CORRELATION BOUNDS ON SOME NONLINEAR SEQUENCE SETS

A DISSERTATION

Submitted in partial fulfillment of the requirements for the award of the degree

of

MASTER OF TECHNOLOGY

in

ELECTRONICS AND COMMUNICATION ENGINEERING

(With Specialization in Communication Systems)

By

NAVEEN KUMAR M.

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE - 247 667 (INDIA)

JUNE, 2008

CANDIDATE'S DECLARATION

I hereby declare that the work being presented in this dissertation entitled **"Correlation Bounds on some Nonlinear Sequence Sets"** in partial fulfillment of the requirements for the award of the degree of MASTER OF TECHNOLOGY with specialization in COMMUNICATION SYSTEMS, submitted in the Department of Electronics and Computer Engineering, Indian Institute of Technology, Roorkee is an authentic record of my own work carried out from July 2007 to June 2008, under the guidance and supervision of **Mr. S. CHAKRAVORTY**, Assistant Professor, Department of Electronics and Computer Engineering, Indian Institute of Technology, Roorkee and **Dr. SUGATA GANGOPADHYAY**, Assistant Professor, Department of Mathematics, Indian Institute of Technology, Roorkee.

I have not submitted the matter embodied in this dissertation for the award of any other degree or diploma.

Date: 30/06/2008

Place: ROORKEE

M. Naveen Kumar

M. NAVEEN KUMAR

CERTIFICATE

This is to certify that the above statement made by the candidate is correct to the best of our knowledge and belief.

Date: 30/6/08

Place: Roorkee

Sugata Ganguli

Dr. SUGATA GANGOPADHYAY

Assistant Professor,

Dept. of Mathematics,

IIT Roorkee,

Roorkee - 247667.

S. Chakravorty

Mr. S. CHAKRAVORTY

Assistant Professor,

E&C Department,

IIT Roorkee,

Roorkee – 247667.

ACKNOWLEDGEMENTS

It is my privilege and pleasure to express my profound sense of respect, gratitude and indebtedness to my guides, **Mr.S.Chakravorty**, Asst. Professor, Department of Electronics and Computer Engineering and **Dr. Sugata Gangopadhyay**, Asst. Professor, Dept. of Mathematics, Indian Institute of Technology, Roorkee, for their inspiration, guidance, constructive criticisms and encouragement throughout this project work.

Thanks are due to the Lab staff Communication Systems Lab, Department of electronics and Computer Engineering, IIT Roorkee for providing necessary facilities.

I am greatly indebted to all my friends, who have graciously applied themselves to the task of helping me with ample morale support and valuable suggestions. Finally, I would like to extend my gratitude to all those persons who directly or indirectly helped me in the process and contributed towards this work.

(M. NAVEEN KUMAR)

ABSTRACT

Pseudo-Noise (PN) sequences with low out-of-phase autocorrelation and low cross-correlation values have many applications as synchronization codes, masking or scrambling codes, and for white noise signals in communication systems, signal sets in Code Division Multiple Access (CDMA) communications, key stream generators in stream cipher cryptosystems, random number generators, and as testing vectors in hardware design. Besides, sequences with large linear span increase the linear complexity of the sequence, thus makes difficult to generate a replica of the sequences for eavesdropping and jamming purposes. This dissertation work focuses on study of various nonlinear sequences and their correlation properties.

Bounds on correlation functions of signals play a major part in evaluating the theoretical performance of the spreading sequences and in sequence set selection for reliable, efficient and secure communication. Welch and Sidelnikov bounds have long been used as a benchmark for testing the merit of signal sets in the design of good CDMA sequence families. Besides, partial correlations are equally important in practice. This dissertation work is focused on determination of the peak partial correlation bounds of binary signals over fading channels.

Binary signals with 2-level autocorrelation values such as maximal length sequences, GMW sequences, Cascaded GMW sequences, quadratic residue sequences, Hall sextic sequences, have importance in synchronization, radar, cryptography etc. In this dissertation, determination of upper bound on peak partial autocorrelation of cascaded GMW sequences using underlying interleaving structure of *m*-sequence is considered.

Synchronous CDMA systems require large set of families with low cross-correlation values as signature sequences. Bent and Semi-bent signal sets have the best nonlinearity possible which makes them more secure to use. This dissertation focuses on obtaining lower bound on maximum correlation of binary signals over fading channels.

TABLE OF CONTENTS

ACKNOWLEDGEMENT ii

ABSTRACT iii

TABLE OF CONTENTS iv

CHAPTER 1. INTRODUCTION 1

1.1 Literature Survey 3

1.1.1 Sequences 3

1.1.2 Correlation Bounds 6

1.2 Problem Statement 8

1.3 Organization of the report 9

CHAPTER 2. PROPERTIES OF PN SEQUENCES 10

2.1 Golomb's Randomness Postulates 11

2.2 Cross-Correlation 13

2.3 Partial Period Correlation 13

2.4 Linear Span 14

2.5 Nonlinearity 14

2.6 Merit Factor 16

CHAPTER 3. BOUNDS ON CORRELATION OF SEQUENCES 17

3.1 Bounds on Maximum Periodic Correlation 17

3.1.1 Complex sequences over non-fading channels 17

3.1.2 Binary signals over fading channels 21

3.2 Bounds on Peak partial Correlation 24

3.2.1 Complex sequences over non-fading channels 24

3.2.2 Binary Signals over fading channels 26

3.3 Bounds on the Peak Partial Correlation of Interleaved Sequences 28

3.3.1 Interleaved sequences 28

3.3.2 Partial Correlation of Interleaved sequences 29

CHAPTER 4. GMW CONSTRUCTIONS 33

4.1 GMW sequences 33

4.1.1 Statistical Properties of GMW sequences 34

a) Autocorrelation 34

b) Linear Span 38

c) Balance Property 39

4.1.2 An Example 39

4.1.3 Partial Autocorrelation of GMW sequences 43

4.2 Cascaded GMW sequences 45

4.2.1 Statistical Properties of Cascaded GMW sequences 46

a) Autocorrelation 46

b) Linear Span 46

4.2.2 Partial Autocorrelation of Cascaded GMW sequences 47

CHAPTER 5. BENT AND SEMI-BENT SEQUENCES 49

5.1 Bent Function Sequences 49

5.1.1 Bent Function 49

a) Properties 49

b) Construction of Bent Functions 50

5.1.2 Modified Bent Functions 50

5.1.3 Statistical Properties of Bent Function Sequences 52

a) Correlation Properties 52

b) Linear Span 54

5.1.4 Mechanization of Bent Sequences 55

5.2 Semi-Bent Sequences 57

5.2.1 Linear Combination of Gold Functions 57

5.2.2 Some Characterizations of Semi-bent Quadratic Functions 60

a) Semi-bent functions for all choices of coefficients 60

b) Semi-bent Quadratic functions from Arithmetic Progression 62

5.2.3 Statistical Properties of Semi-bent sequences 64

a) Cross-correlation 64

b) Linear Span 65

5.2.4 Maximum Periodic Correlation of Semi-bent Sequences over fading channels 65

CHAPTER 6. SIMULATION RESULTS AND DISCUSSION 68

6.1 Correlation Bound on GMW sequences 68

6.2 Correlation Bound on Cascaded GMW sequences 71

6.3 Correlation Bound on semi-bent signal set over fading channel 75

CHAPTER 7. CONCLUSION 77

REFERENCES 79

APPENDIX A. REAL-TIME IMPLEMENTATION 84

A.1. Bent Sequence Generator 84

A.2 Semi-bent Sequence Generator 85

APPENDIX B. 88

B.1. Trace Function 88

B.2 Trace Transform 89

Chapter 1
INTRODUCTION

The world is demanding more from wireless communication technologies than ever before as more people around the world are subscribing to wireless. Add in exciting Third-Generation (3G) wireless data services and applications - such as wireless email, web, digital picture taking/sending, assisted-GPS position location applications, video and audio streaming and TV broadcasting - and wireless networks are doing much more than just a few years ago. Thus, the continuous growth in traffic volume and emergence of new services has begun to change the structure of wireless networks. Future mobile communications systems will be characterized by high throughput, integration of services, and flexibility. The high capacity required to support these characteristics can be obtained by using the spectrum as efficiently as possible and by flexibility in radio resource management.

Spread spectrum code-division multiple access (CDMA) approaches have been proposed for a variety of digital cellular mobile and wireless personal communications systems. The CDMA air interface is used in both 2G and 3G networks. 2G CDMA standards are branded cdmaOne and include IS-95A and IS-95B. CDMA is the foundation for 3G services: the two dominant IMT-2000 standards, CDMA2000 and WCDMA. Three of the five approved radio interface modes for IMT-2000 standards (CDMA2000, TD-SCDMA, WCDMA) are based on CDMA. Thus, CDMA is the fastest growing wireless technology and it will continue to grow at a faster pace than any other technology.

In a world beset by too little RF spectrum to satisfy the ever-growing demands of military, commercial, and private users, although the bandwidth occupancy of a single transmitted signal in spread spectrum communication is much higher than in systems using conventional modulation methods, spread spectrum has almost as many reasons for being the choice of technology. Some of the advantages of spread spectrum are [1]:

- As the signal is spread over a large frequency band, the power spectral density becomes very small.
- CDMA can provide for Multiple Access or Random Access. A large number of codes can be generated, so a large number of users can be permitted to transmit. This kind of multiple access can operate without centralized control.
- Without knowing the spreading code, it is difficult to recover the transmitted data. Moreover, as the spectral density is small, the signal may remain undetected.
- Spreading and despreading makes the signal robust against interference. This also holds for multipath self interference.
- As the bandwidth can be made much larger than the coherence bandwidth of the channel, the system is less susceptible to deep fades at particular frequencies.
- In conjunction with a RAKE receiver, spread spectrum can provide coherent combining of different multipath components.
- The wide bandwidth of spread spectrum signals is useful for location and timing acquisition

Thus, CDMA consistently provides better capacity for voice and data communications compared to other commercial mobile technologies, allowing more subscribers to connect at any given time. All the above advantages have contributed to growing interest in this technology for proposed second- and especially third-generation cellular mobile systems, second-generation wireless LANs and for future wireless communications.

Various advantages of spread-spectrum communication systems that are rooted on spectrum-spreading are attributed to the randomness criterion of spreading sequence (alternatively spreading code, Pseudo-Noise (PN) sequence). Thus, the design of spreading sequences for spread spectrum communications has been a topic of interest over the last 50 years, starting in the arena of military communications - where the terms *spread spectrum* originated since the emphasis then was on spreading the spectrum to 'hide' the transmissions from conventional narrow band receivers or wideband receivers not having access to the correct spreading sequence. Spreading sequences have been widely used as synchronization codes, masking or scrambling codes, and for white noise signals in communication systems, signal sets in CDMA (code division multiple access) communications, key stream generators in stream cipher cryptosystems, random number generators in many cryptographic primitive algorithms for secure authentication, and as testing vectors in hardware design.

A very popular method of band-spreading in spread spectrum systems is to multiply the user data signal by a PN sequence, the bit rate of which is much higher than the data bit rate. The resulting waveform is wideband, noise-like, balanced in phase and has flexible timing structure. When the spread signal is received, the spreading is removed from the desired signal by multiplying with the same PN sequence that is exactly synchronized to the received PN sequence. When despreading is applied to the interference generated by the other user's signals, there is no despreading. Thus, the link performance in spread spectrum systems is affected by

- Multi-User interference
- the asynchronous multipath interference, arising from the delayed signals from
  - the other users as well as
  - user himself

The level of these interferences depends upon the correlation properties of the spreading sequences. Good autocorrelation properties are also crucial for timing recovery and coherent detection. Therefore, the goal of spread spectrum designers for multiple access system is to find a large set of spreading codes such that as many users as possible can use a band of frequencies with as little amount of self and mutual interference as possible.

1.1 Literature Survey

In this section, we provide with a selective survey on various linear and nonlinear sequences and bounds on the maximum correlation.

1.1.1 Sequences

Binary maximal length linear shift register sequences (m-sequences) have been extensively studied in the past [2]. As the name suggests, they are precisely the sequences of maximum possible period (which is $N = 2^n - 1$) from an n-stage linear feedback shift register. These sequences have successfully been applied in different fields such as spread spectrum communication, error control coding, cryptography and signal acquisition and synchronization. Many of these applications are concerned with the correlation properties (both autocorrelation and cross-correlation) and the “noise-like” aspect of m-sequences.

In spread spectrum communication systems, the m-sequences are used for generating direct spread sequences or frequency hopping sequences. In frequency hopping systems the hopping frequencies are assigned to the elements or groups of elements of m-sequences [3]. In both direct spread and frequency hopping systems, the spreading sequences increase the security of the system.

Code division multiple access (CDMA) communication systems not only require a set of sequences which have good synchronization properties but also sequences that are easily distinguished form each other [4]. Preferred pairs of m-sequences [5] are defined as m-sequences which have small three or four-level cross-correlation values. However, for the vast majority of applications more than several sequences are needed. For instance large sets of sequences are needed for typical CDMA communication system, it is not uncommon for thirty or more to be required and for certain random access and hybrid systems the number of sequences required could easily exceed a few hundred. A set of binary Gold sequences (Gold code) [6,7] of period $N = 2^n - 1$ consists of N+2 sequences which can be obtained from a preferred pair of m-sequences. All pairs of sequences of the Gold set have the same three-level cross-correlation values as the preferred pair which is $1 + 2^{(n+2)/2}$ for n = 2 modulo 4. A small binary Kasami set of sequences of period $N = 2^n - 1$ can be obtained from one even degree n = $2m$ primitive polynomial and one degree m primitive polynomial which produces a set of 2^m sequences with maximal cross-correlation value of $1 + 2^m$.

With the increasing number of applications that involve wireless communication among mobile devices, the demand for implementing security in such systems becomes inevitable. However, the above sequences might not be suitable for applications in secure communications, because they are linearly generated which makes it relatively simple to generate a replica of the sequences for eavesdropping, jamming, or ‘spoofing’ purposes. So, many researchers have contributed to the construction of nonlinear sequences which increases the linear complexity of the sequence and consequently reduce the impact of interception and jamming by a hostile user. Gordon, Mills, and Welch have designed a set of GMW sequences which have the property of almost even distribution of each element and a large equivalent linear span (the length of a linear shift register that will generate the sequence) [8]. Klapper *et.al*, designed cascaded GMW sequences [9] which share most important properties of GMW sequences and m-sequences besides having large linear span than GMW sequences in most cases. Binary bent function sequences developed by Olsen, Scholtz, and Welch [10] have the desirable features of a secure communication system and achieve a large equivalent linear span. Kumar and Scholtz [11] have extended the bent function sequences over prime fields and have established an upper bound on the equivalent linear span. Semi bent sequences [12], obtained through a linear combination of gold functions, have three level correlation properties like Gold sequences besides possessing large linear span. In the literature, semi-bent functions are also called 3-valued almost optimal Boolean functions [13], plateaued functions [14] and preferred functions [15]. No and Kumar [16] developed a new set of No sequences which contain a GMW sequence and includes the small set of Kasami sequences as a special case. The linear span of No sequences is greater than or equal to the linear span of GMW sequences.

Kumar and Moreno [17] developed polyphase sequences over nonbinary prime fields GF(p) which are asymptotically optimum with respect to its correlation properties. Compared to the same length Gold set over GF(p), the maximum correlation values of the polyphase sequences can be reduced by approximately $\sqrt{2}$. The set of polyphase sequences has a total of 2p+2 correlation levels. Also, compared to the binary case a nonbinary set yields a larger number of sequences for the same period.

There has recently been much investigation of quasi-synchronous CDMA (QS-CDMA) systems which make use of zero correlation zone (ZCZ) sequence, or low correlation zone (LCZ) sequences, or generalized orthogonal sequences [18]. In QS-CDMA systems, also called ‘approximately synchronous CDMA’ (AS-CDMA) systems, the correlation functions of the spreading sequences employed take zero or very low values for a continuous correlation shift zone around the in-phase shift. The significance of ZCZ/LCZ sequences to QS-CDMA systems is that, even if there are relative delays between the received spreading signals due to the inaccurate access synchronization and the multipath propagation, the orthogonality between the signals is still maintained, as long as the relative delay does not exceed certain limits.

1.1.2 Correlation Bounds

In order to evaluate the theoretical performance of the spreading sequences, it is important to find the tight theoretical limits that set bounds among the sequence length, sequence family size, maximum aperiodic (periodic) autocorrelation sidelobe and maximum aperiodic (periodic) cross-correlation value. In fact, the tight constraint relation among these parameters has been a key and active issue in information theory and communication engineering.

In 1971, Sidelnikov obtained a lower bound for the periodic correlation of sequences over complex roots of unity [19]. In 1974, Welch [20] derived a lower bound for the periodic and aperiodic correlation of complex sequences using the property of inner product which can be considered as a special case of Sarwate bound [21] that yields trade-off between autocorrelation and cross-correlation functions. In 1990, Kumar and Liu provided an improved bound to Welch and Sidelnikov bounds for sequences over complex roots of unity [19]. Later, Levenshtein [22] derived several bounds by introducing 'weights' for shifts of sequences for binary sequence sets, which are tighter than Welch bounds. Peng and Fan [23] obtained a few aperiodic bounds based on Levenshtein's technique, but which are stronger than the Welch bounds, the Sarwate bounds and the Levenshtein bounds.

For the LCZ/ZCZ spreading sequences, Tang and Fan [24,25] established bounds on the periodic and aperiodic correlations based on Welch's technique, which included Welch bounds as special cases. For periodic correlations of LCZ/ZCZ sequences, generalised Sarwate bounds were obtained [26], which included all the previous periodic sequence bounds as special cases, such as Welch bounds, Sarwate bounds and Tang–Fan LCZ bounds. In 2001, Peng et al. [27, 28] obtained new lower bounds on aperiodic correlation of the LCZ sequences, which are stronger than Tang–Fan aperiodic bounds.

Peng and Fan [28] obtained even tighter aperiodic bounds for LCZ sequences over complex roots of unity sequences. The above content is heavily taken from [28].

In CDMA systems where many data bits are spread by each copy of a user's spreading sequences, it was shown in [29] how the multiple-access capability of CDMA systems, in which the period of the signature sequences was much larger than the number of chips per data and multiple data bits are spread by each sequence, can be related to the mean square value of partial correlation for sequence sets. Moreover, an average value and bound on the variance of the partial correlation values for a sequence set can be converted into an upper bound on the probability that a given correlation threshold is exceeded [30]. Information on higher moments can also be used to improve this bound and aid in sequence selection. In [31], a long sequence is used for synchronization, but the correlations are computed over only a short subsequence of that sequence. It was shown that the performance parameter such as mean acquisition time can be improved. In such situations, sequence sets having low absolute values of partial correlation are important.

The moment approach has been pursued for *m*-sequences in [32] and [33] (in fact, because of the shift and add property of *m*-sequences, the partial period correlation distribution for an *m*-sequence can be derived from the distribution of weights of its subsequences). The correlation moments for *m*-sequences and Gold codes have been related to the distribution of codeword weights in shortened Hamming and dual-BCH codes using the MacWilliams and Pless identities, [34, 35]. The higher moments of the partial correlation distribution of an arbitrary binary sequence are described in [36], partial correlation moments for a class of GMW sequences are studied in [37], and bounds on the variance of the partial period autocorrelations of geometric sequences were calculated in [30].

It is obviously desirable to obtain further information about partial correlations, but finding the spectrum of values taken on by the partial period correlation functions for a sequence set seems to be very difficult. By analogy with the periodic case, a natural parameter to study is the peak partial correlation of sequence sets.

Some information on the weight distributions of short subsequences of m-sequences can be found in [38]; this is easily translated into results on partial correlations. Computational results for single-sequences can be found in [35]. Upper bounds on the peak partial autocorrelation for m-sequences can be derived from the results of on the distributions of elements in partial periods of linear recurring sequences. These results can also be applied to yield bounds on peak partial correlations for sequence families in which each sequence has low linear complexity, for example, Gold codes and Kasami sets. The resulting bounds are rather weak. An approach based on the discrete Fourier transform and bounds for character sums has been used to upper-bound the *aperiodic* correlations of -sequences [39], and the aperiodic and *odd* correlations of the small Kasami sets [40]. The above content is heavily taken from [41].

In 1998, K.G. Paterson and P.J.G. Lothian [41] derived a lower partial periodic bound based on Welch's technique. But Paterson-Lothian bounds does not apply to low correlation zone (LCZ) sequences or generalized orthogonal (GO) sequences [42], which can be employed in quasi-synchronous CDMA (QS-CDMA) to eliminate the multiple access interference and multipath interference. Feng and Fan [43] established generalized lower bounds on partial aperiodic correlation of complex roots of unity sequence sets with respect to family size, sequence length, subsequence length, maximum partial aperiodic autocorrelation sidelobe, maximum partial aperiodic crosscorrelation value and the zero or low correlation zone which included all the previous aperiodic sequence bounds such as Sarwate bounds, Welch bounds, Levenshtein bounds, Tang-Fan bounds and Peng-Fan bounds as special cases.

Paterson and Lothian also established a general upper bound on the peak partial autocorrelation and cross-correlations for the class of sequences obtained by interleaving m-sequences and thus were able to obtain the bounds on the sequences sets that are expressible in interleaving form such as GMW sequences, No families and Klapper's TN sequences and d-form sequences [44].

1.2 Problem Statement

Since, nonlinear sequences improve the linear complexity of the sequences, this dissertation is aimed at examining the correlation bounds on some nonlinear sequences.

The objectives of this dissertation are as follows:

- Study of various periodic and partial period correlation bounds and investigate into generalization and improvement of these bounds.
- Study of various nonlinear sequences and their statistical properties.
- Examining for new correlation bounds on some nonlinear sequences over non-fading and fading channels.
- Comparison of obtained bounds through simulation, as it gives further view.

1.3 Organization of the Report

This rest of the dissertation report is organized as follows:

Various properties of PN sequences that are essential for reliable, efficient and secure communication are the discussion of *chapter* 2. *chapter* 3 reviews some existing lower bounds on maximum correlation and peak partial correlation of signals over non-fading and fading channels, upper bound on the peak partial correlation of interleaving sequences and subsequently provides a lower bound on the peak partial correlation of binary signals over fading channels.

Review of statistical properties of GMW and cascaded GMW sequences and upper bounds on the peak partial autocorrelation of GMW and cascaded GMW sequences using their interleaving structure is presented by *chapter* 4.

Chapter 5 reviews the construction and mechanization of modified bent function sequences and their statistical properties, the characterization of semi-bent functions as a linear combination of Gold functions and subsequently an improvement in the lower bound on the maximum correlation of semi-bent sequences over fading channels is presented.

Chapter 6 provides with simulation results in MATLAB for the correlation bounds of GMW, cascaded GMW and semi-bent sequences, and hardware realization of bent function sequences and semi-bent sequences on FPGA. *Chapter* 7 concludes the report. Implementation of Bent and Semi-bent sequence generators on FPGA are introduced in *Appendix*.

Chapter 2

PROPERTIES OF PSEUDO-NOISE (PN) SEQUENCES

In the early years of spread-spectrum transmission, the spread traffic was sent by the simultaneous transmission of a modulated and an unmodulated random wideband signal through different channels. The receiver would use the unmodulated carrier as the reference signal for despreading (correlating) the data-modulated carrier. This is known as the *transmitted reference* (TR) method [45]. The basic advantage of the TR approach was the absence of a significant synchronization problem to resolve at the receiver, since the despreading sequence was transmitted simultaneously with the useful information. The main disadvantages of the TR technique were:

- the potential adversary could listen to the despreading sequence being transmitted
- a jammer could easily spoof the system by sending a pair of waveforms acceptable to the receiver
- performance would be sharply degraded at low SNR environments when noise was present in both signals (information and reference)
- twice the bandwidth and twice the power were needed for the transmission of the information, as the reference signal had to be transmitted as well

Modern spread-spectrum systems employ a technique called *stored reference* (SR) method [45], where the spreading sequence is independently generated both at the transmitter and receiver. The advantage of the SR technique is that a well-designed spreading sequence cannot be predicted simply by monitoring the transmission. The downside is that the deterministic nature of the sequence generation (mandatory for both transmitter and receiver since each must be able to generate the sequences almost simultaneously and independently of each other) implies the sequence is not random, yet possesses some properties that one would expect to find in randomly generated sequences. Such sequences in conjunction with a couple of other criteria to be discussed later are called *pseudo-noise* (PN) or pseudo-random signals.

2.1 Golomb's randomness postulates

Rapidly generated pseudorandom sequences with "good" statistical (randomness) properties are essential components in a wide variety of modern applications including signal synchronization, navigation, radar ranging, random number generation, spread spectrum communications, multipath resolution, error correction, cryptographic systems, Monte Carlo simulations and signal identification in multiple access communication systems. Acceptable sequences should exhibit no statistical bias in the occurrence of individual symbols or small blocks of symbols. With these goals in mind, in his classic book, Golomb [2] defined a *pseudonoise* sequence to be a periodic binary sequence that passes these statistical tests for randomness:

- R-1: Balance property,
- R-2: Run property,
- R-3: Ideal two-level autocorrelation

R-1: Balance property

The seqeunces should have "balance" in every period, i.e., the number of +1's is nearly equal to the number of -1's. (More precisely the disparity should not exceed 1).

