

AD A 056552

AD NO. _____
DDC FILE COPY

REPORT R-785 AUGUST, 1977

UILU-ENG 77-2232

CSL COORDINATED SCIENCE LABORATORY

LEVEL II

12

**BINARY SEQUENCES FOR
SPREAD-SPECTRUM MULTIPLE-
ACCESS COMMUNICATION**

HENRICUS FRANCISCUS ALBERTUS ROEFS

DDC
FORM 17
JUL 18 1978
RECEIVED

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

UNIVERSITY OF ILLINOIS - URBANA, ILLINOIS

78 07 12 026

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER (9) Doctoral thesis	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) BINARY SEQUENCES FOR SPREAD-SPECTRUM MULTIPLE- ACCESS COMMUNICATION	5. TYPE OF REPORT & PERIOD COVERED Technical Report	
6. AUTHOR(s) Henrichus Franciscus Albertus Roefs	14. PERFORMING ORG. REPORT NUMBER R-785, UILU-ENG-77-2232	7. CONTRACT OR GRANT NUMBER(s) DAAB-07-72-C-0259, NSF-ENG-75-22621
9. PERFORMING ORGANIZATION NAME AND ADDRESS Coordinated Science Laboratory University of Illinois at Urbana-Champaign Urbana, Illinois 61801	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBER	
11. CONTROLLING OFFICE NAME AND ADDRESS Joint Services Electronics Program	12. REPORT DATE August 1977	
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) (12) 136p.	13. NUMBER OF PAGES 127	
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited.		15. SECURITY CLASS. (of this report)
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Spread Spectrum Communication Correlation Methods Linear Recursive Sequences		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) The communication capacity of a single wideband satellite channel can be simultaneously shared by a number of users by means of spread-spectrum multiple-access (SSMA). In phase-coded SSMA the multiple-access capability is provided by phase modulating a distinct signature sequence onto the user's carrier which spreads the user data over a wide bandwidth. All of the important code parameters for the analysis of such a system can be derived from the aperiodic correlation functions of the signature sequences. The asymptotic behavior of such code parameters is considered for random binary sequences for which the sequence		

DD FORM 1 JAN 73 1473

EDITION OF 1 NOV 65 IS OBSOLETE

07 12 UNCLASSIFIED

09470078 07 12 UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

20. ABSTRACT (continued)

length grows very large. New sets of pseudo-random or m-sequences with optimal aperiodic autocorrelation and cross-correlation properties are obtained. The relationship between the first few central moments of the aperiodic correlation functions and the characteristic polynomials generating the m-sequences is analyzed and the results are compared with actual sequence data.

Gauss' product of cyclotomic cosets is used to establish new analytical results on the periodic correlation properties of Gold sequences and Kasami sequences yielding subsets of sequences whose correlation parameters satisfy tighter bounds than previously established for the entire sequence sets. Numerical data on the relevant correlation parameters is obtained for a large number of good signature sequences.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

UILU-ENG 77-2232

BINARY SEQUENCES FOR SPREAD-SPECTRUM
MULTIPLE-ACCESS COMMUNICATION

by

HENRICUS FRANCISCUS ALBERTUS ROEFS

This work was supported in part by the Joint Services Electronics Program (U.S. Army, U.S. Navy and U.S. Air Force) under Contract DAAB-07-72-C-0259 and in part by the National Science Foundation under Grant NSF ENG-75-22621.

Reproduction in whole or in part is permitted for any purpose of the United States Government.

Approved for public release. Distribution unlimited.

BINARY SEQUENCES FOR SPREAD-SPECTRUM MULTIPLE-ACCESS COMMUNICATION

BY

HENRICUS FRANCISCUS ALBERTUS ROEFS

Ir., Delft University of Technology, 1970

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Electrical Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 1977

Thesis Adviser: Professor Michael B. Pursley

Urbana, Illinois

BINARY SEQUENCES FOR SPREAD-SPECTRUM MULTIPLE-ACCESS COMMUNICATION

Henricus Franciscus Albertus Roefs, Ph.D.
Department of Electrical Engineering
University of Illinois at Urbana-Champaign, 1977

Abstract

The communication capacity of a single wideband satellite channel can be simultaneously shared by a number of users by means of spread-spectrum multiple-access (SSMA). In phase-coded SSMA the multiple-access capability is provided by phase modulating a distinct signature sequence onto the user's carrier which spreads the user data over a wide bandwidth. All of the important code parameters for the analysis of such a system can be derived from the aperiodic correlation functions of the signature sequences. The asymptotic behavior of such code parameters is considered for random binary sequences for which the sequence length grows very large. New sets of pseudo-random or m-sequences with optimal aperiodic autocorrelation and cross-correlation properties are obtained. The relationship between the first few central moments of the aperiodic correlation functions and the characteristic polynomials generating the m-sequences is analyzed and the results are compared with actual sequence data.

Gauss' product of cyclotomic coefficients is used to establish new analytical results on the periodic correlation properties of Gold sequences and Kasami sequences yielding subsets of sequences whose correlation parameters satisfy tighter bounds than previously established for the entire sequence sets. Numerical data on the relevant correlation parameters is obtained for a large number of good signature sequences.

ACKNOWLEDGMENTS

I wish to thank my advisor, Professor Michael B. Pursley, for his guidance during the research carried out for this study and for introducing me to and stimulating my interest in the field of multiple-access communications.

I would like to acknowledge the stimulating discussions with Dr. D. V. Sarwate and the support given to me by the Department of Electrical Engineering and by the Coordinated Science Laboratory.

I wish to thank Dr. A. H. Haddad and Dr. F. P. Preparata for reading this thesis and serving on the Committee on Final Examination.

I also wish to thank Ms. Gertrude Williams and Mrs. Phyllis Young for their excellent typing of the manuscript.

Last but not least, I would like to thank my wife Cisca for her enduring encouragement and understanding.

TABLE OF CONTENTS

CHAPTER	Page
1. INTRODUCTION.....	1
1.1. Spread-spectrum multiple-access communication.....	1
1.2. Phase-coded SSMA system model.....	2
1.3. Worst-case performance.....	6
1.4. Average performance.....	7
1.5. Outline of the study.....	9
2. CORRELATION PARAMETERS OF RANDOM BINARY SEQUENCES.....	11
2.1. Aperiodic correlation parameters.....	11
2.2. Bounds on the set size of 'good' sequence pairs.....	13
2.3. Asynchronous interference parameters.....	15
2.4. Asynchronous interference versus synchronous interference.....	19
3. CORRELATION PARAMETERS OF M-SEQUENCES.....	23
3.1. Introduction to m-sequences.....	23
3.2. The trinomial structure of m-sequences.....	26
3.3. Autocorrelation functions.....	30
3.4. Periodic cross-correlation of m-sequences; Golomb's theorem.....	33
3.5. Maximal connected sets.....	38
3.6. Aperiodic correlation functions.....	41
4. ON THE MOMENTS OF THE APERIODIC CORRELATION FUNCTIONS.....	46
4.1. Third moment problem.....	46
4.2. Moments of the aperiodic correlation functions.....	47
4.3. Moments of the odd correlation functions.....	47
4.4. Third moment evaluation of m-sequences of length $p = 31$ and $p = 63$	50
4.5. Discussion of $\lambda_{\vec{u}}(l)$ and $\lambda_{\vec{u},\vec{v}}(l)$	52
4.6. Actual data for m-sequences of length $p = 31$ and $p = 63$	58
5. CORRELATION PARAMETERS FOR SUMS OF PAIRS OF M-SEQUENCES.....	60
5.1. Gold sequences.....	60
5.2. Periodic correlation functions of sums of m-sequences.....	62
5.3. Example for m-sequences of length $p = 15$	64
5.4. Sums of pairs of m-sequences up to length $p = 255$	67

CHAPTER	Page
5.4.1. Sequence length $p = 31$	68
5.4.2. Sequence length $p = 63$	70
5.4.3. Sequence lengths $p = 127$ and $p = 255$	74
5.5. Kasami sequences.....	76
5.5.1. Sequence length $p = 63$	79
5.5.2. Sequence length $p = 255$	80
6. CONCLUSIONS.....	85
REFERENCES AND SELECTED BIBLIOGRAPHY.....	86
APPENDIX	
A. INTERFERENCE PARAMETER FOR BARKER SEQUENCES.....	97
B. BOUNDS ON THE APERIODIC CROSS-CORRELATION FUNCTION.....	99
C. CORRELATION PARAMETERS OF AO/LSE M-SEQUENCES.....	101
D. MOMENTS OF APERIODIC CORRELATION FUNCTIONS OF M-SEQUENCES.....	105
D.1. First moments of the aperiodic correlation functions.....	105
D.2. Second moments of the aperiodic correlation functions.....	106
D.3. Expectation of the interference parameter $r(u,v)$	108
D.4. Third moments of the aperiodic correlation functions.....	109
D.5. Expectation of a product of aperiodic correlation functions.....	111
D.6. Relationship between $B_3^u(l)$ and $C_3^u(l)$	112
D.7. Fourth moments of the aperiodic correlation functions.....	113
E. CORRELATION PARAMETERS OF SUMS OF PAIRS OF M-SEQUENCES.....	114
VITA.....	126

CHAPTER 1

INTRODUCTION

1.1. Spread-spectrum multiple-access communication

In recent years there has been a large increase in the number of satellite communication programs for civilian as well as military purposes. Pritchard (1977) lists 32 satellite systems currently in use. A major advantage of a synchronous or geostationary satellite is the wide coverage area which enables a number of widely dispersed users to have simultaneous access to the satellite transporter. The user channel separation can be achieved in a variety of ways:

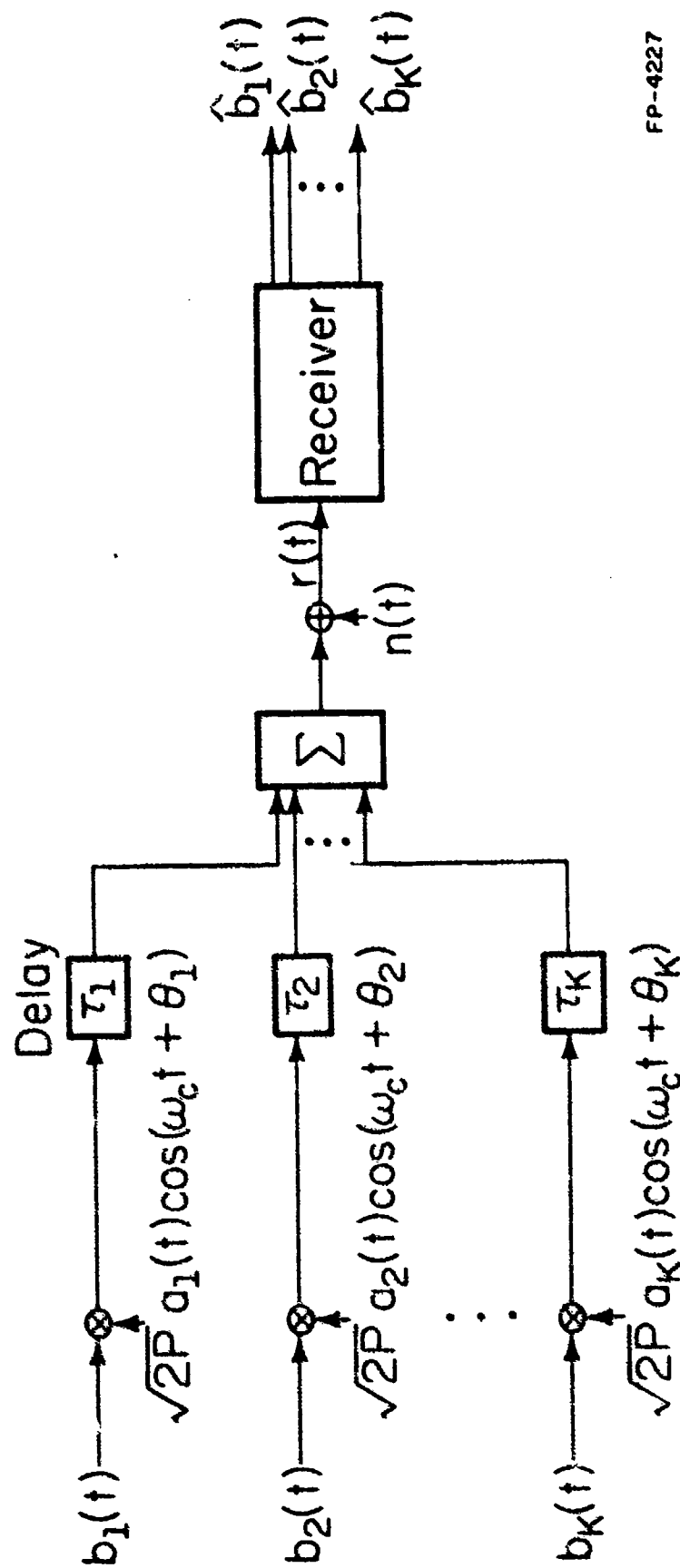
- 1) Frequency-division multiple-access (FDMA) is a common form of multiple-access where each ground station has a different, precisely determined carrier frequency. Single-channel-per-carrier as well as multiplexing to multi-channels-per-carrier is possible and fits well within non-digital terrestrial communication networks.
- 2) If precise time cooperation between the transmitting stations is possible one can adopt the very efficient time-division multiple-access (TDMA) in which each user has the same carrier but operates in a different time slot. TDMA fits better in digitized communication networks.
- 3) In Code-division multiple-access the channel separation is primarily due to coding while no precise frequency or timing cooperation between the transmitting stations is necessary. Applications are, among others, in tracking and data-relay systems (Stampfl, et al., 1970), air traffic control (Stiglitz, 1973) and military satellite communication systems (Gerhardt, 1973). Spread-spectrum techniques are characterized by the use

of a great deal more modulated RF bandwidth than normally would be required for transmitting the user information. The two most common forms of spread-spectrum techniques employed in CDMA are frequency-hopping and direct sequence modulation (Dixon, 1976). Frequency-hopping was used in the TATS modulation system and is described in Drouilhet (1969). In direct sequence modulation the multiple-access capability is provided by a high-rate code sequence which phase modulates -- together with the data sequence -- the user's carrier. The receiver station will recover the information by means of correlation techniques. The phase-coded spread-spectrum multiple-access (SSMA) method is very attractive for communication systems which also require protection against malicious interference and unauthorized listening (Gerhardt, 1973).

The performance of the SSMA system depends on the correlation properties of the high-speed signature sequences. In the past (Aein, 1965), (Blasbalg, 1965) most of the attention was focused on the periodic correlation properties of the signature sequences because in most cases a synchronous communication model was assumed. In the next section we introduce an asynchronous SSMA system model -- earlier presented by Pursley (1974) -- which makes it possible to identify the correlation parameters of interest for the communication performance as well as for the synchronization performance.

1.2. Phase-coded SSMA system model

We will consider the SSMA system model as given in Figure 1 for K transmitting stations or users. The i -th user's data signal $b_i(t)$ is a sequence of positive and negative pulses of duration T and unit amplitude,



FP-4227

Figure 1. Phase-coded spread-spectrum multiple-access system model.

$$b_i(t) = \sum_{l=-\infty}^{\infty} b_{i,l} p_T(t-lT) \quad (1.1)$$

where $b_{i,l} \in \{+1, -1\}$ denotes the i -th user's information bit stream and pulse $p_T(t) = 1$ for $0 \leq t < \tau$ and $p_T(t) = 0$, otherwise. The code wave form which binary phase modulates the user's RF carrier frequency can be expressed as

$$a_i(t) = \sum_{j=-\infty}^{\infty} u_j^{(i)} p_{T_c}(t-jT_c) \quad (1.2)$$

where $\{u_j^{(i)}\}$ represents the discrete signature sequence of the i -th user, and has period $p = T/T_c$ and elements of $\{+1, -1\}$.

For an asynchronous system where no timing reference for the K users is assumed, the received signal at the message destination can be expressed as

$$r(t) = \sum_{i=1}^K (2P)^{\frac{1}{2}} a_i(t-\tau_i) b_i(t-\tau_i) \cos(\omega_c t + \phi_i) + n(t) \quad (1.3)$$

Here $n(t)$ represents the channel noise which we assume to be a white Gaussian process with two-sided spectral density $N_0/2$, ω_c represents the common RF center frequency and P the common signal power. Unequal signal powers can easily be incorporated in the results. If the received signal $r(t)$ is the input to a synchronized correlation receiver matched to the i -th user signal, the output at sample moment $t = T$ is given by Pursley (1974) as

$$Z_i(T) = \left(\frac{P}{2}\right)^{\frac{1}{2}} \{b_{i,0} \cdot T + \sum_{\substack{k=1 \\ k \neq i}}^K S_{i,k}(\tau_k)\} + \int_0^T n(t) a_i(t) \cos \omega_c t dt \quad (1.4)$$

where $S_{i,k}(\tau_k)$ -- with $\{u_j\} = \{u_j^{(1)}\}$ and $\{v_j\} = \{v_j^{(k)}\}$ -- equals
for $l_k T_c \leq \tau_k \leq (l_k + 1)T_c$

$$S_{i,k}(\tau_k) = \begin{cases} b_{k,0} [\theta_{u,v}(l_k) T_c + [\theta_{u,v}(l_{k+1}) - \theta_{u,v}(l_k)] (\tau_k - l_k T_c)] \cos \varphi_k & \text{if } b_{k,0} = b_{k,-1} \\ b_{k,0} [\hat{\theta}_{u,v}(l_k) T_c + [\hat{\theta}_{u,v}(l_{k+1}) - \hat{\theta}_{u,v}(l_k)] (\tau_k - l_k T_c)] \cos \varphi_k & \text{if } b_{k,0} \neq b_{k,-1} \end{cases} \quad (1.5)$$

The discrete cross-correlation functions $\theta_{u,v}(l)$ and $\hat{\theta}_{u,v}(l)$ for the sequences $u = \{u_j\}$ and $v = \{v_j\}$ are defined as

$$\begin{cases} \theta_{u,v}(l) = C_{u,v}(l-p) + C_{u,v}(l), & 0 \leq l \leq p-1 \\ \hat{\theta}_{u,v}(l) = C_{u,v}(l-p) - C_{u,v}(l), & 0 \leq l \leq p-1 \end{cases} \quad (1.6)$$

where $C_{u,v}(l)$ denotes the aperiodic cross-correlation function defined as

$$C_{u,v}(l) = \begin{cases} \sum_{j=0}^{p-1-l} u_j v_{j+l} & 0 \leq l \leq p-1 \\ \sum_{j=0}^{p-1+l} u_{j-l} v_j & 1-p \leq l < 0 \\ 0 & |l| \geq p \end{cases} \quad (1.7)$$

Observe that $C_{u,v}(l) = C_{v,u}(-l)$, thus the periodic (or even) cross-correlation function $\theta_{u,v}(l)$ satisfies $\theta_{u,v}(l) = \theta_{v,u}(p-l)$ where as function $\hat{\theta}_{u,v}(l)$ satisfies $\hat{\theta}_{u,v}(l) = -\hat{\theta}_{v,u}(p-l)$ -- hence, Massey and Uthran (1974) called the latter the odd cross-correlation function.

In order for the correlation receiver to operate properly it should be synchronized with the i -th user's signal. The synchronization decisions are derived from $Z_i(T)$ in (1.4) which will contain the periodic autocorrelation function $\theta_u(l) = \theta_{u,u}(l)$ or the odd autocorrelation function $\hat{\theta}_u(l) = \hat{\theta}_{u,u}(l)$ as long as the receiver is not yet synchronized or has lost synchronization. The autocorrelation functions will also appear in $Z_i(T)$ when multipath interference is present in the channel (Massey and Uthran, 1969).

1.3. Worst-case performance

The function $S_{i,k}(\tau_k)$ in equation (1.4) achieves a maximum value with respect to τ_k and φ_k whenever $\tau_k = \ell_k T_c$, for some integer ℓ_k , and $\varphi_k = 0$. The resulting values of $S_{i,k}(\tau_k)$ are $\pm \theta_{u,v}(\ell_k)$ or $\pm \hat{\theta}_{u,v}(\ell_k)$. Hence the maximum value of the error probability $\Pr\{Z_i(T) > 0 / b_{i,0} = -1\}$ will be minimized by selecting a set of signature sequences for which the peak parameters

$$\theta_{\max}(u,v) = \max\{|\theta_{u,v}(\ell)| : 0 \leq \ell \leq p-1\} \quad (1.8)$$

and

$$\hat{\theta}_{\max}(u,v) = \max\{|\hat{\theta}_{u,v}(\ell)| : 0 \leq \ell \leq p-1\} \quad (1.9)$$

are small. The same result is obtained for $b_{i,0} = +1$.

Not only $\theta_{\max}(u,v)$ itself but also the number of times $|\theta_{u,v}(\ell)|$ takes on this maximum value -- when $\ell = 0, 1, \dots, p-1$ -- is of interest. Let $\|X\|$ denote the cardinality of X , then we define

$$L_c = \|\{\ell : |\theta_{u,v}(\ell)| = \theta_{\max}(u,v)\} ; 0 \leq \ell \leq p-1\| \quad (1.10)$$

Furthermore one defines for a set S of sequences,

$$\theta_c = \max\{\theta_{\max}(u,v) : u \in S, v \in S\}. \quad (1.11)$$

The parameters $\hat{L}_c$ and $\hat{\theta}_c$ are defined as in (1.10) and (1.11) respectively with θ replaced by $\hat{\theta}$.

