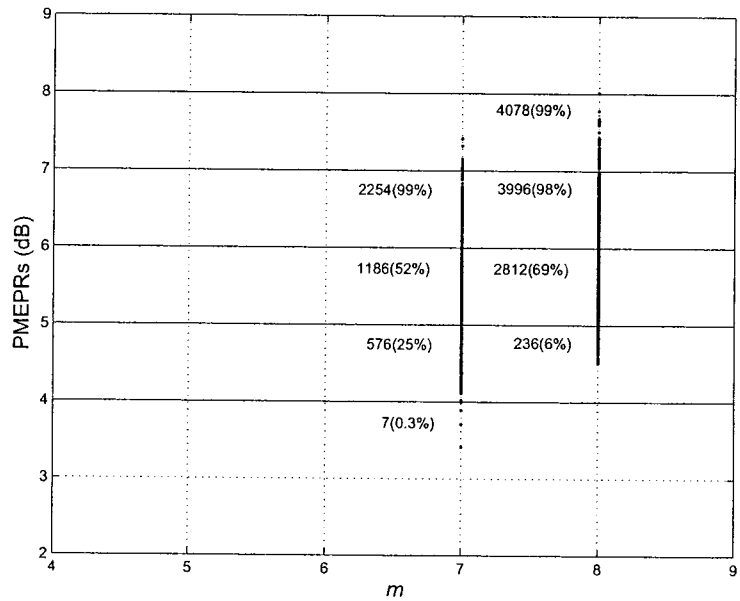


Figure 5.5: PMEPRs (dB) of WG sequences

Table 5.2 compares the maximum values of PMEPRs of the four classes of sequences. For $5 \leq m \leq 8$, only two WG sequences produce PMEPRs bigger than 8 dB. For $m = 5$, 3-term sequences have smaller maximum PMEPR than m-sequences, for $m = 7$ and 8, on the other hand, m-sequences show the smallest maximum PMEPRs of all the sequences.

Tables 5.3, 5.4, 5.5, and 5.6 show that the maximum values of each class of sequences of length $n = 2^m - 1$ meet the maximum upper bounds of PMEPRs chosen by the corresponding merit factors, PSLs and ASLs.

We presented the distributions of PMEPR of the four classes of sequences with length $n = 2^m - 1$, $m = 5, 7, 8$, in Figures 5.6, 5.7, and 5.8. The cumulative distribution of PMEPR is defined by

$$p(x) = P[\text{PMEPR} \leq x] = \frac{\mathcal{N}(\text{PMEPR} \leq x)}{\mathcal{N}_{\text{total}}} \tag{5.8}$$

where $\mathcal{N}(\text{PMEPR} \leq x)$ is the number of sequences with PMEPR$\leq x$ and $\mathcal{N}_{\text{total}}$ is the total number of sequences.

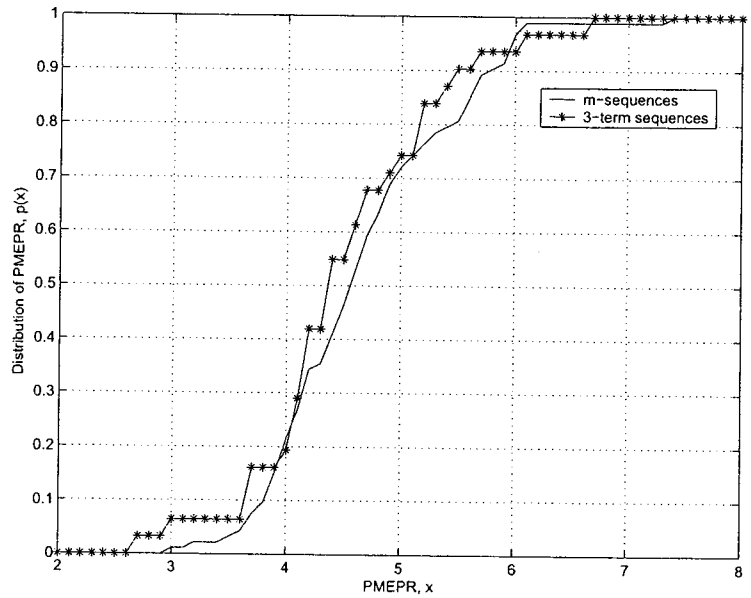


Figure 5.6: Distribution of PMEPRs (dB) of binary sequences with length $31 = 2^5 - 1$

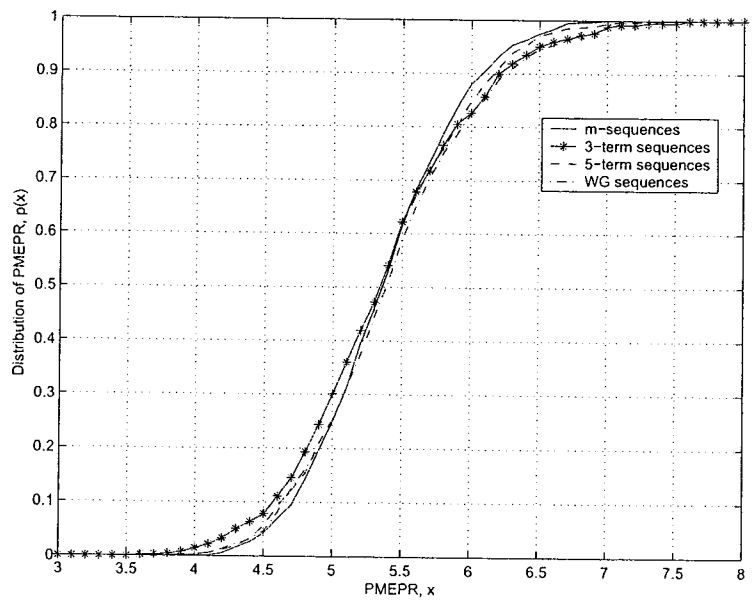


Figure 5.7: Distribution of PMEPRs (dB) of binary sequences with length $127 = 2^7 - 1$

Table 5.2: The maximum values of PMEPR (dB) of the four classes of sequences with length $n = 2^m - 1$

m	m-sequences	3-term sequences	5-term sequences	WG sequences
5	7.37	6.70	-	-
6	6.84	-	-	-
7	7.10	7.81	7.59	7.42
8	7.76	-	7.81	8.01

Table 5.3: Comparing the maximum values of m-sequences with the upper bounds determined by MF, PSL, and ASL

m	m-sequences	ASL	PSL	Merit Factor
5	7.37	7.66	12.65	8.22
6	6.84	8.68	14.25	9.42
7	7.10	9.30	15.65	10.85
8	7.76	10.45	16.70	11.86

From Figure 5.6, 3-term sequences of length 31 produce better PMEPR performance than m-sequences. Both the minimum and maximum values of PMEPRs of 3-term sequences are smaller than those of m-sequences. Especially, if PMEPR$<$ 6 dB, there are always more 3-term sequences of length 31 than m-sequences.