This requirement ensures that spreading sequences have no DC component which effectively avoids a spectral spike at DC or avoids biasing the noise in despreading.

R-2: Run property

In every period, half the runs have length one, one-fourth have length two, one-eighth have length three, and so forth, so that a fraction $1/2^r$ of all runs are of length r for *r* finite. The distribution on run length is called *run-length property* of a sequence.

Runs are undesirable since if there is a run of *k* consecutive 1's or 0's, the data signal over the period of run is just multiplied by constant, which reduces the bandwidth spreading (and its advantages) by roughly a factor of *k*.

R-3: Autocorrelation Property

Let S be a set of M complex-valued sequences of period N. The periodic and aperiodic cross-correlation function of sequences $\underline{\mathbf{a}} = (a_0, a_1, \ldots, a_{N-1})$, $\underline{\mathbf{b}} = (b_0, b_1, \ldots, b_{N-1})$ for $\underline{\mathbf{a}},\underline{\mathbf{b}} \in \mathrm{S}$ are defined by

$$\text{Periodic CCF:} \quad R_{\underline{\mathbf{ab}}}(\tau) = \sum_{i=0}^{N-1} a_i [b_{i+\tau}]^*, \quad \tau \in \mathbb{Z} \tag{2.1}$$

where $\mathbb{Z}$ denotes the set of all integers.

$$\text{Aperiodic CCF:} \quad C_{\underline{\mathbf{ab}}}(\tau) = \begin{cases} \sum_{i=0}^{N-1-\tau} a_i [b_{i+\tau}]^* & 0 \le \tau \le N\text{-}1 \\ \sum_{i=0}^{N-1+\tau} a_{i-\tau} b_i^* & 1-N \le \tau < 0 \\ 0 & |\tau| \ge N \end{cases} \tag{2.2}$$

When $\underline{\mathbf{a}} = \mathbf{b}$, the above correlations become autocorrelation functions (ACF).

From Golomb's postulates [2], the ideal autocorrelation function $R(\tau)$ is two-valued. Explicitly,

$$NR_{\underline{\mathbf{aa}}}(\tau) = \sum_{i=0}^{N-1} a_i a_{i+\tau} = \begin{cases} N & \textbf{if } \tau = 0 \\ K & \textbf{if } 0<\tau<N \end{cases} \tag{2.3}$$

At the receiver, despreading of the received spread spectrum signal is accomplished by a correlator which computes the correlation between the received spread spectrum signal and the local reference sequence. The detection by the receiver of the high in-phase correlation value $R_{\underline{\mathbf{aa}}}(0)$ and low out-of-phase autocorrelation values determines the synchronization between transmitter and receiver necessary for the removal of the encoding sequence and the recovery of the baseband information. Thus, sequences with low out-of-phase autocorrelation sidelobes i.e., $|R_{\underline{\mathbf{aa}}}(\tau)|$ is small for $\tau \neq 0$, finds many applications in communications such as radar distance ranging, sonar distance ranging, coding theory, cryptography and signal synchronization.

However, the following properties also play a vital role in the design of spreading sequences for secure and reliable communication.

2.2 Cross correlation

In multiple access applications, many systems will be operating in the same neighborhood and each communication link will employ a different maximal length sequence. In general, the cross-correlation function between different maximal sequences may be relatively large. Thus, different systems operating in the same environment can interfere with the successful attainment and maintenance of proper synchronization by having the receiver of one communication link lock onto the cross-correlation peaks obtained by correlating with the encoding sequence of a different communication link. Thus the successful use of spread spectrum communication systems in multiplexing applications depends upon the construction of large families of encoding sequences with uniform low cross-correlation values.

The classical goal in sequence design for CDMA systems has been the minimization of the parameter

$$R_{\max} = \max\left\{ \left| R_{\underline{\mathbf{ab}}}(\tau) \right| \quad \text{either } \underline{\mathbf{a}} \neq \underline{\mathbf{b}} \text{ or } \tau \neq 0 \right.$$

Although, in practice, because of data modulation, the correlation that one runs into are typically of an aperiodic rather than a periodic nature, the problem of designing for low aperiodic correlation, however, is a more difficult one. A typical approach, therefore, has been to design based on periodic correlation and then analyze the resulting design for its aperiodic correlation properties.

2.3 Partial-period Correlation

The partial-period cross-correlation between binary sequences $\underline{\mathbf{a}} = \left\{ a_i = (-1)^{s_i} \right\}$ and $\underline{\mathbf{b}} = \left\{ b_i = (-1)^{t_i} \right\}$ over the subsequence of length l beginning at position j and with relative shift k, denoted $PECC(\underline{\mathbf{a}},\underline{\mathbf{b}})(j,k,l)$ is defined by

$$PECC(\underline{\mathbf{a}},\underline{\mathbf{b}})(j,k,l) = \sum_{i=0}^{N-1} \rho(j,l)_i (-1)^{s_i + t_{i+k}} \qquad (2.4)$$

where

$0 \leq j,k < N$ and $1 \leq l \leq N$, and

$$\rho(j,l)_i = \begin{cases} 1 & \text{if } j+kN \le i < j+kN+l, \text{ for some } k \in \mathbb{Z} \\ 0 & \text{otherwise} \end{cases} \tag{2.5}$$

When $\underline{\mathbf{a}} = \underline{\mathbf{b}}$, the above correlations become partial autocorrelation functions $PEAC(\underline{\mathbf{a}},\underline{\mathbf{b}})(j,k,l)$.

In direct-sequence CDMA systems, the pseudorandom sequences used by various users are often very long for reasons of data security. In such situations, full period correlation $R_{\underline{\mathbf{ab}}}(\tau)$ loses some of its value as a design parameter. In order to minimize hardware complexity, correlation over a partial period of the spreading sequences is often used to demodulate data, as well as to achieve synchronization. For this reason, the partial period correlation properties of a sequence are of interest.

2.4 Linear span

The linear span of a sequence is defined as the minimum number of stages of a linear feedback shift register (LFSR) required to generate the given sequence. Thus, the linear span is a measure of the complexity of the sequence structure. Massey [46] has proposed an algorithm to determine the LFSR configuration that can produce a given sequence. This algorithm requires as many chips of a given sequence as twice the linear span of the given sequence. If the sequence's linear span is large, the interceptor needs substantial amount of time to determine the feedback connections of a shift register generator, which can generate the transmitted sequence. In addition to this, the interceptor needs complex hardware to generate the transmitted sequence. Thus, a large complexity or linear span is desired for security of the sequence in anti-jam applications.

2.5 Nonlinearity

Shift register generators are commonly used to produce binary sequences as they are small, light, inexpensive, and offer a rich variety of sequences. For example, an r-stage register has $(2^{2^r})^2$ possible combinations of feedback/feed-forward connections which can be represented as Boolean functions. If the feedback function is linear, then the output sequence is called a LFSR sequence. Otherwise, it is called a nonlinear feedback shift register (NLFSR) sequence. Among these, only 2^r linear feedback connections are possible and only $\frac{\varphi(2^r-1)}{r}$ ($\varphi(.)$is Euler's Totient function) [2] of which have the maximum period of 2^r-1. But the most serious shortcoming of linear feedback is that no more than $2r$ successive outputs are needed to determine the feedback connections and initial state of an r-stage register. The inherent predictability of linear feedback generators have motivated designers to use nonlinear operations on generator outputs to increase greatly the equivalent length which eventually increase the Equivalent Linear Span (ELS) of the sequence, while maintaining a relatively short actual length. High nonlinearity is a crucial criterion for a good sequence design since it assures resistance against linear cryptanalysis.

Let α_i denote an element of vector space V_n and $\mathcal{A}_n=\{\varphi_0,\varphi_1,....,\varphi_{2^{n+1}-1}\}$ denote the set of all affine functions so that the first half consists of linear functions f_{α_i} ordered according to the relation $\varphi_i = f_{\alpha_i}$ for all $i=0,1,.....2^n-1$and the second half consists of the (respective) complements of the functions in the first half. Thus,$\varphi_i = \bar{f}_{\alpha_i}$ for all$i=2^n,2^n+1,....,2^{n+1}-1$.

The nonlinearity of a Boolean function f is defined as

$$N_f = \min_{i=0,1,..2^{n+1}-1} d(f,\phi_i) \tag{2.6}$$

where $d(f,\varphi_i)$is the Hamming distance between function f and affine function φ_i and is given by

$$d(f,g)=2^{n-1}-\frac{1}{2}\langle\zeta_f,\zeta_g\rangle \tag{2.7}$$

where $\zeta_f=(-1)^f$ and $\zeta_g=(-1)^g$ are sequences of Boolean functions f and g respectively

In other words, the nonlinearity of a function is the distance between the function and the set $\mathcal{A}_n$. Nonlinearity measures the quality of a function via its distance to affine functions.

2.6 Merit Factor

The Merit Factor $F_N(\underline{\mathbf{a}})$ of a binary sequence $\underline{\mathbf{a}}$ of length N is defined as

$$F_N(\underline{\mathbf{a}}) = \frac{N^2}{2\sum_{\tau=1}^{N-1} C_{\underline{\mathbf{aa}}}(\tau)^2} \tag{2.8}$$

Since $C_{\underline{\mathbf{aa}}}(\tau) = C_{\underline{\mathbf{aa}}}(-\tau)$ for $1 \le |\tau| \le N-1$ and $C_{\underline{\mathbf{aa}}}(0) = N$, Merit Factor may be regarded as the ratio of the square of the in-phase autocorrelation to the sum of the squares of the out-of-phase aperiodic autocorrelation values. Thus, the merit factor is one measure of the aperiodic autocorrelation properties of a binary sequence. It is also closely connected with the signal to self-generated noise ratio of a communication system in which coded pulses are transmitted and received. Also, it is a measure of the spectral uniformity of the sequence, which is of interest in digital communications.

Let $F(\underline{\mathbf{a}})' = \lim_{N\to\infty} F_N(\underline{\mathbf{a}})$ be the asymptotic merit factor of a binary sequence u as its length goes to infinity. Then, a major design issue on the merit factor is to find binary sequences of length N with high asymptotic merit factors. The best known and theoretically proven asymptotic merit factor of binary sequences generated by constructive ways is 6.

Chapter 3

BOUNDS ON CORRELATION OF SEQUENCES

The correlation properties of PN codes play a major part in the sequence design, since they determine not only the level of multiple access interference i.e., the interference arising from other users of the channel and self-interference due to multipath propagation, but also the code acquisition properties. The first one is affected by the cross-correlation property between different sequences of the family whereas the last two are affected by the auto-correlation property i.e., the correlation between time-shifted versions of the same sequence.

In this chapter, we begin with a review of Sarwate bound [20] which quantifies the trade-off between the maximum magnitudes of the autocorrelation and cross-correlation functions. Welch bound can be easily deduced from Sarwate bound, although Welch derived it using inner products [19]. Then, a lower bound on maximum correlation of binary signals over fading channels is introduced. We then review the lower bound on peak partial correlation of signals over nonfading channels. We then provide a lower bound on peak partial correlation of binary signals over fading channels. Then, we finally conclude with a review of the upper bound for the peak partial correlation of interleaving sequences over non-fading channels.

3.1 Bounds on Maximum Periodic Correlation

3.1.1 Complex sequences over non-fading channels

Let S be a set of M complex-valued sequences of period N, i.e., for every sequence $\underline{\mathbf{a}} \in \mathrm{S}, a_i = a_{i+N}$ for all $i \in \mathbb{Z}$. The periodic cross-correlation function $R_{\underline{\mathbf{ab}}}(\tau)$ for sequences $\underline{\mathbf{a}},\underline{\mathbf{b}} \in \mathrm{S}$ reproduced here from (2.1) is

$$R_{\underline{\mathbf{ab}}}(\tau) = \sum_{i=0}^{N-1} a_i [b_{i+\tau}]^*, \quad \tau \in \mathbb{Z}$$

where a^* denotes the complex conjugate of a. Assume, $R_{\underline{\mathbf{aa}}}(0) = N$ for all $\underline{\mathbf{a}} \in \mathrm{S}$.

Obviously, $|R_{\underline{\mathbf{ab}}}(\tau)| \leq N$ for all $\underline{\mathbf{a}},\underline{\mathbf{b}} \in \mathbf{S}$.

For the set **S**, the maximum periodic cross-correlation magnitude R_c and the maximum out-of-phase periodic autocorrelation magnitude R_a are defined by

$$R_c = \max\left\{|R_{\underline{\mathbf{ab}}}(\tau)| : \underline{\mathbf{a}},\underline{\mathbf{b}} \in \mathbf{S}, \underline{\mathbf{a}} \neq \underline{\mathbf{b}}, 0 \leq \tau \leq N-1\right\}$$

$$R_a = \max\left\{|R_{\underline{\mathbf{aa}}}(\tau)| : \underline{\mathbf{a}} \in \mathbf{S}, 0 < \tau \leq N-1\right\}$$

Theorem **3.1** [20]: For any set **S** of M sequences of period N satisfying $R_{\underline{\mathbf{aa}}}(0) = N$ for all $\underline{\mathbf{a}} \in \mathbf{S}$,

$$\frac{R_c^2}{N} + \frac{N-1}{N(M-1)}\frac{R_a^2}{N} \geq 1 \tag{3.1}$$

Proof: Applying the following identity [**ref 5**],

$$\sum_{\tau=0}^{N-1} |R_{\underline{\mathbf{ab}}}(\tau)|^2 = \sum_{\tau=0}^{N-1} R_{\underline{\mathbf{aa}}}(\tau)\{R_{\underline{\mathbf{bb}}}(\tau)\}^* \tag{3.2}$$

to all members $\underline{\mathbf{a}},\underline{\mathbf{b}} \in S$, gives

$$\begin{aligned}\sum_{\underline{\mathbf{a}}\in\mathbf{S}}\sum_{\substack{\underline{\mathbf{b}}\in\mathbf{S}\\ \underline{\mathbf{a}}\neq\underline{\mathbf{b}}}}\sum_{\tau=0}^{N-1}|R_{\underline{\mathbf{ab}}}(\tau)|^2 + \sum_{\underline{\mathbf{a}}\in\mathbf{S}}\sum_{\tau=0}^{N-1}|R_{\underline{\mathbf{aa}}}(\tau)|^2 &= \sum_{\underline{\mathbf{a}}\in\mathbf{S}}\sum_{\underline{\mathbf{b}}\in\mathbf{S}}\sum_{\tau=0}^{N-1}|R_{\underline{\mathbf{ab}}}(\tau)|^2 \\ &= \sum_{\underline{\mathbf{a}}\in\mathbf{S}}\sum_{\underline{\mathbf{b}}\in\mathbf{S}}\sum_{\tau=0}^{N-1}R_{\underline{\mathbf{aa}}}(\tau)\{R_{\underline{\mathbf{bb}}}(\tau)\}^* \\ &= M^2N^2 + \sum_{\tau=1}^{N-1}\left|\sum_{\underline{\mathbf{a}}\in\mathbf{S}}R_{\underline{\mathbf{aa}}}(\tau)\right|^2\end{aligned}$$

Now,

$$\sum_{\underline{\mathbf{a}}\in\mathbf{S}}\sum_{\substack{\underline{\mathbf{b}}\in\mathbf{S}\\ \underline{\mathbf{a}}\neq\underline{\mathbf{b}}}}\sum_{\tau=0}^{N-1}|R_{\underline{\mathbf{ab}}}(\tau)|^2 + \sum_{\underline{\mathbf{a}}\in\mathbf{S}}\sum_{\tau=0}^{N-1}|R_{\underline{\mathbf{aa}}}(\tau)|^2 \leq M(M-1)NR_c^2 + MN^2 + M(N-1)R_a^2$$

and

$$M^2N^2 + \sum_{\tau=1}^{N-1}\left|\sum_{\underline{\mathbf{a}}\in\mathbf{S}}R_{\underline{\mathbf{aa}}}(\tau)\right|^2 \geq M^2N^2 \quad .$$

$$\therefore\ M(M-1)NR_c^2 + MN^2 + M(N-1)R_a^2 \geq M^2N^2$$

Hence, $$\frac{R_c^2}{N}+\frac{N-1}{N(M-1)}\frac{R_a^2}{N}\geq 1$$

Thus, (3.1) provides a lower bound on either R_a or R_c when the value of the other is known.

Define $R_{\max}=\max\left\{\left|R_{\mathbf{ab}}(\tau)\right| : \underline{\mathbf{a}},\underline{\mathbf{b}}\in\mathbf{S},\underline{\mathbf{a}}\neq\underline{\mathbf{b}},0\leq\tau\leq N-1 \textbf{ or } \underline{\mathbf{a}}=\underline{\mathbf{b}},0<\tau\leq N-1\right\}$

i.e., $R_a=R_c=R_{\max}$.

Substituting this in (3.1),

$$\frac{R_{\max}^2}{N}=\max\left\{\frac{R_c^2}{N},\frac{R_a^2}{N}\right\}\geq\frac{N(M-1)}{NM-1} \tag{3.3}$$

This is known as Welch's bound [19].

Eq (3.1) represents a straight line with $\frac{R_c^2}{N}$ plotted on x-axis and $\frac{R_a^2}{N}$ plotted on y-axis. For any set **S** of M sequences, the point $\left(\frac{R_c^2}{N},\frac{R_a^2}{N}\right)$ cannot lie outside the square of side N. According to (3.3), the point cannot lie inside the shaded square region, while according to (3.1), the point cannot lie below the straight line $x+y(N-1)/(NM-N)=1$ as shown in Fig. 2.1. Here, the x-intercept is always 1, and that the y-intercept is approximately M for large N and M.

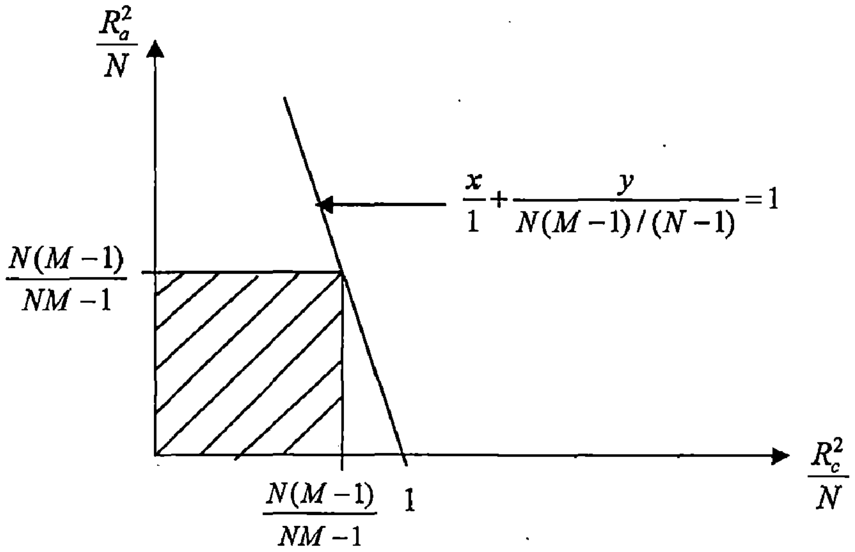


Fig. 2.1. Straight-line lower bound on periodic correlation functions

For M=N, the line passes through (0, N). The straight-line bound of (3.1) is nearly vertical and its steepness implies that if it is desired to reduce the value of $\frac{R_c^2}{N}$ to below 1, then a substantial increase in the value of $\frac{R_a^2}{N}$ must be tolerated.

When $M \le N$, Theorem 3.1 provides the best bound, but for larger values of M, better bound can be obtained from

$$N(M-1)\left(\frac{R_c^2}{N}\right)^s + (N-1)\left(\frac{R_a^2}{N}\right)^s \ge N^s \left[\frac{NM}{\binom{N+s-1}{s}} - 1\right] \tag{3.4}$$

This is the modified version of Welch's result [19]. For s=2 and $M > \frac{1}{2}(N+1)$, (3.4) implies that the point $\left(\frac{R_c^2}{N}, \frac{R_a^2}{N}\right)$, as depicted in Fig. 2.2, cannot lie inside the ellipse

$$\frac{(M-1)(N+1)}{N(2M-1-N)}x^2 + \frac{N^2-1}{N^2(2M-1-N)}y^2 = 1 \tag{3.5}$$

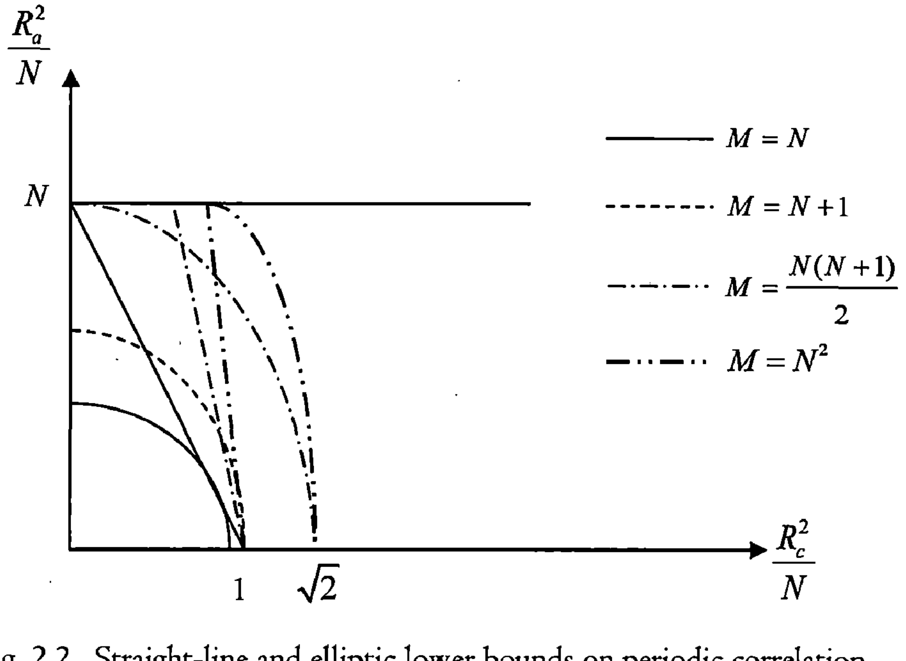


Fig. 2.2. Straight-line and elliptic lower bounds on periodic correlation

This elliptic bound can be used to improve upon (3.1) if $M > N$ but it is not uniformly better than (3.1) unless $M > N^2$ as shown in Fig. 2.2.

The Sidelnikov bound states that for any set with $M \geq N$

$$R_{\max} > \sqrt{2N-2} \tag{3.6}$$

Sidelnikov bound is typically tighter than Welch bound by a factor of $\sqrt{2}$ for a large set size. The main impact of these bounds is that they dictate the limits within which all code designs must lie. Thus, it is not possible to independently design the correlation value and the set size, but it is necessary to allow the increase of the maximum absolute correlation value in order to increase the set size for give code length.

3.1.2 Binary signals over fading channels

Let $\left\{x^{(1)}, x^{(2)}, \ldots, x^{(P)}\right\}$ be the baseband signals that P different users transmit in one symbol duration. Let the user j be assigned the sequence $\underline{\mathbf{c}}_j = \left\{c_0^{(j)}, c_1^{(j)}, \ldots, c_{N-1}^{(j)}\right\}$. Assuming the fading channel is frequency-nonselective and the receiver has perfect channel estimation, the i^{th} chip of the input signal at k^{th} receiver is defined by

$$y_i^{(k)} = \sum_{j=0}^{P-1} h_i^{(j)} x_i^{(j)} c_i^{(j)} + n_i^{(k)} \tag{3.7}$$

After despreading and low-pass filtering for desired user k, the detected signal $\bar{x}^{(k)}$ is

$$\bar{x}^{(k)} = x^{(k)} \sum_{i=0}^{N-1} h_i^{(k)} + \sum_{j=0, j\neq k}^{P-1} x^{(j)} \sum_{i=0}^{N-1} h_i^{(j)} x_i^{(j)} c_i^{(k)} + \sum_{i=0}^{N-1} n_i^{(k)} c_i^{(k)} \tag{3.8}$$

where N is the number of chips in a symbol duration. $h_i^{(j)}$, usually modeled as a random variable, is the wireless channel attenuation experienced by user j, and $n_i^{(k)}$ is real additive white Gaussian noise (AWGN) [47]. In Rayleigh fading channels, the fading amplitudes $h_i^{(j)} = \sqrt{\left[u_i^{(j)}\right]^2 + \left[v_i^{(j)}\right]^2} \geq 0$, where $u_i^{(j)}$ and $v_i^{(j)}$ are two independent zero-mean Gaussian random variables with variance σ^2 [48].

The periodic correlation of $\underline{\mathbf{a}}$, corrupted by a multiplicative fading $\underline{\mathbf{f}} = \left\{f_i = h_i^{(j)}\right\}$, and $\underline{\mathbf{b}}$ is defined by

$$R_{\underline{\mathbf{f}}.\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau) = \sum_{i=0}^{N-1} f_i \left(-1\right)^{s_i + t_{i+\tau}} \tag{3.9}$$

where $a_i = \left(-1\right)^{s_i}$ and $b_i = \left(-1\right)^{t_i}$ are the binary sequences in a signal set **S** with a size *M*, $\underline{\mathbf{f}}.\underline{\mathbf{a}}$ is the sequence whose elements are given by $f_i\left(-1\right)^{s_i}$ and *N* is the period of each sequence a_i and b_i. It is assumed that every user suffers from the same fading amplitude f_i during the same period of time, and the receiver is able to know the accurate value of f_i with the perfect channel estimation.