Pursley (1976a) pointed out that the worst-case probability of detection error $P_{\max}$ can be written as

$$P_{\max} = 1 - \Phi(1 - (\Lambda/p) \sqrt{2\mathcal{E}_b/N_0}) \quad (1.12)$$

where Φ is the standard Gaussian cumulative distribution function, $\mathcal{E}_b = PT$ the energy per data bit and $\Lambda = \max\{\theta_c, \hat{\theta}_c\}$.

For the autocorrelation functions we define the parameters

$$\theta_{\max}(u) = \max\{|\theta_u(\ell)| : 1 \leq \ell \leq p-1\} \quad (1.13)$$

$$L_a = \|\{\ell : |\theta_u(\ell)| = \theta_{\max}(u) ; 1 \leq \ell \leq p-1\}\| \quad (1.14)$$

and
$$\theta_a = \max\{\theta_{\max}(u) : u \in S\} \quad (1.15)$$

The parameters $\hat{\theta}_{\max}(u)$, $\hat{L}_a$ and $\hat{\theta}_a$ are defined as in (1.13), (1.14) and (1.15) respectively, with θ replaced by $\hat{\theta}$. In addition we define

$$c_{\max}(u) = \max\{|c_u(\ell)| : 1 \leq \ell \leq p-1\} \quad (1.16)$$

and

$$c_{\max}(u,v) = \max\{|c_{u,v}(\ell)| : 1-p \leq \ell \leq p-1\} \quad (1.17)$$

1.4. Average performance

The average probability of error as well as the average signal-to-noise ratio at the receiver output are important measures of the

average system performance given a set of signature sequences. The former is hard to compute but Yao (1976) obtained upper and lower bounds on its value. The evaluation of those bounds requires extensive knowledge of the aperiodic cross-correlation functions.

Assume the phase shifts ϕ_k , time delays τ_k and the data symbols $b_{k,0}$ and $b_{k,-1}$, $1 \leq k \leq K$, $k \neq i$ to be mutually independent random variables. Also assume that ϕ_k and τ_k are uniformly distributed over $[0, 2\pi]$ and $[0, T]$ respectively and the data symbols $b_{k,l}$ take on values $+1$ or -1 with equal probability for $k \neq i$. By obtaining the mathematical expectation and the variance of $Z_i(T)$, Pursley (1974) showed that the average (power) signal-to-noise ratio at the i -th user receiver output in an asynchronous SSMA system can be expressed as

$$\text{SNR}_a = \left\{ \frac{N_0}{2\epsilon_b} + Q_a \right\}^{-1} \quad (1.18)$$

where the asynchronous interference Q_a equals

$$Q_a = (6p^3)^{-1} \sum_{\substack{k=1 \\ k \neq i}}^K r(u^{(i)}, u^{(k)}) \quad (1.19)$$

with the interference parameter $r(u, v)$ defined as

$$r(u, v) = \sum_{l=1-p}^{p-1} \{ 2C_{u,v}^2(l) + C_{u,v}(l)C_{u,v}(l+1) \} \quad (1.20)$$

Yao showed that $P_e = 1 - \phi(\sqrt{\text{SNR}_a})$ is a very good approximation of the actual average error probability for many practical values of p and K . Clearly, detailed knowledge of $r(u, v)$ for prospective sets of signatures is important in the performance analysis. In some cases the product

$C_{u,v}(\ell)C_{u,v}(\ell+1)$ does not contribute to $r(u,v)$ as is shown in Appendix A for Barker sequences (Barker, 1953) of odd length p .

Important measures on the autocorrelation functions are

$$M(u) = \sum_{\ell=1}^{p-1} \theta_u^2(\ell) \quad (1.21)$$

and

$$\hat{M}(u) = \sum_{\ell=1}^{p-1} \hat{\theta}_u^2(\ell) \quad (1.22)$$

which can be used -- in addition to the worst-case performance measures -- as sieves for sequences with good synchronization capabilities. Observe that

$$M(u) + \hat{M}(u) = 4S(u) \quad (1.23)$$

where

$$S(u) = \sum_{\ell=1}^{p-1} C_u^2(\ell), \quad (1.24)$$

Parameter $S(u)$ is called the sidelobe energy of a sequence and was previously considered by, among others, Lindner (1975) and Golay (1977).

1.5. Outline of the study

Chapter 2 investigates the various sequence parameters described above, for random binary sequences for which sequence length p grows very large. An approximation of SNR_a is obtained which is very accurate for typical values of K , p and $\mathcal{E}_b/N_0$.

Chapter 3 discusses the code parameters for maximum-length sequences generated by primitive polynomials. New sets of sequences with optimal autocorrelation as well as cross-correlation properties are obtained.

Chapter 4 investigates the relationship between the aperiodic correlation functions of maximum-length sequences and the primitive polynomials which generate those sequences. In particular, the third central moments of the odd correlation functions are obtained and compared with actual sequence data.

Chapter 5 investigates sets of sequences generated by products of primitive polynomials such as Gold sequences (Gold, 1967) and Kasami sequences (Kasami, 1966). A method -- based on Gauss' products of cyclotomic cosets -- is given which yields large subsets of sequences with better correlation properties. The relevant correlation parameters of a large number of good subsets are obtained.

CHAPTER 2

CORRELATION PARAMETERS OF RANDOM BINARY SEQUENCES

This chapter considers the asymptotic behavior of the various code parameters described in Chapter 1, for random binary sequences.

2.1. Aperiodic correlation parameters

In a practical realization of a SSMA system, the signature sequence length p is constrained for obvious technical reasons. Notwithstanding this fact, it is still of interest to study the asymptotic behavior of random binary sequences for which the sequence length p grows very large. By random binary sequences we mean binary sequences of independent identically distributed random variables u_j , for which $\Pr\{u_j=+1\} = \Pr\{u_j=-1\} = \frac{1}{2}$.

Let $0 \leq l \leq p-1$. Then, $C_{u,v}(l) = \sum_{j=0}^{p-1-l} u_j v_{j+l}$. Suppose $|r| \leq p-l$.

In order that $C_{u,v}(l) = r$, it must be that $u_j = v_{j+l}$ for exactly $\frac{1}{2}(p-l+r)$ integer values of j in the range $0 \leq j \leq p-1-l$. Hence, if $p-l+r$ is even, there are

$$b(l, p, r) = \binom{p-l}{\frac{1}{2}(p-l+r)}$$

choices for $(u_0, u_1, \dots, u_{p-1-l})$. Since there are 2^p choices for v and 2^l choices for $(u_{p-l}, \dots, u_{p-1})$, there are a total of

$$h(l, p, r) = 2^p 2^l b(l, p, r) \quad (2.1)$$

sequence pairs (u, v) for which $C_{u,v}(l) = r$, provided $p-l+r$ is even. In the special case that $u=v$, there are

$$h'(\ell, p, r) = 2^\ell b(\ell, p, r), \quad 1 \leq \ell \leq p-1$$

sequence pairs (u, u) , i.e., sequences u , for which $C_u(\ell) = r$, $\ell \neq 0$.

Notice also that $h(0, p, p) = 2^p$.

Recall that

$$C_{\max}(u) = \max \{ |C_u(\ell)| : 1 \leq \ell \leq p-1 \}$$

and

$$C_{\max}(u, v) = \max \{ \hat{C}_{\max}(u, v), \hat{C}_{\max}(v, u) \}$$

where

$$\hat{C}_{\max}(u, v) = \max \{ |C_{u,v}(\ell)| : 0 \leq \ell \leq p-1 \}.$$

Moon and Moser (1968) showed that for $\epsilon > 0$,

$$\left| \frac{\log C_{\max}(u)}{\frac{1}{2} \log p} - 1 \right| \geq \epsilon \quad (2.2)$$

for almost none of the binary sequences of length p , i.e., for only a fraction $\gamma(p)$ of the sequences, where $\lim_{p \rightarrow \infty} \gamma(p) = 0$. Or, alternatively,

$$\Pr \left\{ \left| \frac{\log C_{\max}(u)}{\frac{1}{2} \log p} - 1 \right| \geq \epsilon \right\} \leq \gamma(p) \quad (2.3)$$

for u chosen at random from the set of all possible sequences. In Appendix B we show, analogous to the proof of (2.2) by Moon and Moser, that if u and v are drawn at random from the set of all 2^{2p} sequence pairs, then

$$\Pr \left\{ \left| \frac{\log C_{\max}(u,v)}{\frac{1}{2} \log p} - 1 \right| \geq \epsilon \right\} \leq \tilde{\gamma}(p) \quad (2.4)$$

where $\lim_{p \rightarrow \infty} \tilde{\gamma}(p) = 0$.

2.2. Bounds on the set size of 'good' sequence pairs

A consequence of the expressions (2.3) and (2.4) is the following. Fix $\epsilon \leq 1$. The set of all 2^{2p} sequence pairs is purged of all pairs for which the event in (2.4) occurs. This gives a set $A_1(p)$ which has cardinality $\|A_1(p)\|$. The expected value of $\|A_1(p)\|$ is lower-bounded by

$$E\|A_1(p)\| \geq 2^{2p}(1 - \tilde{\gamma}(p)).$$

Hence, there exists at least one set, say $A_2(p)$, with

$$\|A_2(p)\| \geq 2^{2p}(1 - \tilde{\gamma}(p)).$$

Notice that $A_2(p)$ does not contain any sequence pair of the form (u,u) because $\hat{C}_{\max}(u,u) = p$. This problem is easily resolved, however, because expression (2.3) implies that there exists at least one set, say $B_2(p)$ with

$$\|B_2(p)\| \geq 2^p(1 - \gamma(p)).$$

The union of $A_2(p)$ and $B_2(p)$ yields a set of sequence pairs with cardinality lower-bounded by

$$\|A_2(p) \cup B_2(p)\| \geq 2^{2p}(1 - \tilde{\gamma}(p) + 2^{-p}(1 - \gamma(p))) \quad (2.5)$$

for which $C_{\max}(u)$ as well as $C_{\max}(u,v)$ are contained within the range $[p^{\frac{1}{2}(1-\epsilon)}, p^{\frac{1}{2}(1+\epsilon)}]$. Furthermore, $\|A_2(p) \cup B_2(p)\|$ grows exponentially with p as 2^{2p} because $A_2^c(p)$, which is the complement of $A_2(p)$, and hence $\|A_2(p) \cup B_2(p)\|^c$, contains only a vanishingly small fraction of pairs, i.e., $2^{-2p}\|A_2^c(p)\| \leq \tilde{\gamma}(p)$ and $\lim_{p \rightarrow \infty} \tilde{\gamma}(p) = 0$. Above result shows that there exists at

least one very large set of sequence pairs (u,v) for which

$$p^{\frac{1}{2}-\epsilon} \leq C_{\max}(u) \leq p^{\frac{1}{2}+\epsilon}, \epsilon > 0, u = v \quad (2.6)$$

and

$$p^{\frac{1}{2}-\epsilon} \leq C_{\max}(u,v) \leq p^{\frac{1}{2}+\epsilon}, \epsilon > 0, u \neq v. \quad (2.7)$$

The size of this set grows exponentially with p as 2^{2p} .

Discussion

The growth of the size of at least one set of sequences u , as subset of $A_2(p) \cup B_2(p)$, for which then (2.6) and (2.7) will hold simultaneously, remains an unsolved problem. Schneider and Orr (1975) consider the cardinality of a set $A(p)$ obtained by purging the set of all 2^p sequences, of all sequences which violate the upperbound of (2.6) and which form pairs which in turn violate the upperbound of (2.7). Their use of the upperbound only, is here of minor importance. The purging method itself, however, has a disastrous effect on the lowerbound of the expected value of $\|A(p)\|$. Suppose, for example, that

a certain sequence u will form, with many other sequences v , sequence pairs (u,v) which violate the (upper) bound in (2.7). Schneider and Orr -- see their equation (20) -- not only remove sequence u but all the other sequences v as well, from the set of 2^p sequences. As a result, the lower bound of the expected value of $\|A(p)\|$ will not grow exponentially with p .

2.3. Asynchronous interference parameters

Let u and v be two random binary sequences (not necessarily distinct). With $|\ell| \leq p-1$ and $|r| \leq p - |\ell|$, equation (2.1) implies

$$\Pr\{C_{u,v}(\ell) = r\} = \binom{p - |\ell|}{\frac{p - |\ell| + r}{2}} 2^{-(p - |\ell|)}. \quad (2.8)$$

This probability mass function implies a moment generating function

$$\begin{aligned} M_C(t) &= E\{\exp[tC_{u,v}(\ell)]\} \\ &= \begin{cases} \prod_{j=0}^{p-\ell} E[\exp[tu_j v_{j+\ell}]] & 0 \leq \ell \leq p-1 \\ \prod_{j=0}^{p+\ell} E[\exp[tu_{j-\ell} v_j]] & 1-p \leq \ell < 0 \end{cases} \\ &= \prod_{j=0}^{p-|\ell|} \frac{1}{2}(\exp(t) + \exp(-t)) \\ &= (\cosh t)^{p-|\ell|}. \end{aligned} \quad (2.9)$$

Hence the first four moments of $C_{u,v}(\ell)$ are

$$\begin{aligned}
E\{C_{u,v}(\ell)\} &= \frac{\partial M_c(\tau)}{\partial \tau} \Big|_{\tau=0} = (p-|\ell|)(\cos h\tau)^{p-|\ell|-1} \sin h\tau \Big|_{\tau=0} = 0, \\
E\{C_{u,v}^2(\ell)\} &= \frac{\partial^2 M_c(\tau)}{\partial \tau^2} \Big|_{\tau=0} = 2 \binom{p-|\ell|}{2} (\cos h\tau)^{p-|\ell|-2} \sin^2 h\tau \Big|_{\tau=0} \\
&\quad + (p-|\ell|)(\cos h\tau)^{p-|\ell|-1} \cos h\tau \Big|_{\tau=0} = p-|\ell|. \quad (2.10)
\end{aligned}$$

In a similar manner,

$$E\{C_{u,v}^3(\ell)\} = \frac{\partial^3 M_c(\tau)}{\partial \tau^3} \Big|_{\tau=0} = 0$$

and

$$\begin{aligned}
E\{C_{u,v}^4(\ell)\} &= \frac{\partial^4 M_c(\tau)}{\partial \tau^4} \Big|_{\tau=0} = 4 \binom{p-|\ell|}{2} + \binom{p-|\ell|}{2} + (p-|\ell|) \\
&= 3(p-|\ell|)^2 - 2(p-|\ell|). \quad (2.11)
\end{aligned}$$

Furthermore, for $\ell \neq m$,

$$E\{C_{u,v}(\ell)C_{u,v}(m)/\ell < 0, m < 0\} = \sum_{j=0}^{p-1+\ell} \sum_{n=0}^{p-1+m} E\{u_j v_{j+\ell} u_n v_{n+m}\} = 0.$$

In fact, it is easy to show that

$$E\{C_{u,v}(\ell)C_{u,v}(m)\} = 0 \quad \forall \ell, \forall m, \ell \neq m$$

and

$$E\{C_{u,v}^3(\ell)C_{u,v}(m)\} = 0 \quad \forall \ell, \forall m, \ell \neq m$$

while

$$E\{C_{u,v}^2(l)C_{u,v}^2(m)\} = (p-|l|)(p-|m|) \quad \forall l, \forall m, l \neq m.$$

Above results enable us to calculate the mathematical expectation and the variance of the asynchronous interference Q_a as defined in (1.19).

First we obtain the first and second moment of the interference parameter $r(u,v)$.

$$\begin{aligned} E\{r(u,v)\} &= \sum_{l=1-p}^{p-1} E\{2C_{u,v}^2(l) + C_{u,v}(l)C_{u,v}(l+1)\} \\ &= \sum_{l=1-p}^{p-1} 2(p-|l|) \\ &= 2p^2 \end{aligned} \quad (2.12)$$

and

$$\begin{aligned} E\{r^2(u,v)\} &= E\left\{\sum_{l=1-p}^{p-1} 2C_{u,v}^2(l)\right\}^2 + E\left\{\sum_{l=1-p}^{p-1} C_{u,v}(l)C_{u,v}(l+1)\right\}^2 \\ &\quad + E\left\{2\sum_{l=1-p}^{p-1} 2C_{u,v}^2(l) \sum_{m=1-p}^{p-1} C_{u,v}(m)C_{u,v}(m+1)\right\}. \end{aligned} \quad (2.13)$$

Now

$$\begin{aligned} E\left\{\sum_{l=1-p}^{p-1} 2C_{u,v}^2(l)\right\}^2 &= 4E\left\{\sum_{l=1-p}^{p-1} C_{u,v}^2(l)\right\}^2 + 4E\left\{\sum_{l=1-p}^{p-1} \sum_{\substack{m=1-p \\ l \neq m}}^{p-1} C_{u,v}^2(l)C_{u,v}^2(m)\right\} \\ &= 4 \sum_{l=1-p}^{p-1} [3(p-|l|)^2 - 2(p-|l|)] \\ &\quad + 4 \left[\sum_{l=1-p}^{p-1} (p-|l|) \right]^2 - 4 \sum_{l=1-p}^{p-1} (p-|l|)^2 \\ &= 4p^4 + \frac{16}{3}p^3 - 8p^2 + \frac{8}{3}p \end{aligned} \quad (2.14)$$

and

$$\begin{aligned}
 E\left\{\sum_{\ell=1-p}^{p-1} C_{u,v}(\ell) C_{u,v}(\ell+1)\right\}^2 &= E\left\{\sum_{\ell=1-p}^{p-1} C_{u,v}^2(\ell) C_{u,v}^2(\ell+1)\right\} \\
 &+ E\left\{\sum_{\ell=1-p}^{p-1} \sum_{\substack{m=1-p \\ \ell \neq m}}^{p-1} C_{u,v}(\ell) C_{u,v}(\ell+1) C_{u,v}(m) C_{u,v}(m+1)\right\} \\
 &= \sum_{\ell=1-p}^{p-1} (p-|\ell|)(p-|\ell+1|) \\
 &= \frac{2}{3} p^3 - \frac{2}{3} p
 \end{aligned} \tag{2.15}$$

while

$$E\left\{2 \sum_{\ell=1-p}^{p-1} 2 C_{u,v}^2(\ell) \sum_{m=1-p}^{p-1} C_{u,v}(m) C_{u,v}(m+1)\right\} = 0 . \tag{2.16}$$

Hence, substituting (2.14), (2.15), and (2.16) into (2.13) gives

$$E\{r^2(u,v)\} = 4p^4 + 6p^3 - 8p^2 + 2p . \tag{2.17}$$

In a straightforward manner one obtains with (2.12)

$$\begin{aligned}
 EQ_a &= (6p^3)^{-1} E\left\{\sum_{\substack{k=1 \\ k \neq i}}^K r(u^{(i)}, u^{(k)})\right\} \\
 &= (6p^3)^{-1} (K-1) E\{r(u,v)\} \\
 &= (3p)^{-1} (K-1)
 \end{aligned} \tag{2.18}$$

while

$$\begin{aligned}\text{var}(Q_a) &= E(Q_a^2) - E^2 Q_a \\ &= (36p^6)^{-1}(K-1) \text{var}(r(u,v))\end{aligned}$$

thus

$$\text{var}(Q_a) = (36p^6)^{-1}(K-1)(6p^3 - 8p^2 + 2p)$$

and therefore

$$\text{var}(Q_a) \approx (6p^3)^{-1}(K-1) \quad (2.19)$$

for large sequence length p .

2.4. Asynchronous interference versus synchronous interference

A system is considered to be synchronous when the relative shift τ between the signature sequences equals zero. The RF-phases of the signal carriers, however, are still assumed to be independent random variables, uniformly distributed over the range $[0, 2\pi]$. The signal-to-noise ratio at the output of a correlation receiver, synchronized (frame and bit) with its own signature sequence equals

$$\text{SNR}_s = \left\{ \frac{N_0}{2E_b} + Q_s \right\}^{-1} \quad (2.20)$$

where the synchronous interference Q_s equals

$$Q_s = (2p^2)^{-1} \sum_{\substack{k=1 \\ k \neq 1}}^K r_s(u^{(1)}, u^{(k)}) \quad (2.21)$$

where $r_s(u, v) = C_{u,v}^2(0)$. Wolf and Elspas (1965) derived EQ_s and $\text{var}(Q_s)$

for random binary sequences,

$$EQ_s = (2p)^{-1}(K-1) \quad (2.22)$$

and

$$\text{var}(Q_s) = (2p^2)^{-1}(K-1). \quad (2.23)$$

Of course, in a practical synchronous system, one may want to consider an orthogonal set of signature sequences for which $C_{u,v}(0) = 0$, as long as the synchronization requirements can be met. From (2.18) and (2.22) we have the well-known result, reported by Harris (1973),

$$EQ_a = \frac{2}{3} EQ_s. \quad (2.24)$$

In addition, however, we have now also

$$\text{var}(Q_a) = (3p)^{-1} \left[1 - \frac{4}{3} p^{-1} + \frac{1}{3} p^{-2} \right] \text{var}(Q_s)$$

or

$$\text{var}(Q_a) \approx (3p)^{-1} \text{var}(Q_s) \quad (2.25)$$

for large sequence length p .