Table 5.4: Comparing the maximum values of 3-term sequences with the upper bounds determined by MF, PSL, and ASL

m	3-term sequences	ASL	PSL	Merit Factor
5	6.70	7.85	13.09	8.73
7	7.81	9.94	17.04	10.80

Table 5.5: Comparing the maximum values of 5-term sequences with the upper bounds determined by MF, PSL, and ASL

m	5-term sequences	ASL	PSL	Merit Factor
7	7.59	9.81	16.20	10.82
8	7.81	10.89	18.37	12.01

Table 5.6: Comparing the maximum values of WG sequences with the upper bounds determined by MF, PSL, and ASL

m	WG sequences	ASL	PSL	Merit Factor
7	7.42	9.81	9.84	10.77
8	8.01	10.89	11.01	12.00

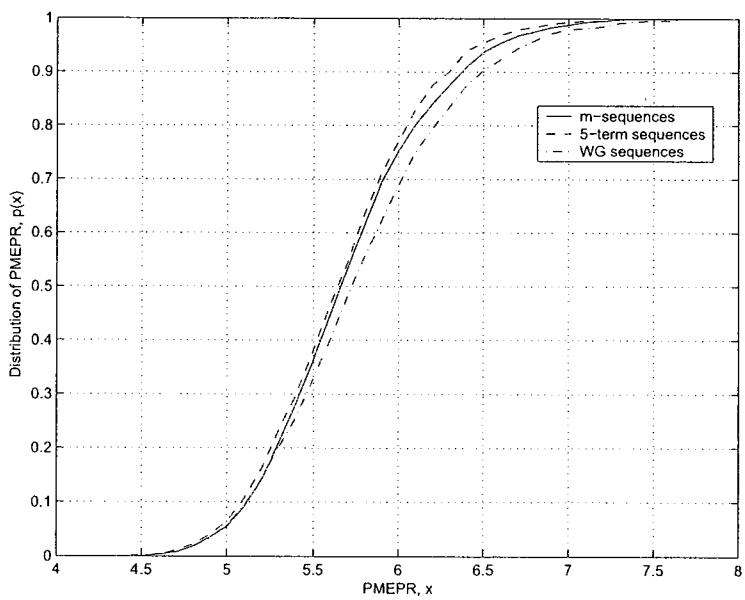


Figure 5.8: Distribution of PMEPRs (dB) of binary sequences with length $255 = 2^8 - 1$

Table 5.7: The number of sequences with length $31 = 2^5 - 1$ classified by their PMEPR value

PMEPRs	m-sequences	3-term sequences	5-term sequences	WG sequences	Total
< 4	40	36	-	-	76
< 5	134	138	-	-	272
< 6	180	174	-	-	354
< 7	184	186	-	-	370
< 8	186	186	-	-	372

Table 5.8: The number of sequences with length $63 = 2^6 - 1$ classified by their PMEPR value

PMEPRs	m-sequences	3-term sequences	5-term sequences	WG sequences	Total
< 4	22	-	-	-	22
< 5	184	-	-	-	184
< 6	348	-	-	-	348
< 7	378	-	-	-	378
< 8	378	-	-	-	378

From Figure 5.7, the distributions of PMEPRs of the four classes sequences with length 127 are very similar. For PMEPR$<$ 5.5 dB, 3-term sequences produce the largest number of sequences in the four classes of sequences. For PMEPR$>$ 5.5 dB, however, there are more m-sequences than any other classes of sequences.

From Figure 5.8, it is clear that 5-term sequences produce the most sequences with PMEPR$\leq x$ for any x in the four classes of sequences of length 255.

Table 5.9: The number of sequences with length $127 = 2^7 - 1$ classified by their PMEPR value

PMEPRs	m-sequences	3-term sequences	5-term sequences	WG sequences	Total
< 4	4	34	4	7	49
< 5	572	690	582	576	2420
< 6	2012	1888	1938	1886	7724
< 7	2284	2260	2274	2254	9072
< 8	2286	2286	2286	2286	9144

Table 5.10: The number of sequences with length $255 = 2^8 - 1$ classified by their PMEPR value

PMEPRs	m-sequences	3-term sequences	5-term sequences	WG sequences	Total
< 4	0	-	0	0	0
< 5	224	-	264	236	724
< 6	3072	-	3148	2812	9032
< 7	4030	-	4052	3996	12078
< 8	4080	-	4080	4078	12238

In Tables 5.7, 5.8, 5.9, 5.10, we classified the four classes of sequences by their PMEPRs, to show the total numbers of sequences of a given length and a given upper bound of PMEPR. Combining the four classes of sequences, we have a large number of sequences with low PMEPRs of a given length.

In conclusion, the numerical results suggest that when $5 \leq m \leq 8$, most of PMEPRs and PAPRs produced by these four classes of binary sequences are below 8 dB. The distributions of PMEPR of the three classes of multiple trace term sequences, i.e., 3-term, 5-term, and WG sequences, are very similar with that of m-sequences, even better than m-sequences in some cases. Especially, 3-term sequences of length 31 and 5-term sequences of length 255 produce more sequences with low PMEPRs than the other classes of sequences with the same length, respectively. For PMEPR$<$ 5.5 dB, 3-term sequences of length 127 also produce the largest number of sequences in the four classes of sequences. Besides, we are able to generate a large number of sequences with low PMEPR by considering 3-term, 5-term and WG sequences as well as m-sequences. Moreover, the number of sequences with low PMEPRs can be increased by evaluating the PMEPRs of the other classes of sequences with two-level autocorrelation [33].

5.4 PMEPR of Orthogonal Codes

Orthogonal codes have been used as spreading codes in CDMA system. In particular, the orthogonal spreading codes are required to have low PMEPRs for MC-CDMA.