Let $R_1 = \max\limits_{\underline{\mathbf{a}},\underline{\mathbf{b}} \in \mathrm{S}, \underline{\mathbf{a}} \neq \underline{\mathbf{b}}} \; \max\limits_{0 \leq \tau < N} \left|R_{\underline{\mathbf{f}}.\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)\right|$ and $R_2 = \max\limits_{\underline{\mathbf{a}} \in \mathrm{S}} \; \max\limits_{0 < \tau < N} \left|R_{\underline{\mathbf{f}}.\underline{\mathbf{a}},\underline{\mathbf{a}}}(\tau)\right|$ be the cross-correlation and out-of-phase autocorrelation of signals in **S** respectively over fading channel. Then, the maximum correlation of signal set **S** is defined by,

$$R_{\max} = \max\left(R_1, R_2\right) \tag{3.10}$$

***Theorem* 3.2** [49]: Let **S** be a signal set of size *M*. Each sequence in **S** is a binary periodic sequence with a period *N*. Then, maximum correlation defined by (3.10) is lower bounded by

$$R_{\max} \geq \sqrt{\frac{MN.\sum\limits_{i=0}^{N-1} f_i^2 - \left(\sum\limits_{i=0}^{N-1} f_i\right)^2}{MN-1}} \tag{3.11}$$

Proof: Expand the signal set **S** to a signal set **T** with a size *MN* including every shift of each sequence in **S**. Then,

$$B = \sum_{\underline{\mathbf{a}},\underline{\mathbf{b}}\in\mathbf{T}} \left|R_{\underline{\mathbf{f}}.\underline{\mathbf{a}},\underline{\mathbf{b}}}(0)\right|^2 \le MN.(MN-1).R_{\max}^2 + MN.R_{\underline{\mathbf{f}}.\underline{\mathbf{a}},\underline{\mathbf{b}}}(0)^2 \qquad (3.12)$$

Also, we have

$$\begin{aligned} B &= \sum_{\underline{\mathbf{a}},\underline{\mathbf{b}}\in\mathbf{T}} \left(\sum_{i=0}^{N-1} f_i(-1)^{s_i+t_i} \right) \\ &= \sum_{i,j} f_i f_j \left(\sum_{\underline{\mathbf{a}}\in\mathbf{T}} (-1)^{s_i+s_j} \right)^2 \ge \sum_{i=0}^{N-1} f_i^2 (MN)^2 \end{aligned} \qquad (3.13)$$

This inequality is from the fact that f_i and f_j are positive. From (3.12) and (3.13),

$$MN(MN-1)\cdot R_{\max}^2 + MN\cdot\left(\sum_{i=0}^{N-1} f_i\right)^2 \ge \sum_{i=0}^{N-1} f_i^2 (MN)^2$$

and the theorem follows.

Corollary **3.1:** Let f_i, $0 \le i \le N-1$, be a fading amplitude with a mean μ and a variance σ^2. If f_i is statistically independent and identically distributed (i.i.d) for sufficiently large L, then $R_{\max}$ is lower bounded by

$$R_{\max} \ge \sqrt{\frac{MN^2\left(\mu^2+\sigma^2\right) - N^2\mu^2}{MN-1}} \qquad (3.14)$$

Proof**:** In the lower bound in Theorem 3.2, if f_i's are i.i.d for sufficiently large N,

$$\sum_{i=0}^{N-1} f_i = N\cdot\mu, \qquad \sum_{i=0}^{N-1} f_i^2 = N\cdot\left(\mu^2+\sigma^2\right) \qquad (3.15)$$

from the weak law of large numbers. Hence, the corollary is immediate from this representation.

Remark **3.1:** In Corollary 3.1, if no fading environment is assumed, $\mu = 1, \sigma = 0$. Then, $R_{\max}$ normalized by a period is given by

$$R_{\max}^{(norm)} = \frac{R_{\max}}{N} \geq \sqrt{\frac{M-1}{MN-1}}$$

This is exactly the same result as Welch's lower bound [19].

***Remark* 3.2:** In (3.12), the equality is satisfied if $\left|R_{\mathbf{f},\underline{\mathbf{a}},\underline{\mathbf{b}}}(0)\right|$ is identical over all sequences $\underline{\mathbf{a}},\underline{\mathbf{b}} \in \mathbf{T}$. It implies that as the correlation function $R_{\mathbf{f},\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)$ of any pair of sequences in **S** over fading channel is flatter, the actual maximum correlation approaches to the lower bound.

3.2 Bounds on Peak Partial Correlation

3.2.1 Complex sequences over non-fading channels

For sequences $\underline{\mathbf{a}},\underline{\mathbf{b}}$ in a sequence set **S** each of period *N*, let the peak cross-correlation between $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ over subsequences of length *l* is defined by

$$PECC_{\max}(\underline{\mathbf{a}},\underline{\mathbf{b}})(l) = \max\left(\left\{\left|PECC(\underline{\mathbf{a}},\underline{\mathbf{b}})(j,k,l)\right| : 0 \leq j,k < N\right\}\right),$$

where $PECC(\underline{\mathbf{a}},\underline{\mathbf{b}})(j,k,l)$ is given by (2.4)

the peak autocorrelation of $\underline{\mathbf{a}}$ over subsequences of length *l* by

$$PEAC_{\max}(\underline{\mathbf{a}})(l) = \max\left(\left\{\left|PEAC(\underline{\mathbf{a}})(j,k,l)\right| : 0 \leq j < N, 1 \leq k < N\right\}\right)$$

and the peak partial correlation for the set **S** over subsequences of length *l* by

$$PEC_{\max}(\mathrm{S})(l) = \max\left\{PECC_{\max}(\underline{\mathbf{a}},\underline{\mathbf{b}})(l), PEAC_{\max}(\underline{\mathbf{a}})(l) : \underline{\mathbf{a}},\underline{\mathbf{b}} \in \mathrm{S}\right\}$$

***Theorem* 3.3** [41]: Let **S** be a set of M sequences of period N and k a positive integer. Then, for every *l* with $1 \leq l \leq N$

$$\left\{PEC_{\max}(\mathrm{S})(l)\right\}^{2k} \geq \frac{l^{2k}}{NM-1}\left(\frac{NM}{\binom{l+k-1}{k}} - 1\right) \tag{3.16}$$

***Proof*:** Construct a signal set **T** with a size *MN* including every subsequence of length *l* of signal set **S** beginning at position j for $0 \leq j < N$.

Obviously,

$$NM\cdot(NM-1)\{PEC_{\max}(\mathrm{S})(l)\}^{2k}+NM\cdot l^{2k}\geq\sum_{\underline{\mathbf{a}},\underline{\mathbf{b}}\in\mathrm{T}}\left|PECC(\underline{\mathbf{a}},\underline{\mathbf{b}})(l)\right|^{2k}\qquad(3.17)$$

Consider,

$$B_k=\sum_{\underline{\mathbf{a}},\underline{\mathbf{b}}\in\mathrm{T}}\left|PECC(\underline{\mathbf{a}},\underline{\mathbf{b}})(l)\right|^{2k}=\sum_{\underline{\mathbf{a}},\underline{\mathbf{b}}\in\mathrm{T}}\left\{\sum_{i=0}^{l-1}a_ib_i^*\right\}^k\left\{\sum_{j=0}^{l-1}a_j^*b_j\right\}^k$$

For $k\geq 1$, one can expand and interchange the order of summations to obtain

$$B_k=\sum_{u_1=0}^{l-1}\cdots\sum_{u_k=0}^{l-1}\sum_{v_1=0}^{l-1}\cdots\sum_{v_k=0}^{l-1}\left|\sum_{\underline{\mathbf{a}}\in\mathrm{T}}\prod_{i=1}^{k}a_{u_i}a_{v_i}^*\right|^2\qquad(3.18)$$

Different choices of the variables $u_1,u_2,\ldots,u_k;v_1,v_2,\ldots,v_k$ give rise to the same product of the a and a^*; the number of choices can be expressed as multinomial coefficients. Then (3.18) may alternatively be expressed as

$$\sum_{\substack{x_0,\ldots x_{l-1}\\ y_0,\ldots y_{l-1}}}\binom{k}{x}\binom{k}{y}\left|\sum_{\underline{\mathbf{a}}\in\mathrm{T}}\prod_{i=0}^{l-1}(a_i)^{x_i}\left(a_i^*\right)^{y_i}\right|^2\qquad(3.19)$$

where

$$x_i,y_i\geq 0,\quad\sum_{i=0}^{l-1}x_i=\sum_{i=0}^{l-1}y_i=k,\text{ and }\binom{k}{x}=\frac{k!}{\prod_i(x_i!)}\quad\binom{k}{y}=\frac{k!}{\prod_i(y_i!)}$$

Since the summands are nonnegative, the terms with $(x_0,\ldots x_{l-1})\neq(y_0,\ldots y_{l-1})$ may be dropped to yield

$$B_k\geq\sum_{x_0,\ldots x_{l-1}}\left[\binom{k}{x}\sum_{\underline{\mathbf{a}}\in\mathrm{T}}\prod_{i=0}^{l-1}\left|(a_i)\right|^{2x_i}\right]^2$$

An application of Cauchy-Schwartz inequality yields

$$B_k \ge \frac{\left[\sum_{x_0,\ldots x_{l-1}} \binom{k}{x} \sum_{\underline{\mathbf{a}}\in \mathrm{T}} \prod_{i=0}^{l-1} |(a_i)|^{2x_i}\right]^2}{\sum_{x_0,\ldots x_{l-1}} 1}$$

where all sums have as their range $\{(x_0,\ldots x_{l-1}) : x_i \ge 0, \sum x_i = k\}$. Interchanging orders of summation and applying the multinomial expansion theorem gives

$$B_k \ge \frac{\left(\sum_{\underline{\mathbf{a}}\in \mathrm{T}} \left(\sum_{i=0}^{L-1} |(a_i)|^2\right)^k\right)^2}{\binom{l+k-1}{k}}$$

Hence,

$$B_k \ge \frac{(NM)^2 l^{2k}}{\binom{l+k-1}{k}} \tag{3.20}$$

Substituting (3.20) in (3.17), we get

$$NM \cdot (NM-1)\{PEC_{\max}(\mathbf{S})(l)\}^{2k} + NM \cdot l^{2k} \ge \frac{(NM)^2 l^{2k}}{\binom{l+k-1}{k}}$$

and the theorem follows.

3.2.2 Binary signals over fading channel

The partial correlation between $\underline{\mathbf{a}}$, corrupted by a multiplicative fading $\underline{\mathbf{f}} = \left\{f_i = h_i^{(j)}\right\}$, and $\underline{\mathbf{b}}$ over subsequence of length l beginning at position j and with relative shift k, denoted $PECC(\underline{\mathbf{f}}.\underline{\mathbf{a}},\underline{\mathbf{b}})(j,k,l)$, is defined by

$$PECC(\underline{\mathbf{f}}.\underline{\mathbf{a}},\underline{\mathbf{b}})(j,k,l) = \sum_{i=0}^{N-1} \rho(j,l)_i \, f_i \, (-1)^{s_i + t_{i+k}} \tag{3.21}$$

where $a_i = (-1)^{s_i}$ and $b_i = (-1)^{t_i}$ are the binary sequences in a signal set S with a size M, $\underline{\mathbf{f}}.\underline{\mathbf{a}}$ is the sequence whose elements are given by $f_i(-1)^{s_i}$ and N is the period of each sequence a_i and b_i, $0 \le j,k < N$ and $1 \le l \le N$, and

$$\rho(j,l)_i = \begin{cases} 1 & \text{if } j + kN \le i < j + kN + l, \text{ for some } k \in \mathbb{Z} \\ 0 & \text{otherwise} \end{cases}$$

Let the peak partial cross-correlation in fading channel between $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ over subsequences of length l be defined by

$$PECC_{\max}(\underline{\mathbf{f}}.\underline{\mathbf{a}},\underline{\mathbf{b}})(l) = \max\left(\left\{\left|PECC(\underline{\mathbf{f}}.\underline{\mathbf{a}},\underline{\mathbf{b}})(j,k,l)\right| : 0 \le j,k < N\right\}\right),$$

and the peak autocorrelation in fading channel of $\underline{\mathbf{a}}$ over subsequences of length l by

$$PEAC_{\max}(\underline{\mathbf{f}}.\underline{\mathbf{a}})(l) = \max\left(\left\{\left|PEAC(\underline{\mathbf{f}}.\underline{\mathbf{a}})(j,k,l)\right| : 0 \le j < N, 1 \le k < N\right\}\right)$$

and the peak partial correlation in fading channelfor the set S over subsequences of length l by

$$PEC_{\max}(\underline{\mathbf{f}} \cdot \mathrm{S})(l) = \max\left\{PECC_{\max}(\underline{\mathbf{f}}.\underline{\mathbf{a}},\underline{\mathbf{b}})(l), PEAC_{\max}(\underline{\mathbf{f}}.\underline{\mathbf{a}})(l) : \underline{\mathbf{a}},\underline{\mathbf{b}} \in \mathrm{S}\right\}$$

***Theorem* 3.4**: Let **S** be a signal set of size M. Each sequence in **S** is a binary periodic sequence with a period N. Then, maximum correlation denoted by $PEC_{\max}(\underline{\mathbf{f}} \cdot \mathrm{S})(l)$ is lower bounded by

$$PEC_{\max}(\underline{\mathbf{f}} \cdot \mathrm{S})(l) \ge \sqrt{\frac{MN.\sum_{i=0}^{l-1} f_i^2 - \left(\sum_{i=0}^{l-1} f_i\right)^2}{MN-1}} \tag{3.22}$$

Proof: The theorem follows by applying the argument of the inner product theorem [19] as in Theorem 3.2 to the set of length l subsequences of sequences from **S**.

3.3 Bounds on the Peak Partial Correlation of Interleaved Sequences

3.3.1 Interleaved Sequences

We describe a method for producing binary sequences of period $2^n - 1$ by interleaving *m*-sequence of period $2^m - 1$ [50].

Suppose that $m \mid n$, α is a primitive element in $GF\left(2^n\right)$ and that $\gcd\left(r, 2^m - 1\right) = 1$. Let

$$T = \frac{2^n - 1}{2^m - 1}.$$

Then α^{rT} is an element of $GF\left(2^m\right)$. Then the binary sequence $\underline{\mathbf{t}}$ with

$$t_i = tr_1^m\left(\alpha^{rTi}\right)$$

is an *m*-sequence of period $2^m - 1$. Here, $tr(\cdot)$ denotes trace function. The definition and properties of trace function are given in appendix ***A***.

For any $i \geq 0$, we can uniquely write $i = i_1 T + i_2$ where $i_1 \geq 0$ and $0 \leq i_2 < T$.

Now, let f be any function from the nonnegative integers to $GF\left(2^m\right)$ that satisfies

$$f(i) = \alpha^{rTi_1} f(i_2), \quad i = i_1 T + i_2 \tag{3.23}$$

and consider a binary sequence $\underline{\mathbf{s}} = s_0, s_1, \ldots$ with

$$s_i = tr_1^m\left[f(i)\right], \quad i \geq 0 \tag{3.24}$$

Suppose $i \geq 0$ and $i = i_1 T + i_2$. For $j \geq 0$, we have

$$\begin{aligned} f(jT + i) &= f\left((j + i_1)T + i_2\right) = \alpha^{rT(j+i_1)} f(i_2) \\ &= \alpha^{rTj} f(i) \end{aligned} \tag{3.25}$$

In particular, taking $j = 2^m - 1$ (so that $jT = 2^n - 1$), we see that $f\left(2^n - 1 + i\right) = f(i)$. Thus $\underline{\mathbf{s}}$ satisfies $s_{2^n - 1 + i} = s_i$. i.e., $\underline{\mathbf{s}}$ has period $2^n - 1$.

Now let $i \geq 0$ be fixed and consider the sequence ω^i with terms $s_i, s_{T+i}, s_{2T+i}, \cdots$. From (3.25), we have

$$s_{jT+i} = tr_1^m\left[\alpha^{rTj} f(i)\right]$$

Thus, if $f(i) = 0$, the terms of ω^i are all zero, whereas if $f(i) \neq 0$, then ω^i is a shift of the m-sequence $\underline{t}$, of period $2^m - 1$ associated with primitive element α^{rT} by some k. The value of the shift k is determined by writing $f(i) = \alpha^{rTk}$.

The sequences ω^i with $0 \leq i < T$ account for all the terms of $\underline{s}$. So $\underline{s}$ is formed by interleaving T sequences of period $2^m - 1$ which are either shifts of an m-sequence or the zero sequence. The shifts used in this interleaving are determined by the values $f(i)$ and we call f the *interleaving function* for $\underline{s}$.

The terms of any sequence obtained by interleaving an m-sequence and the all-zero sequence can be represented as in (3.24) for an appropriate choice of f satisfying (3.23). Many well-known families of sequences such as GMW sequences, Cascaded GMW sequences, No sequences etc., can be expressed in such an interleaved form.

3.3.2 Partial Correlation of Interleaved Sequences

For $0 \leq i < 2^n - 1$, let $\underline{s}_i$ denote the lT-tuple $(s_i, s_{i+1}, \cdots, s_{i+lT-1})$ of consecutive terms from $\underline{s}$. We can decompose s_i into T l-tuples of the form

$$s_{i,j} = \left(s_{i+j}, s_{i+j+T}, \cdots, s_{i+j+(l-1)T}\right), \qquad 0 \leq j < T$$

and from previous discussion, each $s_{i,j}$ is either an l-tuple of consecutive terms of $\underline{t}$ or consists of l zeros, depending on whether $f(j)$ is nonzero or zero.

Let

$$Z(f) = \left|\{j : 0 \leq j < T \text{ and } f(j) = 0\}\right|$$

and suppose that we have a bound on the weight of subsequences of length l of sequence $\underline{t}$, say

$$\left|\frac{wt(t_i)}{l}-\frac{1}{2}\right| \leq B, \quad 0 \leq i < 2^m - 1 \tag{3.26}$$

where $t_i = (t_i, t_{i+1}, \cdots, t_{i+l-1})$. Then, the weight of s_i can be shown to be bounded below by $(T-Z(f))\left(\frac{1}{2}-B\right)l$ and above by $(T-Z(f))\left(\frac{1}{2}+B\right)l$.

The following lemma is now an easy consequence of the above argument.

Lemma **1** [41]**:** Let $\underline{s}$, $\underline{t}$, and the vectors s_i and t_i, be defined as above.. Suppose B is a bound on the weights of the t_i, as in (3.26). Then

$$\left|\frac{wt(s_i)}{lT}-\frac{1}{2}\right| \leq B + \frac{Z(f)}{2T}(1-2B), \quad 0 \leq i < 2^n - 1 \tag{3.27}$$

Theorem **3.5** [41]**:** Suppose f_1 and f_2 are functions satisfying (3.23) (for the same value of r). For $i=1,2$, let sequence $\underline{s}^i$ be obtained by interleaving period 2^m-1 m-sequence $\underline{t}$ according to interleaving function f_i, as in (3.24). Suppose

$$\frac{1}{l}PEAC_{\max}(\underline{t})(l) \leq C \tag{3.28}$$

and write

$$Z(f_1,f_2) = \max_{0 \leq k < 2^n - 1}\left|\{j : f_1(j) + f_2(j+k) = 0, \quad 0 \leq j < T\}\right|$$

Then

$$\frac{1}{lT}PECC_{\max}\left(\underline{s}^1,\underline{s}^2\right)(lT) \leq C + \frac{Z(f_1,f_2)}{T}(1-C) \tag{3.29}$$

***Proof*:** For $0 \leq k < 2^n - 1$, let $\underline{s}$ denote the sequence $\underline{s}^1 + E^k\underline{s}^2$ formed by adding term by term $\underline{s}^1$ and the left shift by k places of $\underline{s}^2$. Then, we have

$$s_i = tr_1^m\left[f_1(i) + f_2(i+k)\right]$$

Now using (3.23), it is easy to show that if $i = i_1T + i_2$, then

$$f_2(i+k) = \alpha^{rTi_1} f_2(i_2+k)$$

and so

$$s_i = tr_1^m\left[\alpha^{rTi_1}\left(f_1(i_2)+f_2(i_2+k)\right)\right], \qquad i = i_1T + i_2$$

Thus the sequence $\underline{s}$ has interleaved form with interleaving function f, where $f(i) = f_1(i) + f_2(i+k)$.

From (3.28) and the shift and add property of the *m*-sequence $\underline{t}$, $B = C/2$ is a bound on the weights of the length l subsequences of $\underline{t}$, as in (3.26). From Lemma 1, we have that the weight of any subsequence s_i of length lT of $\underline{s}$ is bounded as

$$\left|\frac{wt(s_i)}{lT} - \frac{1}{2}\right| \leq B + \frac{Z(f)}{2T}(1-2B)$$

Using the relationship between correlation and weight and the fact that $Z(f) \leq Z(f_1 f_2)$, it now follows that for $0 \leq j < 2^n - 1$

$$\begin{aligned}\frac{1}{lT}\left|PECC\left(\underline{s}^1,\underline{s}^2\right)(j,k,lT)\right| &\leq 2\left[B + \frac{Z(f_1,f_2)}{2T}(1-2B)\right]\\ &= C + \frac{Z(f_1,f_2)}{T}(1-C)\end{aligned}$$

The result (3.29) follows.

Theorem 3.5 can also be easily adapted to bound the out-of-phase partial autocorrelation of an interleaved sequence $\underline{s}$. Let $\underline{s}$ have interleaving function f and define $Z_A(f)$ to be

$$Z_A(f) = \max_{1 \leq k < 2^n - 1}\left|\left\{j : f(j) + f(j+k) = 0, \quad 0 \leq j < T\right\}\right|. \qquad (3.30)$$

Using an argument almost identical to that above, we obtain

$$\frac{1}{lT}\left|PEAC_{\max}(\underline{s})(lT)\right| \leq C + \frac{Z_A(f)}{T}(1-C) \qquad (3.31)$$

$$PECC_{\max}\left(\underline{\mathbf{s}}^1,\underline{\mathbf{s}}^2\right)(l') \le \min\begin{Bmatrix} PECC_{\max}\left(\underline{\mathbf{s}}^1,\underline{\mathbf{s}}^2\right)(lT)+u, \\ PECC_{\max}\left(\underline{\mathbf{s}}^1,\underline{\mathbf{s}}^2\right)((l+1)T)-u \end{Bmatrix}$$

A similar result holds for peak partial autocorrelations.

The significance of bounds (3.29) and (3.31) $Z_A(f)$) is as follows: Suppose we can find an *m*-sequence $\underline{\mathbf{t}}$ whose length l subsequences have partial autocorrelation bounded in absolute value by *C*. Then if we can find a family of interleaving functions $\mathcal{F}$ such that $\max_{f_1,f_2\in\mathcal{F}} Z(f_1,f_2)$ and $\max_{f\in\mathcal{F}} Z_A(f)$ are sufficiently small, we can construct a family of sequences whose peak partial correlation is, roughly speaking, as proportionately small as it is for $\underline{\mathbf{t}}$.

To apply these bounds in practice, we need two ingredients. First, we require bounds on the peak partial autocorrelations for *m*-sequences. Secondly, we need families of interleaving functions $\mathcal{F}$ as described above. In fact, the values of the functions $Z(f_1,f_2)$ and $Z_A(f)$ are already known for several families of functions such as Kasami sequences, Trace Normal (TN) sequences, No sequences etc. They have been used to calculate the full-period correlation properties of the corresponding families of interleaved sequences.

Chapter 4
GMW CONSTRUCTIONS

Binary sequences of period N with 2-level autocorrelation have many important applications in communications and cryptology. In this chapter, we give constructions associated with intermediate subfields for binay 2-level autocorrelation sequences. They include GMW sequences and cascaded GMW sequences. First, we review statistical properties of GMW sequences along with an example and a lower bound on the partial autocorrelation of GMW sequences. Next, we review statistical properties of cascaded GMW sequences. Then, we conclude the chapter by providing a lower bound on partial autocorrelation of cascaded GMW sequences.

4.1 GMW sequences

Let $m \mid n$, and consider a sequence $\underline{s} = \{s_i\}$ of the form

$$\{s_i\} = tr_1^m \left\{ \left[tr_m^n(\alpha^i) \right]^r \right\}, \tag{4.1}$$

where α is a primitive element of $GF(2^n)$, and r is any integer relatively prime to $2^m - 1$ and in the range $1 \le r < 2^m - 1$. These sequences are known as "GMW sequences" [8]. The interior trace function $tr_m^n(\alpha^i)$ may be viewed as an m-sequence, with period $2^n - 1$ having elements in $GF(2^m)$.

Let $T = \dfrac{2^n - 1}{2^m - 1}$

Consider,

$$f(i) = \left[tr_m^n\left(\alpha^i\right) \right]^r \qquad i \ge 0 \tag{4.2}$$

then,

$$f(i) = \left[tr_m^n\left(\alpha^{i_1 T + i_2}\right) \right]^r \quad \text{for} \quad i = i_1 T + i_2$$

Since, α^{i_1T} is an element of $GF(2^m)$, we can write

$$f(i)=\alpha^{rTi_1}f(i_2)$$

So, sequence $s_i=tr_1^m[f(i)]$, has interleaved form as described in section 3.3.1 with interleaving function $f(i)=\left[tr_m^n(\alpha^i)\right]^r$.