Let the asynchronous fluctuation ratio R_a be defined by

$$R_a = 10 \log_{10} \{ [EQ_a - \sqrt{\text{var}(Q_a)}]^{-1} [EQ_a + \sqrt{\text{var}(Q_a)}] \}. \quad (2.26)$$

The synchronous fluctuation ratio R_s is defined as in (2.26) with Q_a replaced by Q_s . Substitution of EQ_a and $\text{var}(Q_a)$ into (2.26) gives

$$R_a = 10 \log_{10} \{ [K-1-3(K-1)^{\frac{1}{2}}(6p)^{-\frac{1}{2}}]^{-1} [K-1+3(K-1)^{\frac{1}{2}}(6p)^{-\frac{1}{2}}] \} \quad (2.27)$$

while a similar substitution with EQ_s and $\text{var}(Q_s)$ gives

$$R_s = 10 \log_{10} \{ [K-1-(2(K-1))^{\frac{1}{2}}]^{-1} [K-1+(2(K-1))^{\frac{1}{2}}] \} \quad (2.28)$$

Expressions (2.27) and (2.28) indicate a rather small value of R_a if compared with R_s . Furthermore, R_s does not depend on the sequence length p but R_a decreases steadily when p increases. The graph in Figure 2 gives R_s and R_a as functions of K for a number of sequence length $p = 2^n - 1$. For example, with $K = 8$ and $p = 127$, $R_a = 0.36$ dB while $R_s = 5.1$ dB. It should be noted that a fluctuation of Q_a does not produce the same fluctuation in SNR_a . For example, with $10 \log_{10}(\mathcal{E}_b/N_0) = 10$ dB, a $\pm \sqrt{\text{var}(Q_a)}$ fluctuation of EQ_a results in an (approximately) ± 0.05 dB fluctuation of SNR_a while a $\pm \sqrt{\text{var}(Q_s)}$ fluctuation of EQ_s results in an (approximately) ± 0.85 dB fluctuation of SNR_s .

Thus, in the analysis and preliminary design of an asynchronous SSMA system, the approximation

$$\text{SNR}_a \approx \left\{ \frac{N_0}{2\mathcal{E}_b} + \frac{K-1}{3p} \right\}^{-1} \quad (2.29)$$

is very accurate for typical values of K , p and $\mathcal{E}_b/N_0$.

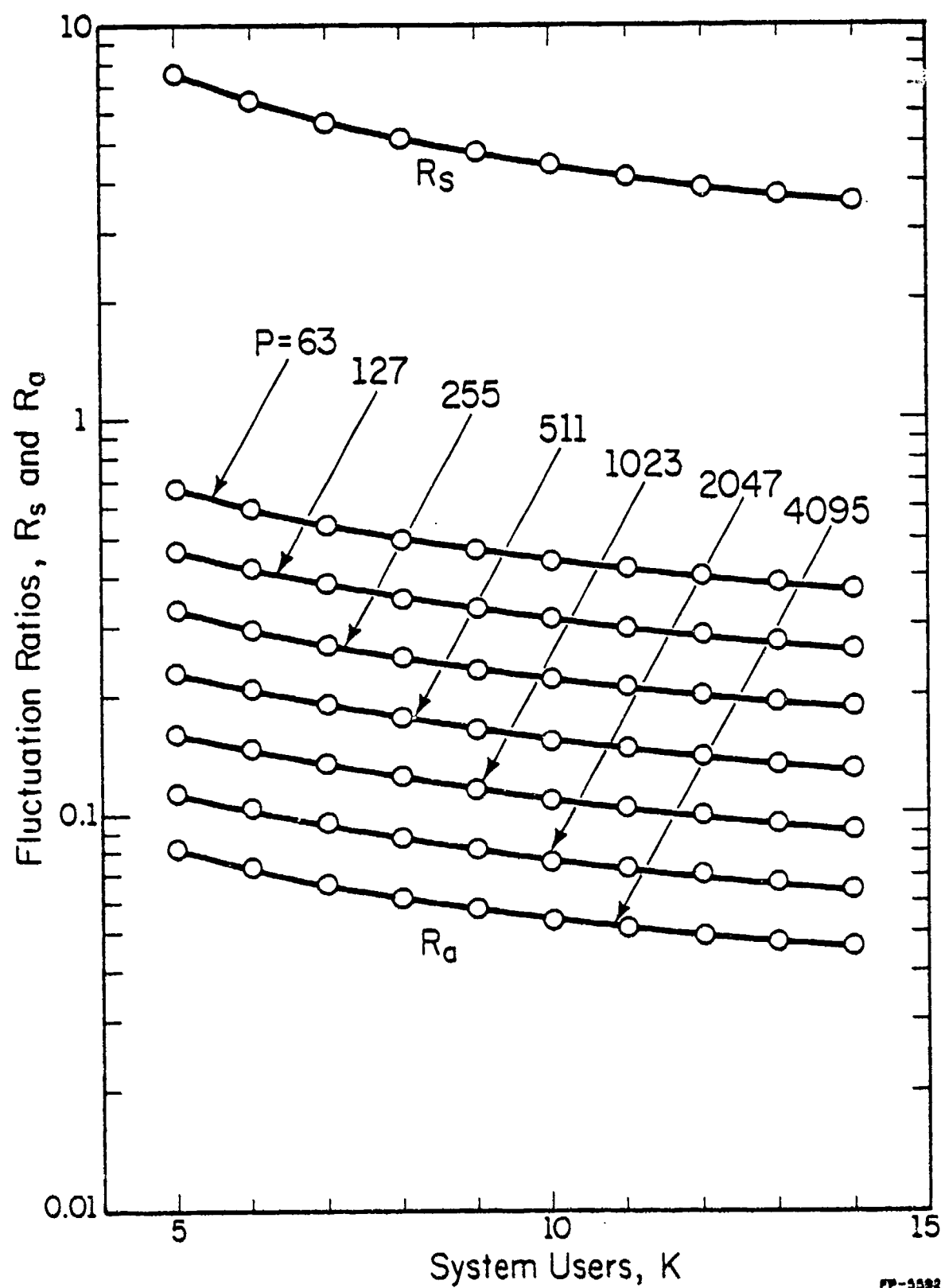


Figure 2. Asynchronous and synchronous fluctuation ratios R_a and R_s versus the number of system users K , for random binary sequences of length $p = 63$ through $p = 4095$.

CHAPTER 3

CORRELATION PARAMETERS OF M-SEQUENCES

In a practical spread spectrum multiple access system, the signature sequences will not be selected at random from the set of all possible sequences of a certain length p . The sequences must possess certain qualities, otherwise the SSMA system will not function properly. A large class of sequence with a number of interesting properties are the maximum-length shift register sequences or m-sequences. They have been studied extensively in the literature by Zierler (1959) and Golomb (1967) and others.

3.1. Introduction to m-sequences

It is convenient to distinguish in our notation between sequence elements $u_j \in \{-1, 1\}$ and sequence elements $\mu_j \in \{1, 0\}$ which are related by

$$u_j = (-1)^{\mu_j}. \quad (3.1)$$

A binary m-sequence μ of period $p = 2^n - 1$, is a sequence which satisfies a recurrence relation of the form

$$\mu_{j+n} = \sum_{i=1}^n f_i \mu_{j+n-i}, \quad j=0, 1, \dots \quad (3.2)$$

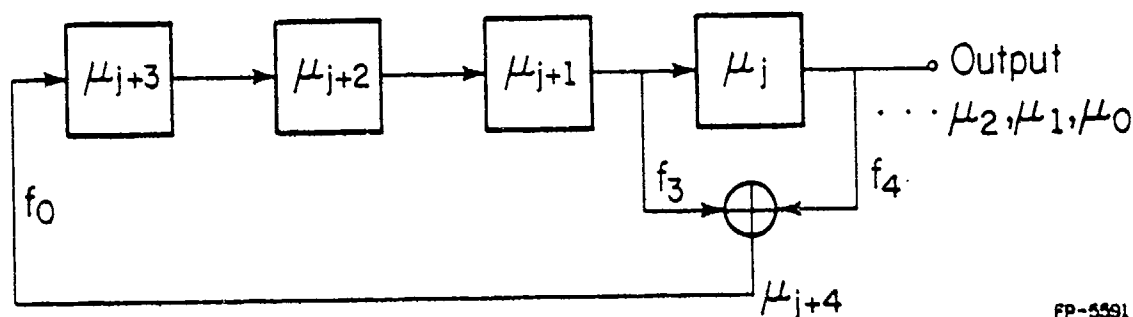
where

$$f(x) = f_0 x^n + f_1 x^{n-1} + \dots + f_{n-1} x + f_n$$

is a primitive polynomial of degree n over $GF(2)$, the binary alphabet $\{0, 1\}$ with addition modulo 2. A polynomial of degree n is primitive if it

divides $x^m - 1$ for $m = 2^n - 1$ but not for any $m < 2^n - 1$. The roots of a primitive polynomial of degree n are primitive elements of the extension field $GF(2^n)$, i.e., they have order $2^n - 1$, and every nonzero element of $GF(2^n)$ can be written as a power of some primitive element β . We denote the minimal polynomial which has β^q as a root by $f_q(x)$. Peterson and Weldon (1972) give extensive tables of primitive polynomials up to degree 34.

Polynomial $f(x)$ represents an n -stage linear feedback shift register where $f_0 = f_n = 1$ and for $0 < i < n$, $f_i = 1$ if there is a feedback tap connected to the i^{th} stage of the register and $f_i = 0$ if not. An example of a shift register represented by $f(x) = x^4 + x + 1$ is given in Figure 3.



FP-5591

Figure 3. Shift register for $f(x) = x^4 + x + 1$; $p = 15$.

Let Tu denote the left cyclic shift of sequence u , i.e.,

$$Tu = T(u_0, u_1, \dots, u_{p-1}) = (u_1, u_2, \dots, u_{p-1}, u_0).$$

Of course, $T\mu$ is equivalent with Tu . Notice that equation (3.2) implies

$$T^n \mu + f_1 T^{n-1} \mu + \dots + f_{n-1} T \mu + \mu = \underline{0} \quad (3.3)$$

where $\underline{0}$ denotes the all-zero sequence.

Let $\text{tr}(x)$ denote the trace of x , defined by

$$\text{tr}(x) = x + x^2 + \dots + x^{2^{n-1}}. \quad (3.4)$$

Then for each nonzero element ψ in $GF(2^n)$, there exists a solution μ of the recurrence relation (3.2) specified by

$$\mu_j = \text{tr}(\psi \beta^j). \quad (3.5)$$

A proof can be found in Lint (1973). The various solutions $\mu, \mu \neq 0$, of (3.2) are simply shifted versions of each other; i.e., the sequences $\mu, T\mu, T^2\mu, \dots, T^{p-1}\mu$ are in the same equivalence class with respect to shift operator T ; μ is called the cycle representative. The m -sequence corresponding to $\psi = 1$ satisfies the important property

$$\mu_j = \mu_{2j}, \quad \forall j \quad (3.6)$$

and is said to be in its natural orientation or characteristic form.

Henceforth μ (or u) denotes the m -sequence in its natural orientation.

Furthermore, $T^k \mu$ corresponds with $\psi = \beta^k$. For each degree n , up to $n = 168$, Willett (1976) has computed the characteristic form of one m -sequence.

Let v be any other m -sequence of the same length as μ . Suppose v satisfies a recurrence relation specified by $f_q(x)$ and let v be in its natural orientation, then

$$v_j = u_{qj}, \quad \forall j. \quad (3.7)$$

Equation (3.7) implies that the characteristic m-sequence v can readily be determined from the characteristic m-sequence u . Table 1 gives all characteristic m-sequences up to and including length $p = 255$. The primitive polynomials $f(x)$ are denoted in the usual octal notation, for example

$$\begin{aligned} f(x) &= x^4 + x + 1 = 0.x^5 + 1.x^4 + 0.x^3 + 0.x^2 + 1.x + 1 \\ &\equiv [0 \ 1 \ 0 \ 0 \ 1 \ 1] \equiv 0 \ 2 \ 3. \end{aligned}$$

The initial start position or loading of the shift register is also denoted in octal notation

$$\mu = (\mu_0, \mu_1, \dots) = (0, 0, 0, 1, 0, 0, \dots) \equiv 0 \ 4 \ 6 \ 5.$$

Of course the last two digits of 0465 are here redundant. Henceforth, all loading of shift registers will be given in octal notation except when indicated otherwise, by means of an asterisk, e.g., as in Table 4.

3.2. The trinomial structure of m-sequences

Another important property of m-sequence μ is the so called shift - and - add property, i.e.,

$$\mu_{j+r} = \mu_{j+l} + \mu_j, \quad \forall j \quad (3.8)$$

for some r and $l \neq 0$. In terms of the corresponding m-sequence u over $\{+1, -1\}$, equation (3.8) becomes $u_{j+r} = u_{j+l}u_j$ for some r and $l \neq 0$,

Table 1. Characteristic m-sequences of length $p = 15, 31, 63, 127$ and 255 .

	Poly.	Loading	Poly.	Loading
$p = 15$	023	0465	031	3654
$p = 31$	045 075 067	4547 7670 7211	051 057 073	4127 4460 7316
$p = 63$	103 147 155	0103 3753 3313	141 163 133	3752 3210 0441
$p = 127$	211 217 235 367 277 325 203 313 345	4021 4126 4543 7671 4441 7337 4020 7655 7214	221 361 271 357 375 253 301 323 247	4464 7756 4566 7313 7757 4024 7752 7230 4103
$p = 255$	435 551 747 453 545 543 703 765	0107 0445 3773 0566 3216 0546 3317 3650	561 455 717 651 515 615 607 537	0543 0543 3234 3316 1455 3670 3772 0106

which will be used extensively in Chapter 4. Equation (3.8) can also be expressed in terms of the cyclic shift operator T ,

$$T^{r(l)}\mu + T^l\mu + \mu = \underline{0}. \quad (3.9)$$

Recall that m -sequence μ already satisfies a recurrence relation as in (3.2), specified by a minimal polynomial $f(x)$. Hence (3.9) specifies for each $l \neq 0$ a binary trinomial of the form

$$x^{r(l)} + x^l + 1 \quad (3.10)$$

which should be divisible by $f(x)$.

Let η_x denote the cyclotomic coset of integers $x' \bmod p$ containing x as smallest element, i.e.,

$$\eta_x = \{x' : x' = 2^j x \bmod p, x \leq x' ; j = 0, 1, \dots\}. \quad (3.11)$$

In some cases η_x will be denoted as $[x]$ or x if so indicated. The cyclotomic cosets of integers modulo p , up to $p = 255$ are tabulated in Table 2. On each horizontal line a coset and its reciprocal are grouped together, whenever such a reciprocal exists.

The trinomials in (3.10) have algebraic properties which considerably reduce the effort of finding $r(l)$ for each value of l . Most important is the property that whenever $l \in \eta_x$ and $l' \in \eta_x$, then $r(l) \in \eta_y$ and $r(l') \in \eta_y$, for some x and y . For example, this can be observed from Table 3 where the trinomials $x^{r(l)} + x^l + 1$, divisible by $f(x) = x^4 + x + 1$, are tabulated. A more detailed discussion on trinomials can be found in Lindholm (1968). In Chapter 4 and 5 we will use the trinomial structure of the m -sequences extensively.

Table 3. Trinomials $x^{r(l)} + x^l + 1$ divisible by $f(x) = x^4 + x + 1$

$x^4 + x + 1$	$x^{13} + x^6 + 1$	$x^{12} + x^{11} + 1$
$x^8 + x^2 + 1$	$x^9 + x^7 + 1$	$x^{11} + x^{12} + 1$
$x^{14} + x^3 + 1$	$x^2 + x^8 + 1$	$x^6 + x^{13} + 1$
$x + x^4 + 1$	$x^7 + x^9 + 1$	$x^3 + x^{14} + 1$
$x^{10} + x^5 + 1$	$x^5 + x^{10} + 1$	

3.3. Autocorrelation functions

The autocorrelation function of a signature sequence plays a key role in obtaining word synchronization in the correlation receiver and in reducing the effects of multipath interference. The periodic autocorrelation function $\theta_u(\tau) = -1$ for all $\tau \neq 0 \bmod p$ for m-sequences is nearly ideal in this respect and one of the main advantages of m-sequences. Of course ease of generation is another advantage.

While thus $\theta_{\max}(T^k u) = 1$, $\forall k$ for m-sequences, the companion parameter $\hat{\theta}_{\max}(T^k u)$ defined in (1.13) is very sensitive to the selected cyclic shift T^k of u . To find cyclic shifts for which $\hat{\theta}_{\max}(T^k u)$ is minimal, a computer search is required. In the process of searching the best T^k , a number of ties may occur (i.e., a number of different values of k in T^k result in the same minimal $\hat{\theta}_{\max}(T^k u)$). Hence, a second condition is applied to the already selected values of k reducing the number of ties considerably. The second condition is stated in the following definition which is due to Massey and Uffner (1969).

Definition 1. An m-sequence $u' = T^{k'} u$ is auto-optimal (AO) -- with respect to $\hat{\theta}_{\max}(T^k u)$ -- when the following conditions are satisfied in successive order:

a) $\hat{\theta}_{\max}(u') \leq \hat{\theta}_{\max}(T^k u), \forall k$

b) The cardinality $\hat{L}_a$ of the set

$$\{l: |\hat{\theta}_{u'}(l)| = \hat{\theta}_{\max}(u'); 0 < l \leq p-1\}$$

is smallest for sequence u' .

Observation: It follows immediately from this definition that an auto-optimal m-sequence generated by primitive polynomial $f(x)$ of degree n has a reciprocal -- generated by $f'(x) = x^n f(1/x)$ -- which is AO too.

Table 4 specifies for each primitive polynomial of degree $n = 7$, the loading or start position $u_0, u_1, \dots, u_6$ of the shift register such that the generated m-sequence is AO. There are two distinct cyclic shifts of the m-sequence generated by $f(x) = x^7 + x + 1$ (203), both which are AO. They are indicated as 203a and 203b. Then, the reciprocal polynomial $f(x) = x^7 + x^6 + 1$ (301) will generate two distinct AO m-sequences too. The resulting values of $\hat{\theta}_{\max}(u)$ and $\hat{L}_a$ for u' are as indicated.

Clearly, there is not one unique set of eighteen auto-optimal m-sequences of length $p = 127$ as was reported by Massey and Ufran (1969). Table 4 shows that a total of four distinct sets of eighteen m-sequences each can be selected by choosing two m-sequences, which are not cyclic shifts of each other, from the set {203a, 203b, 301a, 301b}. Furthermore, the auto-optimal m-sequences of Massey and Ufran do not seem to be reciprocal pairs.

Table 4. Auto-optimal m-sequences of length $p = 127$.

Poly.	Loading*	Poly.	Loading*	$\hat{\theta}_{\max}(u)$	$\hat{L}_a$	$S(u)$
211	0010000	221	1001101	17	6	2183
217	0000101	361	1111111	15	12	2015
235	0001100	271	1000101	17	10	2283
247	0010111	345	0110001	17	8	2255
277	1110001	375	0101010	19	4	2295
357	1110010	367	0110101	17	4	2563
323	1110111	313	1000111	17	4	2203
203a	1101101	301a	0010010	17	4	2087
203b	0000001	301b	1111111	17	4	2403
325	0000101	253	1101100	19	6	2483

The sidelobe energy parameter $S(u)$, as defined in (1.24) can also be used as a sieve for m-sequences. In particular, we might use $S(u)$ to further distinguish between AO m-sequences, because for m-sequences,

$$\hat{M}(u) = \sum_{\ell=1}^{p-1} \hat{\theta}_u^2(\ell) = 4 S(u) - p + 1 \quad (3.12)$$

one of the important parameters in the direct sequence SSMA system. Hence, it is convenient to extend the definition of auto-optimality further by including $S(u)$ as a next sieve.

Definition 2. An m-sequence $U = T^{k^*} u$ is indicated as AO/LSE whenever U is auto-optimal and has lowest sidelobe energy $S(U)$ among all auto-optimal shifts of u .

When the m-sequences generated by polynomials 203b and 301b are deleted from Table 4, the table will give the AO/LSE m-sequences of length $p = 127$.

3.4. Periodic cross-correlation of m-sequences; Golomb's theorem

Let u and v be characteristic m-sequences generated by the primitive polynomials $f_1(x)$ and $f_q(x)$ respectively. Both m-sequences are constant over cyclotomic cosets, i.e.,

$$u_j = u_{2j} = \chi(\eta_i) \quad \text{for } j \in \eta_i \quad (3.13)$$

and
$$v_j = v_{2j} = \chi(\eta_{qi}) \quad \text{for } j \in \eta_{qi} \quad (3.14)$$

where

$$\chi(\eta_{qi}) = (-1)^{\text{tr}(\beta^{qi})} \quad (3.15)$$

The periodic cross-correlation $\theta_{u,v}(\tau)$ is also constant over cyclotomic cosets, i.e.,

$$\theta_{u,v}(\tau') = \theta_{u,v}(2\tau') \triangleq \theta_{u,v}(\eta_\tau), \quad \tau' \in \eta_\tau \quad (3.16)$$

Gold and Kopitzke (1965) have computed the periodic cross-correlation $\theta_{u,v}(\tau)$ for m-sequences of length $p \leq 8191$. The same data can be obtained by means of an elegant theorem of Golomb (1968), which is derived as follows.