In Section 2.3.7, we described the method constructing orthogonal codes using binary sequences with two-level autocorrelation. In this section, the numerical results of PMEPR of orthogonal codes generated by the four classes

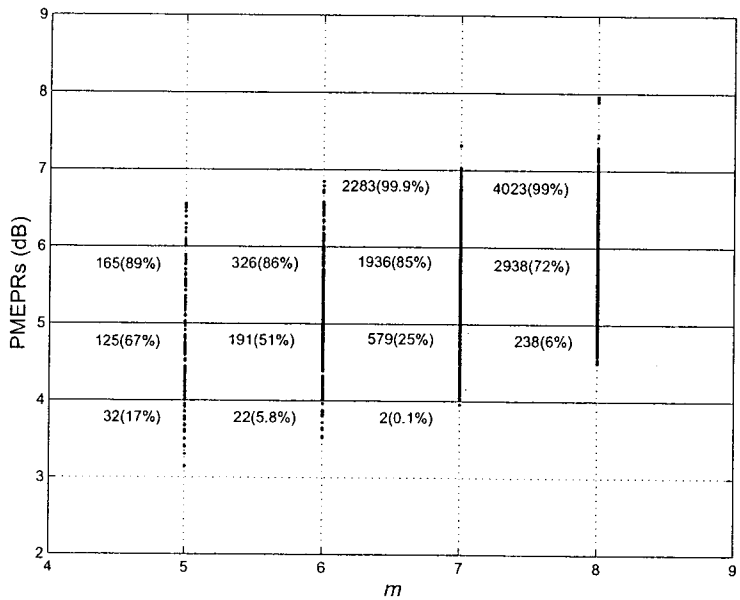


Figure 5.9: PMEPRs (dB) of OC_m

of binary sequences are presented. From Section 2.3.7, for a cyclically distinct sequence of length $n = 2^m$, we can generate an orthogonal code set with size 2^m by considering all its phase shifts. Therefore, for a given length, we can generate $\frac{\phi(2^m-1)}{m}$ orthogonal code sets, which equal to the number of all different primitive polynomials of order m. We calculated the PMEPRs of orthogonal codes generated by all m-sequences, 3-term, 5-term and WG sequences with short length $n = 2^m$, $5 \leq m \leq 8$, where m is an integer, denoted by OC_m, OC_3, OC_5 and $\mathrm{OC}_{\mathrm{WG}}$, respectively. The calculations show us the PMEPR properties of all codes in the set OC_*, which is a union of $\frac{\phi(2^m-1)}{m}$ orthogonal code sets, and in which not every pair of codes is orthogonal. Then we compared the PMEPRs of the code sets to that of Walsh code sets of length 2^m, $5 \leq m \leq 8$. The first codes c_0 of orthogonal code sets and Walsh code sets are all 1's sequences which are discarded in our analysis of PMEPRs, since they produce a trivial value $\mathrm{PAPR}(c_0) = 2^m$.

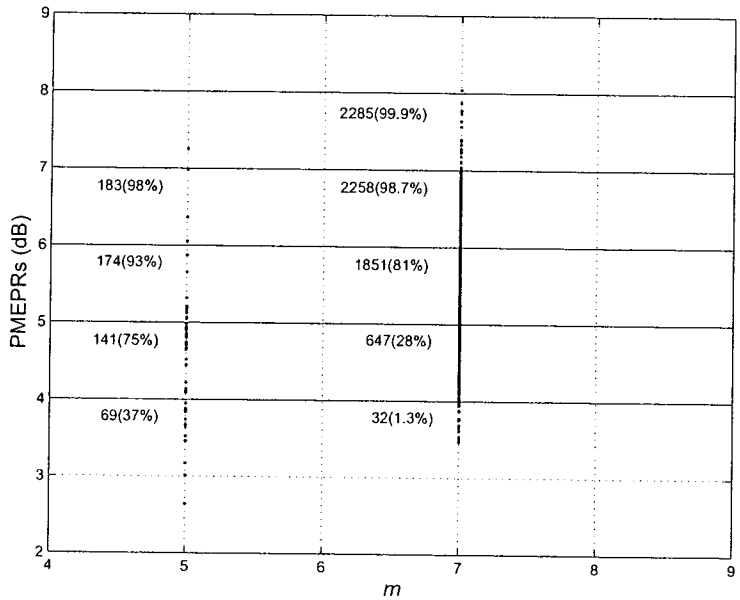


Figure 5.10: PMEPRs (dB) of OC_3

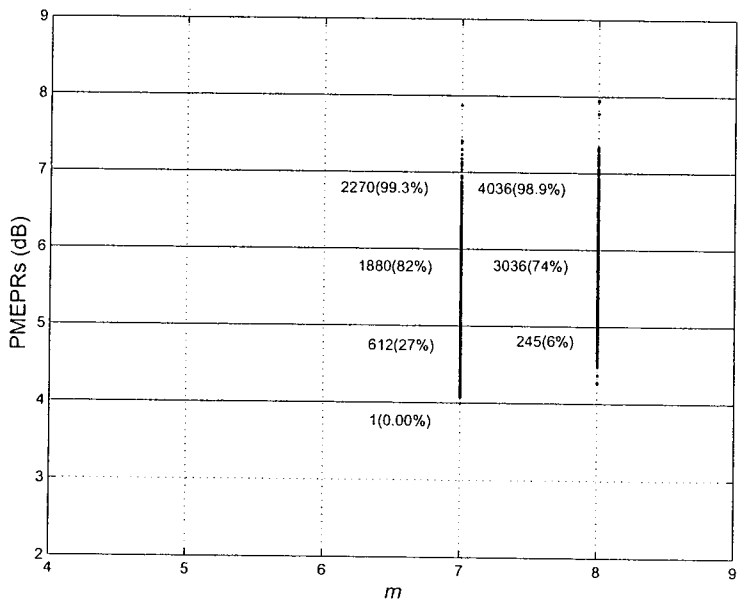


Figure 5.11: PMEPRs (dB) of OC_5

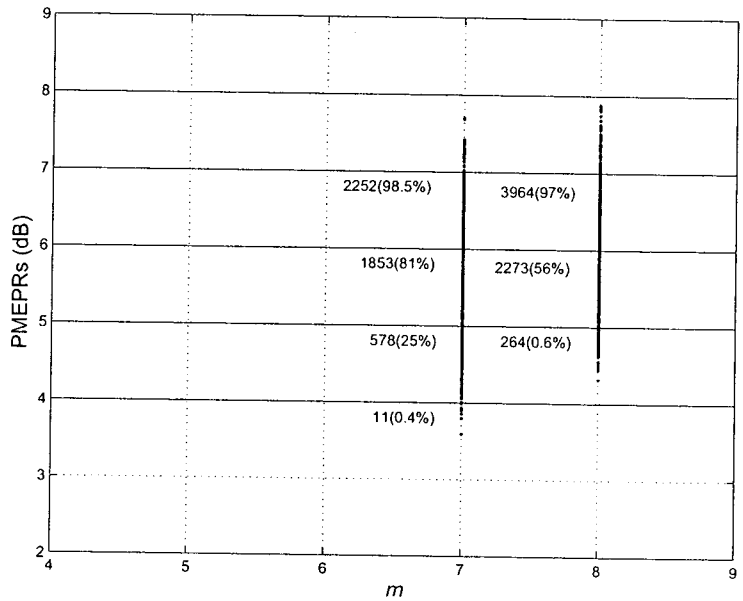


Figure 5.12: PMEPRs (dB) of $\mathrm{OC}_{\mathrm{WG}}$

Table 5.11: The maximum values of PMEPR (dB) of orthogonal codes generated by the 4 classes sequences with length $n = 2^m$

m	OC_m	OC_3	OC_5	$\mathrm{OC}_{\mathrm{WG}}$
5	6.55	7.25	-	-
6	6.85	-	-	-
7	7.32	8.04	7.87	7.70
8	7.96	-	7.95	7.88