Lemma **4.1** [8]: Let an m-sequence over $GF(2^m)$, be defined by

$$s_i^{'}=tr_m^n(\alpha^i)$$

where α is a primitive element of $GF(2^n)$, then every segment of T consecutive symbols from $\{s_i^{'}\}$ contains exactly $\frac{2^{n-m}-1}{2^m-1}$ zeros.

Proof: The field element α^T has order 2^m-1 and, hence, belongs to the ground field $GF(2^m)$. Therefore, by the linearity property (b) of the trace function, it follows that for any integer j,

$$tr_m^n\left(\alpha^i\right)=\alpha^{-jT}tr_m^n\left(\alpha^{i+jT}\right) \tag{4.3}$$

Since α^{-jT} is not zero, it follows that when one trace in (4.3) is zero, so is the other; thus, the zero locations in $\{s_i^{'}\}$ are subject to a T periodicity. Consequently, every segment of T symbols from $\{s_i^{'}\}$ contains the same number of zeros, that number being easily evaluated from the fact that $2^{n-m}-1$ zeroes occur in one period, i.e., 2^n-1 symbols, of $s_i^{'}$.

4.1.1 Statistical Properties of GMW sequences

a) Autocorrelation

Theorem **4.1** [8]: Let $\{a_i\}$ be a GMW sequence whose elements are given by

$$\{a_i\} = (-1)^{tr_1^m\left\{\left[tr_m^n(\alpha^i)\right]^r\right\}},$$

where α is a primitive element of $GF(2^n)$, and r, $0 < r < 2^m - 1$, is relatively prime to $2^m - 1$. Then the periodic autocorrelation function $R_{\underline{\mathbf{aa}}}(\tau)$ of $\{a_i\}$ is given by

$$\begin{aligned} R_{\underline{\mathbf{aa}}}(\tau) &\triangleq \sum_{i=0}^{2^n-2} a_{i+\tau} a_i \\ &= \begin{cases} 2^n - 1, & \tau = 0 \mod 2^n - 1 \\ -1, & \tau = 0 \mod 2^n - 1 \end{cases} \end{aligned} \tag{4.4}$$

***Proof*:** It follows immediately from trace function linearity that

$$R_{\underline{\mathbf{aa}}}(\tau) = \sum_{i=0}^{2^n-2} (-1)^{tr_1^m\left(\left[tr_m^n(\alpha^{i+\tau})\right]^r + \left[tr_m^n(\alpha^i)\right]^r\right)} \tag{4.5}$$

Express the index i in (4.5) as

$$i = i_1 + i_2 T \quad i_1 \geq 0,\ 0 \leq i_2 < 2^m - 1 \tag{4.6}$$

Using the linearity of the inner traces in (4.5) gives

$$R_{\underline{\mathbf{aa}}}(\tau) = \sum_{i_1=0}^{T-1} \sum_{i_2=0}^{2^m-2} (-1)^{tr_1^m\left(\alpha^{rTi_2}\delta(\tau, i_1)\right)} \tag{4.7}$$

$$\text{where } \delta(\tau, i_1) = \left[tr_m^n\left(\alpha^{i_1+\tau}\right)\right]^r + \left[tr_m^n\left(\alpha^{i_1}\right)\right]^r \tag{4.8}$$

Since r is relatively prime to $2^m - 1$, α^{rT} is a primitive element of $GF(2^m)$, and α^{rTi_2} takes on the values of all non-zero elements of that field as i_2 varies over its range. Hence, including the zero element of $GF(2^m)$ in the sum of (4.7) gives

$$R_{\underline{\mathbf{aa}}}(\tau) = -T + \sum_{i_1=0}^{T-1} \sum_{\beta \in GF(2^m)} (-1)^{tr_1^m(\beta\delta(\tau, i_1))} \tag{4.9}$$

By the linear property of trace function, when $\delta(\tau, i_1)$ is not zero, the inner sum vanishes because half the exponents are zero and half are one. Let $N_0(\tau)$ denote the number of values i_1 in the range $0 \le i_1 < T$ for which $\delta(\tau, i_1)$ is zero. Then (4.9) reduces to

$$R_{\underline{\mathbf{aa}}}(\tau) = -T + 2^m N_0(\tau) \tag{4.10}$$

Since r is relatively prime to $2^m - 1$ and therefore has an inverse modulo $2^m - 1$, it follows that

$$\begin{aligned} \delta(\tau, i_1) = 0 &\Leftrightarrow tr_m^n\left(\alpha^{i_1+\tau}\right) = tr_m^n\left(\alpha^{i_1}\right) \\ &\Leftrightarrow tr_m^n\left(\left(\alpha^\tau - 1\right)\alpha^{i_1}\right) = 0 \end{aligned} \tag{4.11}$$

When $\left(\alpha^\tau - 1\right)$ is zero, the right-hand equation in (4.11) is satisfied for all i_1. If $\left(\alpha^\tau - 1\right)$ is not zero, then Lemma 4.1 can be applied with (4.11) to determine $N_0(\tau)$. Thus,

$$N_0(\tau) = \begin{cases} T & \tau = 0 \bmod 2^n - 1 \\ \dfrac{2^{n-m} - 1}{2^m - 1} & \tau \ne 0 \bmod 2^n - 1 \end{cases} \tag{4.12}$$

and (4.4) follows by substitution of (4.12) into (4.10). The results of the theorem is independent of the choice of r and hence that all GMW sequences have the ideal correlation properties of m-sequences.

***Theorem* 4.2** (Power of a trace: Binary case) [51, 52]: For $1 < r < 2^m - 1$, we write $r = 2^{i_1} + \ldots + 2^{i_k}$, a binary number. Then

(i)

$$\begin{aligned} tr_m^n(x)^r &= \left(x + x^q + \ldots + x^{q^{l-1}}\right)^r \quad \left(here\ q = 2^m, l = n/m\right) \\ &= \sum_{\mathbf{t} \in \mathbb{Z}_l^k} x^{\tau_r(\mathbf{t})} \end{aligned} \tag{4.13}$$

where $\mathbf{t} = (t_1, t_2, \ldots, t_k), 0 \le t_j < l$, or equivalently, $\mathbf{t} \in \mathbb{Z}_l^k = \{(t_1, t_2, \ldots, t_k) \mid t_k \in \mathbb{Z}_l\}$ and

$$\tau_r(\mathbf{t}) = 2^{i_1 + mt_1 + \ldots + i_k + mt_k} \tag{4.14}$$

(ii) $\tau_r(\mathbf{t}) < 2^n - 1$, for all $\mathbf{t} \in \mathbb{Z}_l^k$.

(iii) $\tau_r(\mathbf{t})$ is a one-to-one mapping from $\mathbb{Z}_l^k$ to $\mathbb{Z}_{2^m-1}$. In other words, we have

$$\tau_r(\mathbf{t}) \neq \tau_r\left(\mathbf{t}'\right) \in \mathbb{Z}_l^k$$

(iv) $\tau_r(\mathrm{t}) \equiv r\left(\bmod\ 2^m - 1\right)$

(v) $w\left(tr_m^n(x)^r\right) = l^k$ where $w(\bullet)$ represents hamming weight.

***Proof*:**

(i) Expanding $tr_m^n(x)^{\mathbf{r}}$, then

$$\begin{aligned} tr_m^n(x)^r &= \left(x + x^q + \ldots + x^{q^{l-1}}\right)^r \\ &= \prod_{j=1}^{k}\left(x^{2^{i_j}} + x^{2^{i_j}q} + \ldots + x^{2^{i_j}q^{l-1}}\right) \end{aligned}$$

Since $q = 2^m$, we have

$$tr_m^n(x)^r = \prod_{j=1}^{k}\left(x^{2^{i_j}} + x^{2^{i_j+m}} + \ldots + x^{2^{i_j}+(l-1)m}\right) \tag{4.15}$$

The exponent of x in the expansion of (4.15) is a sum of k elements where each is taken from a different row of the following matrix:

$$A = \begin{bmatrix} 1 & 2^m & 2^{2m} & \cdots & 2^{(l-1)m} \\ 2 & 2^{1+m} & 2^{1+2m} & \cdots & 2^{1+(l-1)m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 2^m - 1 & 2^{m-1+m} & 2^{m-1+2m} & \cdots & 2^{m-1+(l-1)m} \end{bmatrix}_{m \times l}.$$

In other words, any exponent of x in the expansion of (4.15) can be represented as

$$\tau_r(\mathrm{t}) = \begin{array}{ccccccc} 2^{i_1+mt_1} & + & 2^{i_2+mt_2} & + & \cdots & + & 2^{i_k+mt_k} \\ \downarrow & & \downarrow & & \cdots & & \downarrow \\ \text{taken from row } i_1 & & \text{from row } i_2 & & \cdots & & \text{taken from row } i_k \end{array}$$

where $\mathbf{t} \in \mathbb{Z}_l^k = \left\{\left(t_1, t_2, \ldots, t_k\right) \mid t_k \in \mathbb{Z}_l\right\}$. Thus assertion 1 is established.

(ii) Note that the numbers in matrix A are the base of binary numbers in $\mathbb{Z}_{2^n-1}$. Since $1 < r < 2^m - 1$, then $k < m$. Thus the binary number $\tau_r(\mathbf{t})$ has the Hamming weight $k < m < n$. So

$$\tau_r(\mathbf{t}) < 2^n - 1, \text{ for all } \mathbf{t} \in \mathbb{Z}_l^k.$$

(iii) Since any integer in $\mathbb{Z}_{2^n}$ has a unique binary representation, together with assertion 2, it follows that

$$\tau_r(\mathbf{t}) \neq \tau_r(\mathbf{t}'), \text{ for all } \mathbf{t} \neq \mathbf{t}' \in \mathbb{Z}_l^k.$$

(iv) Note that $2^{jm} \equiv 1\left(\bmod 2^m - 1\right)$. From (4.14), we have

$$\tau_r(\mathbf{t}) \equiv 2^{i_1} + \ldots + 2^{i_k} \equiv r\left(\bmod 2^m - 1\right), \text{ for all } \mathbf{t} \in \mathbb{Z}_l^k$$

(v) This is immediate from assertion (iii) because there are l^k elements in $\mathbb{Z}_l^k$.

b) Linear Span

***Theorem* 4.3** [8]: Let $\{s_i\}$ be a GMW sequence whose elements are given by

$$\{s_i\} = tr_1^m\left\{\left[tr_m^n(\alpha^i)\right]^r\right\},$$

Where α is a primitive element of $GF(2^n)$ and r, $0 < r < 2^m - 1$, is relatively prime to $2^m - 1$. The, the linear span L of $\{s_i\}$ is given by

$$L = m(n/m)^{w(r)}, \tag{4.16}$$

where $w(r)$ is the number of ones in the base-2 representation of r.

***Proof*:** Key [53] has derived the upper bound on linear span of nonlinear sequences by counting the number of nonzero coefficients in the expansion of the sequence in terms of powers of primitive element, α of $GF\left(2^n\right)$. This same technique is applied to determine the linear span of GMW sequences.

Let $x = \alpha^i$ and expanding the outer trace function, we have

$$s_i = t(x)+t(x)^2+\cdots+t(x)^{2^{m-1}}, \quad t(x)=tr_m^n(x)^r$$

where $t(x)\neq t(x)^{2^i}\left(\mathrm{mod}\ \mathrm{x}^{2^n}-x\right)$. Thus, $t(x)$ is a power of a trace function. According to Theorem 4.2, the number of non-zero coefficients in $t(x)$ is given by $(n/m)^{w(r)}$; $w(t(x))=(n/m)^{w(r)}$. For any $0\leq j<m,\ w\left(t(x)^{2^j}\right)=(n/m)^{w(r)}$.

Thus we get $w(s_i)=m(n/m)^{w(r)}$ and thus the theorem follows.

c) Balance Property

Let $\boldsymbol{c}$ denote a k-tuple over GF(2), and let $N_{\boldsymbol{c}}$ denote the number of occurrences of $\boldsymbol{c}$ in one period (2^n-1 initial positions) of a sequence $\{s_i\}$, i.e., $N_{\boldsymbol{c}}$ is the number of values of j in the range $N_{\boldsymbol{c}}$, for which

$$\left(s_j, s_{j+1}, \ldots, s_{j+k-1}\right)=\boldsymbol{c} \tag{4.17}$$

Then $\{s_i\}$ is called *k-tuple balanced* if N_c is 2^{n-k} for all but one choice of ***c***.

A uniform distribution on k-tuple occurrences is achieved in GMW sequences for a restricted range of k, as stated in the following theorem.

Theorem **4.4** [8]: Let $\{s_i\}$ be the GMW sequence defined by (4.1). Then, the number N_c of positions within one period of $\{\boldsymbol{S_i}\}$ at which the k-tuple $\boldsymbol{c}$ occurs, is given by

$$N_c=\begin{cases} 2^{n-k}, & for\ c\neq 0,\ 1\leq k\leq \dfrac{n}{m} \\ 2^{n-k}-1, & for\ \ c\neq 0,\ 1\leq k\leq \dfrac{n}{m} \end{cases} \tag{4.18}$$

4.1.2 An Example [8]

A GMW sequence of period 63 is defined by

$$s_i = tr_1^3\left(\left[tr_3^6\left(\alpha^n\right)\right]^3\right) \tag{4.19}$$

where $z^6+z^5+z^2+z+1$ is the minimum polynomial of α over $GF(2)$. One simple plan for mechanizing a generator for $\{s_i\}$ is to construct a generator for the *m*-sequence $tr_3^6(\alpha^n)$ and use a ROM to complete the mapping to $GF(2)$. The elements of $GF(8)$ are 0 and α^{9i}, $i=0,1,\ldots,6$, and the minimum polynomial of α over $GF(8)$ is easily determined (see appendix) to be $z^2+\alpha^{54}z+\alpha^9$. A block diagram of the generator employing $GF(8)$ arithmetic is shown in Figure 4.1.

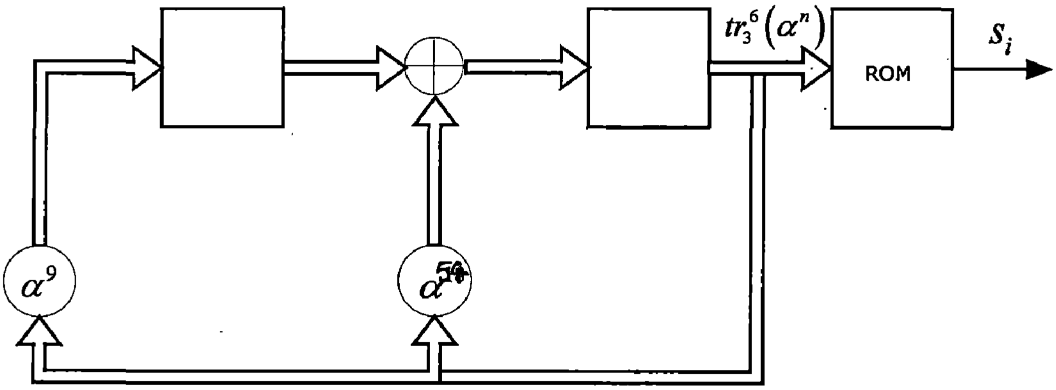


Figure 4.1 A GMW sequence generator in the Galois configuration with elements in GF(8).

The actual mechanization takes advantage of the fact that $GF(8)$ is a three-dimensional vector space over $GF(2)$ with basis $1,\alpha^9,\alpha^{18}$. That is, an element from $GF(8)$ can be written as

$$\gamma=\gamma_0\cdot 1+\gamma_1\alpha^9+\gamma_2\alpha^{18}, \tag{4.20}$$

with $\gamma_0,\gamma_1,\gamma_2$ in $GF(2)$. Table 4.1 lists this representation along with the ROM mapping, $tr_1^3(\gamma^3)$.

The multiplications required in the generator of Figure 4.1 are easily mechanized in this representation.

$$\begin{aligned}\alpha^{54}\gamma &= \alpha^{54}\gamma_0 + \gamma_1 + \alpha^9\gamma_2 \\ &= \left(\alpha^{18}+1\right) + \gamma_1 + \alpha^9\gamma_2 \\ &= \left(\gamma_0+\gamma_1\right)1 + \gamma_2\alpha^9 + \gamma_0\alpha^{18}\end{aligned} \qquad (4.21)$$

Similarly,

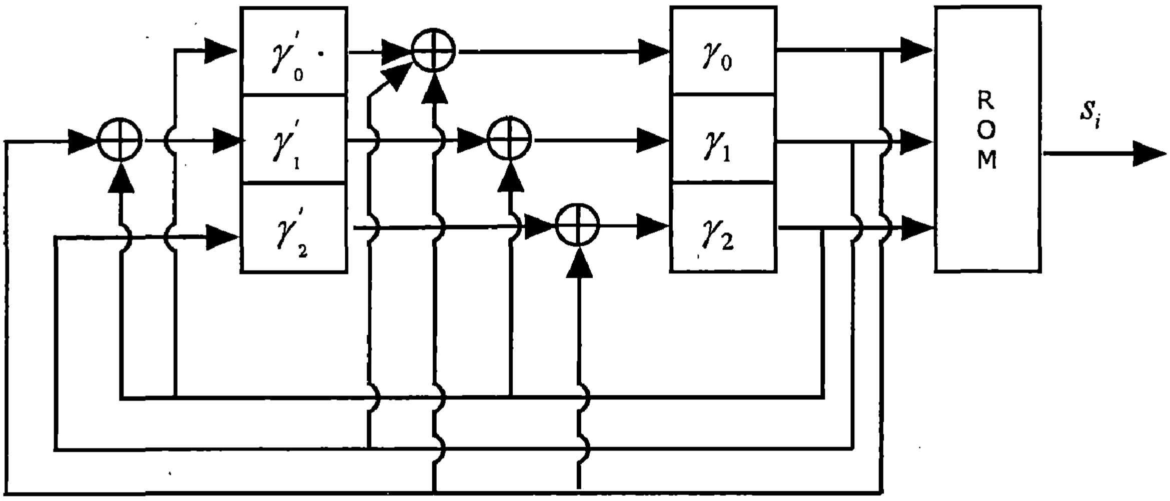
$$\alpha^9\gamma = \gamma_2\cdot 1 + \left(\gamma_0+\gamma_2\right)\alpha^9 + \gamma_1\alpha^{18} \qquad (4.22)$$

Table 4.1: Representation for GF(8) elements, and the ROM mapping for *r*=3

γ	γ_0	γ_1	γ_2	$tr_1^3(\gamma^3)$
0	0	0	0	0
1	1	0	0	1
α^9	0	1	0	1
α^{18}	0	0	1	1
α^{27}	1	1	0	0
α^{36}	0	1	1	1
α^{45}	1	1	1	0
α^{54}	1	0	1	0

This results in the mechanization of Figure 4.2(a). One period of each of the sequences produced in this generator is shown in Figure 4.2(b). Notice the periodically recurring zeros in the $GF(8)$ sequences (T is 9 in this example), an example of the structure exploited in the proof of Theorem 4.1.

Since r is 3, the base-2 expansion of r has weight 2, and Theorem 4.2 states that the linear span in this case is 12. When the final trace operation to $GF(2)$ is carried out, the remaining cyclic shifts of the binary coefficients listed in Table 4.1 are added to give twelve distinct coefficients in all.



(a)

γ_0: 011100011001110110000011110010010101001101000010001011011111101
γ_1: 000011110010010101001101000010001011011111101011100011001110110
γ_2: 001110110000011110010010101001101000010001011011111101011100011

γ'_0: 100111011000001111001001010100110100001000101101111110101110001
γ'_1: 001001010100110100001000101101111110101110001100111011000001111
γ'_2: 000001111001001010100110100001000101101111110101110001100111011

s_i: 010011101011101001011100011001111110010010111001110100000001010

(b)

Figure 4.2 (a) A GF(2) mechanization of the GMW sequence generator in Example. (b) Sequences produced in this generator.

The k-tuple statistics of the output sequence in this sequence are shown in Table 4.2. As indicated by this data, the k-tuple statistics of a GMW sequence are not uniformly distributed for all k less than the number of memory elements used.

Table 4.2 *K*- tuple statistics for the GMW sequence of length 63

k	(k-tuple: Occurrences per period)
1	$(0:31), (1:32)$
2	$(00:15), (01:16), (10:16), (11:16)$
3	$(000:6), (100:9), (010:9), (001:9)$
	$(110:7), (101:7), (011:7), (111:9)$
4	$(0000:4), (1000:2), (0100:5), (0010:5)$
	$(0001:2), (1100:4), (0110:1), (0011:4)$
	$(1001:7), (1010:4), (0101:4), (1110:6)$
	$(0111:6), (1011:3), (1101:3), (1111:3)$

4.1.3 Partial Autocorrelation of GMW sequences

***Theorem* 4.5** [41]: Let $\underline{s} = \{s_i\}$ be a GMW sequence whose elements are given by

$$\{s_i\} = tr_1^m\left\{\left[tr_m^n(\alpha^i)\right]^r\right\},$$

where α is a primitive element of $GF(2^n)$ and r, $0 < r < 2^m - 1$, is relatively prime to $2^m - 1$. Suppose

$$\frac{1}{l} PEAC_{\max}(\underline{t})(l) \le C$$

where $\underline{t}$ is an m-sequence of period $2^m - 1$. Then,

$$\frac{1}{lT}\left|PEAC_{\max}(\underline{s})(lT)\right| \le C + \frac{2^{n-m} - 1}{2^n - 1}(1 - C) \tag{4.23}$$

***Proof*:** From previous discussion, a GMW sequence $\underline{s}$ of period $2^n - 1$ has interleaving function f with

$$f(i) = \left[tr_m^n(\alpha^i)\right]^r$$

where $gcd\left(r,2^{m'}-1\right)=1$. Following in the lines of Theorem 3.5, consider the sequence $\underline{s}'$ with

$$s_i' = tr_1^m\left(g(i)\right) \tag{4.24}$$

where $g(j)=f(j)+f(j+k)$ for $1 \le k < 2^n-1$. Now $g(j)=0$ if and only if

$$\left[tr_m^n\left(\alpha^j\right)\right]^r = \left[tr_m^n\left(\alpha^{j+k}\right)\right]^r$$

Since $gcd\left(r,2^m-1\right)=1$, the above equation is equivalent to writing

$$tr_m^n\left(\alpha^j\right)=tr_m^n\left(\alpha^{j+k}\right)$$

i.e., $$tr_m^n\left[\alpha^j\left(1+\alpha^k\right)\right]=0$$

Since $tr_m^n\left[\alpha^j\left(1+\alpha^k\right)\right]$ is an m-sequence over $GF\left(2^m\right)$, from Lemma 4.1 the number of zeros j of this last function with $0 \le j < T$ is $\dfrac{2^{n-m}-1}{2^m-1}$. Thus, $Z_A(f)$ as defined in (3.30) satisfies

$$Z_A(f)=\frac{2^{n-m}-1}{2^m-1} \tag{4.25}$$

Let the m-sequence $\underline{t}$ with $t_i = tr_1^m\left(\alpha^{rTi}\right)$ satisfies

$$\frac{1}{l}PEAC_{\max}\left(\underline{t}\right)(l) \le C$$

Then, applying the autocorrelation version of Theorem 3.5, we deduce that the GMW sequence s satisfies

$$\begin{aligned}\frac{1}{lT}\left|PEAC_{\max}\left(\underline{s}\right)(lT)\right| &\le C+\frac{Z_A(f)}{T}(1-C)\\ &\le C+\frac{2^{n-m}-1}{2^n-1}(1-C)\end{aligned}$$

Since $n \ge 2m$, the factor $\dfrac{2^{n-m}-1}{2^n-1}$ is approximately equal to 2^{-m}. So the peak partial autocorrelation of the GMW sequence is atmost roughly ClT for window length lT.

Taking $r=1$, we obtain the same bound on the peak partial autocorrelation for m-sequences of period 2^n-1.

4.2 Cascaded GMW sequences

Cascaded GMW sequences [9] share many of the most desirable properties of both the geometric sequences and the GMW sequences. They have the same periodic autocorrelation properties and balanced property as m-sequences of the same period, but in many cases have greater linear complexity than GMW sequences.

Let $n_1,n_2,\ldots,n_m$ and $r_1,r_2,\ldots,r_{m-1}$ be positive integers satisfying $n_i \mid n_{i+1}$, $r_i<2^{n_i}$ and $gcd\left(r_i,2^{n_i}-1\right)=1$ for $i=1,2,\ldots m-1$. Let α be a primitive element of $GF\left(2^{n_m}\right)$. Then, the sequence $s=\{s_i\}$ of the form

$$\{s_i\}=tr_1^{n_1}\left(tr_{n_1}^{n_2}\left(\cdots tr_{n_{m-1}}^{n_m}\left(\alpha^i\right)^{r_{m-1}}\cdots\right)^{r_1}\right) \tag{4.26}$$

is called a cascaded GMW sequence from $GF\left(2^{n_m}\right)$ to $GF(2)$.