The Gauss' product of cyclotomic cosets η_x and η_y is defined as

$$\eta_x \eta_y = \{(s+t) \bmod p : s \in \eta_x, t \in \eta_y\} \quad (3.17)$$

Hence, one can write the following equality

$$\sum_{s \in \eta_x} \sum_{t \in \eta_y} (-1)^{\text{tr}(\beta^{s+t})} = \sum_{r \in \eta_x \eta_y} (-1)^{\text{tr}(\beta^r)} \quad (3.18)$$

Let $|\eta_x|$ denote the cardinality of cyclotomic coset η_x . Then, from the definition of $\theta_{u,v}(\tau)$, equations (3.15), (3.16) and (3.18), one obtains Golomb's

Theorem 1:
$$\theta_{u,v}(\eta_\tau) = \frac{1}{\|\eta_\tau\|} \sum x_u(\eta_{-\tau}\eta_i) x(\eta_{qi}) \quad (3.19)$$

where
$$x_u(\eta_x \eta_y) = \sum_{r \in \eta_x \eta_y} (-1)^{\text{tr}(\beta^r)} \quad (3.20)$$

and the sum in (3.19) is over all the integers i which represent distinct cyclotomic cosets η_i . Expression (3.19) represents a multiplication of a vector

$$\underline{x}_q = (x(\eta_{qi}))_i \quad (3.21)$$

of 'coset assignments' to m -sequence v , and the normalized matrix

$$\underline{x}_u = \left[\frac{1}{\|\eta_x\|} x_u(\eta_x \eta_y) \right] . \quad (3.22)$$

In order to obtain $\underline{x}_u$ for some m -sequence u of period p one needs the array of Gauss' cyclotomic coset products $\{\eta_x \eta_y\}$. Golomb (1963) specified $\{\eta_x \eta_y\}$ for $p = 15$ -- here reproduced in Table 5 -- and $p = 31$; we present $\{\eta_x \eta_y\}$ for $p = 63$ in Table 6, where η_x is indicated by $[x]$.

An example of Golomb's theorem

Let u and v be m -sequences of length $p = 15$ generated by the polynomials $f_1(x) = x^4 + x + 1$ (023) and $f_7(x) = x^4 + x^3 + 1$ respectively. The cyclotomic cosets are $\eta_0 = \{0\}$, $\eta_1 = \{1, 2, 4, 8\}$, $\eta_3 = \{3, 6, 12, 9\}$, $\eta_5 = \{5, 10\}$ and $\eta_7 = \{7, 14, 13, 11\}$. The vectors of coset assignments to m -sequences u and v are

$$\begin{aligned} \underline{x}_1 &= (x(\eta_0), x(\eta_1), x(\eta_3), x(\eta_5), x(\eta_7)) \\ &= (1, 1, -1, 1, -1) \end{aligned}$$

Table 5. Gauss' products of cyclotomic cosets; $p = 15$

	η_0	η_1	η_3	η_5	η_7
η_0	η_0	η_1	η_3	η_5	η_7
η_1	η_1	$\eta_1 + 2\eta_3 + 2\eta_5$	$\eta_1 + 2\eta_5 + 2\eta_7$	$\eta_3 + \eta_7$	$4\eta_0 + \eta_1 + \eta_3 + \eta_7$
η_3	η_3	$\eta_1 + 2\eta_5 + 2\eta_7$	$4\eta_0 + 3\eta_3$	$\eta_1 + \eta_7$	$2\eta_1 + 2\eta_5 + \eta_7$
η_5	η_5	$\eta_3 + \eta_7$	$\eta_1 + \eta_7$	$2\eta_0 + \eta_5$	$\eta_1 + \eta_3$
η_7	η_7	$4\eta_0 + \eta_1 + \eta_3 + \eta_7$	$2\eta_1 + 2\eta_5 + \eta_7$	$\eta_1 + \eta_3$	$2\eta_3 + 2\eta_5 + \eta_7$

and

$$\underline{x}_7 = (x(\eta_0), x(\eta_7), x(\eta_3), x(\eta_5), x(\eta_1))$$

$$= (1, -1, -1, 1, 1) .$$

Evaluation of the Gauss' products $\{\eta_x \eta_y\}$ in Table 5 with (3.20) and (3.22) results in the matrix

$$\underline{x}_{\underline{u}} = \begin{bmatrix} 1 & 4 & -4 & 2 & -4 \\ 1 & 0 & 0 & -2 & 0 \\ -1 & 0 & -2 & 0 & 2 \\ 1 & -4 & 0 & 2 & 0 \\ -1 & 0 & 2 & 0 & -2 \end{bmatrix} . \quad (3.23)$$

Multiplication of $\underline{x}_{\underline{u}}$ and $\underline{x}_7$ results in a vector

$$\underline{\theta}_{\underline{u}, \underline{v}}(\eta_{-\underline{r}}) = (-1, -1, 3, 7, -5)$$

Table 6. Gauss' products of cyclotomic cosets, $[x] \equiv \eta_x$; $p = 63$.

	[0]	[1]	[3]	[5]	[7]	[9]	[11]
[0]			[3]	[5]	[7]	[9]	[11]
[1]		[1]	[3]	[5]	[7]	[9]	[11]
[3]		[1]+2[3] +2[5]+2[9]	[1]+2[7] +([11]+[13])+[5]	[3]+[7]+2[9] +([11]+[13])+3[21]	[1]+2[9]+2[15] +([11]+[23])	[5]+([11]+[13])	[3]+2[13]+[15] +2[23]+2[27]
[5]		[1]+2[7]+[11] +([13])+[5]	[3]+[9] +2[15]+2[27]	[1]+[5]+[11] +([13])+2[23]	2[5]+2[13]+2[31]	[3]+3[21]+[15]	[5]+2[7]+[11] +2[23]+[31]
[7]		[3]+[7]+2[9] +([11])+[13]+3[21]	[1]+[5]+[11] +([13])+2[23]	[5]+2[11]+2[15] +2[27]	2[3]+[15]+[13] +2[27]+[31]	[7]+[13]+[23]	[1]+[7]+3[21] +2[27]+[31]+[15]
[9]		[1]+2[9]+2[15] +([11])+[23]	2[5]+2[13] +2[31]	2[3]+[15]+[13] +2[27]+[31]	6[0]+3[7]+6[21]	[1]+[11]+[23]	[1]+[11]+[23] +2[9]+2[15]
[11]		[5]+([11])+[13]	[3]+3[21]+[15]	[7]+[13]+[23]	[1]+[11]+[23]	[9]+2[27]	[5]+[23]+[31]
[13]		[3]+2[13]+[15] +2[23]+2[27]	[5]+2[7]+[11] +2[23]+[31]	[1]+[7]+3[21] +2[27]+[31]+[15]	[1]+[11]+[23] +2[9]+2[15]	[5]+[23]+[31]	2[3]+2[9]+[11] +2[31]
[15]		[5]+[7]+[13] +([15])+3[21]+[23]	2[11]+[1]+[13] +2[23]+[31]	[3]+[15]+[31] +2[9]+2[23]	2[3]+[5]+[13] +2[27]+[31]	[7]+[11]+[31]	6[0]+[3]+[7] +([11]+[13])+[15]
[21]		[1]+2[31]+[5] +([13])+[23]	6[0]+[3]+2[9] +([15])+3[21]+2[27]	[1]+2[7]+[5] +([11])+[31]	2[1]+2[11]+2[23]	[15]+2[3]	[1]+[11]+[5] +2[13]+[31]
[23]		[11]+[23]	[3]+2[27]	[13]+[31]	2[7]	[15]	[1]+[23]
[27]		[3]+([11])+[15] +2[27]+2[31]	[1]+2[7]+[13] +2[23]+[31]	6[0]+[3]+[5] +([7]+[15])+[23]	[1]+2[9]+[11] +2[15]+[23]	[1]+[13]+[31]	[1]+[3]+[15] +2[27]+2[5]
[31]		[7]+[31]+[23]	[3]+2[15]	[11]+[1]+[31]	[5]+[13]+[31]	3[0]+[9]+[27]	[1]+[7]+[13]
		[1]+6[0]+[3] +([7]+[15])+[31]	2[1]+[5]+[11] +2[23]+[31]	2[1]+[3]+[13] +2[9]+[15]	2[3]+[5]+[13] +2[27]+[31]	[1]+[5]+[7]	[3]+2[9]+[23] +3[21]+[7]+[15]

Table 6. (continued).

	[13]	[15]	[21]	[23]	[27]	[31]
[0]	[13]	[15]	[21]	[23]	[27]	[31]
[1]	$(5) \cdot (7) \cdot (13) \cdot (15) \cdot 3(21) \cdot (23)$	$(1) \cdot 2(31) \cdot (5) \cdot (13) \cdot (23)$	$(11) \cdot (23)$	$(3) \cdot (11) \cdot (15) \cdot 2(27) \cdot 2(31)$	$(7) \cdot (31) \cdot (23)$	$(1) \cdot 6(0) \cdot (3) \cdot (7) \cdot (15) \cdot (31)$
[3]	$2(11) \cdot (1) \cdot (13) \cdot 2(23) \cdot (31)$	$6(0) \cdot (3) \cdot 2(9) \cdot (15) \cdot 3(21) \cdot 2(27)$	$(3) \cdot 2(27)$	$(1) \cdot 2(7) \cdot (13) \cdot (23) \cdot (31)$	$(3) \cdot 2(15)$	$2(1) \cdot (5) \cdot (11) \cdot (23) \cdot (31)$
[5]	$(3) \cdot (15) \cdot (31) \cdot 2(9) \cdot 2(23)$	$(1) \cdot 2(7) \cdot (5) \cdot (11) \cdot (31)$	$(13)(31)$	$6(0) \cdot (3) \cdot (5) \cdot (7) \cdot (15) \cdot (23)$	$(1) \cdot (11) \cdot (31)$	$2(1) \cdot (3) \cdot (13) \cdot 2(9) \cdot (15)$
[7]	$2(3) \cdot (5) \cdot (13) \cdot 2(27) \cdot (31)$	$2(1) \cdot 2(11) \cdot 2(23)$	$2(7)$	$(1) \cdot 2(9) \cdot (11) \cdot 2(15) \cdot (23)$	$(5) \cdot (13) \cdot (31)$	$2(3) \cdot (5) \cdot (13) \cdot 2(27) \cdot (31)$
[9]	$(7) \cdot (11) \cdot (31)$	$(15) \cdot 2(3)$	[15]	$(1) \cdot (13) \cdot (31)$	$3(0) \cdot (9) \cdot (27)$	$(1) \cdot (15) \cdot (7)$
[11]	$6(0) \cdot (3) \cdot (7) \cdot (11) \cdot (13) \cdot (15)$	$(1) \cdot (11) \cdot (5) \cdot 2(13) \cdot (31)$	$(1) \cdot (23)$	$(1) \cdot (3) \cdot (15) \cdot 2(27) \cdot 2(5)$	$(1) \cdot (7) \cdot (13)$	$(3) \cdot 2(9) \cdot (23) \cdot (5) \cdot (7) \cdot 3(21)$
[13]	$2(1) \cdot 2(15) \cdot 2(27) \cdot (13)$	$(1) \cdot 2(7) \cdot (5) \cdot (13) \cdot (23)$	$(5) \cdot (31)$	$(1) \cdot (3) \cdot (7) \cdot 2(9) \cdot 3(21) \cdot (31)$	$(1) \cdot (5) \cdot (23)$	$(3) \cdot (5) \cdot (15) \cdot 2(9) \cdot 2(11)$
[15]	$(1) \cdot 2(7) \cdot (5) \cdot (13) \cdot (23)$	$2(3) \cdot 4(27) \cdot 2(9) \cdot (15)$	$2(9) \cdot (15)$	$2(5) \cdot (11) \cdot (13) \cdot 2(23) \cdot (31)$	$3(21) \cdot (3) \cdot (15)$	$2(7) \cdot (11) \cdot (13) \cdot 2(23) \cdot (31)$
[21]	$(5) \cdot (31)$	$2(9) \cdot (15)$	$2(0) \cdot (21)$	$(1) \cdot (11)$	[3]	$(5) \cdot (13)$
[23]	$(1) \cdot (3) \cdot (7) \cdot 2(9) \cdot 3(21) \cdot (31)$	$2(5) \cdot (11) \cdot (13) \cdot 2(23) \cdot (31)$	$(1) \cdot (11)$	$(23) \cdot 2(3) \cdot 2(13) \cdot 2(9)$	$(5) \cdot (7) \cdot (11)$	$(7) \cdot (11) \cdot (13) \cdot (15) \cdot 3(21) \cdot 2(27)$
[27]	$(1) \cdot (5) \cdot (23)$	$3(21) \cdot (3) \cdot (15)$	[3]	$(5) \cdot (7) \cdot (11)$	$2(9) \cdot (27)$	$(11) \cdot (13) \cdot (23)$
[31]	$(3) \cdot (5) \cdot (15) \cdot 2(9) \cdot 2(11)$	$2(7) \cdot (11) \cdot (13) \cdot 2(23) \cdot (31)$	$(5) \cdot (13)$	$(7) \cdot (11) \cdot (13) \cdot (15) \cdot 3(21) \cdot 2(27)$	$(11) \cdot (13) \cdot (23)$	$(11) \cdot 2(15) \cdot 2(27) \cdot (31) \cdot (23)$

or alternatively

$$\theta_{u,v}(\tau) = \begin{cases} -1 & \text{if } \tau \in \eta_0 \\ -5 & \text{if } \tau \in \eta_1 \\ 3 & \text{if } \tau \in \eta_3 \\ 7 & \text{if } \tau \in \eta_5 \\ -1 & \text{if } \tau \in \eta_7 \end{cases} \quad (3.24)$$

Whenever two m-sequences, say w and z are decimations of the m-sequences u and v respectively such that $w_j = u_{sj}$ and $z_j = v_{sj}$, then

$$\theta_{w,z}(\tau) = \sum_{j=0}^{p-1} u_{sj} v_{sj+s\tau} = \theta_{u,v}(s\tau) \quad (3.25)$$

Hence, to obtain all periodic cross-correlation values for the m-sequences of a certain length p , it suffices to determine one matrix X_u . For $p = 15$ and $p = 31$, a matrix X_u is given in (3.23) and in Golomb (1968) respectively. Table 7 and 8 specify a matrix X_u obtained by evaluating the Gauss' products of cyclotomic cosets for the indicated m-sequences of length $p = 63$ and $p = 127$.

We will encounter Gauss' product of cyclotomic cosets in combination with Golomb's theorem again in Chapter 5 where the periodic cross-correlation of Gold sequences and Kasami sequences are discussed.

3.5. Maximal connected sets

Gold and Kopitzke (1965) obtained from their data, sets of m-sequences of period p , called maximal connected sets, which are the largest possible subsets of m-sequences for which any two sequences in the same set have a preferred three-valued periodic cross-correlation

Table 7. Gauss' products of cyclotomic cosets evaluated for
m-sequence u with octal polynomial 103; p = 63.

	0	1	3	5	7	9	11	13	15	21	23	27	31
χ_u	1	6	6	-6	6	3	-6	6	-6	-2	-6	3	-6
	1	2	2	2	-2	-1	2	-2	-2	-2	-2	-1	2
	1	2	2	-2	-2	-1	-2	-2	2	2	2	-1	-2
	-1	2	-2	-4	2	1	0	-2	0	0	0	-1	4
	1	-2	-2	2	2	-1	-2	2	-2	2	-2	-1	2
	1	-2	-2	2	-2	3	-6	-2	2	-2	2	3	2
	-1	2	-2	0	-2	-3	0	2	0	0	0	3	0
	1	-2	-2	-2	2	-1	2	2	2	-2	2	-1	-2
	-1	-2	2	0	-2	1	0	2	4	0	-4	-1	0
	-1	-6	6	0	6	-3	0	-6	0	0	0	3	0
	-1	-2	2	0	-2	1	0	2	-4	0	4	-1	0
	1	-2	-2	-2	-2	3	6	-2	-2	2	-2	3	-2
	-1	2	-2	4	2	1	0	-2	0	0	0	-1	-4

Table 8. Gauss' products of cyclotomic cosets evaluated for
m-sequence u with octal polynomial 211; p = 127.

	0	1	3	5	7	9	11	13	15	19	21	23	27	29	31	43	47	55	63
χ_u	-1	7	7	7	-7	7	-7	7	-7	-7	-7	-7	-7	7	-7	7	7	-7	7
	1	7	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	7	-1	-1	-1	-1
	1	-1	-1	3	-1	-1	-1	-1	3	-5	3	3	-1	3	-1	-5	-1	-1	3
	1	-1	3	-1	3	-5	-5	-1	3	3	-1	-1	-1	-1	-1	3	-1	-1	3
	-1	-1	-1	3	1	-1	1	-1	-3	5	-3	-3	1	3	1	-5	-1	1	3
	1	-1	1	-5	-1	3	3	-1	3	-1	-5	-1	3	-1	-1	-1	3	-1	3
	-1	-1	-1	-5	1	3	-3	-1	-3	1	5	1	-3	-1	1	-1	3	1	3
	1	-1	-1	-1	-1	-1	-1	7	-1	-1	-1	-1	-1	-1	-1	-1	-1	7	-1
	-1	-1	3	3	-3	3	-3	-1	1	1	-3	5	1	-5	1	-1	-1	1	-1
	-1	-1	-5	3	5	-1	1	-1	1	-3	-3	1	-3	-1	1	3	3	1	-1
	-1	-1	3	-1	-3	-5	5	-1	-3	-3	1	1	1	-1	1	3	-1	1	3
	-1	-1	3	-1	-3	-1	1	-1	5	1	1	-3	-3	3	1	-1	3	1	-5
	-1	-1	-1	-1	1	3	-3	-1	1	-3	1	-3	5	3	1	3	-5	1	-1
	1	-1	3	-1	3	-1	-1	-1	-5	-1	-1	3	3	3	-1	-1	3	-1	-5
	-1	7	-1	-1	1	-1	1	-1	1	1	1	1	1	-1	-7	-1	-1	1	-1
	1	-1	-5	3	-5	-1	-1	-1	-1	3	3	-1	3	-1	-1	3	3	-1	-1
	1	-1	-1	-1	-1	3	3	-1	-1	3	-1	3	-5	3	-1	3	-5	-1	-1
	-1	-1	-1	-1	1	-1	1	7	1	1	1	1	1	-1	1	-1	-1	-7	-1
	1	-1	3	3	3	3	3	-1	-1	-1	3	-5	-1	-5	-1	-1	-1	-1	-1

function, i.e., $\theta_{u,v}(\tau)$ takes on the values $-2^{\lfloor (n+2)/2 \rfloor - 1}$, $2^{\lfloor (n+2)/2 \rfloor - 1}$ and -1 only. Any pair of primitive polynomials which yields a sequence pair with a preferred three-valued periodic cross-correlation is called a preferred pair of polynomials as discussed in Pursley (1976). Clearly, for preferred pairs of polynomials, which generate m-sequences u and v , the peak parameter $\theta_{\max}(u,v)$ defined in (1.8) equals

$$\theta_{\max}(u,v) = 2^{\lfloor (n+2)/2 \rfloor} + 1.$$

For example, the first six polynomials in Table 4 form a maximal connected set S of six m-sequences of the same length $p = 127$ for which

$$\theta_c = \max\{\theta_{\max}(u,v) : u \in S, v \in S\} = 1 + 2^{\lfloor (6+2)/2 \rfloor} = 17.$$

Other m-sequences of length $p = 127$, not maximal connected, can form pairs with correlation peak values as high as $\theta_{\max}(u,v) = 41$. The size of a maximal connected set of m-sequences is rather small. In fact all sets have a cardinality less or equal to six for $p \leq 4095$ while in some cases, such as for $n \equiv 0 \pmod{4}$, the cardinality is zero.

In a first analytical result, Gold (1967) established a bound on $\theta_{\max}(u,v)$ as a function of u and v .

Theorem 2: Let $f_1(x)$ be a primitive polynomial of degree n and let β be a root of $f_1(x)$ in $GF(2^n)$. If $f_t(x)$ is the minimal polynomial of β^t where $t = 2^{\lfloor (n+2)/2 \rfloor} + 1$, then $\theta_{\max}(u,v) \leq t$ for the sequences generated by $f_1(x)$ and $f_t(x)$.

Notice that $f_t(x)$ does not have to be primitive. Theorem 2 is a special case of more general results obtained by Kasami (1966) for a

large number of values $t = 2^h + 1$. One such a result is

Theorem 3: Let $f_1(x)$ as in Theorem 2 and $f_t(x)$ is the minimal polynomial of $f_t(x)$ where $t = 2^h + 1$ and $0 < h < n$. Let c denote the greatest common divisor of the integers n and h . If n/c is odd then $\theta_{u,v}(\tau) = -1$ for $2^n - 2^{n-c} - 1$ values of τ , $\theta_{u,v}(\tau) = -1 - 2^{(n+c)/2}$ for $2^{n-c-1} - 2^{(n-c-2)/2}$ values of τ and $\theta_{u,v}(\tau) = -1 + 2^{(n+c)/2}$ for $2^{n-c-1} + 2^{(n-c-2)/2}$ values of τ .

A more complete discussion is given by Pursley (1976). The results of Gold and Kasami form a basis for the construction of large sets of sequences with good periodic correlation properties and are discussed in Chapter 5.

3.6. Aperiodic correlation functions

From the analysis of the direct sequence SSMA system as presented in Chapter 1, it is clear that the odd cross-correlation function $\hat{\theta}_{u,v}(\ell)$, as defined in (1.6) is as important as $\theta_{u,v}(\ell)$. As shown in sections 3.4 and 3.5, $\theta_{u,v}(\ell)$ displays certain regularities as a function of ℓ and the polynomials $f(x)$ which generate u and v . The odd cross-correlation $\hat{\theta}_{u,v}(\ell)$, however, seems to be refrained from any such regularities -- and must be computed for each ℓ -- hence the peak parameter $\hat{\theta}_{\max}(u,v)$, as parameter $\hat{\theta}_{\max}(u)$, is very sensitive to the cyclic shifts of the sequences u and v .

Whenever the phase shifts of the sequences are already fixed due to other requirements such as a low value of the autocorrelation parameter $\hat{\theta}_{\max}(u)$, the cross-correlation parameters can readily be computed.