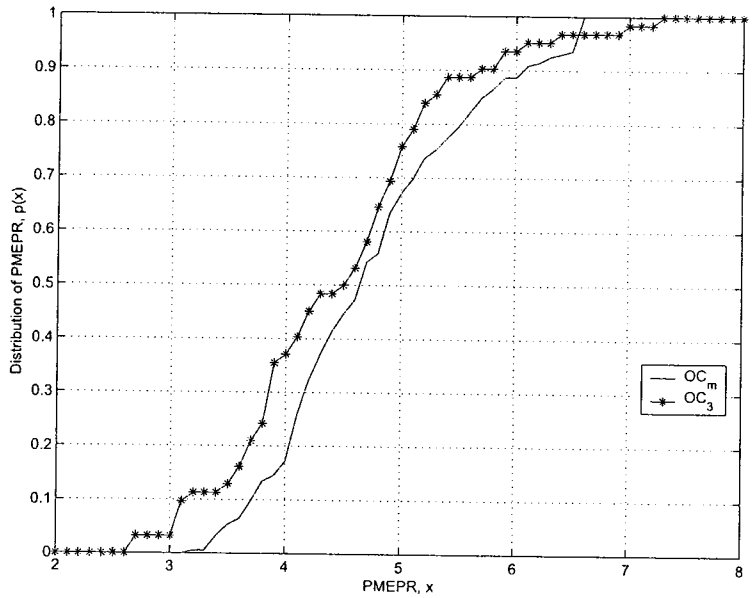


Figure 5.13: Distribution of PMEPRs (dB) of orthogonal codes generated by binary sequences with length $32 = 2^5$

Figures 5.9, 5.10, 5.11 and 5.12 show the PMEPRs of orthogonal codes generated by the four classes of binary sequences. The numbers below the lines PMEPRs=4, 5, 6, 7, 8 dB, present the numbers of orthogonal codes of given length $n = 2^m$ with PMEPRs <4, 5, 6, 7, 8 dB, respectively. We also displayed the percentages corresponding to the numbers.

Table 5.11 compares the maximum values of PMEPR of orthogonal codes generated by the four classes of sequences with length $n = 2^m$. For $5 \leq m \leq 8$, only one OC_3 for $m = 7$ produces PMEPR bigger than 8 dB. For $5 \leq m \leq 7$, OC_m shows the lowest maximum PMEPR of all sequences. For $m = 8$, on the other hand, the OC_{WG} shows the lower PMEPR than any other classes of sequences.

We presented the distributions of PMEPR of orthogonal codes generated by the four classes of sequences with length $n = 2^m$, $m = 5, 7, 8$, in Figures

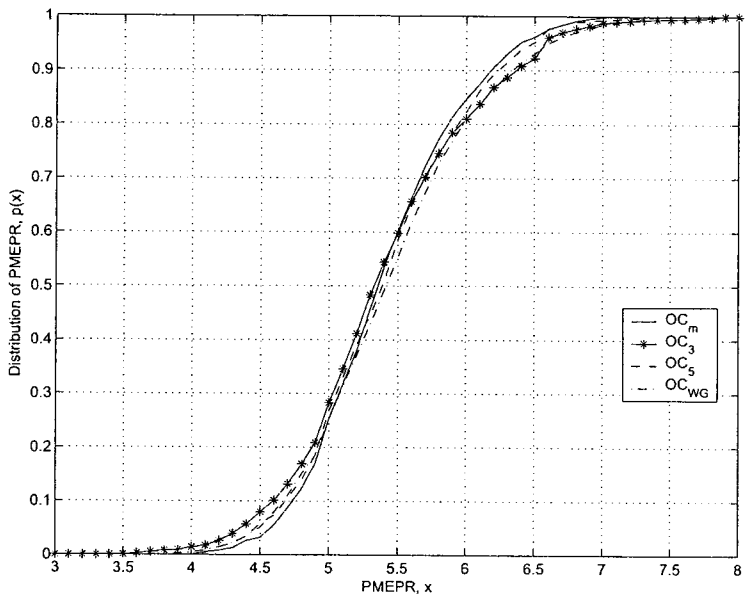


Figure 5.14: Distribution of PMEPRs (dB) of orthogonal codes generated by binary sequences with length $128 = 2^7$

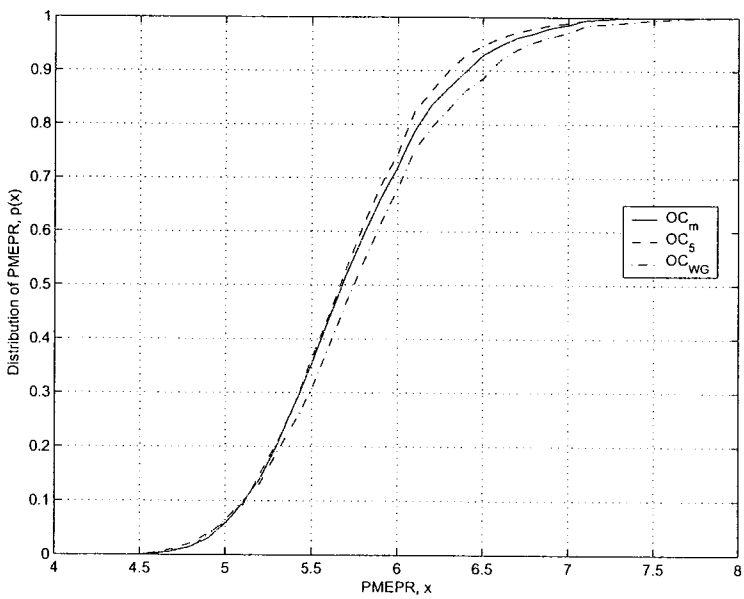


Figure 5.15: Distribution of PMEPRs (dB) of orthogonal codes generated by binary sequences with length $256 = 2^8$

5.13, 5.14, and 5.15. The cumulative distribution of PMEPR of orthogonal codes is defined by (5.8).