Let $T=\dfrac{2^{n_m}-1}{2^{n_1}-1}$

Consider,

$$f(i)=tr_{n_1}^{n_2}\left(\cdots tr_{n_{m-1}}^{n_m}\left(\alpha^i\right)^{r_{m-1}}\cdots\right)^{r_1} \qquad i\geq 0 \tag{4.27}$$

then,

$$f(i)=tr_{n_1}^{n_2}\left(\cdots tr_{n_{m-1}}^{n_m}\left(\alpha^{i_1T+i_2}\right)^{r_{m-1}}\cdots\right)^{r_1} \quad \text{for} \quad i=i_1T+i_2$$

which implies

$$f(i)=\alpha^{rTi_1}f(i_2) \text{ where } r=r_1\cdot r_2\cdot\ldots\cdot r_{m-1}.$$

So, the sequence $s_i=tr_1^{n_1}\left[f(i)\right]$, has interleaved form as described in section 3.3.1 with interleaving function $f(i)$ as defined in (4.27).

4.2.1 Statistical Properties of Cascaded GMW sequences

a) Autocorrelation

***Theorem* 4.6** [8]: Let $\{a_i\}$ be a cascaded GMW sequence whose elements are given by

$$\{a_i\} = (-1)^{tr_1^{n_1}\left(tr_{n_1}^{n_2}\left(\cdots tr_{n_{m-1}}^{n_m}\left(\alpha^i\right)^{r_{m-1}}\cdots\right)^{r_1}\right)},$$

where α is a primitive element of $GF(2^{n_m})$, and $r_1, r_2, \ldots, r_{m-1}$, $r_i < 2^{n_i}$ with $gcd\left(r_i, 2^{n_i}-1\right) = 1$. Then the periodic autocorrelation function $R_{\underline{\mathbf{aa}}}(\tau)$ of $\{a_i\}$ is given by

$$\begin{aligned} R_{\underline{\mathbf{aa}}}(\tau) &\triangleq \sum_{i=0}^{2^{n_m}-2} a_{i+\tau}a_i \\ &= \begin{cases} 2^{n_m}-1, & \tau = 0 \bmod 2^{n_m}-1 \\ -1, & \tau = 0 \bmod 2^{n_m}-1 \end{cases} \end{aligned} \tag{4.28}$$

b) Linear span

***Theorem* 4.7** [51, 52]: Let $\{s_i\}$ be a cascaded GMW sequence whose elements are given by

$$\{s_i\} = tr_1^{n_1}\left(tr_{n_1}^{n_2}\left(\cdots tr_{n_{m-1}}^{n_m}\left(\alpha^i\right)^{r_{m-1}}\cdots\right)^{r_1}\right),$$

Where α is a primitive element of $GF(2^{n_m})$ and and $r_1, r_2, \ldots, r_{m-1}$, $r_i < 2^{n_i}$ with $gcd\left(r_i, 2^{n_i}-1\right) = 1$. Then, the linear span L of $\{s_i\}$ is given by

$$L = n_1\left(n_2/n_1\right)^{w(r_1)}\left(n_3/n_2\right)^{w(r_2)}\cdots\left(n_m/n_{m-1}\right)^{w(r_{m-1})}, \tag{4.29}$$

where $w(r_i)$ is the number of ones in the base-2 representation of r_i, $i = 1, 2, \ldots m-1$.

Proof : This result can be established by repeatedly applying Theorem 4.2 to $g_i\left(tr_{n_i}^{n_{i+1}}(x)\right)$ where $g_i(x)$ is a cascaded GMW sequence from $GF\left(2^{n_i}\right)$ to $GF(2)$.

4.2.2 Partial Autocorrelation of Cascaded GMW sequences

***Theorem* 4.8**: Let $\{s_i\}$ be a cascaded GMW sequence whose elements are given by

$$\{s_i\} = tr_1^{n_1}\left(tr_{n_1}^{n_2}\left(\cdots tr_{n_{m-1}}^{n_m}\left(\alpha^i\right)^{r_{m-1}}\cdots\right)^{r_1}\right),$$

Where α is a primitive element of $GF(2^{n_m})$ and $r_1, r_2, \ldots, r_{m-1}$, $r_i < 2^{n_i}$ with $gcd\left(r_i, 2^{n_i}-1\right) = 1$. Suppose

$$\frac{1}{l}PEAC_{\max}\left(\underline{t}\right)(l) \leq C$$

where $\underline{t}$ is an m-sequence of period $2^{n_1}-1$. Then,

$$\frac{1}{lT}\left|PEAC_{\max}\left(\underline{s}\right)(lT)\right| \leq C + \frac{2^{n_m-n_1}-1}{2^{n_m}-1}(1-C) \tag{4.30}$$

Proof: From previous discussion, a cascaded GMW sequence $\underline{s}$ of period $2^{n_m}-1$ has interleaving function *f* with

$$f(i) = tr_{n_1}^{n_2}\left(\cdots tr_{n_{m-1}}^{n_m}\left(\alpha^i\right)^{r_{m-1}}\cdots\right)^{r_1}$$

Consider the sequence $\underline{s}'$ with

$$s_i' = tr_1^{n_1}\left(g(i)\right) \tag{4.31}$$

where $g(j) = f(j) + f(j+k)$ for $1 \leq k < 2^{n_m}-1$.

The sequence $\underline{s}'$ also has interleaved form with interleaving function *g*. So $\underline{s}'$ is formed by interleaving sequences of period $2^{n_1}-1$ which are either shifts of an m-sequence or the zero sequence.

From out-of-phase auto-correlation property of cascaded GMW sequences,

$$\sum_{i=0}^{2^{n_m}-2}(-1)^{s_i'} = -1 \;\Rightarrow\; w\left(s_i'\right) = 2^{n_m-1}$$

Since, all the ones correspond to m-sequences, there are $2^{n_m-n_1}$ m-sequences and thus $2^{n_m-n_1}\left(2^{n_m-1}-1\right)$ zeros in s_i' correspond to m-sequences. From the discussion of section 3.3.1, it is evident that all the remaining zeros occur when $g(j)=0$. Since, $g(j)$ is periodic with period $2^{n_1}-1$, the number of zeros j of this last function with $0\leq j<T$ is $\frac{2^{n_m-n_1}-1}{2^{n_1}-1}$ zeros.

Thus, $Z_A(f)$ as defined in (3.30) satisfies

$$Z_A(f)=\frac{2^{n_m-n_1}-1}{2^{n_1}-1} \tag{4.32}$$

Let the m-sequence $\underline{t}$ with $t_i=tr_1^{n_1}\left(\alpha^{rTi}\right)$ where $r=r_1\cdot r_2\cdot\ldots\cdot r_{m-1}$ satisfies

$$\frac{1}{l}PEAC_{\max}(\underline{t})(l)\leq C$$

Then, applying the autocorrelation version of Theorem 3.5, we deduce that the cascaded GMW sequence s satisfies

$$\begin{aligned}\frac{1}{lT}\left|PEAC_{\max}(\underline{s})(lT)\right| &\leq C+\frac{Z_A(f)}{T}(1-C)\\ &\leq C+\frac{2^{n_m-n_1}-1}{2^{n_m}-1}(1-C)\end{aligned}$$

Since $n_m\geq 2n_1$, the factor $\frac{2^{n_m-n_1}-1}{2^{n_m}-1}$ is approximately equal to 2^{-n_1}. So the peak partial autocorrelation of the GMW sequence is at most roughly ClT for window length lT. Our bound also applies to peak partial autocorrelation of m-sequences of period 2^{n_m-1}. Thus, our bound is independent of the values of $r_i<2^{n_i}$, $i=1,2,\ldots m-1$.

Chapter 5

BENT AND SEMIBENT SEQUENCES

CDMA communication systems require binary sequence sets with large size and with low correlation values to employ more users with minimum level of interference. In this chapter, we introduce constructions for Bent and Semi-bent signal sets. First, we review bent and modified bent functions, statistical properties of bent function sequence set and mechanization of sequence. Next, we describe the problem of determining when a linear combination of the Gold functions is semi-bent. This leads to several characterizations of semi-bent functions. We finally conclude this chapter by providing statistical properties of semi-bent sequences and an improved upper bound over fading channels for semi-bent sequence set.

5.1 Bent Function Sequences

5.1.1 Bent Function

Definition [54]: A boolean function *F(X)* mapping V_n into V_1 is bent if its Fourier transform coefficients $\tilde{F}(\wedge)$ are all +1 or -1 where

$$\tilde{F}(\wedge) \triangleq 2^{-n/2} \sum_{X \in V_n} (-1)^{F(X)} (-1)^{X^T \wedge} \quad \text{for all } \wedge \in V_n \tag{5.1}$$

Where $F(X) + X^T \wedge$ is called linear translate of $F(X)$.

a) Properties

1) Let F be a bent function and G, defined by $(-1)^{G(X)} = \tilde{F}(\wedge)$ is also a bent function. Then, G is bent and hence F and G are duals.
2) If $F(x)$ is a bent function on V_n, then n is even, n=2k; the degree of $F(x)$ is almost k, except for the case k=1.
3) Let f be a function in $\mathcal{F}_n$. Then f is bent if and only if $d(f, A_n) = N_{\max}$ where $N_{\max} = 2^{n-1} - 2^{\frac{n}{2}-1}$ is the largest value of non-linearity.

b) Construction of Bent Functions

Theorem 5.1 (Rothaus class I) [54, 10]: Let $X, Y \in V_k$, let $C \in V_{2k}$ and let $G(X)$ be an arbitrary function mapping V_k to V_1. Then $F(Z)$ defined by,

$$F(Z) = X^T Y + G(X) + C^T Z, \qquad Z \triangleq \begin{bmatrix} X \\ Y \end{bmatrix} \tag{5.2}$$

is a bent function on V_{2k}.

***Theorem* 5.2** (Rothaus Class II). [54] : Let $A(X), B(X), C(X)$ be bent functions on V_{2k} such that $A(X)+B(X)+C(X)$ is also bent. Let $y, z \in V_1$. Then the function

$$\begin{aligned} Q(x,\ y,\ z) \ = \ A(x)B(x) \ + \ B(x)C(x) \ + \ C(x)A(x) + [A(x) \ + \ B(x)]y \ + \\ [A(x) \ + \ C(x)]z \ + yz \end{aligned} \tag{5.3}$$

is a bent function on V_{2k+2}.

***Theorem* 5.3** (Maiorana McFarland Class) [55] : Let k be an arbitrary positive integer and $n = 2k$. Then the function f mapping V_n to V_1 given by

$$f(x) = x_2.\pi(x_1) + g(x_1) \tag{5.4}$$

where $x_1, x_2 \in V_k$ are defined by $x = [x_1,\ x_2]$; π is an arbitrary permutation of V_k and g is an arbitrary function mapping V_k to V_1, is bent.

5.1.2 Modified Bent functions

Modified Bent functions [55] are defined on the Galois field $GF(2^n)$, and their transform properties are relative to trace transform (refer to Appendix B for trace transform and its properties). But, the above class bent functions are defined on the space of k-tuples V_k and their transform properties are relative to Fourier transform. The second difference is easily resolved, as $GF(2^n)$ is a linear vector space of dimension n. By selecting a trace-orthogonal of self-complementary basis $\{\beta_1, \beta_2, \ldots, \beta_n\}$, the trace inner product

$$tr(\lambda x) = \sum_{i,j} \lambda_i X_j tr(\beta_i \beta_j)$$

becomes $\sum_i \lambda_i X_i$ and the trace transform on $GF(2^n)$ can be identified with the Fourier transform on V_n.

The extension of bent functions to $GF(2^n)$ is accomplished by introducing a linear mapping L from $GF\left(2^n\right)$ *onto* V_k and, for a function F on V_k, defining a function f on $GF(2^n)$ by $f(x) = F(L(x))$.

***Theorem* 5.4** [16]: Let L be an onto linear mapping from $GF(2^n)$ to V_k and let F be a real valued function on V_k. Define f on $GF(2^n)$ by $f(x) = F(L(x))$. Then

$$\hat{f}(\lambda) = \begin{cases} 0 & \text{for } \lambda \notin \text{range}(L^*) \\ 2^{(n-k)/2}.\tilde{F}(Z) & \text{for } \lambda \in \text{range}(L^*), L^* = \lambda \end{cases} \tag{5.5}$$

Where L^* is the adjoint of L is, $\hat{f}$ is the trace transform and $\tilde{F}$ is the Fourier transform

Proof: The adjoint is defined as follows: for every linear function, $l(x)$ mapping $GF(2^n)$ into $GF(2)$, there is a unique element λ of $GF(2^n)$ such that $l(x) \equiv tr(x\lambda)$. For every Z in V_k, $L(x)^T Z$ defines a unique linear function of $GF(2^n)$. Thus for every Z in V_k there is a unique λ in $GF(2^n)$ such that $tr(x\lambda) \equiv L(x)^T Z$. The correspondence $Z \rightarrow \lambda$ defines the mapping L^*. Since L is onto, $Z \neq Y \Rightarrow L^*(Z) \neq L^*(Y)$.

Now,

$$\begin{aligned} \hat{f}(\lambda) &= 2^{-n/2} \sum_{x \in GF(2^n)} f(x)(-1)^{tr(\lambda x)} \\ &= 2^{-n/2} \sum_{x \in GF(2^n)} F(L(x))(-1)^{tr(\lambda x)} \end{aligned}$$

$$\begin{aligned} \hat{f}(\lambda) &= 2^{-n/2} \sum_{x \in GF(2^n)} 2^{-k/2} \sum_{Z \in V_k} \tilde{F}(Z)(-1)^{L(x)^T Z} (-1)^{tr(\lambda x)} \\ &= 2^{-(n+k)/2} \sum_{Z \in V_k} \tilde{F}(Z) \sum_{x \in GF(2^n)} (-1)^{tr(x(\lambda + L^*(Z))} \end{aligned}$$

The innermost sum is zero from trace property (d) unless $\lambda = L^*(Z)$. Thus the entire sum is zero unless λ is in the range space of L^*. When $\lambda = L^*(Z)$ the inner sum is 2^n and hence,

$$\hat{f}(\lambda) = 2^{-(n+k)/2}.2^n.\tilde{F}(Z) \quad \text{when } \lambda = L^*(Z) \tag{5.6}$$

Olsen, Scholtz and Welch (OSW) [10] defined a collection of sequences $\mathbf{S} = \{\underline{\mathbf{s}}_Z : Z \in V_k\}$ by

$$s_i^Z = (-1)^{F(L(\alpha^i)) + L(\alpha^i)^T Z + tr(\sigma\alpha^i)} \tag{5.7}$$

where $F(Z)$ be a bent function on V_k; L be a *onto* linear mapping from $GF(2^n)$ to V_k such that $\text{range}(L^*) = \{\delta x_o : \delta \in GF(2^{n/2})\}$; $n = 0 \bmod 4$, $k = n/2$; α be a primitive element on $GF(2^n)$; σ be a nonzero element in $GF(2^{n/2})$ and x_0 is a root of the equation $z^2 + z + w = 0$ that generates $GF(2^n)$ on $GF(2^{n/2})$

where $\sum_{j=0}^{n/2-1} w^{2^j} = 1 \quad w \in GF(2^{n/2})$

$$GF(2^n) = \{\delta x_0 + \gamma : \delta, \gamma \in GF(2^{n/2})\} \tag{5.8}$$

5.1.3 Statistical properties of Bent function sequences

a) Correlation Properties

***Theorem* 5.5 [10]**: The magnitude of cross correlation values and out-of-phase autocorrelation values of members of $\mathbf{S}$ are bounded by $2^{n/2} + 1$.

Proof: The cross correlation between $\underline{\mathbf{a}} = \{s_i^Z\}$ and $\underline{\mathbf{b}} = \{s_i^Y\}$ is given by

$$R_{\underline{\mathbf{ab}}}(\tau) = \sum_{i=0}^{2^n-2} s_i^Z s_{i+\tau}^Y \tag{5.9}$$

Consider functions on $GF(2^n)$

$$r_Z(x) = (-1)^{F(L(x)) + L(x)^T Z + tr(\sigma x)} \quad \text{and} \quad r_Y(x) = (-1)^{F(L(x)) + L(x)^T Y + tr(\sigma x)}$$

Then, from trace transform property (c)

$$\begin{aligned} R_{\underline{\mathbf{ab}}}(\tau) &= -r_Z(0)r_Y(0) + \sum_{x\in GF(2^n)} r_Z(\alpha^\tau x)r_Y(x) \\ &= -r_Z(0)r_Y(0) + \sum_{\lambda\in GF(2^n)} \hat{r}_Z(\alpha^{-\tau}\lambda)\hat{r}_Y(\lambda) \ . \end{aligned}$$

whence,

$$\left|R_{\underline{\mathbf{ab}}}(\tau)\right| \le 1 + \sum_{\lambda\in GF(2^n)} \left|\hat{r}_Z(\alpha^{-\tau}\lambda)\right|\left|\hat{r}_Y(\lambda)\right| \tag{5.10}$$

Define

$$\mathbb{S} = \left\{\delta x_0 + \sigma : \delta \in GF(2^{n/2})\right\} \tag{5.11}$$

and define multiplicative shifts of $\mathbb{S}$ as

$$y\mathbb{S} = \left\{\lambda y : \lambda \in \mathbb{S}\right\} \Rightarrow \left\{\lambda : \hat{r}_Z(y^{-1}\lambda) \ne 0\right\} \tag{5.12}$$

then

(i) from theorem 5.4 $\quad \left|\hat{r}_Z(\lambda)\right| = \begin{cases} 2^{(n-k)/2} & \text{for } \lambda \in \mathbb{S}, \\ 0 & \text{for } \lambda \notin \mathbb{S} \end{cases}$ (5.13)

(ii) from theorem 4 in [~~7~~ 10] $\quad \max\limits_{0<\tau<2^n-1} \left|\mathbb{S} \cap \alpha^\tau \mathbb{S}\right| = 1$ (5.14)

By Parsvel's Theroem, $2^n = \sum\limits_{x\in GF(2^n)} \left|r_Z(x)\right|^2 = \sum\limits_{\lambda\in\mathbb{S}} \left|\hat{r}_Z(\lambda)\right|^2$

Hence, we can bound the trace transform as

$$B_{r_Z} \triangleq \max_{\lambda} \left|\hat{r}_Z(\lambda)\right|^2 \ge \frac{2^n}{\left|\mathbb{S}\right|}$$

since, $\left|\mathbb{S}\right| = 2^{n/2}$,

$$B_{r_Z} \ge 2^{n/2} \tag{5.15}$$

Using (5.11) and (5.12), the cross-correlation bound (5.10) can be simplified to

$$\left|R_{\underline{\mathbf{ab}}}(\tau)\right| \le 1 + \sqrt{B_{r_Z} B_{r_Y}} \left|\mathbb{S} \cap \alpha^\tau \mathbb{S}\right| \tag{5.16}$$

From (5.14) and (5.15), (5.16) becomes

$$\left|R_{\underline{\mathbf{ab}}}(\tau)\right| \le 1 + 2^{n/2} \tag{5.17}$$

and hence the theorem.

For $\tau = 0$, the cross correlation is

$$R_{\underline{ab}}(0) = \sum_{i=0}^{2^n-2} s_i^Z s_i^Y$$

$$= \sum_{i=0}^{2^n-2} (-1)^{L(\alpha^i)^T.(Z+Y)}$$

Using adjoint of L this can be written as

$$R_{\underline{ab}}(0) = \sum_{i=0}^{2^n-2} (-1)^{tr(\alpha^i(L^*(Z+Y)))}$$

$$= -1 + \sum_{x \in GF(2^n)} (-1)^{tr(x(L^*(Z+Y)))}$$

For $Z \neq Y,\ \ L^*(Z+Y) \neq 0$. Therefore, from trace property (d)

$$\sum_{x \in GF(2^n)} (-1)^{tr(x(L^*(Z+Y)))} = 0$$

Hence,

$$R_{\underline{ab}}(0) = -1 \tag{5.18}$$

Equations (5.17) and (5.18) indicate that the sequence set **S** correspond to a set of ±1 sequences for which all non-trivial normalized correlations are bounded in magnitude by $\left(2^{n/2}+1\right)/\left(2^n-1\right)$. This bound rapidly approaches $2^{-n/2}$ as n increases and hence the set of sequences designed has nearly optimal correlation properties and asymptotically achieves the Welch bound.

b) Linear span

***Theorem* 13 [11]**: The ELS l of every family of bent-function sequences of length 2^n-1 obtained from the set of all linear translates of a bent function over V_k of degree d satisfies the upper bound

$$l \leq \sum_{i=1}^{d-1}\binom{n}{i} + \binom{k}{d}2^d - \sum_{i=1}^{\lceil (d-1)/2 \rceil}\binom{k}{i} \tag{5.19}$$

Setting d=k if n>4 and d=2 if n=4 in (5.19) results in an upper bound to the maximum achievable ELS of a family of bent-function sequences of length $2^n - 1$.

***Theorem* 14** [11]: The minimum achievable ELS l of every family of bent-function sequences of length $2^n - 1$ obtained from the set of all linear translates of a bent function V_k of degree d satisfies the lower bound

$$l \geq \binom{k}{d}.2^d + \frac{1}{2}\sum_{i=2}^{d-1}\binom{k}{i}2^i + n, \qquad n > 8,\ 2 < d \leq \frac{k}{2} \tag{5.20}$$

$$\begin{aligned} l &\geq \frac{1}{2}\binom{k}{d}.2^d + n, \\ &= 2\binom{k}{2} + n, \qquad n \geq 8, d = 2 \end{aligned} \tag{5.21}$$

$$\begin{aligned} l &\geq \binom{k}{d}.2^d + n, \\ &= 8, \qquad n = 4, d = 2 \end{aligned} \tag{5.22}$$

5.1.4 Mechanization of Bent Sequences

To read out the function $r_Z(x)$, $x \in GF(2^n)$, in the order specified by α^t, $t = 0,1,2,..$, α^t must be represented in terms of the trace-orthogonal basis β. If the minimum polynomial of the primitive element α of $GF(2^n)$ is $z^n + \sum_{i=1}^{n-1} a_i z^i + 1$, over $GF(2)$, then the coefficients $A(t)$ of α^t with respect to the basis $\alpha^T = (1, \alpha, \alpha^2, ...\alpha^{n-1})$ can be generated by a feedback shift register as shown in fig(5).

Hence,

$$\alpha^t = A^T(t)\alpha \tag{5.23}$$

Let the matrix Q over $GF(2)$ denote the transformation of the basis β into basis α, i.e.,

$$\alpha = Q\beta \tag{5.24}$$

Then $\alpha^t = A^T(t)Q\beta = X^T A(t)$ (5.25)

where

$$X(t) = Q^T A(t) \tag{5.26}$$

is the transformation which expresses α^t in the β basis. The remaining processing required to generate $r_Z(\alpha^t)$ is also shown in Fig. 5.1. The advantage of bent sequences is that they can be readily initialized into any assigned code sequence and can be rapidly hopped from code sequence to code sequence. From observation of Fig. 5.1, the code sequence selection is simply made by specifying Z

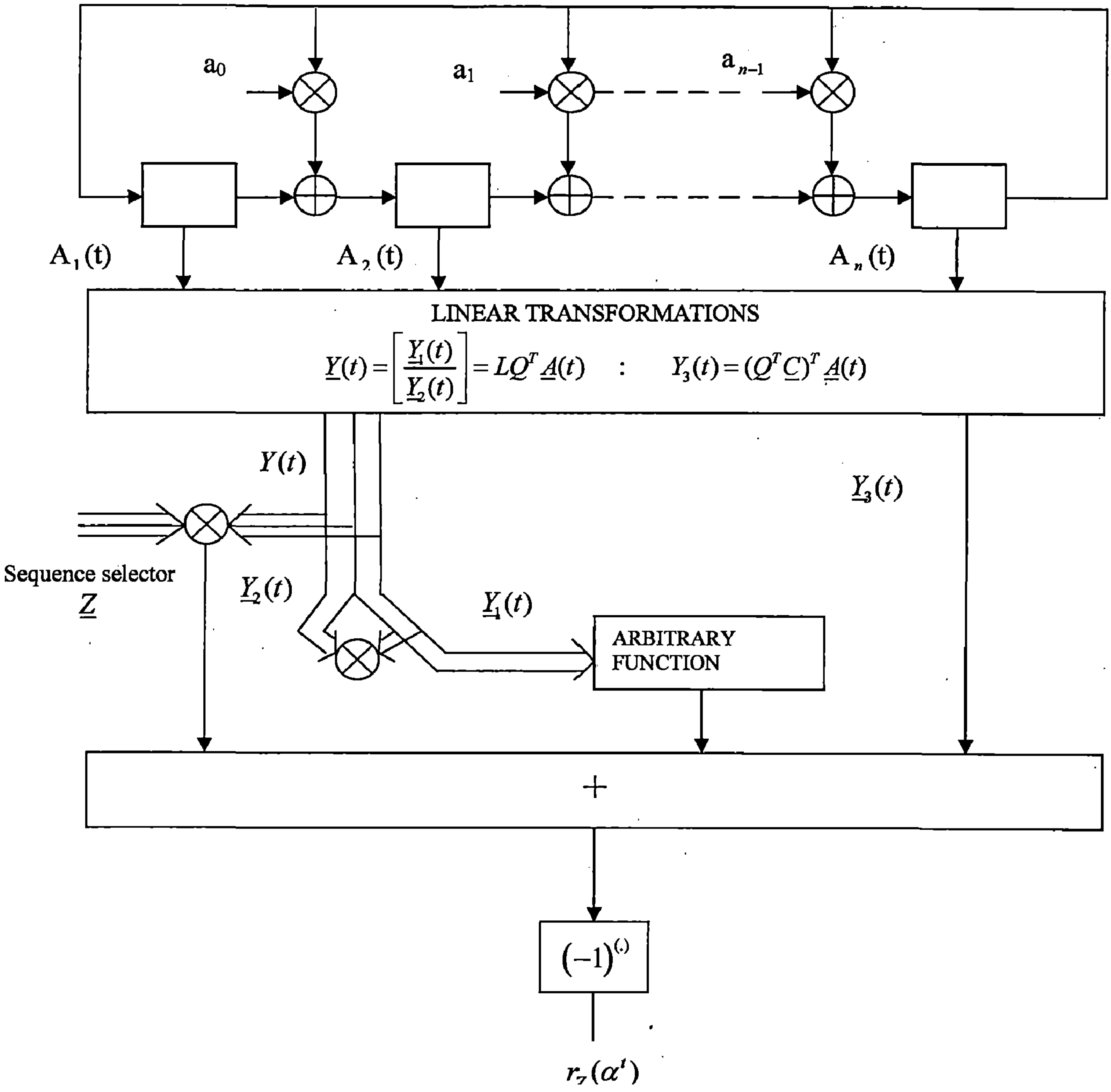


Fig.5.1. Generation of a bent sequence [55]

5.2 Semi-bent Sequences

Definition **5.2** [12]: Let n be odd. The function $f : GF\left(2^n\right) \to GF(2)$ is semi-bent if Hadamard transform $\left|\hat{f}(\lambda)\right| \in \left\{0, 2^{(n+1)/2}\right\}$ for all $\lambda \in GF\left(2^n\right)$.