For example, in Table 9 the parameters $\hat{\theta}_{\max}(u)$, $\theta_{\max}(u,v)$ and $\hat{\theta}_{\max}(u,v)$ are tabulated on, below and above the diagonal respectively, for the auto-optimal m-sequences of length $p = 127$. These sequences are indicated by the polynomials $f(x)$ which generate them. The symmetries in the table are due to the fact that $\hat{\theta}_{\max}(u',v') = \hat{\theta}_{\max}(u,v)$ and $\theta_{\max}(u',v') = \theta_{\max}(u,v)$ whenever u' and v' are reciprocals of u and v respectively (see Section 3.3). Whenever $v = T^k u$, $\theta_{\max}(u,v) = \hat{\theta}_{\max}(u,v) = p$. Hence, those values are omitted from the table. Notice also that for the maximal connected set S formed by the first six m-sequences in Table 9,

$$\hat{\theta}_c = \max\{\hat{\theta}_{\max}(u,v) : u \in S, v \in S\} = 33.$$

The interference parameter $r(u,v)$ as defined in (1.20) for the auto-optimal m-sequences of length $p = 127$ is tabulated in Table 10. The auto-optimal m-sequences in Table 10 are, as in Table 9, indicated by the polynomials $f(x)$ which generate them. Only one-fourth of the interference parameter values are tabulated because $r(u,v) = r(u,v')$ whenever v and v' are reciprocal sequences. Notice the higher interference between an m-sequence and itself or its reciprocal. This is a good argument, not to use an m-sequence and its reciprocal in the same set of signature sequences.

It is not surprising that m-sequences, which have many characteristics in common with random binary sequences, yield values of $r(u,v)$ which are close to $Er(u,v) = 2p^2$ as in (2.12). In fact, all values of $r(u,v)$ in Table 10 -- the values on the diagonal excluded -- are within the range $[Er(u,v) \pm \sqrt{\text{var}(r(u,v))}]$ for random binary sequences.

In Appendix C, the correlation parameters $\hat{\theta}_{\max}(u)$, $\theta_{\max}(u,v)$ and $\hat{\theta}_{\max}(u,v)$, as well as interference parameter $r(u,v)$ are given for the AO/LSE m-sequences (see Definition 2) of length $p = 31, 63, 127$ and 255.

Whenever it is possible to relax the autocorrelation requirements, one might try to minimize the cross-correlation parameter $\hat{\theta}_{\max}(u,v)$. Even for small sets of sequences, however, the amount of computation required to find the cyclic shifts which, for example, minimize $\hat{\theta}_c$ becomes rapidly prohibitive. A discussion about the computational complexity of the correlation problem is given by Pursley and Sarwate (1976). Sywyk (1975) obtained some results for auto-optimal m-sequences of length $p = 63$. A sub-optimal result for the above mentioned maximal connected set S of six m-sequences of length $p = 127$ is reported in Table 11. With the indicated binary loading, one obtains $\hat{\theta}_c = 29$ compared with $\hat{\theta}_c = 33$ for the auto-optimal loading. Notice, however, that $\hat{\theta}_a$ has increased from a previous low value of $\hat{\theta}_a = 19$ (see Table 4) to $\hat{\theta}_a = 23$. The resulting values of $r(u,v)$ are also given in Table 11.

Finally, to obtain an indication of how small $\hat{\theta}_c$ could be, a triple of polynomials (211,217,235) was selected from the maximal connected set S. We established that a lowest value $\hat{\theta}_c = 23$ is achieved for two sets of register loadings, here reported in Table 12. Notice that $\hat{\theta}_a = 29$ and $\hat{\theta}_c = 21$ respectively.

Table 11. Maximal connected set of m-sequences for which $\hat{\theta}_c = 29$
and interference parameters $r(u,v)$ for this set.

Poly.	Loading*	$\hat{\theta}_{\max}(u)$		217	235	247	277	357
211	1101010	19						
217	1101111	23	211	32770	28998	33202	32870	32290
235	1101000	19	217		32810	33014	33050	32038
247	1111111	23	235			30298	31550	32730
277	0111111	23	247				32458	33350
357	0101110	23	277					33482

Table 12. Optimal triples of m-sequences { 211, 217, 235 } with $\hat{\theta}_c = 23$
and interference parameters $r(u,v)$ for these triples.

Poly.	Loading*	$\hat{\theta}_{\max}(u)$		217	235
211	0100000	21			
217	1010011	29	211	30494	28738
235	1111101	23	217		33362
				217	235
211	0100000	21			
217	0010001	19	211	29714	28790
235	1110111	19	217		32442

CHAPTER 4

ON THE MOMENTS OF THE APERIODIC CORRELATION FUNCTIONS

While the relationship between the periodic correlation parameters of m -sequences and the polynomials $f(x)$ is rather well-understood (see Chapter 3), it is less clear how those polynomials relate to the aperiodic correlation parameters. In this chapter we report our work on one particular relationship which had the potential of being a possible sieve for m -sequences with good aperiodic correlation parameters.

4.1. Third moment problem

Our investigations were inspired by the work of Lindholm (1968) who was interested in the weight distribution of M -tuples of long m -sequences. He actually established a relationship between the polynomial $f(x)$ which generates the m -sequence and the moments of the M -tuple weight distribution. Related results were obtained by Wainberg and Wolf (1970) who derived the first six moments of the M -tuple weight distribution while Weathers, et al., (1974) obtained expressions for hybrid m -sequences.

In this chapter we consider the first few moments of the aperiodic correlation function values when the correlated m -sequences have an at random selected cyclic phase shift. In particular, we obtain the first few moments of the odd correlation function values. For a number of m -sequences, the moments were evaluated, and compared with actual data acquired from those m -sequences.

4.2. Moments of the aperiodic correlation functions

Let $\tilde{u} = T^x u$ and $\tilde{v} = T^y v$ be two cyclic shifts of m -sequences u and v respectively. When we assume x and y to be uniformly distributed over the integer values in the range $[0, p-1]$, the moments of the aperiodic autocorrelation function $C_{\tilde{u}}(l)$ and the aperiodic cross-correlation function $C_{\tilde{u}, \tilde{v}}(l)$ can be calculated in a relatively straightforward manner, as is shown in Appendix D.

In Appendix D it is also shown that the mathematical expectation of the interference parameter $r(\tilde{u}, \tilde{v})$ equals,

$$E\{r(\tilde{u}, \tilde{v})\} = 2(p^2 - 1 + p^{-1}) \quad (4.1)$$

which is practically equal to the mathematical expectation of $E\{r(u, v)\}$ for random sequences as derived in Section 2.3. Furthermore, the results in Appendix D enable us to derive in Section 4.3, the first three central moments of the odd correlation functions $\hat{\theta}_{\tilde{u}, \tilde{v}}(l)$ and $\hat{\theta}_{\tilde{u}}(l)$.

4.3. Moments of the odd correlation functions

With the odd cross-correlation function

$$\hat{\theta}_{\tilde{u}, \tilde{v}}(l) = C_{\tilde{u}, \tilde{v}}(l-p) - C_{\tilde{u}, \tilde{v}}(l), \quad 0 \leq l \leq p-1 \quad (4.2)$$

one obtains with (D3),

$$E\{\hat{\theta}_{\tilde{u}, \tilde{v}}(l)\} = p^{-2}(2l-p) \quad (4.3)$$

Similarly with (D4),

$$E\{\hat{\theta}_{\tilde{u}}(\ell)\} = p^{-1}(p-2\ell), \quad \ell \neq 0. \quad (4.4)$$

The variance of $\hat{\theta}_{\tilde{u},\tilde{v}}(\ell)$ follows from (D5) and (D9)

$$\begin{aligned} \text{var}\{\hat{\theta}_{\tilde{u},\tilde{v}}(\ell)\} &= E\{\hat{\theta}_{\tilde{u},\tilde{v}}^2(\ell)\} - E^2\{\hat{\theta}_{\tilde{u},\tilde{v}}(\ell)\} \\ &= p\{1 + p^{-3}[(p-2\ell)^2 - p] + p^{-5}(p-2\ell)\} \end{aligned} \quad (4.5)$$

while with (D6) and (D10) one obtains

$$\text{var}\{\hat{\theta}_{\tilde{u}}(\ell)\} = 4\ell p^{-2}(p+1)(p-\ell), \quad \ell \neq 0. \quad (4.6)$$

The third central moment of $\hat{\theta}_{\tilde{u},\tilde{v}}(\ell)$ is denoted as

$$\lambda_{\tilde{u},\tilde{v}}(\ell) = E\{[\hat{\theta}_{\tilde{u},\tilde{v}}(\ell) - E\{\hat{\theta}_{\tilde{u},\tilde{v}}(\ell)\}]^3\}$$

With (4.3) and (4.5) this reduces to

$$\lambda_{\tilde{u},\tilde{v}}(\ell) = E\{\hat{\theta}_{\tilde{u},\tilde{v}}^3(\ell)\} + \xi(\ell)$$

where

$$\xi(\ell) = p^{-6}\{(2\ell-p)^3(2-3p^2) - 3p^3(p^2-1)(2\ell-p)\} \quad (4.7)$$

and, after substitution of (D13) and (D17),

$$\begin{aligned} E\{\hat{\theta}_{\tilde{u},\tilde{v}}^3(\ell)\} &= p^{-2}\{(2-3p)(p-2\ell) + 6\binom{\ell}{3}^2 - 6\binom{p-\ell}{3}^2 + \frac{3}{2}\ell^2(p-\ell)^2(p-2)(p-2\ell)\} \\ &\quad + 6p^{-2}(p+1)\{-\binom{\ell}{3}[B_3^u(\ell) + B_3^v(\ell)] + \binom{p-\ell}{3}[B_3^u(p-\ell) + B_3^v(p-\ell)]\} \\ &\quad + \binom{\ell}{2}(p-\ell)[C_3^u(\ell) + C_3^v(\ell)] - \binom{p-\ell}{2}\ell[C_3^u(p-\ell) + C_3^v(p-\ell)] + \\ &\quad + 6p^{-2}(p+1)^2\{B_3^u(\ell)B_3^v(\ell) + C_3^u(p-\ell)C_3^v(p-\ell) \\ &\quad - C_3^u(\ell)C_3^v(\ell) - B_3^u(p-\ell)B_3^v(p-\ell)\}. \end{aligned} \quad (4.8)$$

For the third central moment of $\theta_{\tilde{u}}(\ell)$ one obtains with (D14), (D19), (4.4) and (4.6),

$$\lambda_{\tilde{u}}(\ell) = E\{\hat{\theta}_{\tilde{u}}^3(\ell)\} + \delta(\ell)$$

where

$$\delta(\ell) = p^{-3}(p-2\ell)[4\ell(\ell-p)(2+3p) - p^2] \quad (4.9)$$

and

$$\begin{aligned} E\{\hat{\theta}_{\tilde{u}}^3(\ell)\} &= 8E\{C_{\tilde{u}}^3(\ell-p)\} + 12E\{C_{\tilde{u}}^2(\ell-p)\} + 6E\{C_{\tilde{u}}(\ell-p)\} + 1 \\ &= 2\ell p^{-1}\{3(2p+1) - 2\ell(3+2\ell)\} + 1 + 48p^{-1}(p+1)B_3^u(\ell). \end{aligned} \quad (4.10)$$

Hence,

$$\lambda_{\tilde{u}}(\ell) = 8\ell^2 p^{-3}(p+1)[3p-\ell(p+2)] + 48p^{-1}(p+1)B_3^u(\ell). \quad (4.11)$$

$B_3^u(\ell)$ represents the number of trinomials (see Chapter 3) of degree up to but not including ℓ , which are divisible by the primitive polynomial $f(x)$ which generates m -sequence μ (or u).

$C_3^u(\ell)$ represents the number of trinomials of degree ℓ and higher, with the exponent of the intermediate term smaller than or equal to $\ell-1$, which are divisible by the primitive polynomial $f(x)$ which generates m -sequence μ (or u).

It is shown in Appendix D that

$$C_3^u(\ell) + 3B_3^u(\ell) = C_3^v(\ell) + 3B_3^v(\ell) = \binom{\ell}{2}. \quad (4.12)$$

To find $B_3^u(\ell)$ -- and thus $C_3^u(\ell)$ -- one can use Lindholm's equality

$$B_3^u(\ell) = \ell \tilde{B}_3^u(\ell) - \sum_{j=1}^{\tilde{B}_3^u(\ell)} d_j. \quad (4.13)$$

Here $\tilde{B}_3^u(\ell)$ equals the number of trinomials of the form $x^{d_j} + x^{c_j} + 1$, with $1 \leq c_j < d_j \leq \ell-1$, which are divisible by $f(x)$.

Notice that (4.8) and (4.10) imply

$$\lambda_{\tilde{u}, \tilde{v}}(\ell) = -\lambda_{\tilde{u}, \tilde{v}}(p-\ell) \quad (4.14)$$

and

$$\lambda_{\tilde{u}}(\ell) = -\lambda_{\tilde{u}}(p-\ell) \quad (4.15)$$

which reduces the number of computations for each parameter with a factor of 1/2. Furthermore, for any m-sequence μ of length $p = 2^n - 1$ generated by polynomial $f(x)$ of degree n , there does not exist a trinomial $x^{d_j} + x^{c_j} + 1$ with $d_j < n$, which is divisible by $f(x)$. Hence, for $\ell < n$

$$B_3^u(\ell) = C_3^u(\ell) = 0, \quad \forall u. \quad (4.16)$$

4.4. Third moment evaluation for m-sequences of length $p = 31$ and $p = 63$

In this section the third central moments of the odd cross-correlation and autocorrelation functions as discussed in Section 4.3 are evaluated for the m-sequences of length $p = 31$ and $p = 63$. As an example, the values of $B_3^u(\ell)$ and $C_3^u(\ell)$ for the m-sequences generated by $f_1(x) = x^5 + x^2 + 1$ (045), $f_3(x) = x^5 + x^4 + x^3 + x^2 + 1$ (075) and $f_5(x) = x^5 + x^4 + x^2 + x + 1$ (067) respectively, are given in Table 13. Reciprocal polynomials give the same values for $B_3^u(\ell)$ (and thus for $C_3^u(\ell)$).

To demonstrate this Table 13, consider $B_3^u(11)$ and $C_3^u(11)$ for the m-sequence u generated by $f_1(x) = x^5 + x^2 + 1$. The trinomials of the form $x^{d_j} + x^{c_j} + 1$ contributing to $\tilde{B}_3^u(11)$ are $x^5 + x^2 + 1$ and $x^{19} + x^4 + 1$, i.e., $\tilde{B}_3^u(11) = 2$. Hence, $B_3^u(11) = 7$ and with (4.12) one obtains

Table 13. $B_3^u(l)$ and $C_3^u(l)$ for m-sequences of length $p = 31$.

$$f_1(x) = x^5 + x^2 + 1 \quad f_3(x) = x^5 + x^4 + x^3 + x^2 + 1 \quad f_5(x) = x^5 + x^4 + x^2 + x + 1$$

$$f_{15}(x) = x^5 + x^3 + 1 \quad f_7(x) = x^5 + x^3 + x^2 + x + 1 \quad f_{11}(x) = x^5 + x^4 + x^3 + x + 1$$

 $l \quad B_3^u(l) \quad C_3^u(l)$

1	0	0
2	0	1
3	0	3
4	0	6
5	0	10
6	1	12
7	2	15
8	3	19
9	4	24
10	5	30
11	7	34
12	9	39
13	11	45
14	13	52
15	16	57
16	19	63
17	23	67
18	27	72
19	32	75
20	38	76
21	45	75
22	52	75
23	60	73
24	69	69
25	79	63
26	90	55
27	101	48
28	113	39
29	126	28
30	140	15
31	155	0

 $l \quad B_3^u(l) \quad C_3^u(l)$

1	0	0
2	0	1
3	0	3
4	0	6
5	0	10
6	0	15
7	0	21
8	0	28
9	1	33
10	3	36
11	5	40
12	7	45
13	10	48
14	13	52
15	16	57
16	19	63
17	23	67
18	28	69
19	34	69
20	40	70
21	47	69
22	55	66
23	63	64
24	71	63
25	80	60
26	90	55
27	101	48
28	113	39
29	126	28
30	140	15
31	155	0

 $l \quad B_3^u(l) \quad C_3^u(l)$

1	0	0
2	0	1
3	0	3
4	0	6
5	0	10
6	0	15
7	0	21
8	1	25
9	2	30
10	3	36
11	4	43
12	6	48
13	8	54
14	11	58
15	15	60
16	20	60
17	25	61
18	30	63
19	35	66
20	41	67
21	47	69
22	54	69
23	62	67
24	71	63
25	80	60
26	90	55
27	101	48
28	113	39
29	126	28
30	140	15
31	155	0

$C_3^u(11) = 34$. The trinomials of the form $x^{d_j} + x^{c_j} + 1$ and their respective contributions to $C_3^u(11)$ are tabulated below,

Trinomial	Contribution
$x^5 + x^2 + 1$	3
$x^{10} + x^4 + 1$	6
$x^{16} + x^9 + 1$	2
$x^{18} + x + 1$	10
$x^{20} + x^8 + 1$	3
$x^{22} + x^7 + 1$	4
$x^{27} + x^6 + 1$	4
$x^{29} + x^3 + 1$	<u>2</u>
Total: 34 .	

The parameters $\lambda_{\tilde{u}}(l)$ and $\lambda_{\tilde{u},\tilde{v}}(l)$ for m-sequences of length $p = 31$ are sketched in Figure 4 and Figure 5 respectively. The same parameters for m-sequences of length $p = 63$ are sketched in Figure 6 and Figure 7.

4.5. Discussion of $\lambda_{\tilde{u}}(l)$ and $\lambda_{\tilde{u},\tilde{v}}(l)$

It is clear from the results in the previous section that the mean and the variance of the odd correlation function values do not depend on the particular m-sequences selected. The third central moments $\lambda_{\tilde{u}}(l)$ and $\lambda_{\tilde{u},\tilde{v}}(l)$, however, clearly do depend on the polynomials $f(x)$ as specified by the expressions in Section 4.3. While $\lambda_{\tilde{u}}(l)$ and $\lambda_{\tilde{u},\tilde{v}}(l)$, $\forall l$, are equal to zero for random binary sequences (see Section 2.3), for the m-sequences they vary widely when l takes on values in its range. Recall that a third central moment provides a measure of skewness being positive, zero or negative as the distribution has a long positive tail, is

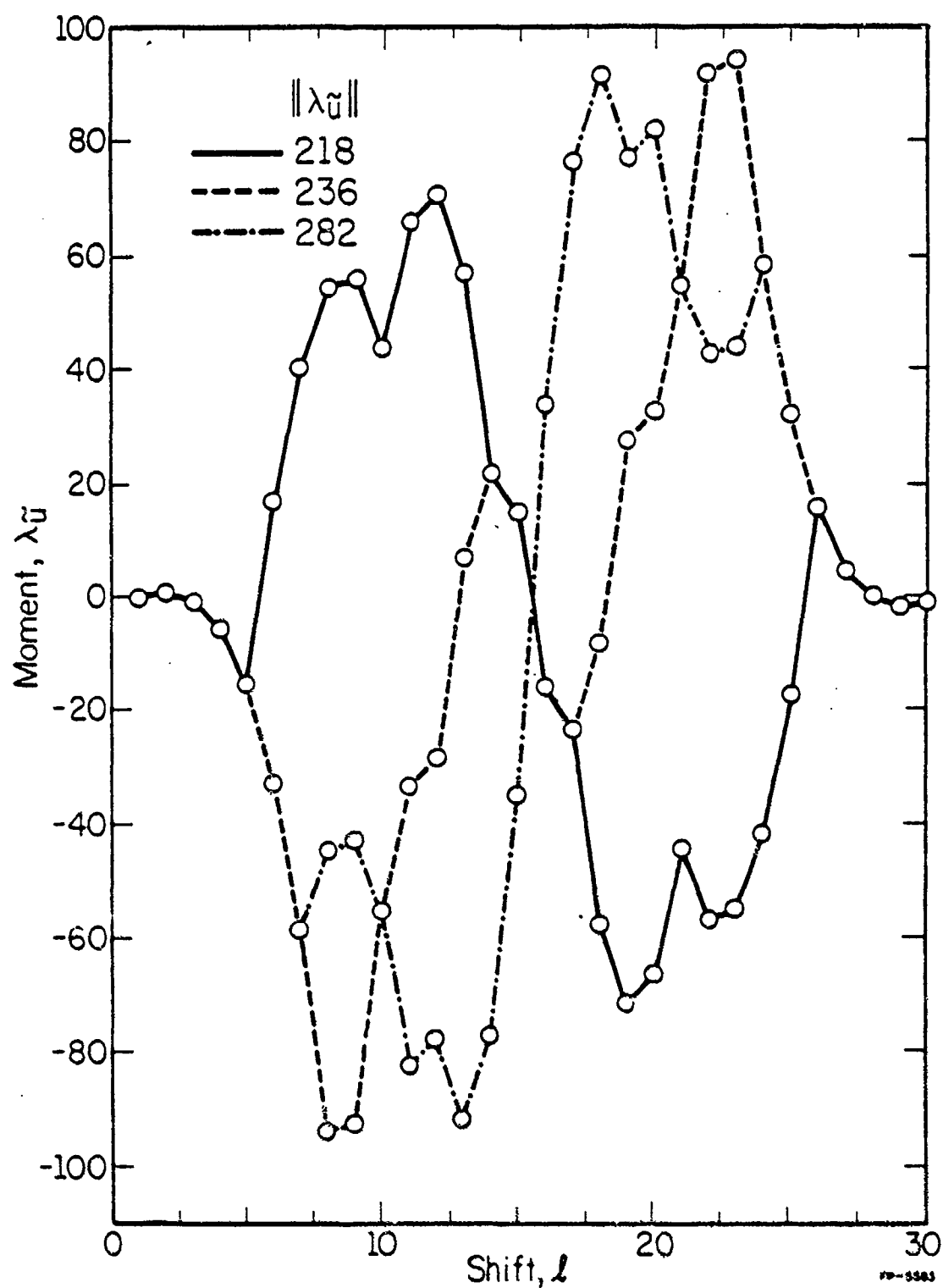


Figure 4. Third central moments of the odd autocorrelation function for m-sequences; $p = 31$.