From Figure 5.13, OC_3 of length 32 produces better PMEPR performance than OC_m. For PMEPR< 6.5 dB, we always have more orthogonal codes of length 32 from OC_3 than from OC_m.

From Figure 5.14, the distributions of PMEPRs of the orthogonal codes with length 127 are very similar. For PMEPR< 5.5 dB, OC_3 produces the largest number of orthogonal codes. For PMEPR> 5.5 dB, however, there are more orthogonal codes from OC_m than from OC_3, OC_5 and OC_{WG}.

From Figure 5.15, for 4.5 dB <PMEPR< 5.5 dB, the distributions of PMEPRs of OC_m and OC_5 are almost same, better than OC_{WG}. For PMEPR> 5.5 dB, on the other hand, OC_5 produces the most orthogonal codes of low PMEPRs in the codes generated by the four classes of sequences with length 255.

Figures 5.16, 5.17, 5.18, and 5.19 show the maximum PMEPRs of individual orthogonal code sets generated by binary sequences, compared to maximum PMEPRs of Walsh code sets. In the figures, note that each point shows the maximum PMEPR of an orthogonal code set produced by a decimation factor to a sequence. First, all the maximum PMEPRs of Walsh code sets with size 2^m, $5 \leq m \leq 8$ are bigger than 15 dB, while the maximum PMEPRs of the orthogonal code sets generated by the four classes of sequences are below 9 dB. Second, considering the orthogonal codes generated by a class of sequences of given length, the maximum PMEPRs of each code sets are similar. In other words, the variation of maximum PMEPRs is so small that we may choose any orthogonal code set corresponding to a decimation factor for low PMEPR. Moreover, there is only one Walsh code set of size 2^m, while there are $\frac{\phi(2^m-1)}{m}$ code sets of size 2^m for a given class of

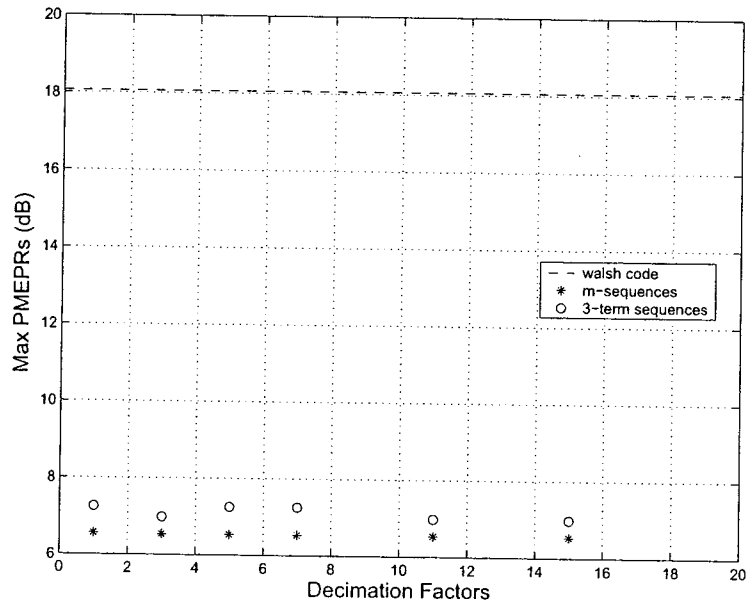


Figure 5.16: Maximum values of orthogonal code sets with the maximum value of Walsh code set over length $2^5 = 32$

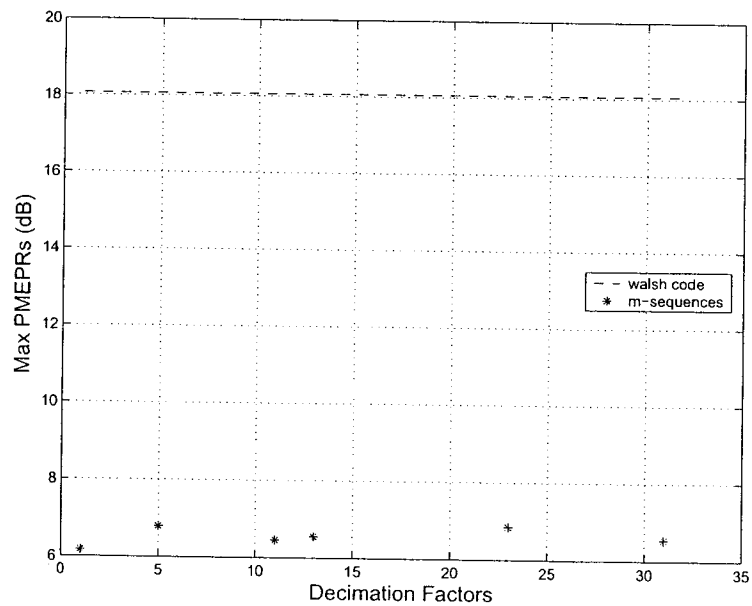


Figure 5.17: Maximum PMEPRs of orthogonal code sets and Walsh code sets over length $2^6 = 64$

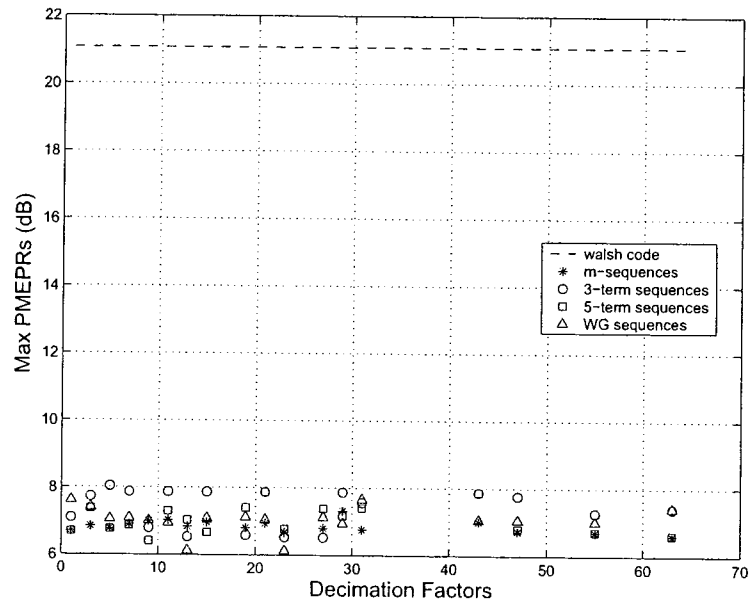


Figure 5.18: Maximum PMEPRs of orthogonal code sets and Walsh code sets over length $2^7 = 128$