The semi-bent functions are widely studied in cryptography and have been investigated under various names, including 3-valued almost optimal Boolean functions, plateaued functions and preferred functions.

5.2.1 Linear Combination of Gold Functions

Assume that n is odd. Consider linear combination of the Gold functions of the form

$$f(x) = \sum_{i=1}^{(n-1)/2} c_i tr_1^n\left(x^{2^i+1}\right) \tag{5.27}$$

where $c_i \in \{0,1\}$ for $1 \le i \le (n-1)/2$, is semi-bent. Let $Q_2(n)$ denote the set of all functions described by (5.27). This section shows how to determine whether the function $f(x) \in Q_2(n)$ is semi-bent using elementary algebraic techniques.

Lemma **5.1** [12, 56]: Let n be odd and let $c_i \in \{0,1\}$ for $1 \le i \le (n-1)/2$. Suppose the function f is defined as

$$f(x) = \sum_{i=1}^{(n-1)/2} c_i tr_1^n\left(x^{2^i+1}\right)$$

for all $x \in GF\left(2^n\right)$. Then f is semi-bent if and only if the cyclic matrix

$$L = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & c_2 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & c_1 & \cdots & c_{n-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & c_4 & \cdots & c_0 \end{pmatrix} \tag{5.28}$$

has rank n -1 over $GF(2)$, where we define $c_0 = 0$ and $c_{n-i} = c_i$ for $i = 1,2,\ldots,(n-1)/2$.

Proof**:** Using the Welch squaring method:

$$\begin{aligned}\hat{f}(\lambda)^2 &= \sum_{x,y}(-1)^{tr(\lambda x)+f(x)}(-1)^{tr(\lambda y)+f(y)} \\ &= \sum_{x,w}(-1)^{tr(\lambda x)+f(x)tr(\lambda(x+w))+f(x+w)} \qquad (\text{where } y=x+w) \\ &= \sum_{w}(-1)^{tr(\lambda w)+f(w)}\sum_{x}(-1)^{\phi(x,w)} \quad .\end{aligned}$$

where $\phi(x,w)=f(w)+f(x)+f(x+w)$. We simplify ϕ as follows:

$$\begin{aligned}\phi(x,w) &= \sum_{i=1}^{(n-1)/2} c_i\left[tr\left(x^{2^i+1}\right)+tr\left(w^{2^i+1}\right)+tr\left((x+w)^{2^i+1}\right)\right] \\ &= \sum_{i=1}^{(n-1)/2} c_i tr\left(x^{2^i}w+w^{2^i}x\right)\end{aligned}$$

Since $tr\left(a^2\right)=tr(a)$, we get

$$\begin{aligned}\phi(x,w) &= \sum_{i=1}^{(n-1)/2} c_i tr\left(x\left(w^{2^{n-i}}+w^{2^i}\right)\right) \\ &= tr\left(xL(w)\right)\end{aligned}$$

where

$$L(w)=\sum_{i=1}^{(n-1)/2} c_i\left(w^{2^{n-i}}+w^{2^i}\right) \tag{5.29}$$

Here, L is a linear function, and under a normal basis $\left\{\alpha,\alpha^2,\alpha^4,\ldots,\alpha^{2^{n-1}}\right\}$ of $GF\left(2^n\right)$, the matrix representation of L is given by the matix (5.28).

Also, we have that

$$\sum_{x}(1)^{\phi(x,w)}=\sum_{x}(-1)^{tr(xL(w))}=\begin{cases}2^n & \text{if } L(w)=0 \\ 0 & \text{otherwise}\end{cases}$$

Therefore,

$$\hat{f}(\lambda)^2=2^n\sum_{w\in\ker(L)}(-1)^{tr(\lambda w)+f(w)}$$

Let dim(ker(L)) = k. Hence, $tr(\lambda w)+f(w)$ is a linear function on ker(L) from the definition of ϕ. Therefore,

$$\sum_{w\in\ker(L)} (-1)^{tr(\lambda w)+f(w)} \in \{2^k, 0\}$$

depending on whether the exponent is zero function or a non-zero linear function, respectively. Hence,

$$\hat{f}(\lambda)\in\{0, 2^{(n+k)/2}\}$$

for all λ if and only if dim(ker(L)) = k. In particular, f is semi-bent if and only if $\dim(\ker(L))=1$, i.e., when

$$\operatorname{rank}(L)=n-1. \tag{5.30}$$

***Theorem* 5.1** [12]: Let n be odd and let $c_i\in\{0,1\}$ for $1\le i\le(n-1)/2$. Suppose the function f is defined as

$$f(x)=\sum_{i=1}^{(n-1)/2} c_i tr_1^n\left(x^{2^i+1}\right)$$

for all $x\in GF(2^n)$. Then f is semi-bent if and only if $gcd\left(c(x), x^n+1\right)=x+1$, where

$$c(x)=\sum_{i=1}^{(n-1)/2} c_i\left(x^i+x^{n-i}\right) \tag{5.31}$$

***Proof*:** Note that the rows of matrix (5.28) span a cyclic code C generated by the vector $(c_0, c_1, \ldots, c_{n-1})$. The vectors of C can be represented by polynomials in the quotient ring $GF(2)[x]/(x^n+1)$, where

$$C=\operatorname{span}\{c(x), xc(x), \ldots, x^{n-1}c(x)\}$$

and

$$c(x)=\sum_{i=1}^{(n-1)/2} c_i\left(x^i+x^{n-i}\right)$$

Some of the well known useful facts about cyclic codes are [56]:

1. There exists a unique monic polynomial $g(x)$, called the *generator polynomial*, such that $g(x) \mid v(x)$ for all $v(x) \in C$.
2. $\operatorname{rank}(L) = \dim(C) = n - \deg(g(x))$.
3. $g(x) = gcd(c(x), x^n + 1)$.

From (5.30) and fact 2 above, it is evident that $\deg(g(x)) = 1$. Thus, to ensure that *f* is semi-bent, it is enough to show that $gcd(c(x), x^n + 1) = x + 1$.

***Lemma* 5.2** [12]: Let *n* be odd and let $g(x)$ be the generator polynomial of the cyclic code C generated by $c(x) = \sum_{i=1}^{(n-1)/2} c_i(x^i + x^{n-i})$, where $c_i \in \{0,1\}$ for $1 \le i \le (n-1)/2$. Then $g(x) = (x+1)h(x)$, where $\deg(h(x))$ is even.

5.2.2 Some characterizations of Semi-bent Quadratic Functions

5.2.2.1 Semi-bent Functions for All Choices of Coefficients

By analyzing the GCD condition in theorem 5.1, several nice characterizations of families of semi-bent quadratic functions on $GF(2^n)$ are obtained in [12]. In this section, the question of determining odd integers *n* for which all non-zero functions $f(x) \in \mathcal{Q}_2(n)$ are semi-bent is addressed.

***Lemma* 5.3** [12]: Let *n* be odd. If all non-zero functions $f(x) \in \mathcal{Q}_2(n)$ are semi-bent, then *n* is prime.

Henceforth, the function $f(x) \in \mathcal{Q}_2(n)$ where *n* is an odd prime are only considered.

***Lemma* 5.4** [12]: Let *p* be an odd prime. The factorization of $x^p + 1$ over $\mathbb{Z}_2[x]$ into irreducible factors is of the form

$$x^p + 1 = (x+1)h_1(x)h_2(x)\ldots h_t(x) \tag{5.32}$$

where each $h_i(x)$ is a polynomial of degree $\text{ord}_p(2)$ and $t=(p-1)/\text{ord}_p(2)$.

Suppose that p is an odd prime and $\text{ord}_p(2)=p-1$. Then x^p+1 has two irreducible factors by Lemma 5.4.

***Theorem* 5.2** [12]: Suppose p is an odd prime such that $\text{ord}_p(2)=p-1$. Then every non-zero functions in $Q_2(p)$ is semi-bent.

***Proof*:** By Lemma 5.4 and from Theorem 5.1, the theorem follows.

The first ten such primes are 3, 5, 11, 13, 19, 29, 37, 53, 59 and 61. A conjecture of Artin states that there exists an infinite number of such primes.

Consider the next case, when $p=2s+1$ is a prime, s is odd and $ord_p(2)=s$. In this situation, x^p+1 will have three irreducible factors of odd degree that is evident from Lemma 5.4.

***Theorem* 5.3** [12]: Suppose $p=2s+1$ is a prime such that s is odd and $ord_p(2)=s$. Then every non-zero functions in $Q_2(p)$ is semi-bent.

***Proof*:** By Lemma 5.4, Lemma 5.2 and from Theorem 5.1, the theorem follows.

The first ten such primes are as follows:

7, 23 ,47, 71, 79, 103, 167, 191, 199, 239.

In next corollary, Sophie Germain primes, which are the primes p of the form $p=2q+1$, where q is prime, are considered.

***Corollary* 5.1** [12]: Suppose that $p=2q+1$ where p and q prime, then every non-zero function in $Q_2(p)$ is semi-bent.

The first ten Sophie-Germain primes are as follows

5, 7, 11, 23, 47, 59, 83, 107, 167, 179.

The Sophie Germain primes are well studied in number theory and it is conjectured that there are infinite number of such primes.

Theorem 5.4 [12]: The only integers n such that all non-zero functions in $\mathcal{Q}_2(n)$ are semi-bent are the primes mentioned in Theorems 5.2 and 5.3.

5.2.2.2 Semi-bent Quadratic Functions from Arithmetic Progressions

In this, semi-bent functions formed by a sum of gold functions corresponding to an arithmetic progression are characterized. These contain semi-bent functions which are a sum of two Gold functions as a special case.

Theorem 5.5 [12]: Let n be odd. Consider the function $f(x) \in \mathcal{Q}_2(n)$ defined as

$$f(x) = tr_1^n\left(x^{2^a+1}\right) + tr_1^n\left(x^{2^{a+d}+1}\right) + \ldots + tr_1^n\left(x^{2^{a+(r-1)d}+1}\right) + tr_1^n\left(x^{2^{a+rd}+1}\right) \qquad (5.33)$$

Then f is semi-bent if $gcd(2a+rd,n)=1=gcd((r+1)d,n)$. Further, if $gcd(d,n)=1$, then $gcd(2a+rd,n)\neq 1$ or $gcd((r+1)d,n)\neq 1$ implies f is not semi-bent.

Proof: The polynomial $c(x)$ corresponding to $f(x)$ is

$$\begin{aligned} c(x) &= x^a + \cdots + x^{a+rd} + x^{n-a-rd} + \cdots + x^{n-a} \\ &= \left(1 + x^{n-(2a+rd)}\right)\left(x^a + \cdots + x^{a+rd}\right) \\ &= \left(1 + x^{n-(2a+rd)}\right)x^a\left(\frac{1+x^{(r+1)d}}{1+x^d}\right) \end{aligned}$$

The gcd of the numerator and x^n+1 is equal to $x+1$ if $gcd(2a+rd,n)=1=gcd((r+1)d,n)$. In this case, $f(x)$ is bent by Theorem 5.1. Now suppose that $gcd\left(1+x^d, x^n+1\right) = x+1$ (i.e., $gcd(d,n)=1$). Then,

$$gcd\left(c(x), x^n+1\right) = x+1$$

if and only if

$$gcd(2a+rd,n)=1=gcd((r+1)d,n).$$

***Corollary* 5.2** [12]: Let n be odd. Consider the function $f(x) \in Q_2(n)$ defined as $f(x) = tr_1^n\left(x^{2^i+1}\right) + tr_1^n\left(x^{2^j+1}\right)$. Then $f(x)$ is semi-bent if and only if $gcd(i+j,n) = 1 = gcd(i-j,n)$.

***Remark* 5.1:** when $n = p$ is prime in Theorem 5.5, all functions corresponding to arithmetic progressions are semi-bent.

***Lemma* 5.5** [56]: Let n be odd and $n = 2s+1$. Then, $2^n - 1$ and $2^i + 1$ are relatively prime for $1 \le i \le s$.

***Semi-bent Signal Set*:** Let n be odd prime as in theorems 5.2 and 5.3. For $0 \le j < 2^n - 1$, let $\underline{s}_j = \left\{s_i^{(j)}\right\}$ be a binary sequence whose elements are given by

$$s_i^{(j)} = tr_1^n\left(\alpha^{i+j}\right) + \sum_{k=1}^{(n-1)/2} c_k tr\left(\alpha^{d_k i}\right), \quad i = 0,1,\ldots,2^n - 2 \tag{5.34}$$

where $c_k \in \{0,1\}$ for $1 \le k \le (n-1)/2$, α is primitive element in $GF\left(2^n\right)$ and $d_k = 2^k + 1$. Then $\underline{s}_j$ is called a semi-bent sequence. Let $\underline{s}_{2^n-1} = \left\{tr\left(\alpha^i\right)\right\}$ and $\underline{s}_{2^n} = \sum_{k=1}^{(n-1)/2} c_k tr\left(\alpha^{d_k i}\right)$. The set given by

$$\mathrm{S} = \left\{\underline{s}_j \mid 0 \le j \le 2^n\right\} \tag{5.35}$$

is said to be semi-bent signal set.

Note that $\underline{s}_j$ is a sum of $\underline{s}_{2^n-1}$ at shift j and $\underline{s}_{2^n}$ for $0 \le j < 2^n - 1$. Thus S has $2^n + 1$ shift-distinct sequences.

5.2.3 Statistical Properties of Semi-bent sequences

In this section, we derive correlation and linear span properties of semi-bent sequences. Semi-bent sequences share same correlation properties as Gold sequences besides having large linear span than that of Gold sequences.

a) Cross-Correlation

***Theorem* 5.6:** Let n be odd prime as in theorem 5.2 or 5.3 and $d_k = 2^k + 1$ with $2^n - 1$ and $2^k + 1$ relatively prime. Then, the correlation of the semi-bent signal set (5.35) is given by

$$R_{\underline{\mathbf{ab}}}(\tau) = \begin{cases} 2^n - 1 & \tau = 0, \underline{\mathbf{a}} = \underline{\mathbf{b}} \\ \left\{-1, -1 \pm 2^{(n+1)/2}\right\} & \underline{\mathbf{a}} \neq \underline{\mathbf{b}} \;\; or \;\; \tau \neq 0, \underline{\mathbf{a}} = \underline{\mathbf{b}} \end{cases} \tag{5.36}$$

where $\underline{\mathbf{a}} = (-1)^{s_i^{(j)}}$ and $\underline{\mathbf{b}} = (-1)^{s_i^{(l)}}$

***Proof*:**

Case 1: When $\tau = 0,$ *and* $\underline{\mathbf{a}} = \underline{\mathbf{b}}$, it is evident that

$$R_{\underline{\mathbf{ab}}}(\tau) = 2^n - 1$$

Case2: When $\underline{\mathbf{a}} \neq \underline{\mathbf{b}}$ *or* $\tau \neq 0, \underline{\mathbf{a}} = \underline{\mathbf{b}}$, then

$$\begin{aligned} R_{\underline{\mathbf{ab}}}(\tau) &= \sum_{i=0}^{2^n-2} (-1)^{s_{i+\tau}^{(j)} + s_i^{(l)}} \\ &= \sum_{i=0}^{2^n-2} (-1)^{tr\left(\alpha^{i+j+\tau}\right) + \sum\limits_{k=1}^{(n-1)/2} c_k tr\left(\left(\alpha^{i+\tau}\right)^{d_k}\right) + tr\left(\alpha^{i+l}\right) + \sum\limits_{k=1}^{(n-1)/2} c_k tr\left(\left(\alpha^{i}\right)^{d_k}\right)} \\ &= \sum_{i=0}^{2^n-2} (-1)^{tr\left(\alpha^{i}\left(\alpha^{l+j+\tau}\right)\right) + \sum\limits_{k=1}^{(n-1)/2} c_k tr\left(\alpha^{id_k}\left(1+\alpha^{\tau d_k}\right)\right)} \end{aligned}$$

Let $x = \alpha^i$, $\lambda = \alpha^{j+l+\tau}$ and $\beta_k = 1 + \alpha^{\tau d_k}$. Then,

$$R_{\underline{\mathbf{ab}}}(\tau)=\sum_{i=0}^{2^n-2}(-1)^{tr(\lambda x)+\sum_{k=1}^{(n-1)/2}c_k tr\left(\beta_k x^{d_k}\right)}$$

$$=-1+\sum_{x\in GF\left(2^n\right)}\left(-1\right)^{tr(\lambda x)+\sum_{k=1}^{(n-1)/2}c_k tr\left(\beta_k x^{d_k}\right)}.$$

By using Welch's squaring method as in Lemma 5.1, we get

$$R_{\underline{\mathbf{ab}}}(\tau)+1=\left\{0,\pm 2^{(n+1)/2}\right\}.$$

Hence, the theorem.

b) Linear Span

The linear complexity of the semi-bent sequences is computed as follows:

If $f(x)$ given by (5.27) has l_c nonzero c_i's for $1\le i\le(n-1)/2$, or equivalently l_c nonzero trace terms from $GF\left(2^n\right)$ to $GF(2)$, then the linear complexity L of the semi bent sequences in (5.34) is given by

$$L=n\cdot l_c+n \tag{5.37}$$

where the maximum linear complexity is obtained by

$$L_{\max}=\left(n^2+n\right)/2$$

at $l_c=(n-1)/2$.

5.2.4 Maximum Periodic correlation of Semi Bent sequences over fading channels

In the above section, we derived correlation and linear span of semi-bent sequences over non-fading channels. Now, we derive an improvement in the lower bound in Theorem 3.2 for a semi-bent signal set.

Theorem* 5.7:** In a semi-bent signal set defined by (5.35) which has size $M = 2^n + 1$ and period of each sequence as $N = 2^n - 1$ for ***n odd prime as in theorems 5.2 and 5.3, the maximum correlation of sequences over fading channel satisfies

$$R_{\text{max,semi-bent}} \geq \sqrt{\frac{2^{2n} \sum_{i=0}^{2^n-2} f_i^2 - \left(\sum_{i=0}^{2^n-2} f_i \right)^2}{2^{2n} - 1}} \tag{5.38}$$

***Proof*:** In (3.13), we can write

$$\sum_{\underline{\mathbf{a}} \in \mathrm{T}, i \neq j} (-1)^{s_i + s_j} = \sum_{t=0}^{2^n-2} \left[(-1)^{\sum_{k=1}^{(n-1)/2} c_k \left(tr_1^n\left(\alpha^{(i+t)d_k}\right) + tr_1^n\left(\alpha^{(j+t)d_k}\right)\right)} \cdot \left(\left(\sum_{r=0}^{2^n-2} (-1)^{tr_1^n\left(\alpha^{i+r+t}\right) + tr_1^n\left(\alpha^{j+r+t}\right)} \right) + 1 \right) \right]$$
$$+ \sum_{t=0}^{2^n-2} (-1)^{tr_1^n\left(\alpha^{i+t}\right) + tr_1^n\left(\alpha^{j+t}\right)}$$

From, the shift-and-add property, and the balance property of *m*-sequence,

$$\sum_{r=0}^{2^n-2} (-1)^{tr_1^n\left(\alpha^{i+r+t}\right) + tr_1^n\left(\alpha^{j+r+t}\right)} = \sum_{t=0}^{2^n-2} (-1)^{tr_1^n\left(\alpha^{i+t}\right) + tr_1^n\left(\alpha^{j+t}\right)} = -1$$

for $i \neq j$. Thus, $\sum_{\underline{\mathbf{a}} \in \mathrm{T}, i \neq j} (-1)^{s_i + s_j} = -1$, and (3.13) becomes

$$\begin{aligned} B &= \sum_i f_i^2 \left(\sum_{\underline{\mathbf{a}} \in \mathrm{T}} (-1)^{s_i + s_i} \right)^2 + \sum_{i,j,i \neq j} f_i f_j \left(\sum_{\underline{\mathbf{a}} \in \mathrm{T}} (-1)^{s_i + s_j} \right)^2 \\ &= \sum_i f_i^2 . (MN)^2 + \left(\sum_i f_i \right)^2 - \sum_i f_i^2 \end{aligned} \tag{5.39}$$

From (3.12) and (5.39), the lower bound in Theorem 3.2 is slightly changed for a semi-bent signal set, and the result follows.

For an independently and identically distributed f_i for a sufficiently large n, we have asymptotic bound, or

$$R_{\text{max,semi-bent}}^{(asymp)} \geq \sqrt{\frac{2^{2n}\left(2^n-1\right)\left(\mu^2+\sigma^2\right)-\left(2^n-1\right)^2\mu^2}{2^{2n}-1}} \approx \sqrt{2^{2n}\left(\mu^2+\sigma^2\right)} \tag{5.40}$$

from (3.15). It is noted that the asymptotic lower bound in a semi-bent signal set is determined by the length of the sequence and the first and second order statistics of the distribution of fading.

If we assume a slow fading environment, the contribution of $R_{\max}^2$ to B will be approximately a half. It is because when each fading amplitude is constant over a period, then $\left|R_{\underline{\mathbf{f}},\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)\right|^2$ in (3.12) is approximately two-valued with equal distribution similar to the one of a semi-bent signal set without fading [49], and one of them is negligible compared to the other. Hence, (3.12) can be changed into

$$B \approx \frac{MN(MN-1)}{2}R_{\max}^2 + ML\left(\sum_{i=0}^{N-1} f_i\right)^2 \tag{5.41}$$

From (5.41) and (5.39), approximated maximum correlation of sequences in a Semi-bent signal set is

$$R_{\text{max,semi-bent}}^{(slow)} \approx \sqrt{2}\sqrt{\frac{2^{2n}\sum_{i=0}^{2^n-2} f_i^2 - \left(\sum_{i=0}^{2^n-2} f_i\right)^2}{2^{2n}-1}} \tag{5.42}$$

which is a $\sqrt{2}$ times of lower bound in a Semi-bent signal set. From this approximation, we note that as fading gets slower, the actual maximum correlation approaches to $R_{\text{max,semi-bent}}^{(slow)}$.

Chapter 6

SIMULATION RESULTS AND DISCUSSIONS

6.1 Correlation Bound on GMW sequences

We compute the peak partial autocorrelations of the set of period $N = 2^{12} - 1$ GMW sequences having *m*=6, *n*=12, α a root of the primitive polynomial $z^{12} + z^6 + z^4 + z + 1$, and $r \in \{1, 5, 11, 13, 23\}$

i.e., $\{s_i\} = tr_1^6\left(tr_6^{12}\left(\alpha^i\right)^r\right)$

In this sequence, the zeros repeat with period of $T = \frac{2^{12} - 1}{2^6 - 1} = 65$. Fig. 6.1 plots peak partial autocorrelations of the GMW sequences against *l*, the subsequence length and the lower bound from Theorem 3.3. We may observe the symmetry of the graph about the line $l = 2047$ because the full period autocorrelation can be expressed as the sum of two partial autocorrelations of length l and $N - l$. It is apparent that the peak partial autocorrelations are larger when $r > 1$ than they are when $r = 1$.

We also compute the upper bounds obtained using Theorem 4.5 together with the peak partial autocorrelations of underlying $2^6 - 1$ *m*-sequences. Fig. 6.2 plots these bounds and the computed peak correlations for the period $2^{12} - 1$ GMW sequences with $r = 1$ and $r = 5$.. Clearly, this upper bound is not particularly good. Note that the interleaving bound in Theorem 4.5 for GMW sequence with $r = 5$ is usually lower than that for the GMW sequence with $r = 1$(a $2^{12} - 1$ period *m*-sequence). This is because the period 63 *m*-sequence corresponding to primitive element α^{5T} has generally lower peak partial autocorrelations than that corresponding to primitive α^T.