— 045 (051); --- 075 (057); - · - · - 067 (073).

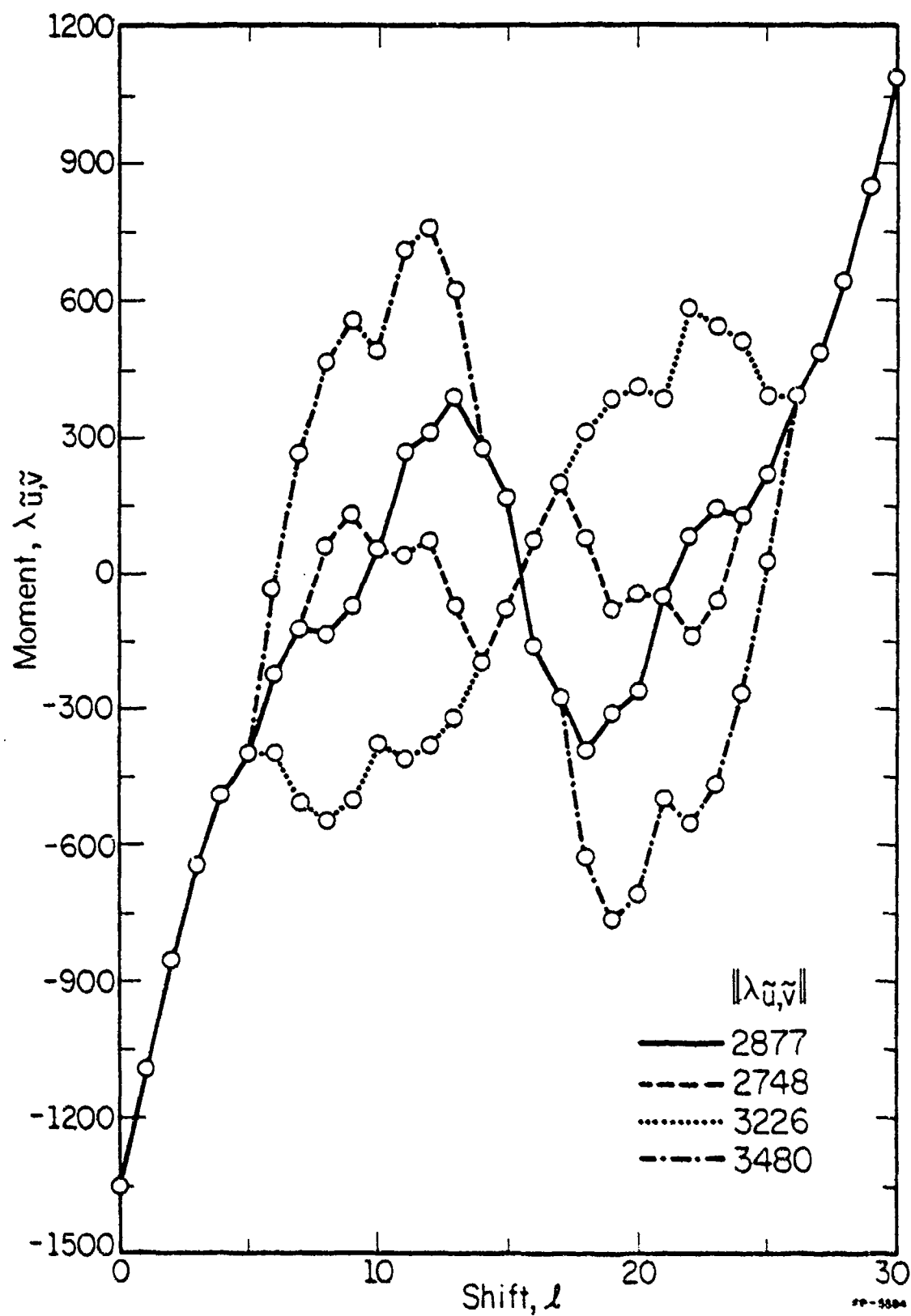


Figure 5. Third central moments of the odd cross-correlation function for m-sequences; $p = 31$.

— (045,075); --- (045,067); (067,075); -.- (045,051).

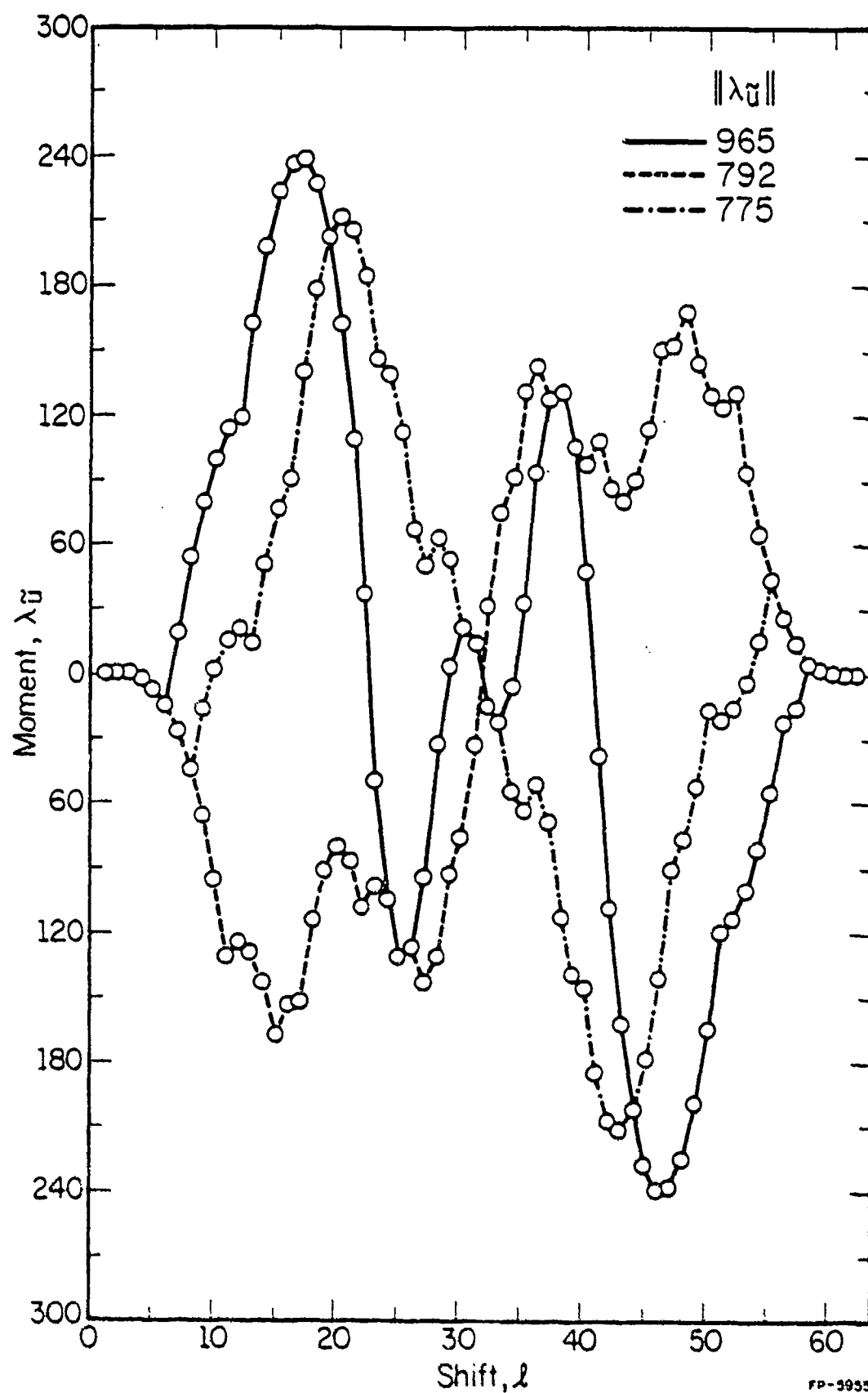


Figure 6. Third central moments of the odd autocorrelation function for m-sequences; $p = 63$.

— 103 (141); - - - 147 (163); - · - · - 133 (155).

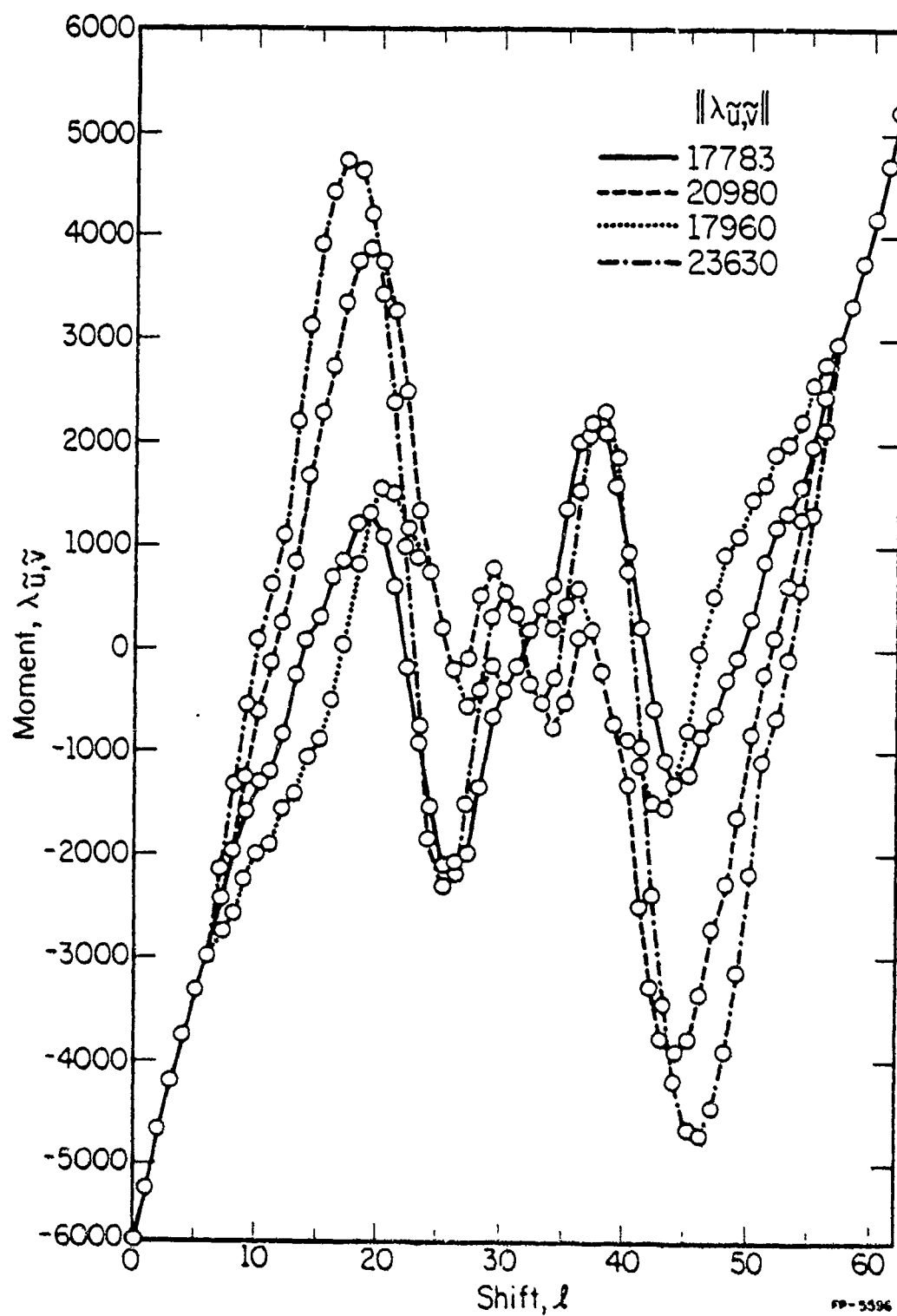


Figure 7. Third central moments of the odd cross-correlation function for m-sequences; $p = 63$.

— (103,147); --- (103,133); (147,133); -.- (103,141).

symmetrical or has a long negative tail. Hence, the various sets

$$\lambda_{\tilde{u}} = \{\lambda_{\tilde{u}}(\ell); \ell = 1, 2, \dots, p-1\}$$

and
$$\lambda_{\tilde{u}, \tilde{v}} = \{\lambda_{\tilde{u}, \tilde{v}}(\ell); \ell = 0, 1, \dots, p-1\}$$

for different m-sequences and m-sequence pairs respectively could be potentially useful as sieves for sequences with good correlation properties. For example, let $u' = T^{x'} u$ with x' chosen at random from the integer values in $[0, p-1]$. The set of values $\{\hat{\theta}_{\tilde{u}}(\ell); \ell = 1, 2, \dots, p-1\}$ for m-sequence u' can be modelled as a realization of the set of random variables $\{\hat{\theta}_{\tilde{u}}(\ell); \ell = 1, 2, \dots, p-1\}$. Hence one could expect some correlation between parameters such as $\hat{\theta}_{\max}(u')$ or $\min_{x'} \hat{\theta}_{\max}(u')$ and $\lambda_{\tilde{u}}$.

On the other hand, this correlation might not be high enough to show up in the above mentioned parameters when the actual m-sequences, selected with $\lambda_{\tilde{u}}$ as sieve, are compared. Furthermore, if such a correlation exists, it is not yet clear which measure on the values in $\lambda_{\tilde{u}}$ and $\lambda_{\tilde{u}, \tilde{v}}$ should be chosen to use as the actual sieve.

One measure might be the presence of a certain number of high positive or negative peaks in $\lambda_{\tilde{u}}$ or $\lambda_{\tilde{u}, \tilde{v}}$.

Another measure might be the Euclidean norm $\|\lambda_{\tilde{u}, \tilde{v}}\|$ of the vector $(\lambda_{\tilde{u}, \tilde{v}}(0), \lambda_{\tilde{u}, \tilde{v}}(1), \dots, \lambda_{\tilde{u}, \tilde{v}}(p-1))$, i.e.,

$$\|\lambda_{\tilde{u}, \tilde{v}}\| = \left\{ \sum_{\ell=0}^{p-1} \lambda_{\tilde{u}, \tilde{v}}^2(\ell) \right\}^{1/2}. \quad (4.17)$$

The norm $\|\lambda_{\tilde{u}}\|$ is defined in a similar way, with $\ell \neq 0$. An insert in the Figures 4 through 7 gives the Euclidean norms for the indicated m-sequences.

A problem with both measures, and presumably will all, is the dominating and equalizing presence of the high peaks in $\lambda_{\tilde{u}}$ and $\lambda_{\tilde{u},\tilde{v}}$ for $l < n$, which do not depend on $f(x)$.

4.6. Actual data for m-sequences of length $p = 31$ and $p = 63$

In this section we present some actual data obtained for the m-sequences used in Section 4.4. Additional data can be found in Sywyk's work (1975).

Let F_a denote the number of times a certain value of $\hat{\theta}_{\max}(u')$ occurs when x' in $u' = T^{x'}u$ takes on the values $0, 1, \dots, p-1$. Similarly, F_c denotes the number of times a certain value of $\hat{\theta}_{\max}(u', v')$ occurs when x' and y' in $u' = T^{x'}u$ and $v' = T^{y'}v$ respectively, both take on the values $0, 1, \dots, p-1$. F_a and F_c are tabulated in Table 14 for a number of m-sequences with the polynomials $f(x)$ in octal notation.

While a larger number of positive or negative peaks in $\lambda_{\tilde{u}}$ (or $\lambda_{\tilde{u},\tilde{v}}$) or a higher value of $\|\lambda_{\tilde{u}}\|$ (or $\|\lambda_{\tilde{u},\tilde{v}}\|$) might indeed have some positive correlation with a larger number of high values of $\hat{\theta}_{\max}(u')$ (or $\hat{\theta}_{\max}(u', v')$), the effect as a whole seems rather weak. Actually, the data shows that the m-sequences do behave rather much alike. Other results, collected while obtaining auto-optimal Gold sequences and Kasami sequences (see Chapter 5) do not give more conclusive information.

Hence, we conclude that $\lambda_{\tilde{u}}$ and $\lambda_{\tilde{u},\tilde{v}}$, while interesting on their own merits, are less useful as sieves for the selection of m-sequences with good correlation parameters such as a low worst-case value of $\hat{\theta}_{\max}(u')$ or $\hat{\theta}_{\max}(u', v')$.

Table 14. Fa and Fc for some m-sequences of length $p = 31$ and $p = 63$. $p = 31$

Poly.	$\hat{\theta}_{\max}(u') :$	7	9	11	13
045 (051)	Fa :	4	18	9	0
075 (057)	Fa :	9	13	8	1
067 (073)	Fa :	4	16	9	2

Poly. pairs	$\hat{\theta}_{\max}(u', v') :$	7	9	11	13	15	17	19	21
(045, 057)	Fc :	0	53	339	333	156	56	20	4
(045, 073)	Fc :	1	60	321	342	166	53	14	4
(057, 073)	Fc :	0	39	324	336	176	66	18	2
(045, 051)	Fc :	10	188	336	216	121	67	21	2

 $p = 63$

Poly.	$\hat{\theta}_{\max}(u') :$	11	13	15	17	19	21
103 (141)	Fa :	8	7	22	16	9	1
147 (163)	Fa :	9	17	24	11	2	0
133 (155)	Fa :	9	22	18	12	2	0

CHAPTER 5

CORRELATION PARAMETERS FOR SUMS OF PAIRS OF M-SEQUENCES

In the previous chapters the discussion has been limited to m-sequences because those sequences have excellent periodic auto-correlation properties. Sets of m-sequences with good periodic cross-correlation properties, however, have a small cardinality (see Section 3.5). In this chapter we will expand our discussion to larger sets of potentially good signature sequences due to Gold (1967) and Kasami (1966).

5.1. Gold sequences

Theorem 2 in section 3.5 yields a pair of m-sequences of common period $p = 2^n - 1$ for which the pairwise cross-correlation is bounded by $2^{\lfloor (n+2)/2 \rfloor} + 1$. Here $n \not\equiv 0 \pmod{4}$ otherwise $f_t(x)$ is not primitive.

In fact, the greatest common divisor of p and t in Theorem 2 is

$$\gcd(p, t) = \begin{cases} 1 & n \not\equiv 0 \pmod{4} \\ 3 & n \equiv 0 \pmod{4} \end{cases} \quad (5.1)$$

as was pointed out by Sarwate (1976).

Above result is contained in the stronger and more general Theorem 3 which yields preferred pairs of primitive polynomials for n odd and $c = 1$ or $n \equiv 2 \pmod{4}$ and $c = 2$ but not for $n \equiv 0 \pmod{4}$. More preferred polynomial pairs can be found when $t = 2^h + 1$ in Theorem 3 is replaced by $2^{2h} - 2^h + 1$, as reported by Golomb (1968). Furthermore, the number of polynomials for which this theorem holds can be doubled with a proposition in Pursley (1976). This proposition states that polynomial pairs $(f_1(x), f_t(x))$ and $(f_1(x), f_q(x))$ generate m-sequence pairs with

similar cross-correlation values whenever

$$qt = 2^i \bmod (2^n - 1), \text{ for some } i, \quad 0 \leq i \leq n-1. \quad (5.2)$$

Analytical results such as above, as well as experimental results such as discussed in section 3.4 yield m-sequence pairs (u, v) such that $\theta_{\max}(u, v) = 2^{\lfloor (n+2)/2 \rfloor} + 1$. Furthermore, it enabled Gold (1967) and Kasami (1966) to formulate the following important result.

Theorem 4: Let $f_1(x)$ and $f_t(x)$ be a preferred pair of polynomials of degree n whereby $n \not\equiv 0 \pmod{4}$. The shift register with the product $f_1(x) f_t(x)$ as its characteristic polynomial will generate a set of $2^n + 1$ distinct sequences of period $p = 2^n - 1$. Any pair of sequences in this set has a cross-correlation function bounded by $2^{\lfloor (n+2)/2 \rfloor} + 1$, and any sequence in the set has an autocorrelation function whose out-of-phase values are also bounded by $2^{\lfloor (n+2)/2 \rfloor} + 1$.

These sequences and all their cyclic shifts are usually referred to as Gold sequences. The set of distinct sequences in Theorem 4 consists of characteristic m-sequences μ and v generated by $f_1(x)$ and $f_t(x)$ respectively and sequences of the type $w = \mu + T^k v$, $k = 0, 1, \dots, p-1$, whereby the addition is modulo 2. Hence, the Gold sequences can also be generated by two shift registers with characteristic polynomials $f_1(x)$ and $f_t(x)$ respectively and one modulo 2 adder (see Dixon (1976)).

Clearly the periodic cross-correlation function between m-sequences μ and v in the set of Gold sequences is three-valued because $f_1(x)$ and $f_t(x)$ are a preferred pair. The periodic cross-correlation of m-sequence μ and sequence $w = \mu + T^k v$ can be regarded as a special case

of the periodic cross-correlation function $\theta_{w,z}(\ell)$ of the sequences $w = \mu + T^k v$ and $\zeta = \mu + T^m v$, with $w_j = (-1)^{w_j}$ and $z_j = (-1)^{z_j}$, i.e., $w = u \cdot T^k v$ and $z = u \cdot T^m v$, which is discussed in the next section.