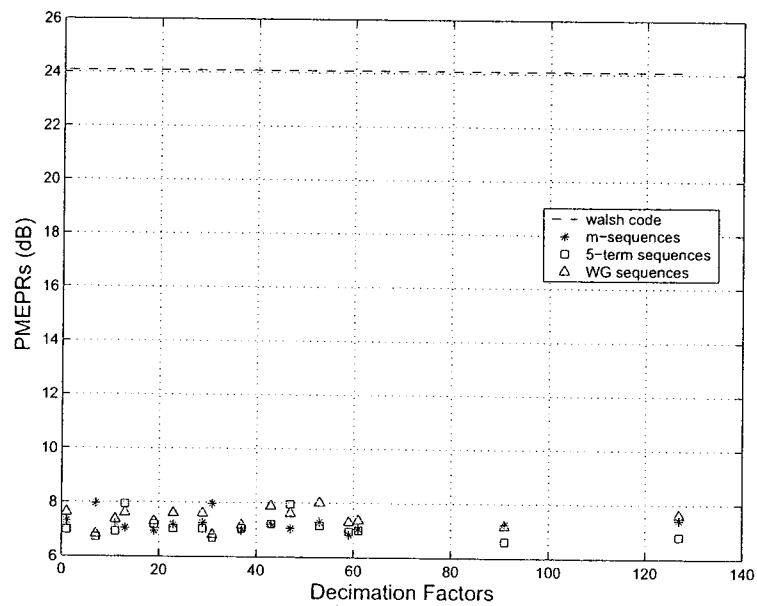


Figure 5.19: Maximum PMEPRs of orthogonal code sets and Walsh code sets over length $2^8 = 256$

Table 5.12: The number of code sets with maximum PMEPRs<7dB of length $n = 2^m$

m	OC_m	OC_3	OC_5	OC_{WG}	Total
5	6	3	-	-	9
6	6	-	-	-	6
7	15	5	9	4	33
8	3	-	7	0	10

Table 5.13: The number of code sets with maximum PMEPRs<8dB of length $n = 2^m$

m	OC_m	OC_3	OC_5	OC_{WG}	Total
5	6	6	-	-	12
6	6	-	-	-	6
7	18	17	18	18	71
8	16	-	16	16	48

binary sequences with length $n = 2^m - 1$.

In Tables 5.12 and 5.13, we counted the number of orthogonal code sets generated by the four classes of sequences of length $n = 2^m$, where PMEPRs of all codes are less than 7 and 8 dB . Combining the orthogonal code sets from different classes of sequences, we can obtain a large number of orthogonal code sets of low PMEPR. The codes in each code set can be implemented by using LFSRs without considering the nonzero initial state.

In conclusion, the above results suggest that for $5 \leq m \leq 8$, most of PMEPRs and PAPRs produced by orthogonal codes generated by the four classes of binary sequences are below 8 dB. For PMEPR< 6.5 dB, there are more orthogonal codes from OC_3 of length 32 than from OC_m, for PMEPR< 5.5 dB, OC_3 of length 128 produces the largest number of orthogonal codes

with low PMEPRs, and for PMEPR> 5.5, OC_5 with length 255 produces the most orthogonal codes with low PMEPR. Compared to Walsh codes, the orthogonal code sets generated by the four classes of sequences have lower maximum PMEPRs. Moreover, the orthogonal code sets can be implemented efficiently by a simple LFSR structure, where the feedback configuration of LFSR has little influence on maximum PMEPR. Therefore, the orthogonal code sets generated by the four classes of binary sequences can replace Walsh codes to obtain low PAPR in multicarrier communications.

Chapter 6

Conclusions and Future Works

This thesis has investigated the autocorrelation and the power characteristics of special classes of binary sequences with ideal two-level autocorrelation, i.e., m-sequences, 3-term, 5-term, and Welch-Gong sequences, for the potential applications to multicarrier communications.

The aperiodic autocorrelations of the classes of sequences with length $n = 2^m - 1$ $(5 \leq m \leq 21)$ have been calculated and analyzed via merit factors, peak sidelobe levels (PSL), and average sidelobe levels (ASL). It is conjectured that the MFs of 3-term, 5-term and WG sequences asymptotically approach to 3. Following the previous research on the growth rates of PSLs and ASLs of binary sequences, we conjectured the new normalization factors of PSLs and ASLs of the four classes of sequences.

Then, we calculated and discussed the peak-to-mean-envelope-power ratios (PMEPRs) produced by the four classes of sequences with short length $n = 2^m - 1$ $(5 \leq m \leq 8)$. The results suggest that most of PMEPRs and PAPRs produced by the four classes of sequences are below 8 dB. The distributions of PMEPR of the three classes of multiple-trace term sequences are very similar. Especially, 3-term sequences of length 31 and 5-term sequences of

length 255 produce more sequences with lower PMEPR than any other class of sequences. We also calculated the PMEPRs of orthogonal codes generated by the four classes of sequences with short length $n = 2^m$ $(5 \leq m \leq 8)$. Compared to the PMEPRs of Walsh code sets, the orthogonal code sets provide lower PMEPR, where most of PMEPRs are less than 8 dB. Moreover, the binary sequences can generate various code sets according to distinct primitive polynomials with a negligible variation of maximum PMEPRs. That mean the code sets generated by binary sequences can be implemented efficiently by simple LFSR structures. Consequently, the orthogonal code sets can replace Walsh codes to obtain small PAPR in multicarrier communications.

In the future, more numerical results for large sequence lengths $n = 2^m - 1$ $(m \geq 22)$ may confirm our conjecture on MFs and the growth rates of PSLs and ASLs. Also, in an effort to search for good codes to reduce PAPR of multicarrier communication systems, more new classes of sequences with ideal two-level autocorrelation should be studied as the future work.

Acknowledgements

I wish to express my most sincere gratitude to my supervisor, Dr. Nam Yul Yu, for his continuing support and inspiring supervision throughout my research. I would like to thank my co-supervisor Dr. Zhiwei Mao and Dr. K. Natarajan for their help and suggestions. I would also like to acknowledge Dr. Ruizhong Wei and Dr. Hassan Naser for their efforts as examiners of this thesis.

I thank all my friends at Lakehead University for their friendship, moral support and technical discussion during the past two years.

I wish to express my deepest thanks to my family, my parents, my grandparents and my uncle for their continuous love and support.

Bibliography

[1] IEEE Std., *Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*, IEEE standard 802.11-2007 ed., 2007.

[2] IEEE Std., *Part 16: Air interface for fixed broadband wireless access systems*, IEEE standard 802.16-2004 ed., 2004.