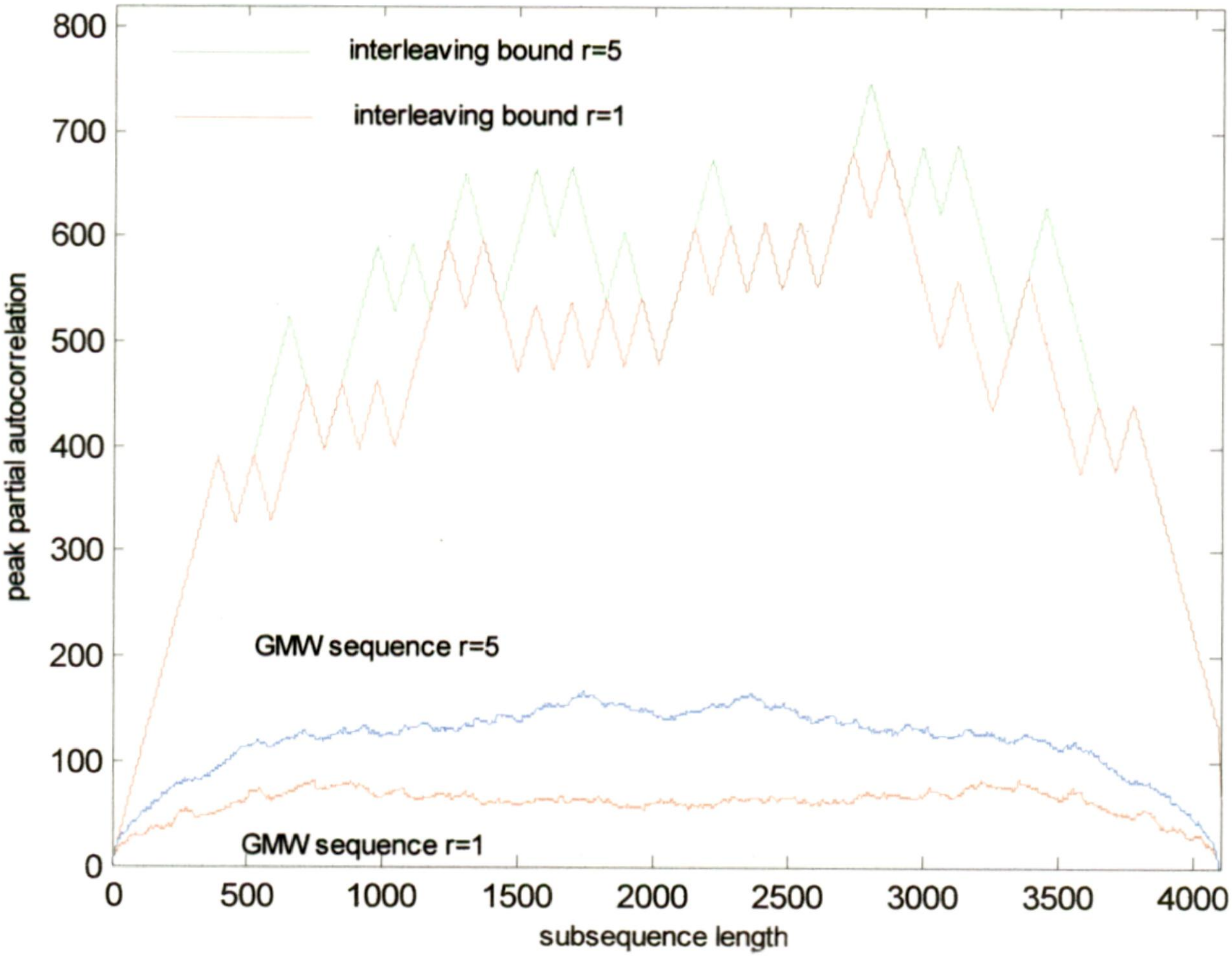


Fig. 6.2. Bounds on the peak partial autocorrelations of period $N = 2^{12} - 1$ GMW sequences

6.2 Correlation Bound on Cascaded GMW sequences

We perform the similar analysis as above for cascaded GMW sequences. We have computed the peak partial autocorrelations of the set of period $N = 2^{12} - 1$ cascaded GMW sequences having $n_1 = 3, n_2 = 6, n_3 = 12$, α a root of the primitive polynomial $z^{12} + z^6 + z^4 + z + 1$, and $r_1 = 5$, $r_2 \{1, 11, 13, 31\}$.

i.e., $$\{s_i\} = tr_1^{n_1}\left(tr_{n_1}^{n_2}\left(tr_{n_2}^{n_3}\left(\alpha^i\right)^{r_2}\right)^{r_1}\right)$$

In this sequence, the zeros repeat with period of $T = \dfrac{2^{12} - 1}{2^3 - 1} = 585$.

In Fig. 6.3, we compare the peak partial autocorrelations of cascaded GMW sequences with the lower bound obtained from Theorem 3.3 combined with the knowledge of the peak partial autocorrelations of underlying m-sequence of period $2^3 - 1$. Note that the lower bound is not tighter in these cases.

Fig. 6.4 depicts the comparison of peak partial autocorrelations of cascaded GMW sequences and underlying m-sequences of period $2^3 - 1$ with upper bound in Theorem 4.8. Again, it is clear that our upper bound leaves an improvement in these cases. we have plotted the bounds (and the computed peak correlation) for the period $2^{12} - 1$ cascaded GMW sequences with $r_1 = 5, r_2 = 11$, $r_1 = 5, r_2 = 13$, $r_1 = 1, r_2 = 1$.

Fig. 6.5 plots the comparison of the bounds from Theorem 4.5 and Theorem 4.8 for peak partial autocorrelations of GMW sequences. It is apparent that the upper bound from Theorem 4.5 is tighter than that from Theorem 4.8 for GMW sequences.

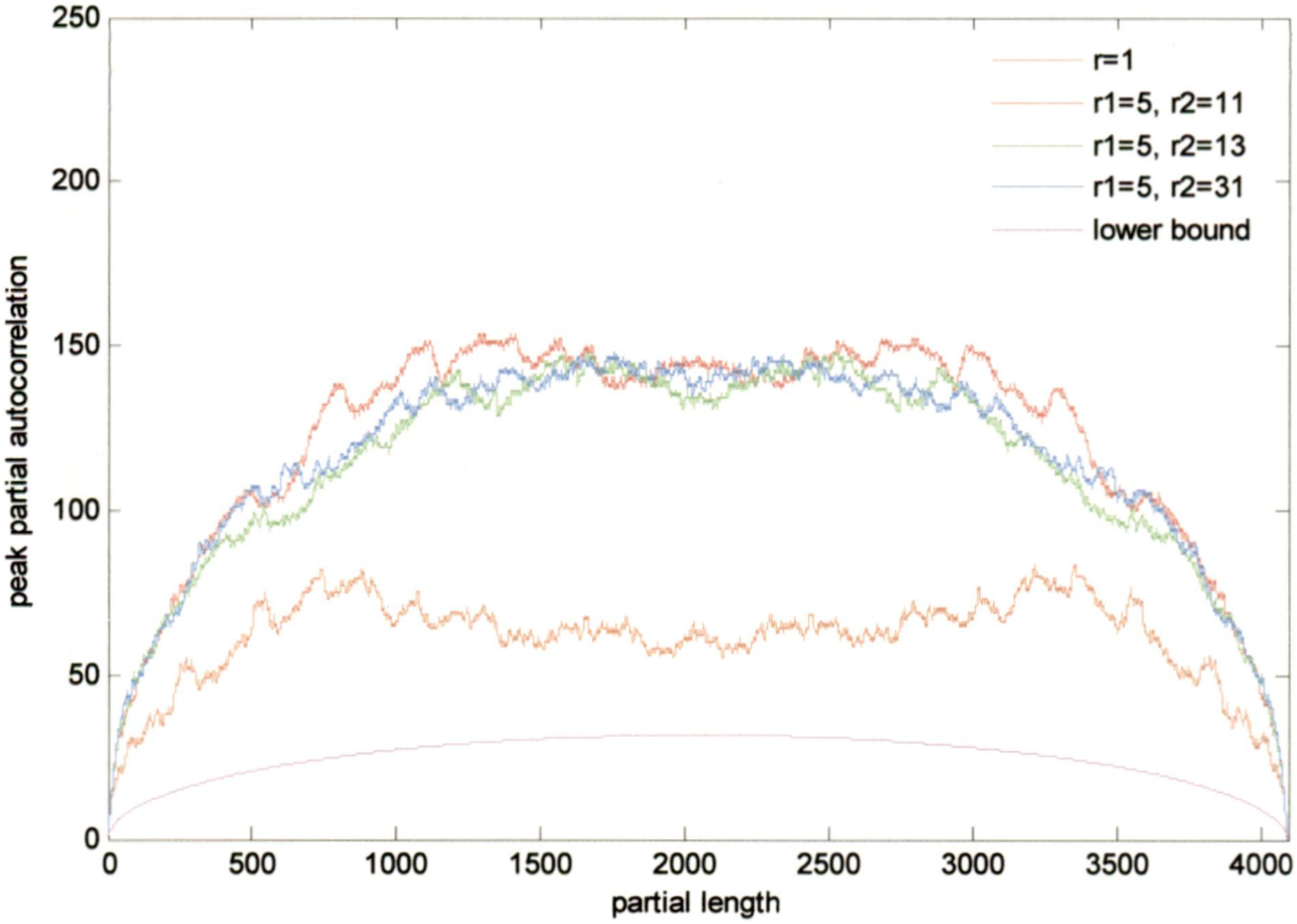


Fig. 6.3. Peak partial autocorrelations of period $N = 2^{12} - 1$ cascaded GMW sequences

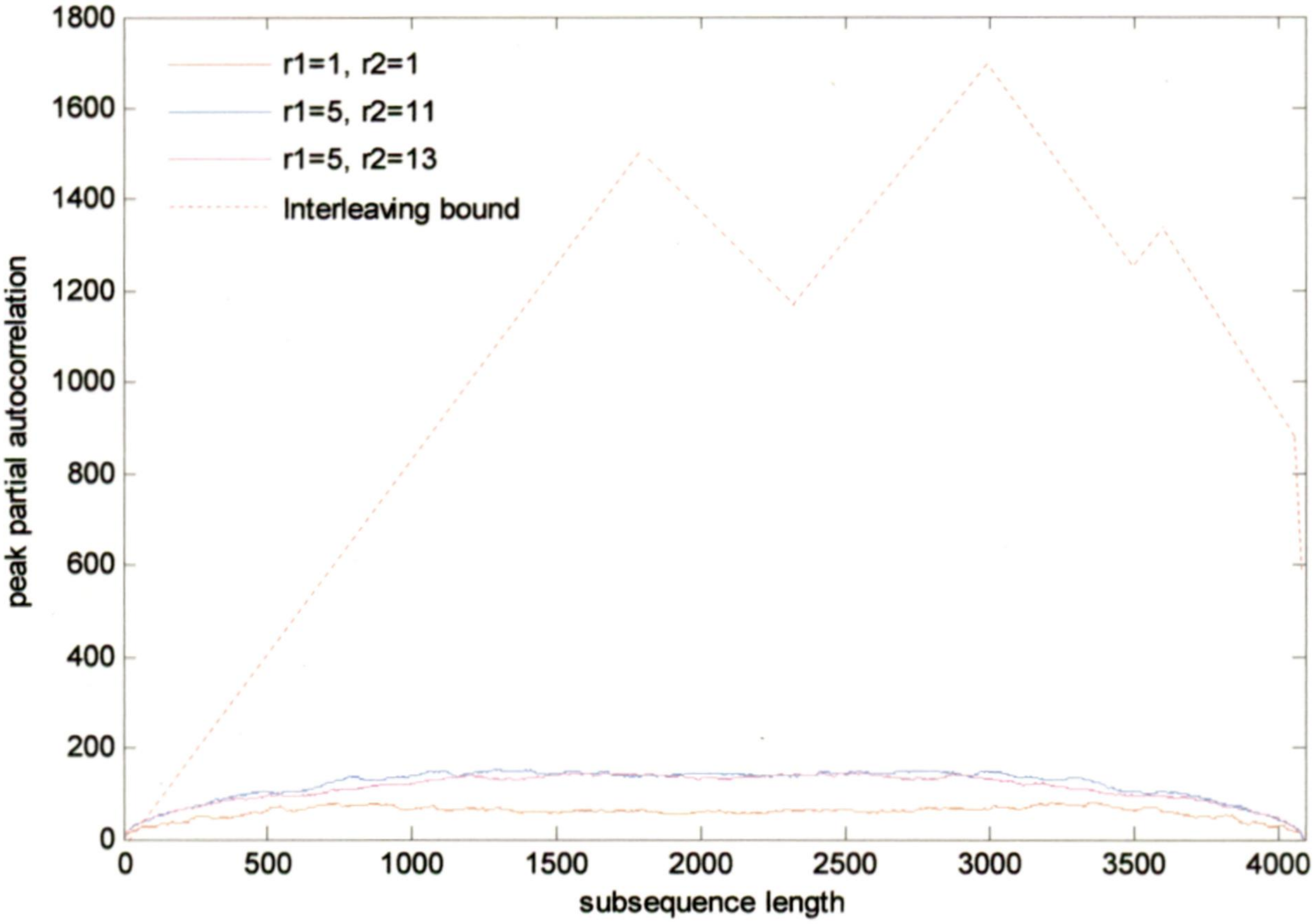


Fig. 6.4. Bounds on the peak partial autocorrelations of period $N = 2^{12} - 1$ cascaded GMW sequences.

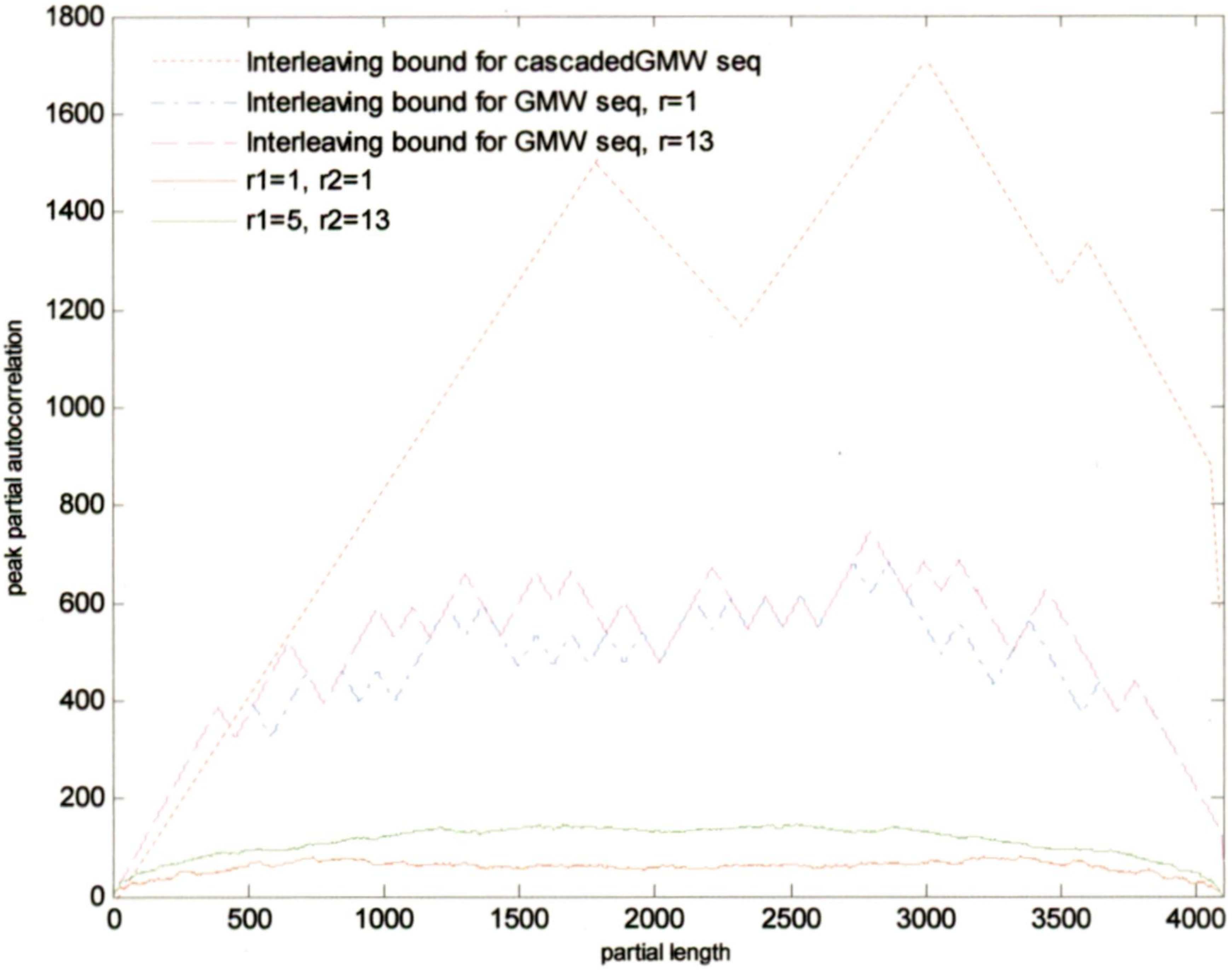


Fig. 6.5. Comparison of bounds on the peak partial autocorrelations of period $N = 2^{12} - 1$

GMW and cascaded GMW sequences

6.3 Correlation Bound on semi-bent signal set over fading channel

To analyze the statistical behavior of correlation of signals over Rayleigh fading, channels with independent and uncorrelated fading amplitudes are simulated respectively. Independent channels have i.i.d. fading for each chip in the signal. On the other hand, the rapidity of fading amplitudes is characterized by $f_D T_c$ where $f_D T_c$ represents maximum Doppler shift and $1/T_c$ is the sampling rate.

Assuming every user suffers from the same fading amplitude during the same period of time, and the receiver is able to know the accurate value of fading amplitudes with the perfect channel estimation, simulation is run ten times for a signal set in a Rayleigh channel environment but with different random amplitudes. In each trial, $k_{\max}$, the worst cross correlation of the signal set, is computed for semi-bent signal set with $n = \{5,7\}$. $k_{\max}$ is defined as

$$k_{\max} = \max_{\{k,i\}} R_{\max}$$

where $R_{\max}$ is as defined in (3.10), $k = 0,1,\ldots M-1$ and $i = k+1,\ldots,M-1$.

We define $k_{\max}^{(norm)} = k_{\max} / N$. Table 6.1 shows the average $k_{\max}^{(norm)}$ over all the trials for semi-signal set in Rayleigh fading with independent and uncorrelated fading amplitudes. It is apparent that $k_{\max}^{(norm)}$ decreases when the sequence period increases or fading becomes slower.

From Table 6.2, it is apparent that the worst case cross correlation of the semi-bent signal set satisfy the derived lower bounds in all trials. As we can observe from Table 6.2, the lower bounds approach the asymptotic bounds in independent fading for semi-bent signal set. From Table 6.3, it is evident that the lower bounds become tighter and $R_{\text{max,semi-bent}}^{(slow)}$ is more accurate when fading gets slower.

Table 6.1. Average $k_{\max}^{(norm)}$ of Semi-bent signal sets

Fading Type	$k_{\max}^{(norm)}$, n=5	$k_{\max}^{(norm)}$,n=7
Independent	0.7272	0.3757
$f_D T_c$ = 0.001	0.2818	0.2549
$f_D T_c$ = 0.0001	0.2291	0.1293

Table 6.2. $k_{\max}$ and asymptotic bound of Semi-bent signal sets

n	$k_{\max}$	Lower bound	Asymptotic bound
5	22.545	7.4571	7.6601
7	47.715	14. 7414	14.8456

Table 6.3. $k_{\max}$ and $R_{\max,\text{semi-bent}}^{(slow)}$ of Semi-bent signal sets in uncorrelated fading

n	$f_D T_c$	$k_{\max}$	Lower bound	$R_{\max,\text{semi-bent}}^{(slow)}$
5	0.001	8.7358	4.4042	6.2253
	0.0001	7.1021	3.8022	5.3771
7	0.001	36.184	12.4680	17.6324
	0.0001	16.425	5.3803	7.6089

Chapter 7
CONCLUSION

Pseudo-random sequences with good correlation properties, large linear complexity and balance statistics are widely used in modern communications and cryptology. This dissertation work has focused on study of correlation bounds on some nonlinear sequence sets since the correlation properties and their bounds are important in the selection and design of good sequence sets in CDMA systems and other applications.

This dissertation work can be summarized as follows:

- ✓ A lower bound on the peak partial correlation of binary signals over fading channels, using argument of Welch's inner product theorem, is established.

- ✓ An upper bound on the peak partial autocorrelation of cascaded GMW sequences, exploiting the underlying interleaved structure, is established. In order to obtain our bound, we require bounds on the peak partial autocorrelation of *m*-sequences. In [41], such bounds were developed using character sum approach while computational bounds can be conveniently developed for periods up to about $2^{20}-1$. As simulation results depicts, our bound is rather weak and leaves room for an improvement. It is also apparent that the bound in theorem 4.3 is tighter than that in theorem 4.8 for GMW sequences. However, our results do appear to be the first known guaranteed upper bound on peak partial autocorrelation of cascaded GMW sequences

- ✓ An improvement on the lower bound on the maximum correlation over fading channels is established for semi-bent sequences. . Asymptotic bound and slow fading approximation of the maximum correlation are obtained for independent and correlative channels respectively. As simulation results show, the lower bound is tighter in slow fading channel than in independent channel for a frequency-nonselective Rayleigh fading channel.

7.1 Future Work

Here, we come up with some proposals to continue the investigation performed in this dissertation study.

- Since our correlation bound on cascaded GMW sequences is rather weak, an investigation into a refined one can be undertaken. A more fruitful approach may be to find new sequences designed specifically with peak partial correlations in mind.

- The periodic and partial period correlation bounds of signals over fading channels examined in this dissertation are constrained to have uniform signal energy. These can be generalized to allow for arbitrary signal energy for each member of the signal set, with a view to consider the application of QAM signals to CDMA. Further, these bounds can be extended to investigate an improvement for complex roots of unity sequences.

Other correlations which have not been dealt with in this work include:

- *odd correlations* – these are as important in practice as the partial correlations.

- *Hamming correlations* – used as an important measure in evaluating goodness of Frequency Hopping sequence design.

- *additive correlations* – used as an important measure in the analysis of correlation attacks on cryptographic systems.

In these areas, many problems remain unsolved, or had been only partially solved.

REFERENCES

[1] A.J. Viterbi, *Principles of Spread Spectrum Communication*, Addison-Wesely Wireless Communication Series, 1995.

[2] S.W. Golomb, *Shift Register Sequences*. San Francisco: Holden-Day, 1967.

[3] J. J. Komo, S.C. Liu, "Maximal length sequences for frequency hopping," *IEEE Journal on selected areas in communications*, vol. 8, no. 5, pp. 819-822, June 1990

[4] D.V. Sarwate and M.B. Pursley, "Cross-Correlation properties of Pseudorandom and Related Sequences," *Proc. IEEE*, vol. 68, no. 5, pp.593-619, May 1980.

[5] J.J. Komo, "Crosscorrelation of *m*-sequences over nonprime finite fields," *Electronic Letters*, vol.25, no. 4, pp. 288-289, Feb. 1989.

[6] R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing," *IEEE Trans. Information Theory*, vol. IT-13, no.4, pp.619-621, Oct. 1967.

[7] R. Gold, "Maximal Recursive Sequences with 3-valued Recursive Cross-Correlation Functions," *IEEE Trans. Inform. Theory*, vol. IT-14, no.1, pp.154-156, Jan. 1968.

[8] R.A. Scholtz and L.R. Welch, "GMW Sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, no.3, pp. 548-553, May 1984.

[9] A. Klapper, A.H. Chan and M. Goresky, "Cascaded GMW Sequences," *IEEE Trans. Inform. Theory*, vol. 39, no.1, pp. 177-183, Jan. 1993.

[10] J.D. Olsen, R.A. Scholtz, and L.R. Welch, "Bent Function Sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 858-864, Nov. 1982.

[11] P.V. Kumar and R.A. Scholtz, "Bounds on the linear span of Bent Sequences," *IEEE Trans. Inform, Theory*, vol. IT-29, pp. 854-862, Nov. 1983.

[12] K. Khoo, G. Gong and D.R. Stinson, "A New Characterization of Semi-bent and Bent Functions on Finite Fields," *Designs, codes and cryptography*, 38, pp. 279-295, 2006.

[13] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine, "On cryptographic properties of the cosets of *R(*1,*m)*," *IEEE Trans. on Inform. Theory*, vol. 47, no. 4, pp. 1494–1513, May 2001.

[14] Y. Zheng and X. M. Zhang, "Relationships between bent functions and complementary plateaued functions," *Lecture Notes in Computer Science*, vol. 1787, pp. 60–75, 1999.

[15] G. Gong and K. Khoo, "Additive autocorrelation of resilient boolean functions," *Lecture Notes in Computer Science*, vol. 3006, pp. 275–290, 2004.

[16] J.S. No and P.V.Kumar, "A New Family of Binary Pseudorandom Sequences having optimal period Correlation Properties and Large Liner Span," *IEEE Trans. Inform. Theory*, vol. IT-35, pp. 371-379, Mar. 1989.

[17] P.V. Kumar and O. Moreno, "Polyphase sequences with periodic correlation properties better than binary sequences", *IEEE Trans. on Info. Theory*, vol. IT-37, no.3, pp. 603-616, May 1991.