5.2. Periodic correlation functions of sums of m-sequences

Let $d_H(\omega, \zeta)$ denote the Hamming distance between any two sequences ω and ζ , both of length p , and let $W_H(\omega)$ denote the Hamming weight of sequence ω . As before we assume the m-sequences μ (or u) and v (or v) to be in their characteristic form. Then

$$\begin{aligned}\theta_{w,z}(\ell) &= p - 2d_H(\omega, T^\ell \zeta) \\ &= p - 2W_H(\omega + T^\ell \zeta) \\ &= p - 2W_H(\mu + T^\ell v + T^\ell \mu + T^{m+\ell} v) .\end{aligned}$$

Therefore

$$\theta_{w,z}(\ell) = \begin{cases} p & \text{if } \ell = 0 \bmod p, m = k \\ -1 & \text{if } \ell = 0 \bmod p, m \neq k \\ -1 & \text{if } \ell + m - k = 0 \bmod p, m \neq k \\ \theta_{u,v}(k+s(\ell)-r(\ell)) , & \text{otherwise} \end{cases} \quad (5.3)$$

whereby

$$\begin{cases} T^{r(\ell)} \mu + T^\ell \mu + \mu = \underline{0} \\ T^{s(\ell)} v + T^{\ell+m-k} v + v = \underline{0} \end{cases} \quad (5.4)$$

and $\underline{0}$ the all-zero sequence. As a special case one obtains, with $u \neq w$,

$$\theta_{u,w}(\ell) = \begin{cases} -1 & , \ell = 0 \bmod p \\ \theta_{u,v}(k+\ell-r(\ell)) , & \text{otherwise} . \end{cases} \quad (5.5)$$

The choice of μ and v characteristic in ω and ζ is not essential for equations (5.3) and (5.5) and would merely constitute a change in shift l because

$$\theta_{\tilde{u}, \tilde{v}}(l) = \theta_{u, v}(l + y - x \bmod p), \quad \forall l \quad (5.6)$$

where $\tilde{u} = T^x u$ and $\tilde{v} = T^y v$.

Given a value of $m-k$, the trinomial equations in (5.4) (see Section 3.2) specify for each l the binary trinomials $x^{r(l)} + x^l + 1$ and $x^{s(l)} + x^{l+m-k} + 1$ which should be divisible by $f_1(x)$ and $f_t(x)$ respectively.

For $l = 1, 2, \dots, p-1$, the factor $l - r(l)$ in equation (5.5) takes on all the values in its range and $l \neq r(l)$. This implies, among others, that $\theta_{u, w}(l)$ in (5.5) will again be a three valued cross-correlation function when u and v are preferred m -sequences.

The factor $s(l) - r(l)$ in equation (5.3), however, will take on specific values in $[0, p-1]$. Those values will depend on $m-k$ as well as the trinomial structure of the m -sequences involved. With the difference $s(l) - r(l)$ determined for all l , $\theta_{u, v}(k + s(l) - r(l))$ still is a function of k .

In the special case that $m=k$, equations (5.4) imply that $s(l) - r(l) \in \eta_y$ if $l \in \eta_i$ for some i and y . Then if one adds a value $k \in \eta_x$ to $s(l) - r(l)$, the resulting sum $k + s(l) - r(l) \in \eta_x \eta_y$, the Gauss' product of cyclotomic cosets η_x and η_y as defined in (3.17).

Above facts explain why certain choices of k in the sequence $\omega = \mu + T^k v$ can yield a peak parameter $\theta_{\max}(\omega) < \theta_{\max}(u, v)$ and certain (k, m) in sequence pair $(\omega = \mu + T^k v, \zeta = u + T^m v)$ can yield a peak parameter $\theta_{\max}(\omega, \zeta) < \theta_{\max}(u, v)$. Here $\theta_{\max}(u, v)$ is assumed to be obtained from the

tables of Gold and Kopitzke (1965), Golomb's theorem (1968) or Kasami's results (1966). Of course, other correlation parameters will depend on (k,m) too.

From the results such as above, we can formulate;

Theorem 5: Let $f_1(x)$ and $f_t(x)$ generate the set $\mathcal{L}$ of distinct Gold sequences μ , v and $\omega = \mu + T^k v$, $k = 0, 1, \dots, p-1$ as in Theorem 4. Any m -sequence in $\mathcal{L}$ has a three-valued cross-correlation function with any other sequence in $\mathcal{L}$. A sequence pair of the type $(\omega = \mu + T^k v, \zeta = \mu + T^m v)$ will have, as a function of (k,m) , a three-valued or in some cases a two-valued cross-correlation function. Furthermore any sequence in $\mathcal{L}$ of the type $\omega = \mu + T^k v$ will have, as a function of k , an autocorrelation function with out-of-phase values $\{-1, -1 \pm 2^{\lfloor (n+2)/2 \rfloor}\}$ or in some cases $\{-1, -1 + 2^{\lfloor (n+2)/2 \rfloor}\}$.

It should be noted that equation (5.3) is not restricted to preferred pairs of polynomials. Hence, our investigation -- in the next sections -- not only includes Gold sequences but many other sequences of the type $\omega = \mu + T^k v$. Furthermore, we will study in Section 5.5 the special case $t = 2^{n/2} - 1$, n even, i.e., polynomial $f_t(x)$ is not primitive. The next section illustrates our approach with an example for sequence length $p = 15$.

5.3. Example for m -sequences of length $p = 15$

Let μ and v be the two m -sequences of length $p = 15$ generated by polynomials $f_1(x) = x^4 + x + 1$ and $f_7(x) = x^4 + x^3 + 1$ respectively.

As was shown in Section 3.4

$$\theta_{u,v}(\ell) = \begin{cases} -1 & \text{if } \ell \in \pi_0 \\ -5 & \text{if } \ell \in \pi_1 \\ 3 & \text{if } \ell \in \pi_3 \\ 7 & \text{if } \ell \in \pi_5 \\ -1 & \text{if } \ell \in \pi_7 \end{cases} \quad (5.7)$$

Hence, $\theta_{\max}(u,v) = 7$.

Case 1: $m=k$

With u generated by $f_1(x) = x^4 + x + 1$ one immediately obtains $T^4u + Tu + u = 0$ as a (trivial) first trinomial satisfying (5.4). The other trinomials of the form specified by (5.4) are tabulated in Table 15 for the polynomials $f_1(x)$ as well as $f_7(x)$. Observe from this table that $s(\ell) - r(\ell) \bmod 15 \in \pi_0, \pi_1$ and π_5 . Let $k \in \pi_7$. Then the sum $k + s(\ell) - r(\ell) \bmod 15 \in \pi_0\pi_7, \pi_1\pi_7$ and $\pi_5\pi_7$. This implies, with Table 5, that $k + s(\ell) - r(\ell) \bmod 15 \notin \pi_5, \forall \ell$, and therefore $\theta_w(\ell) = \theta_{u,v}(k + s(\ell) - r(\ell)) \neq \theta_{u,v}(\pi_5) = \theta_{\max}(u,v) = 7$. Hence, $\theta_{\max}(w) = 5$ for $k \in \pi_7$ while $\theta_{\max}(w) = 7$ for $k \notin \pi_7$.

Case 2: $m \neq k$

Let Gx denote a series of values,

$$Gx = (x \cdot 2^j \bmod p), \quad j = 0, 1, \dots, n-1 \quad (5.8)$$

and let

$$G(x,y) = ((x \cdot 2^j \bmod p, y \cdot 2^j \bmod p)), \quad j = 0, 1, \dots, n-1 \quad (5.9)$$

Table 15. Trinomial structure of m -sequences of length $p = 15$.

Case 1: $m = k$	
	$l : 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12 \ 13 \ 14 \ 0$
(023)	$r(l) : 4 \ 8 \ 14 \ 1 \ 10 \ 13 \ 9 \ 2 \ 7 \ 5 \ 12 \ 11 \ 6 \ 3 ==$
(031)	$s(l) : 12 \ 9 \ 4 \ 3 \ 10 \ 8 \ 13 \ 6 \ 2 \ 5 \ 14 \ 1 \ 7 \ 11 ==$
	$s(l)-r(l) : 8 \ 1 \ 5 \ 2 \ 0 \ 10 \ 4 \ 4 \ 10 \ 0 \ 2 \ 5 \ 1 \ 8 ==$
	$7+s(l)-r(l) : 0 \ 8 \ 12 \ 9 \ 7 \ 2 \ 11 \ 11 \ 2 \ 7 \ 9 \ 12 \ 8 \ 0 ==$

Case 2: $m = k + 1$	
	$l : 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12 \ 13 \ 14 \ 0$
(023)	$r(l) : 4 \ 8 \ 14 \ 1 \ 10 \ 13 \ 9 \ 2 \ 7 \ 5 \ 12 \ 11 \ 6 \ 3 ==$
(031)	$s(l) : 9 \ 4 \ 3 \ 10 \ 8 \ 13 \ 6 \ 2 \ 5 \ 14 \ 1 \ 7 \ 11 == 12$
	$s(l)-r(l) : 5 \ 11 \ 4 \ 9 \ 13 \ 0 \ 12 \ 0 \ 13 \ 9 \ 4 \ 11 \ 5 == ==$

($==$ denotes the exceptional cases in equation (5.3))

Table 16. Sequence pairs (w, z) for which $\hat{\theta}_{\max}(w, z) < 7$;

$$w = u \cdot T^k v, \quad z = u \cdot T^m v; \quad p = 15.$$

$m-k$	k	(k, m)
G1	G2, G3, G4,	G(2,3), G(3,4), G(4,5),
G3	G0, G2, G7,	G(0,3), G(2,5), G(7,10),
G5	G2	G(2,7)

denote a series of pairs. This notation can simply be extended to triples $G(x,y,z)$ etc.

Consider $m=k+1$. Table 15 indicates the resulting trinomials of the form specified in (5.4) and the resulting values of $s(l) - r(l) \bmod 15$. Observe that $k + s(l) - r(l) \bmod 15 \notin \Pi_5$ whenever $k = 2, 3$ or 4 . Again let (k,m) indicate the sequence pair $(w = \mu + T^k v, \zeta = \mu + T^m v)$, then $\theta_{w,z}(l) = \theta_{u,v}(k+s(l) - r(l)) \neq \theta_{\max}(u,v) = 7$ for the sequence pair $(k,m) = (2,3), (3,4)$ and $(4,5)$. In fact one finds that a series of values $m-k = G1$ implies a series of values $k = G2, G3$, and $G4$ or, alternatively, a series of sequence pairs $(k,m) = G(2,3), G(3,4)$ and $G(4,5)$ for which $\theta_{\max}(w,z) \neq 7$ (in fact ≤ 5). Table 16 shows the results for $m-k = Gx$, $x = 1, 3$ and 5 .

Examination of Table 16 reveals four triples (k_{i1}, k_{i2}, k_{i3}) where k_{ij} indicates sequence $w_{ij} = \mu + T^{k_{ij}} v$, for which the pairwise peak magnitude of the periodic cross-correlation function equals 5 instead of 7. Those triples are $G(1,5,11)$.

In the next section results for sequences of longer length will be discussed.

5.4. Sums of pairs of m-sequences up to length $p = 255$

The trinomial structure of the m-sequences μ and v and its relation with the periodic autocorrelation and cross-correlation functions of $w = \mu + T^k v$, $k \in [0, p-1]$ has been investigated for sequence lengths up to $p = 255$. The autocorrelation properties are the least attractive aspects of the sequences w if compared with m-sequences. Hence, those aspects received most of our attention. In many cases the AO/LSE phase

shifts W of sequences w were determined and the cross-correlation values of interesting subsets have been computed.

5.4.1. Sequence length $p = 31$

The trinomials for the m -sequences of length $p = 31$ are specified in Table 17 and are easily obtained from each other with the decimation property (3.7) of m -sequences.

Except in the case that the sequences are generated by reciprocal polynomials, the m -sequences μ and ν will be preferred pairs, i.e., $\theta_{\max}(u, v) = 1 + 2^{\lfloor (5+2)/2 \rfloor} = 9$. With the Gauss' products of cyclotomic cosets of integers modulo 31 as specified by Golomb (1968) one obtains here $\theta_{\max}(w) = 2^{\lfloor (5+2)/2 \rfloor} - 1 = 7$ for exactly one value of k namely $k \in \pi_0 = 0$ or $w = \mu + \nu$ (and all cyclic shifts of w). Table 18 gives the results for the periodic cross-correlation parameter $\theta_{\max}(w, z)$. The asterisk indicates that $\theta_{w,z}(\ell)$ will be a two-valued function for indicated values of (k, m) .

A complete set of periodic autocorrelation parameters $\theta_{\max}(w)$, L_a and $M(w)$ for all values of $k \in \pi_x$ is shown in Table 19. The decimation property (3.7) and proposition (5.2) imply here that pairs of columns of k -values in this table can be obtained from each other by simple transformations of cosets π_x .

As was the case for m -sequences, peak parameter $\hat{\theta}_{\max}(w)$ will again depend on the cyclic shift of sequence w . Furthermore, recall that $M(w) + \hat{M}(w) = 4S(w)$, $\forall w$. Here $M(w)$ is constant over $k \in \pi_x$, some x . Hence, the sidelobe energy can be used as a sieve for low values of $\hat{M}(w)$ as long as $k \in \pi_x$, some x , and Definition 2 (Section 3.3) can simply be

Table 17. Trinomial structure of m-sequences of length $p = 31$.

	ℓ	:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
(045)	$r(\ell)$	:	18	5	29	10	2	27	22	20	16	4	19	23	14	13	24	...
(075)	$r(\ell)$	:	20	9	26	18	8	21	29	5	2	16	12	11	17	27	25	...
(067)	$r(\ell)$	:	19	7	11	14	29	22	2	28	15	27	3	13	12	4	9	...
(057)	$r(\ell)$	:	12	24	8	17	28	16	9	3	7	25	30	1	27	18	21	...
(073)	$r(\ell)$	:	13	26	23	21	7	15	5	11	25	14	8	30	1	10	6	...
(051)	$r(\ell)$	:	14	28	5	25	3	10	16	19	24	6	23	20	30	1	22	...

Table 18. Good $\theta_{\max}(w)$ or $\theta_{\max}(w,z)$; $w = u \cdot T^k v$, $z = u \cdot T^m v$; $p = 31$.

u	v	β^q	$\theta_{\max}(u,v)$	$\theta_{\max}(w)$	$k \in \eta_x([x])$	$\theta_{\max}(w,z)$	(k,m)
045	075	β^3	9	7	[0]	7*	G(5,10)
045	067	β^5	9	7	[0]	9	all
045	051	β^{15}	11	7	[0]	7	G(1, 2)
045	057	β^7	9	7	[0]	9	all
045	073	β^{11}	9	7	[0]	7*	G(1, 2)

Table 19. Periodic autocorrelation functions for $w = u \cdot T^k v$ with $k \in \eta_x([x])$; $p = 31$.

$\theta_{\max}(w)$ La M(w)				k				$\theta_{\max}(w)$ La M(w)				k
u: 045				045				u: 045				
v: 075				073				v: 051				
				067								
				057								
7	10	510		[0]	[0]	[0]	[0]	7	10	590		[0]
9	2	766		[5]	[1]	[7]	[15]	9	4	654		[11]
9	4	830		[11]	[15]	[11]	[7]	9	4	878		[7]
9	6	798		[15]	[3]	[1]	[11]	9	8	1134		[5]
9	6	1086		[7]	[5]	[5]	[3]	11	2	958		[3]
9	8	1054		[1]	[7]	[3]	[1]	11	2	1054		[15]
9	10	1310		[3]	[11]	[15]	[5]	11	2	1150		[1]

extended to sums of pairs of m-sequences as well.

For the m-sequences u and v generated by $f_1(x) \equiv 045$ and $f_3(x) \equiv 075$ respectively, Table 44 in Appendix E gives for each value of k the cyclic shift y for which $W = T^y(u \cdot T^k v)$ is an AO/LSE sequence. As an alternative specification of W , the table also gives the AO/LSE (octal) loading of the shift register with characteristic polynomial $f_1(x)f_3(x)$. Tables 45 and 46 give similar results for the polynomial pairs $(f_1(x), f_5(x))$ and $(f_5(x), f_3(x))$ respectively. Notice that in each table, for each value of k , the AO/LSE cyclic shift y yields $\hat{\theta}_{\max}(w) \leq \theta_{\max}(w)!$

A good choice for a subset of the AO/LSE sequences W in Table 44 is the set specified by $\{W: k \in \pi_0, \pi_5\}$, supplemented with the AO/LSE m-sequences U and V . In Table 47, the peak parameters $\hat{\theta}_{\max}(w)$, $\hat{\theta}_{\max}(w, z)$ and $\theta_{\max}(w, z)$ for this subset are tabulated. As predicted by Table 18, the periodic cross-correlation parameter $\theta_{\max}(w, z)$ equals 7 instead of 9 for a number of sequence pairs (w, z) . The interference parameter $r(w, z)$ for this subset is tabulated in Table 48.

Finally we point out that the data in the Tables 44 through 46 can be related -- via equation (5.3) -- to the various cases in Figure 5 (Section 4.4). No specific correlation, however, could be established between, say, norm $\|\lambda_{\sim, \sim}\|$ and occurrences of $\hat{\theta}_{\max}(w)$.

5.4.2. Sequence length $p = 63$

As in Section 5.4.1, one obtains with the trinomial structure and Gauss' products of cyclotomic cosets of integers modulo $p = 63$ (Table 6) the results tabulated in Table 20. Let $\mathcal{J}'$ denote the set of distinct Gold sequences μ, v and $w = \mu + T^k v$, with μ and v generated by

Table 20. Good $\theta_{\max}(w)$ or $\theta_{\max}(w,z)$; $w = u \cdot T^k v$, $z = u \cdot T^m v$; $p = 63$.

u	v	$\theta_{\max}(u,v)$	$\theta_{\max}(w)$	$k \in \eta_x([x])$	$\theta_{\max}(w,z)$	(k,m)
103	147	17	15	$[0],[11],[27]$	15*	$\{G(44,45), G(45,50), G(37,44),$ $G(45,54), G(22,25), G(61,62),$ $G(59,62), G(55,62), G(0,11)\}$
103	155	23	15	$[7], [9],[11],$ $[15],[31]$	9	$G(12,21), G(33,42)$
103	141	15	13	$[13],[21]$	13	$G(0,1), G(17,18), G(20,21),$ $G(32,33), G(44,45), G(47,48),$ $G(55,56), G(1,4), G(20,23),$ $G(22,25), G(26,29), G(27,30),$ $G(34,37), G(2,7), G(11,16),$ $G(13,18), G(20,25), G(22,27),$ $G(26,31), G(31,36), G(39,44),$ $G(47,52), G(58,0), G(14,21),$ $G(15,22), G(30,37), G(39,46),$ $G(6,15), G(7,16), G(11,20),$ $G(14,23), G(20,29), G(29,38),$ $G(9,20), G(10,21), G(20,31),$ $G(36,47), G(46,57), G(59,7),$ $G(0,21), G(6,27), G(9,30)$
103	163	23	15	$[3], [5], [7],$ $[11],[27]$	9	$G(21,30), G(42,51)$
103	133	17	15	$[0], [1],[27]$	15*	$G(0,1), G(27,32), G(45,54),$ $G(1,4), G(1,8), G(16,27),$ $G(10,17), G(17,20), G(5,10)$

the preferred polynomial pair (103,147). The data in Table 20 shows, for example, that a subset of sequences $\{w: k \in \pi_0, \pi_{11}, \pi_{27}\}$ yields a peak parameter $\theta_{\max}(w) = 2^{\lfloor (6+2)/2 \rfloor} - 1 = 15$. Notice also that in some sets of sequences w , with u and v generated by a non-preferred polynomial pair, a considerable decrease of $\theta_{\max}(w)$ or $\theta_{\max}(w,z)$ can be achieved -- if compared with $\theta_{\max}(u,v)$ -- for certain choices of k or (k,m) . Table 21 specifies certain combinations of (k,m) -- up to four sequences in a subset -- for which the periodic peak parameters are both equal or better than $\theta_{\max}(u,v)$ for a specific (u,v) pair.

A complete set of periodic autocorrelation parameters is shown in Table 22. Furthermore, all AO/LSE sequences $W = T^y(u \cdot T^k v)$ were obtained for the polynomial pairs (103,147) and (103,133) with the results reported in Appendix E, Tables 49 and 50. For the AO/LSE phase shifts of sequences w in the subset $\{w: k \in \pi_0, \pi_{11}, \pi_{27}\}$ of $\mathcal{S}'$, the values of $\hat{\theta}_{\max}(w)$, $\hat{\theta}_{\max}(w,z)$ and $\theta_{\max}(w,z)$ as well as $r(w,z)$ are shown in Tables 51 and 52 respectively. Observe that $\theta_{\max}(w,z) = 15$, in fact the function $\theta_{w,z}(\ell)$ is two-valued for a large number of pairs of sequences as was predicted in Table 20.

Of course, other requirements may lead to different choices of subsets. For example, one might want to achieve a lower average value -- over a subset -- of the interference parameter $r(w,z)$. Tables 53 and 54 show the peak correlation parameters and $r(w,z)$ for the subset $\{w: k \in \pi_3, \pi_{21}, \pi_9; k \neq 18\}$. For this subset, the average value of $r(w,z)$ is 19% lower than for subset $\{w: k \in \pi_0, \pi_{11}, \pi_{27}\}$.