[3] A. Peled and A. Ruiz, "Frequency domain data transmission using reduced computational complectly algorithms," *Acoustics, speech, and signal processing, IEEE international conference*, vol. 5, pp. 964–967, 1980.

[4] R. Prasad and S. Hara, "An overview of multicarrier CDMA," *Proc. of Fourth International Symposium on spread spectrum techniques and application (ISSSTA '96)*, pp. 107–114, 1996.

[5] J. Jedwab, "Comment: M-sequences for OFDM peak-to-average power ratio reduction and error correction," *Electronic Letters*, vol. 33, pp. 1293–1294, 1997.

[6] F. M. Roemer, "The multitone channel," *Journal Audio Engineering Society*, vol. 41, pp. 158–173, 1993.

[7] S. H. Han and J. H. Lee, "An overview of peak-to-average power ratio reduction techniques for multicarrier transmission," *IEEE Wireless Communications*, pp. 56–65, 2005.

[8] A. E. Jones, T. A. Wilknson, and S. K. Barton, "Block coding scheme for the reduction of peak to mean envelope power ratio of multicarrierr transmission schemes," *Electron.Lett*, vol. 30, no. 22, pp. 2098–2099, 1994.

[9] A. E. Jones and T. A. Wilkson, "Combined coding for error control and increased robustness to system nonlinearities in OFDM," *Proc. IEEE 45th Veh. Technol. Conf. (VTC'96)*, pp. 904–908, 1996.

[10] R. D. J. van Nee, "OFDM codes for peak-to-average power reduction and error correction," *IEEE Globecomm 1996*, pp. 740–744, 1996.

[11] X. Li and J. A. Ritcey, "M-sequences for OFDM peak-to-average power ratio reduction and error correction," *Electronics Letters*, vol. 33, no. 7, pp. 555–556, 1997.

[12] C. Tellambura, "Use of m-sequences for OFDM peak-to-average power ratio reduction," *Electronics Letters*, vol. 33, no. 15, pp. 1300–1301, 1997.

[13] A. Goldsmith, *Wireless Communication*. Cambridge University Press, 2008.

[14] IEEE Std., *Carrier sense multiple access with collision detection (CMSA/CD) access method and physical layer specifications*, IEEE standard 802.20-2008 ed., 2008.

[15] IEEE Std., *Overview and Architecture*, IEEE standard 802.20-2008 ed., 2008.

[16] *3GPP TS 25.213: Technical Specification Group Radio Access NetWork; Spreading and modulation (FDD)(Release 1999)*, Dec. 2003.

[17] H. Liu and G. Li, *OFDM-based Broadband Wireless Networks.* Wiley, 2005.

[18] V. K. Garg, *IS-95 CDMA and cdma2000.* Prentice Hall, 2000.

[19] R. H. Barker, *Group sunchronizing of binary system.* New York: Academic Press, 1953.

[20] M. J. E. Golay, "Multislit spectroscopy," *J. Opt. Soc. Amer.*, vol. 39, pp. 437–444, 1949.

[21] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFMD, Golay complementary sequences and Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. IT-45, no. 7, pp. 2397–2417, 1999.

[22] H. Ochiai and H. Imai, "Block coding scheme based on complementary sequences for multicarrier signals," *IEICE Trans.Fundamentals*, vol. E80-A, pp. 2136–2143, 2000.

[23] S. W. Golomb and G. Gong, *Signal Design for Good Correlation.* Cambridge University Press, 2005.

[24] J. Seberry and M. Yamada, "Hadamard matrices, sequences, and block designs," *Contemporary Design Theory: A Collection of Surveys*, 1992.

[25] S. W. Golomb, *Shift-register sequences.* San Francisco, CA: Holden-Day, 1967.

[26] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.*, vol. 14, no. 4, 1962.

[27] J. S. No, "Generalization of GMW sequences and No sequences," *IEEE. Trans. Inform. Theory*, vol. 42, pp. 260–262, 1996.

[28] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number theory.* Springer-Verlag, 2nd ed., 1991.

[29] L. D. Baumert, *Cyclic Difference Sets.* Springer-Verlag, 1971.

[30] M. Hall, "A survey of difference sets," *Proc. Amer. Math. Soc.*, vol. 7, pp. 975–986, 1956.

[31] A. Maschietti, "Difference sets and hyperovals," *Designs, Codes and Cryptography*, vol. 14, pp. 89–98, 1998.

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

[33] J. F. Dillon and H. Dobbertin, "New cyclic difference sets with singer parameters," *Finite Fields and Their Application 10*, pp. 342–389, 2004.

[34] J. Jedwab, "A survey of the merit factor problem for binary sequences," *Sequences and their application–Proc. SETA 2004*, vol. 3468, pp. 30–55, 2005.

[35] M. J. E. Golay, "A class of finite binary sequences with alternate auto-correlation values equal to zero," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 449–450, 1972.

[36] H. E. Jensen and T. Høholdt, "Binary sequences with good correlation properties," *Applied algebra, Algebraic algorithms and error-correcting codes*, vol. 356, pp. 306–320, 1989.

[37] T. Høholdt and H. E. Jensen, "Determination of the merit factor of legendre sequences," *IEEE Trans. Inform. Theory*, no. 34, pp. 161–164, 1988.

[38] J. W. Moon and L. Moser, "On the correlation function of random binary sequences," *SIAM J. Appl. Math.*, pp. 340–343, 1968.

[39] M. N. Cohen, J. M. Baden, and P. E. Cohen, "Biphase codes with minimum peak sidelobes," *Proc.IEEE Nat. Radae Conf.*, pp. 62–66, 1989.

[40] D. Dmitriev and J. Jedwab, "Bounds on the growth rate of the peak sidelobe level of binary sequences," *Advances in Mathematics of Communications*, vol. 00, no. 0, pp. 1–15, 2007.

[41] R. J. McEliece, "Correlation properties of sets of sequences derived from irreducible cyclic codes," *Inf. Contr.*, vol. 45, pp. 18–25, 1980.

[42] D. V. Sarwate, "An upper bound on the aperiodic autocorrelation function for a maximal-length sequence," *IEEE Trans. Inf. Theory*, vol. IT-30, pp. 685–687, 1984.

[43] J. Jedwab and K. Yoshida, "The peak sidelobe level of families of binary sequences," *IEEE Trans. Inform. Theory*, vol. 52, pp. 2247–2254, 2006.

[44] S. Litsyn, *Peak Power Control in Muliticarrier Communications*. Cambridge University Press, 2007.

[45] C. Tellambura, "Upper bound on peak factor of n-multiple carriers," *Electronics Letters*, vol. 33, pp. 1608–1609, 1997.