[18] X.H. Tang, and P.Z. Fan, "A class of pseudonoise sequences over GF(P) with low correlation zone," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1644–1649, May 2001.

[19] P.V. Kumar, and C.M. Liu, "On lower bounds to the maximum correlation of complex roots-of-unity sequences," *IEEE Trans. Inf. Theory*, vol. 36, no. 3, pp. 633–640, May 1990.

[20] L.R. Welch, "Lower Bounds on the Maximum Cross Correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397-399, May 1974.

[21] D.V. Sarwate, "Bounds on Cross correlation and Autocorrelation of Sequences," *IEEE Trans. Inform. Theory*, vol. IT-25, no.6, pp. 720-724, Nov. 1979.

[22] V.I. Levenshtein, "New lower bounds on aperiodic crosscorrelation of binary codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 284–288, Jan. 1999

[23] D.Y. Peng and P.Z. Fan, "Bounds on the aperiodic auto and cross-correlation of binary sequences with low or zero correlation zone," *IEEE Press*, USA, pp. 882–886, Aug. 2003.

[24] X.H. Tang, and P.Z. Fan and S. Matsufuji, "Lower bounds on the maximum correlation of sequence set with low or zero correlation zone," *Electronic Letters*, vol. 36, no. 6, pp. 551–552, Mar. 2000.

[25] X.H. Tang, and P.Z. Fan, "Bounds on aperiodic and odd correlations of spreading sequences with low and zero correlation zone," *Electronic Letters*, vol. 37, no. 19, pp. 1201–1203, Sept. 2001.

[26] D.Y. Peng and P.Z. Fan, "Generalised Sarwate bounds on periodic autocorrelations and cross-correlations of binary sequences," *Electronic Letters*, vol. 38, no. 24, pp. 1521–1523, Nov. 2002

[27] D.Y. Peng and P.Z. Fan, “Lower bounds on the aperiodic correlation of LCZ and ZCZ sequences,” *Proc. 1st Int. Workshop on Sequence Design and Applications for CDMA Systems (IWSDA’ 2001)*, Chengdu, China, pp. 99–106, Sept. 2001.

[28] D.Y. Peng and P.Z. Fan, “Generalized sarwate bounds on the aperiodic correlation of sequences over complex root of unity,” *IEEE Proc. Communications*, vol. 151, no. 4, pp. 375-382, Aug. 2004.

[29] M. B. Pursley, D.V. Sarwate, T. U. Basar, “Partial correlation effects in direct sequence spread-spectrum multiple-access communications systems,” *IEEE Trans. Commun.*, vol. COM-32, pp. 567–573, May 1984.

[30] A.M. Klapper and M. Goresky, “Partial period autocorrelations of geometric sequences,” *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 494–502, Mar. 1994

[31] D.E. Cartier, “Partial correlation properties of pseudonoise (PN) codes in noncoherent synchronization/detection schemes,” *IEEE Trans. On Commun.* vol. 24, no. 8, pp.898–903, Aug. 1976.

[32] J. H. Lindholm, “An analysis of the pseudo-randomness properties of subsequences of long m-sequences,” *IEEE Trans. Inform. Theory*, vol. IT-14, no.4, pp. 569–576, July 1968.

[33] S. Wainberg and J. K. Wolf, “Subsequences of pseudorandom sequences,” *IEEE Trans. Commun. Technol.*, vol. COM-18, no.5, pp. 606–612, Oct. 1970.

[34] N. E. Bekir, L. R. Welch, and R. A. Scholtz, “Partial-period correlation properties of PN sequences,” in *IEEE Nat. Telecommunications Conf. Rec.*, vol. 3, pp. 35.1.1–35.1.4, 1978.

[35] S. A. Fredricsson, “Pseudo-randomness properties of binary shift register sequences,” *IEEE Trans. Inform. Theory*, vol. IT-21, no.1, pp. 115–120, Jan. 1975

[36] P. V. Kumar, “The partial-period correlation moments of arbitrary binary sequences,” in *IEEE Global Telecommunications Conf. Rec.* pp. 499–503, Dec. 1985.

[37] J.-S. No and P. V. Kumar, “On the partial-period correlation moments of GMW sequences,” in *IEEE Military Communications Conf. Rec.*, pp. 33.6.1–33.6.4, Mar. 1987.

[38] P. V. Kumar and V. K. Wei, “Minimum distance of logarithmic and fractional partial m-sequences,” *IEEE Trans. Inform. Theory*, vol. 38, no.5, pp. 1474–1482, Sept. 1992.

[39] D. V. Sarwate, “An upper bound on the aperiodic autocorrelation function for a maximal-length sequence,” *IEEE Trans. Inform. Theory*, vol. 30, no.4, pp. 685–687, July 1984.

[40] J. Lahtonen, "On the odd and aperiodic correlation properties of the Kasami sequences," *IEEE Trans. Inform. Theory*, vol. 41, no.5, pp. 1506–1508, Sept. 1995.

[41] K. G. Paterson, J. G. Lothian, " Bounds on partial correlations of sequences," IEEE Trans. Information Theory, vol 44, no. 3, pp. 1164–1175, May 1998.

[42] P.Z. Fan, N. Suehiro, N. Kuroyanagi, X.M. Deng: A class of binary sequences with zero correlation zone. IEEE Electron. Lett., vol.35, no. 10, pp.777–779, May 1999 .

[43] L. Feng and P.Z. Fan, " General bounds on partial aperiodic correlation of complex roots of unity sequences," *SETA 2006, LNCS*, pp. 342-350, 2006.

[44] A. M. Klapper, "d-form sequences: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, no.2, pp. 423–431, Mar. 1995.

[45] R.A. Scholtz, "The Origins of Spread-Spectrum Communications," *IEEE Trans. Communications*, vol. COM-30, no. 5, pp. 822-854, May 1982.

[46] J.L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, no.1, pp. 122-127, Jan. 1969.

[47] A.Duel-Hallen, J.Holtzman and Z. Zvonar, "Multi-user Detection for CDMA Systems," *IEEE Personal communications Magazine*, April 1995.

[48] J.G. Proakis, *Digital communications*, 3rd ed., McGraw-Hill, 1995.

[49] F.L. Chiu, N.Y. Yu and G. Gong, "Maximum Correlation of Binary Signals over Fading Channels," *IEEE International Symposium on Information Theory, ISIT 2005*, pp. 1913-1917, Sept. 2005.

[50] G. Gong, "Theory and applications of *q*-ary interleaved sequences," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 400-411, Mar. 1995.

[51] G. Gong, "*Q*-ary Cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 42, no.1, pp. 263-267, Jan. 1996.

[52] S.W. Golomb and G. Gong, *Signal Design with Good Correlation: for Wireless Communiations, Cryptography, and Radar Applications*, Cambridge University Press, 2005.

[53] E.L. Key, "An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators," IEEE Trans. Inform. Theory, vol. IT-22, no. 6, pp. 732-736, Nov. 1976.

[54] O.S.ROTHAUS, "On Bent Functions," *Journ. Of Combinatorial Theory* (A) 20, pp. 300-305, 1976.

[55] Serhat Sagdicoglu, "Cryptological Viewpoint of Boolean functions," MS Thesis, Middle East Technical University, Dept. of Mathematics, Sept. 2003.

[56] F.J. MacWilliams and N.J. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland, 1977.

Appendix A
REAL-TIME IMPLEMENTATION

A.1 Bent Sequence Generator

Consider a primitive polynomial of degree 8, $z^8+z^4+z^3+z^2+1$ with root α in $GF(2^8)$, as a characteristic polynomial of a Galois linear feedback shift register (LFSR). This register's state sequence has period 255, and contents of the shift register represent the field element X in the basis $\left[\alpha^i : \ i=0,1,...,7\right]$.

The set $\left[\alpha^{17i} : \ i=0,1,2,3\right]$ is composed of elements having order dividing 15, α^{17} being primitive in $GF(16)$, and hence these elements form a basis for the subfield $GF(16)$.

One possible choice for the element x_0, which must be outside of $GF(16)$ is α,

With the above stated choices, the 4 X 8 basis reduction matrix M has (i,j) th entry

$$m_{ij} = tr_2^{256}\left(\alpha^{17(i-1)+(j-1)+1}\right)$$

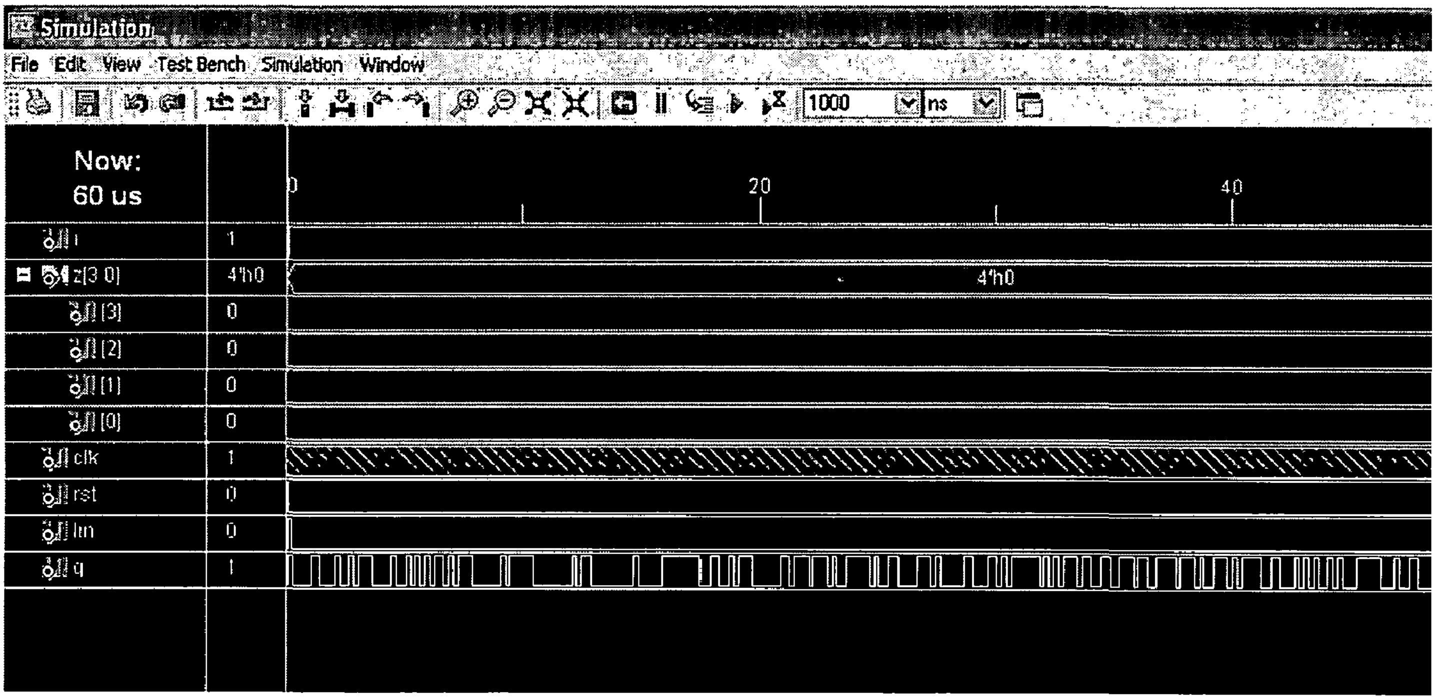
$$M = LQ^T = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

A suitable choice for the vector $\sigma = Q^T C$, which must be outside the row space of M is

$$\sigma^T = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Employing a bent function of the form given in Fig. 5.1, operating on $LQ^T A(t)$, with the arbitrary function $G(.)$ being a two input AND gate, the resulting bent sequence generator is simulated using XILINX ISE simulator and implemented on SPARTAN-3 FPGA. The ISE simulator output for the bent function sequence is as shown in Fig. 6.6.

The maximum magnitudes of the cross-/out of phase auto-correlation values of the above designed sequences are from the set $\{1,15,17\}$. The equivalent linear span calculated using Berlekamp-Massey algorithm of these sequences is 24 when the arbitrary function is an AND gate. For Ex-OR gate this value is 32.



Now: 60 us	
i	1
z[3:0]	4'h0
[3]	0
[2]	0
[1]	0
[0]	0
clk	1
rst	0
lin	0
q	1

Fig. 6.6 Example Simulation output of a sequence in ISE simulator

A.2 Semi-bent Sequence Generator

In this section, we consider the implementation of semi-bent sequence generator of period 127. Taking n=7, the semi-bent signal set in (5.34) can be reduced to

$$s_i^{(j)} = tr_1^n\left(\alpha^{i+j}\right) + \sum_{k=0}^{3} tr\left(\alpha^{i\left(2^k+1\right)}\right) \quad i = 0,1,\ldots,2^n-2,\ 0 \le j < 2^n-1$$

The above trace representation of semi-bent sequences can be realized using LFSR for each of the trace term. Each trace term represents an m-sequence of period 127.

Consider primitive polynomials of degree 7, z^7+z^3+1, $z^7+z^3+z^2+z+1$,, $z^7+z^4+z^3+z^2+1$ and $z^7+z^5+z^4+z^3+z^2+z+1$ with roots $\alpha,\alpha^3,\alpha^5,\alpha^9$ in $GF\left(2^7\right)$ respectively, as characteristic polynomials of LFSR's.

The shift registers for generating the four *m*-sequences and the corresponding semi-bent sequences are shown in Fig. 6.7. In this case, there are $2^7+1=129$ different sequences, corresponding to the 129 relative phases of the four *m*-sequences. Of these, 127 sequences are non-maximal-length sequences.

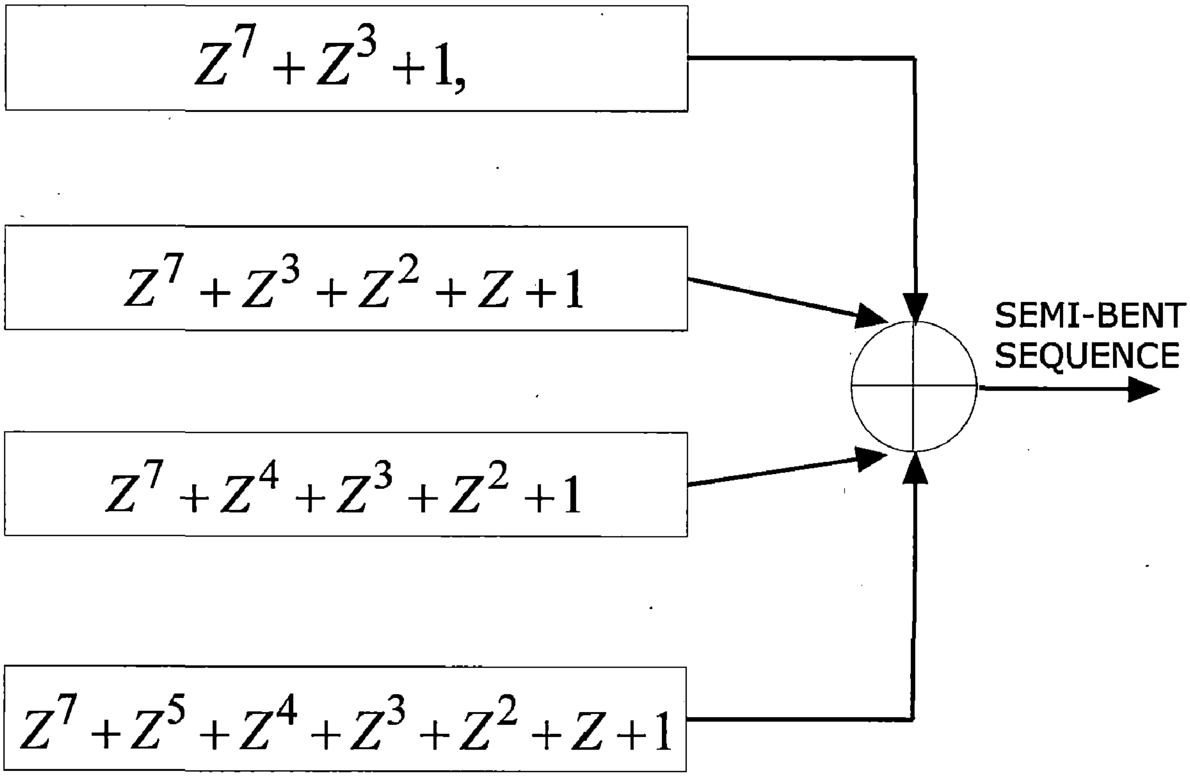
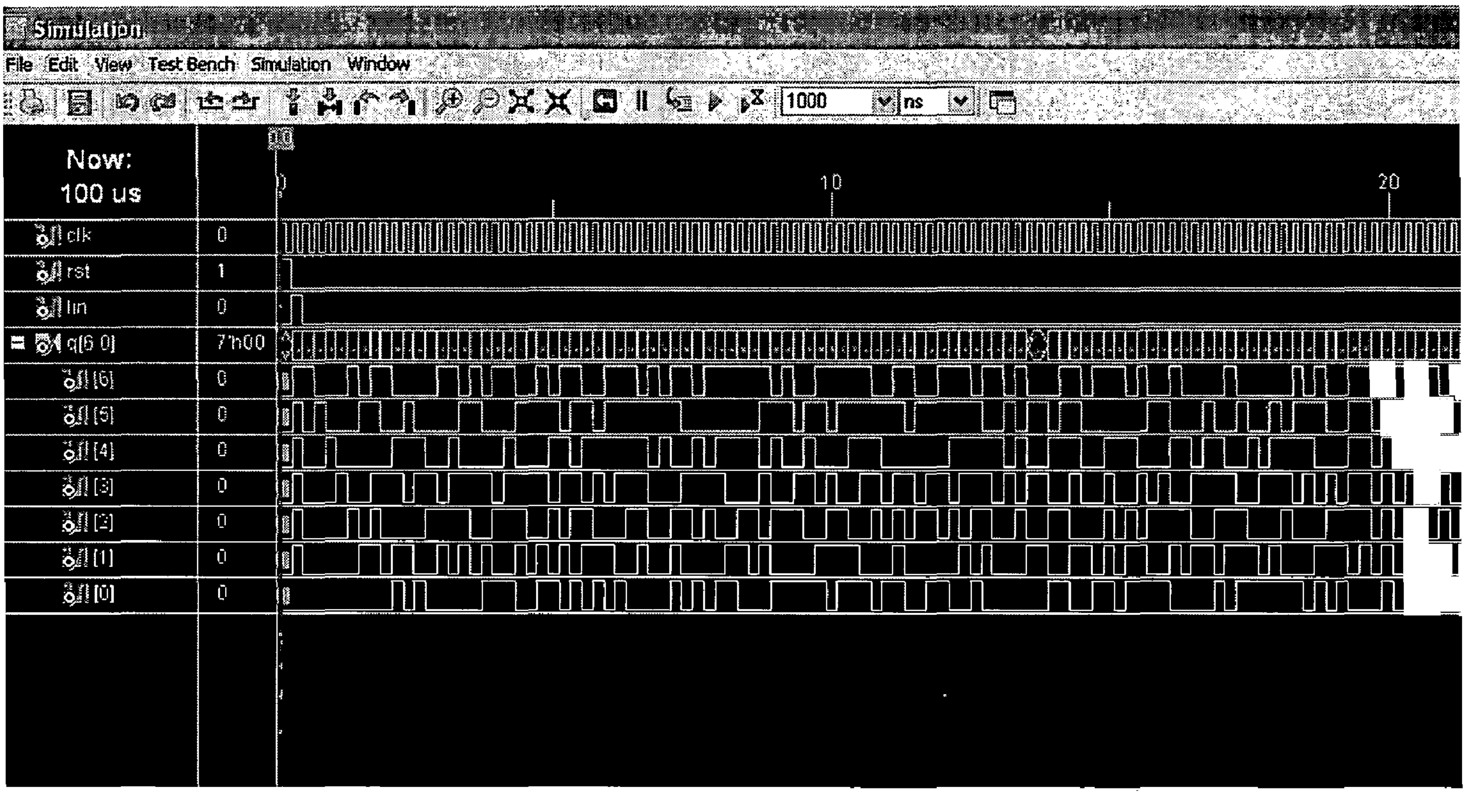


Fig. 6.7. Generation of Semi-bent sequences of period 127.

This resulting semi-bent sequence generator is is simulated using XILINX ISE simulator and implemented on SPARTAN-3 FPGA. The ISE simulator output is shown in Fig. 6.8. The out-of-phase autocorrelation and crosscorrelation functions of the above semi-bent signal set is a three valued i.e., $\{-1,15,-17\}$. The linear span of the resulting sequences is 56.



clk 0
rst 1
lin 0
q[6:0] 7'h00
[6] 0
[5] 0
[4] 0
[3] 0
[2] 0
[1] 0
[0] 0

Fig. 6.8 Example Simulation output of a sequence in ISE simulator

APPENDIX B

B.1 Trace Function

The trace function [8] $tr_J^M(\alpha)$, with n divisible by m, maps elements α in $GF(2^n)$ into elements of a subfield $GF(2^m)$, according to the relation

$$tr_m^n(\alpha) = \sum_{i=0}^{(n/m)-1} \alpha^{2^{mi}} \tag{1}$$

The trace function has the following properties:

a) $tr_m^n(\alpha) = tr_m^n(\alpha^{2^{mi}}) \quad \forall\ \alpha \in GF(2^n),$ for all i

b) $tr_m^n(a\alpha + b\beta) = atr_m^n(\alpha) + btr_m^n(\beta)$ for all $a, b \in GF(2^m)$ and $\alpha, \beta \in GF(2^n)$

c) The equation $tr_m^n(\alpha) = b$ for b any fixed element in $GF(2^m)$ has exactly 2^{n-m} solutions α in $GF(2^n)$.

d) Identifying the additive and multiplicative identities in $GF(2)$ with their counterparts in the real numbers, the following computational result in the real numbers is valid: $\sum_{\alpha \in GF(2^n)} (-1)^{tr_1^n(\delta\alpha)} = 0$ for all choices of δ, $\delta \neq 0$, in $GF(2^n)$.

e) $tr_1^n(\alpha) = tr_1^m(tr_m^n(\alpha)) \quad \forall\ \alpha \in GF(2^n)$.

The trace function can be used to explicitly define an m-sequence. An m-sequence $\{b_i\}$ of elements from $GF(2)$ is defined as the nonzero solution, unique to within shift, of a linear recursion

$$b_i = \sum_{j=1}^{n} m_j b_{i-j} \tag{2}$$

with coefficients $m_j \in GF(2)$, where the corresponding polynomial

$$m_\alpha(z) = z^M + \sum_{j=1}^{n} m_i z^{n-j}$$

is called the characteristic polynomial of the sequence, is the minimum polynomial over $GF(2)$ of a primitive element α in $GF(2^n)$.

The sequence $\{b_i\}$ with

$$b_i \triangleq tr_1^n(\alpha^i) \tag{3}$$

is the nonzero solution to (2) since, using the linearity of the trace function (property 2),

$$\begin{aligned} b_i - \sum_{j=1}^{n} m_j b_{i-j} &= tr_1^n(\alpha^n) + \sum_{j=1}^{n} m_j tr_1^n(\alpha^{i-j}) \\ &= tr_1^n(m_\alpha(\alpha)\alpha^{i-n}) = 0 \end{aligned}$$

The real valued sequence $\{a_n\}$, with

$$\{a_i\} \triangleq \left\{ \begin{array}{ll} 1, & \text{if } b_i = 0 \\ -1, & \text{if } b_i = 1 \end{array} \right\} = (-1)^{b_i} \tag{4}$$

where $\{b_i\}$ is the m-sequence over $GF(2)$, will be referred as the *real* m-sequence.

B.2 Trace transform

The trace transform $\hat{r}(\lambda)$ of $r(x)$ is defined as

$$\hat{r}(\lambda) \triangleq \frac{1}{2^{n/2}} \sum_{x \in GF(2^n)} r(x)(-1)^{tr(x\lambda)} \tag{5}$$

for all $\lambda \in GF(2^n)$

This is a real valued function which preserves inner product between two sequence functions on $GF(2^n)$

Properties:

a) Inversion:

$$r(x) = \frac{1}{2^{n/2}} \sum_{\lambda \in GF(2^n)} \hat{r}(\lambda)(-1)^{tr(x\lambda)}$$

b) Multiplicative Shifting Theorem:

$$\text{For } y \neq 0,\ \ s(x) = r(yx) \text{ for all } x \Leftrightarrow \hat{s}(\lambda) = \hat{r}(y^{-1}\lambda), \quad \text{for all } \lambda$$

c) Parsvel's Relatıon:

$$\sum_{x\in GF(2^n)} r(x)s(x) = \sum_{\lambda\in GF(2^n)} \hat{r}(\lambda)\hat{s}(\lambda)$$

d) Additive Shifting Theorems:

$$s(x) = r(x+y),\ \text{ for all x} \Leftrightarrow \hat{s}(\lambda) = \hat{r}(\lambda)\left(-1\right)^{tr(y\lambda)} \quad \text{for all } \lambda$$

$$\hat{s}(\lambda) = \hat{r}(\lambda+y),\ \text{ for all } \lambda \Leftrightarrow s(x) = r(x)\left(-1\right)^{tr(xy)} \quad \text{for all } x$$