Appendix A

Basic Primitive Polynomials

In Table A.1, we listed the basic primitive polynomials which have been used in our experiments over $GF(2)$ of every degree up to 21 [23]. In the second column of Table A.1, we represent a primitive polynomial $f(x) = x^m + d_{m-1}x^{m-1} + \cdots + d_1x + d_0$ as a vector $(d_0, d_1, \ldots, d_{m-1})$. For example, for $m = 5$, the primitive polynomial is $f(x) = x^5 + x^3 + 1$.

Table A.1: Basic primitive polynomials over GF(2) of degree m: $5 \leq m \leq 21$

m	$(d_0, d_1, \ldots, d_{m-1})$
5	10010
6	110000
7	1100000
8	10111000
9	100010000
10	1001000000
11	10100000000
12	110010100000
13	1101100000000
14	11010100000000
15	110000000000000
16	1011010000000000
17	10010000000000000
18	111001000000000000
19	1110010000000000000
20	10010000000000000000
21	101000000000000000000

Appendix B

Trace Representations of 3-term, 5-term and WG Sequences

In Tables B.1 and B.2, we listed the trace exponents of 3-term and 5-trem sequences.

In Tables B.3, B.4 and B.5, we listed the trance exponents of WG sequences.

Table B.1: Trace representations of 3-term sequences of length $n = 2^m - 1$, $5 \leq m \leq 21$

	Trace exponents		
m	q_0	q_1	q_2
5	1	5	7
7	1	9	13
9	1	17	25
11	1	33	49
13	1	65	97
15	1	129	193
17	1	257	385
19	1	513	769
21	1	1025	1537

Table B.2: Trace representations of 5-term sequences of length $n = 2^m - 1$, $7 \leq m \leq 20$

	Trace exponents				
m	q_0	q_1	q_2	q_3	q_4
7	1	5	21	13	29
8	1	9	37	29	39
10	1	9	73	57	121
11	1	17	137	121	143
13	1	17	273	241	497
14	1	33	529	497	543
16	1	33	1057	993	2017
17	1	65	2081	2017	2111
19	1	65	4161	4033	8129
20	1	129	8257	8129	8319

Table B.3: Trace representations of WG sequences of length $n = 2^m - 1$, $7 \leq m \leq 16$

m	The number of terms	The trace exponents
7	5	1, 3, 7, 9, 29
8	5	19, 39, 13, 21, 29
10	13	1, 5, 11, 3, 13, 7, 15, 69, 89, 35, 105, 71, 121
11	13	69, 139, 35, 141, 71, 143, 25, 41, 57, 73, 89, 105, 121
13	29	1, 9, 19, 5, 21, 11, 23, 3, 25, 13, 27, 7, 29, 15, 31, 265, 305, 133, 337, 267, 369, 67, 401, 269, 433, 135, 465, 271, 497
14	29	265, 531, 133, 533, 267, 535, 67, 537, 269, 539, 135, 541, 271, 543, 49, 81, 113, 145, 177, 209, 241, 273, 305, 337, 369, 401, 433, 465, 497
16	61	1, 17, 35, 9, 37, 19, 39, 5, 41, 21, 43, 11, 45, 23, 47, 3, 49, 25, 51, 13, 53, 27, 55, 7, 57, 29, 59, 15, 61, 31, 63, 1041, 1121, 521, 1185, 1043, 1249, 261, 1313, 1045, 1377, 523, 1441, 1047, 1505, 131, 1569, 1049, 1633, 525, 1697, 1051, 1761, 263, 1825, 1053, 1889, 527, 1953, 1055, 2017

Table B.4: Trace representations of WG sequences of length $n = 2^m - 1$, $17 \leq m \leq 19$

m	The number of terms	The trace exponents
17	61	1041, 2083, 521, 2085, 1043, 2087, 261, 2089, 1045, 2091, 523, 2093, 1047, 2095, 131, 2097, 1049, 2099, 525, 2101, 1051, 2103, 263, 2105, 1053, 2107, 527, 2109, 1055, 2111, 97, 161, 225, 289, 353, 417, 481, 545, 609, 673, 737, 801, 865, 929, 993, 1057, 1121, 1185, 1249, 1313, 1377, 1441, 1505, 1569, 1633, 1697, 1761, 1825, 1889, 1953, 2017
19	125	1, 33, 67, 17, 69, 35, 71, 9, 73, 37, 75, 19, 77, 39, 79, 5, 81, 41, 83, 21, 85, 43, 87, 11, 89, 45, 91, 23, 93, 47, 95, 3, 97, 49, 99, 25, 101, 51, 103, 13, 105, 53, 107, 27, 109,55, 111, 7, 113, 57, 115, 29, 117, 59, 119, 15, 121, 61, 123, 31, 125, 63, 127, 4129, 8129 4289, 2065 4417, 4131, 4545, 1033, 4673, 4133, 4801, 2067, 4929, 4135, 5057, 517, 5185, 4137, 5313, 2069, 5441, 4139, 5569, 1035, 5697, 4141, 5825, 2071, 5953, 4143, 6081, 259, 6209, 6721, 4149, 4145, 6337, 2073, 6465, 4147, 6593, 1037, 6849, 2075, 6977, 4151, 7105, 519, 7233, 4153, 7361, 2077, 7489, 4155, 7617, 1039, 7745, 4157, 7873, 2079, 8001, 4159,

Table B.5: Trace representations of WG sequences of length $n = 2^m - 1$, $m = 20$

m	The number of terms	The trace exponents
20	125	4129, 8259, 2065, 8261, 4131, 8263, 1033, 8265, 8283, 4133, 8267, 2067, 8269, 4135, 8271, 517, 8273, 4137, 8275, 2069, 8277, 4139, 8279, 1035, 8281, 4141, 2071, 8285, 4143, 259, 8289, 4145, 8291, 2073, 8293, 4147, 8295, 1037, 8297, 4149, 8299, 2075, 8301, 4151, 8303, 519, 8305, 4153, 8307, 2077, 8309, 4155, 8311, 1039, 8313, 4157, 8315, 2079, 8317, 4159, 8319, 193, 321, 449, 577, 705, 833, 961, 1089, 1217, 1345, 1473, 1601, 1729, 1857, 1985, 2113, 2241, 2369, 2497, 2625, 2753, 2881, 3009, 3137, 3265, 3393, 3521, 3649, 3777, 3905, 4033, 4161, 4289, 4417, 4545, 4673, 4801, 4929, 5057, 5185, 5313, 5441, 5569, 5697, 5825, 5953, 6081, 6209, 6337, 6465, 6593, 6721, 6849, 6977, 7105, 7233, 7361, 7489, 7617, 7745, 7873, 8001, 8129, 8287,