Let $\mathcal{S}''$ be the set of distinct sequences u , v and $w = u + T^k v$, with u and v generated by polynomial pair (103,141). A low value of $\theta_{\max}(w) = 13$ -- with $\theta_w(\ell)$ in this case a seven valued function -- is achieved for

Table 21. Good $\theta_{\max}(w)$ and $\theta_{\max}(w,z)$ for selected second combinations;

$$w = u \cdot T^k v; z = u \cdot T^m v; p = 63.$$

u	v	$\theta_{\max}(w)$	$\theta_{\max}(w,z)$	Good (k,m) combinations
103	147	15	15	$\left\{ \begin{array}{l} G(44,45), G(45,50), G(37,44), \\ G(45,54), G(22,25), G(0,11), \\ G(44,45,50), G(0,11,44), G(0,11,25), \\ G(45,54,50), G(11,25,27,54) \end{array} \right.$
103	155	15	15	$G(15,18), G(30,51), G(51,62), G(47,50),$ $G(55,62), G(37,44), G(9,18)$
103	141	15	13	$G(0,1,4), G(20,9,31), G(17,18,61),$ $G(20,11,44), G(18,13,47), G(22,25,15),$ $G(22,25,27), G(44,39,54)$
103	163	15	15	$G(34,37), G(45,48), G(6,11), G(10,17),$ $G(37,44), G(45,54), G(12,33)$
103	133	15	15	$G(0,1), G(27,32), G(45,54),$ $G(1,4), G(1,8), G(16,27),$ $G(0,1,4), G(0,1,8), G(1,4,54),$ $G(1,45,54), G(1,4,54,27)$

Table 22. Periodic autocorrelation functions for $w = u \cdot T^k v$

$$\text{with } k \in \eta_x([x]); p = 63.$$

u: 103 103 v: 147 133					u: 103 103 v: 155 163					u: 103 v: 141				
$\theta_{\max}(w)$	La	M(w)	k	k	$\theta_{\max}(w)$	La	M(w)	k	k	$\theta_{\max}(w)$	La	M(w)	k	k
15	14	3198	[0]	[0]	15	2	2110	[7]	[7]	13	6	3182	[21]	[21]
--	--	----	[11]	[1]	15	2	2366	[31]	[11]	13	6	3502	[13]	[13]
--	--	----	[27]	[27]	15	4	2110	[9]	[27]	15	2	3646	[31]	[31]
17	2	5118	[31]	[5]	15	4	2622	[15]	[3]	15	2	3742	[11]	[11]
17	4	2110	[15]	[15]	15	4	3390	[11]	[5]	15	2	3902	[7]	[7]
--	--	----	[13]	[31]	23	2	3166	[5]	[1]	15	2	4062	[15]	[15]
--	--	----	[23]	[11]	23	2	3678	[23]	[31]	15	4	3438	[23]	[23]
17	8	4158	[3]	[3]	23	2	4126	[1]	[13]	15	4	3982	[3]	[3]
--	--	----	[5]	[13]	--	--	----	[13]	[23]	15	4	4302	[5]	[5]
--	--	----	[7]	[7]	23	4	6686	[3]	[15]	15	4	4782	[1]	[1]
17	12	6206	[1]	[23]	23	4	7038	[27]	[9]	15	6	2526	[0]	[0]
--	--	----	[21]	[21]	23	12	10110	[0]	[0]	15	6	4606	[9]	[9]
17	16	8254	[9]	[9]	23	14	9374	[21]	[21]	15	6	5022	[27]	[27]

the subset $\{\omega: k \in \eta_{13}, \eta_{21}\}$ of $\mathcal{S}''$. A low value of $\theta_{\max}(\omega, z) = 13$ is achieved for many pairs in the subset $\{\omega: k \in \eta_{11}, \eta_{27}\}$ of $\mathcal{S}''$. The AO/LSE phase shifts of the sequences in subset $\{\omega: k \in \eta_{13}, \eta_{21}\}$ and $\{\omega: k \in \eta_{11}, \eta_{27}\}$ are reported in Appendix E, Table 55. The peak correlation parameters and $r(\omega, z)$ for the subset $\{\omega: k \in \eta_{11a}, \eta_{27a}\}$ are shown in Tables 56 and 57.

It should be noted that for sequence length $p = 63$, lower periodic peak parameters can be achieved for the slightly smaller sets of Kasami sequences (Section 5.5).

5.4.3. Sequence lengths $p = 127$ and $p = 255$

For sequence length $p = 127$ it is not possible to specify values of k in $\omega = \mu + T^k v$ such that $\theta_{\max}(\omega) = \theta_{\max}(u, v)$, whenever μ and v are a preferred pair of m -sequences. An ordering, however, of the values $k \in \eta_x$ as a function of the cardinality L_a of the set $\{\ell: |\theta_w(\ell)| = \theta_{\max}(\omega)\}$ can be found for the preferred polynomial pairs. Table 23 gives the results.

Let $\mathcal{S}$ be the set of Gold sequences μ, v and $\omega = \mu + T^k v$ with μ and v generated by the preferred polynomial pair (211, 217). A good choice for a set of sequences in $\mathcal{S}$ with low values of L_a might be the subset $\{\omega: k \in \eta_0, \eta_7, \eta_3\}$ supplemented of course with μ and v . Table 58 in Appendix E specifies the AO/LSE phase shifts of the sequences in subset $\{\omega: k \in \eta_0, \eta_7, \eta_3\}$ as well as $\{\omega: k \in \eta_5\}$. The latter merely for comparative reasons. For the subset $\{\omega: k \in \eta_0, \eta_7\}$ supplemented with U and V , the peak correlation parameters and $r(\omega, z)$ are given in Appendix E, Tables 59 and 60. In addition Table 61 provides the cardinality L_c of the set $\{\ell: |\theta_{w,z}(\ell)| = \theta_{\max}(\omega, z)\}$ for the sequences in above subset. In the case that $z = u$ or $z = v$, $L_c = 28$ for $k \in \eta_0$ and $L_c = 27$ for $k \in \eta_7$.

Table 24 gives results for non-preferred polynomial pairs.

Table 23. Periodic autocorrelation functions for $w = u \cdot T^k v$
 with $k \in \eta_x([x])$ and (u, v) a preferred pair; $\theta_{\max}(w) = 17$; $p = 127$.

		u:	211	211	211	211	211	211	211	211	211
		v:	217	277	325	301	235	253	203	357	247
La	M(w)	k	k	k	k	k	k	k	k	k	k
14	10430	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
18	13374	[7]									[43]
20	13502		[19]						[29]		
20	14398		[43]	[1]	[21]	[13]	[19]	[29]	[31]		
--	-----				[47]		[31]				
22	14526	[3]		[9]	[23]	[9]	[43]	[7]			[11]
--	-----	[13]		[43]		[29]		[13]			[55]
22	15422		[13]	[5]		[27]		[9]	[5]		
--	-----		[15]						[63]		
24	15550	[19]	[7]	[31]	[55]	[19]	[5]	[5]	[1]	[13]	
--	-----			[29]	[27]	[15]	[7]	[31]			
24	16446	[15]		[3]	[7]	[7]	[55]	[47]			[21]
--	-----	[27]									[23]
26	16574	[9]	[3]		[15]		[9]		[19]	[19]	
--	-----		[9]		[29]		[63]		[11]		
--	-----		[27]						[23]		
26	17470	[29]		[27]		[43]		[21]			[5]
26	13438				[1]		[13]				
28	14462	[23]	[63]	[21]	[9]	[1]	[47]	[23]	[9]	[29]	
--	-----					[11]					
28	17598	[43]									[63]
28	18494		[29]		[3]		[29]		[15]		
30	15486	[1]	[5]	[13]	[13]	[31]	[21]	[63]	[7]	[27]	
--	-----	[55]	[1]	[23]	[19]		[15]	[1]	[21]	[31]	
--	-----		[11]						[55]		
30	18622			[11]		[3]		[3]			
32	16510	[11]	[21]	[55]	[5]	[63]	[3]	[15]	[3]	[1]	
--	-----	[21]	[55]	[7]	[63]	[23]	[23]	[19]	[13]	[3]	
--	-----	[31]		[19]				[43]		[9]	
--	-----	[63]		[47]				[55]		[47]	
34	17534	[47]	[31]	[15]	[11]	[5]	[1]	[27]	[27]	[15]	
--	-----					[21]					
--	-----					[47]					
36	18558		[47]			[55]			[43]		
--	-----		[23]						[47]		
38	19582	[5]		[63]	[43]		[11]	[11]			[7]
--	-----				[31]		[27]				

Table 24. Good $\theta_{\max}(w)$; $w = u \cdot T^k v$ and (u, v) a non-preferred pair; $p = 127$.

u	v	$\theta_{\max}(u, v)$	$k \in \eta_x([x])$	$\theta_{\max}(w)$
211	367	41	[0], [3], [5], [7], [9], [11], [19], [21], [29], [31], [55], [63]	23
211	313	41	[47]	17
211	345	41	[31]	17
211	221	21	[01]	19
211	361	41	[63]	17
211	271	41	[63]	17
211	375	41	[0], [1], [7], [19], [21], [23], [27], [29], [31], [43], [47], [63]	23

Finally, Table 25 gives some results for sequences of length $p = 255$. No preferred polynomial pairs exist for this length and good periodic correlation properties for $p = 255$ can better be achieved with the small sets of Kasami sequences (Section 5.5).

5.5. Kasami sequences

In the previous sections we investigated subsets of sequences $w = \mu + T^k v$ with μ and v both m -sequences of period $p = 2^n - 1$ generated by primitive polynomials of degree n .

Let n be even. In this section we consider a special class of sequences again of the type $w = \mu + T^k v$: μ is an m -sequence of period $p = 2^n - 1$ generated by primitive polynomial $f_1(x)$ and v is a sequence of period $p' = 2^{n/2} - 1$ generated by irreducible polynomial $f_s(x)$ of degree

Table 25. Good $\theta_{\max}(w)$; $w = u \cdot T^k v$; $p = 255$.

u	v	$\theta_{\max}(u,v)$	$k \in \eta_x([x])$	$\theta_{\max}(w)$
435	551	63	[1], [7], [13], [15], [21], [23], [25], [27], [31], [37], [39], [45], [47], [51], [53], [61], [87], [95], [111], [127]	33
435	747	65	[9], [27], [87]	33
435	545	47	[51], [119]	31
435	543	63	[1], [9], [25], [27], [29], [31], [37], [39], [43], [61], [63], [87], [95]	31
435	455	31	All	31
435	703	95	[3], [11], [37], [61], [63], [91]	33
435	607	63	[17], [85], [119]	17
435	561	31	All	31
435	765	31	All	31
435	717	63	[3], [9], [13], [19], [21], [29], [31], [39], [53], [55], [95], [111], [127]	31
435	651	47	[17], [51]	31
435	615	65	[39], [63], [87]	33
435	537	63	[5], [7], [9], [15], [19], [23], [25], [27], [31], [37], [39], [45], [47], [51], [53], [59], [63], [91], [111], [127]	33

$n/2$ whereby $s = 2^{n/2} + 1$. One can think of v as a concatenation of $2^{n/2} + 1$ m -sequences v' of length $p' = 2^{n/2} - 1$. A shift register with $f_1(x)f_s(x)$ as characteristic polynomial will generate $2^{n/2}$ sequences of period $p = 2^n - 1$ (μ and $\omega = \mu + T^k v$, $k = 0, 1, \dots, 2^{n/2} - 1$). Those sequences, and their cyclic shifts, are referred to as Kasami sequences. Kasami (1966) specified the distribution of the Hamming weight of those sequences. From this weight distribution it follows that the periodic cross-correlation $\theta_{u,v}(\tau)$ takes on the value $\theta_{u,v}(\tau) = 2^{n/2} - 1$ for $2^{n-1} + 2^{n/2-1}$ values of τ and $\theta_{u,v}(\tau) = -2^{n/2} - 1$ for $2^{n-1} - 2^{n/2-1} - 1$ values of τ , where $\tau \in [0, p-1]$.

Of course $\theta_{u,v}(\tau_2) = \theta_{u,v}(\tau_1)$ whenever $\tau_2 = \tau_1 \bmod p'$. Hence, we can determine $\theta_{u,v}(\tau)$, $\tau \in \eta_x$ by specifying $\theta_{u,v}(\tau)$ for $\tau \in \eta_x'$ whereby η_x' denotes the cyclotomic coset of integers modulo p' .

Again $\omega = \mu + T^k v$ and $\zeta = \mu + T^m v$, with μ and v' , and thus v , in their natural orientation. Immediately we have

$$\theta_{\max}(w) \leq \theta_{\max}(w, z) \leq 2^{n/2} + 1. \quad (5.10)$$

As in Section 5.2 it follows that

$$\theta_{w,z}(\ell) = \begin{cases} p & \text{if } \ell = 0 \bmod p, m-k = 0 \bmod p' \\ -p/p' & \text{if } \ell = 0 \bmod p, m-k \neq 0 \bmod p' \\ -1 & \text{if } \ell \neq 0 \bmod p, \ell+m-k = 0 \bmod p' \\ \theta_{u,v}(k+s(\ell)-r(\ell)), & \text{otherwise} \end{cases} \quad (5.11)$$

where functions $s(\ell)$ and $r(\ell)$ are specified as in equation (5.4) and $p/p' = 2^{n/2} + 1$. As a special case one obtains, with $u \neq w$,

$$\theta_{u,w}(\ell) = \begin{cases} -p/p' & \text{if } \ell \equiv 0 \pmod{p} \\ \theta_{u,v}(k+\ell-r(\ell)), & \text{otherwise.} \end{cases} \quad (5.12)$$

Notice that $|\theta_{w,z}(0)| = 2^{n/2} + 1 = \theta_{\max}(u,v)$ whenever $m-k \not\equiv 0 \pmod{p'}$. Therefore $\theta_{\max}(w,z) < \theta_{\max}(u,v)$ is impossible for any subset of pairs of Kasami sequences, and our main attention will focus on the number of times $\theta_{\max}(w,z)$ occurs for subsets of Kasami sequences.

5.5.1. Sequence length $p = 63$

Let $f_1(x) = x^6 + x + 1$ (103) generate m -sequence u of period $p = 2^6 - 1 = 63$. Then $f_s(x) = x^3 + x^2 + 1$ (015) with $s = 2^3 + 1 = 9$ will generate sequence v of period $p' = 2^3 - 1 = 7$. With the matrix X_u of Table 7 one obtains $\theta_{u,v}(\ell) = 7$ for $\ell \in \eta_0'$ and η_3' while $\theta_{u,v}(\ell) = -9$ for $\ell \in \eta_1'$.

Case 1: $m-k \equiv 0 \pmod{p'}$

With the trinomial structure of m -sequence u and v' it is easy to show that function $k + s(\ell) - r(\ell) \pmod{p'}$ in (5.11) does take on values in η_1' , for all k . Thus $\theta_{\max}(w) = \theta_{\max}(u,v) = 9$. However the cardinality La of the set $\{\ell: |\theta_w(\ell)| = \theta_{\max}(w)\}$ is a function of k and one finds

$$La = \begin{cases} 22 & \text{if } k \in \eta_1' \\ 24 & \text{if } k \in \eta_0', \eta_3'. \end{cases} \quad (5.13)$$

Case 2: $m-k \not\equiv 0 \pmod{p'}$

Let

$$G'(x,y) = ((x \cdot 2^j \pmod{p'}, y \cdot 2^j \pmod{p'})), \quad j = 0, 1, \dots \quad (5.14)$$

denote a series of pairs (x,y) . With the same method as used in Section 5.3 it is easy to show that for sequence pairs $(\omega = \mu + T^k v, \zeta = \mu + T^m v)$ the cardinality L_c equals

$$L_c = \begin{cases} 27 & \text{if } (k,m) = G'(0,1), G'(1,3), G'(1,5), G'(1,6) \\ 18 & \text{if } (k,m) = G'(1,2) \\ 20 & \text{if } (k,m) = G'(0,3), G'(3,5) . \end{cases} \quad (5.15)$$

Observe that $G'(1,2,4)$ are triples for which $L_a = 22$ and $L_c = 18$.

In the special case that m -sequence μ is correlated with $\omega = \mu + T^k v$ one finds $L_c = 28$ for $k \in \eta_0'$ and η_3' while $L_c = 27$ for $k \in \eta_1'$.

Table 26 specifies the AO/LSE phase shifts of above discussed Kasami sequences. The peak correlation parameters and $r(w,z)$ are given in Tables 27 and 28 respectively.

5.5.2. Sequence length $p = 255$

The results for this sequence length are of particular interest because no preferred pairs of polynomials can be selected thus no sets of Gold sequences exist.

Let $f_1(x) = x^8 + x^4 + x^3 + x^2 + 1$ (435) generate m -sequence μ of period $p = 2^8 - 1 = 255$. Then $f_s(x) = x^4 + x + 1$ (023) with $s = 2^4 + 1 = 17$ will generate sequence v of period $p' = 15$. One obtains $\theta_{u,v}(\ell) = 15$ for $\ell \in \eta_1'$ and η_3' while $\theta_{u,v}(\ell) = -17$ for $\ell \in \eta_0', \eta_5'$ and η_7' .

As in 5.5.1. one has $\theta_{\max}(w) = \theta_{\max}(w,z) = 17$ for all w and (w,ζ) . For sequences ω , one finds for cardinality L_a

Table 26. AO/LSE sequences U and $W = T^y(u \cdot T^k v)$; $u:103$, $v:015$; $p = 63$.

$\theta_{\max}(w)$	La	M(w)	k	Loading	y	$\hat{\theta}_{\max}(w)$	$\hat{La}$	S(w)	$\hat{M}(w)$
9	24	3422	0	3733	60	13	4	1455	2398
9	22	3358	1	1771	33	11	4	1395	2222
			2	4506	60	11	8	1331	1966
			4	0263	8	11	6	1427	2350
9	24	3422	3	5261	6	13	2	1483	2510
			5	1043	55	11	4	1423	2270
			6	6544	33	11	2	1247	1566
1	62	62	U	0206	1	11	2	427	1646

Table 27. Correlation values for the AO/LSE sequences U and $W = T^y(u \cdot T^k v)$; $u:103$, $v:015$; $p = 63$.

k	0	1	2	4	3	5	6	U
0	13	19	19	21	23	17	15	21
1	9	11	23	17	17	15	23	21
2	9	9	11	19	19	17	17	15
4	9	9	9	11	17	23	21	21
3	9	9	9	9	13	21	21	19
5	9	9	9	9	9	11	21	17
6	9	9	9	9	9	9	11	21
U	9	9	9	9	9	9	9	11

Table 28. Interference parameter $r(w, z)$ for the AO/LSE sequences U and $W = T^y(u \cdot T^k v)$; $u:103$, $v:015$; $p = 63$.

k	1	2	4	3	5	6	U
0	9570	7402	8106	7338	6846	7838	8962
1		6518	7982	7030	6842	8074	9022
2			6950	6614	6962	6242	6854
4				7742	6642	8770	8830
3					6002	6986	7638
5						7126	6674
6							8282

$$L_a = \begin{cases} 110 & \text{if } k \in \eta_0', \eta_5' \\ 112 & \text{if } k \in \eta_1', \eta_3' \end{cases} \quad (5.16)$$

For the sequence pairs (ω, ζ) one finds for cardinality L_c

$$L_c = \begin{cases} 102 & \text{if } (k, m) = \begin{cases} G'(0,5), G'(0,7); G'(7,14), G'(7,13); \\ G'(5,7), G'(5,14), G'(5,13), G'(5,11). \end{cases} \\ 104 & \text{if } (k, m) = \begin{cases} G'(1,2), G'(1,4); G'(3,6), G'(3,12); \\ G'(1,3), G'(1,6), G'(1,12), G'(1,9). \end{cases} \\ 119 & \text{if } (k, m) = \begin{cases} G'(0,1), G'(0,3); G'(1,5), G'(1,10); \\ G'(3,5), G'(3,10); \\ G'(1,7), G'(1,14), G'(1,13), G'(1,11); \\ G'(3,7), G'(3,14), G'(3,13), G'(3,11). \end{cases} \end{cases} \quad (5.17)$$

In the special case that m -sequence μ is correlated with ω one obtains $L_c = 119$ for $k \in \eta_0', \eta_5'$ and η_7' while $L_c = 120$ for $k \in \eta_1'$ and η_3' .

Table 29 specifies the AO/LSE phase shifts of above discussed sequences while Tables 30 and 31 report the resulting peak correlation parameters and $r(w, z)$. Observe from Table 30 that $\theta_c = 17$ and $\hat{a}_c = 51$ for the set of AO/LSE Kasami sequences of length $p = 255$ generated by polynomial pair $(f_1(x), f_9(x)) = (103, 023)$. In contrast, $\theta_c = 95$ and $\hat{\theta}_c = 81$ for the set of AO/LSE m -sequences of length $p = 255$ as reported in Table 42!

Table 31. Interference parameter $r(w, z)$ for AO/LSE sequences U and $W = T^y(u \cdot T^k v)$; $u:435$, $v:023$; $p = 255$.

k	1	2	4	8	3	6	12	9	5	10	7	14	13	11	U
0	125734	123698	130722	129994	124526	120830	132730	128542	131150	130534	132078	129018	123522	115362	135574
1		123394	119914	118442	123686	118158	121346	120782	112358	124318	128670	115058	116570	113026	128382
2			113198	113622	116578	115546	117742	127706	122034	130410	125074	125542	118446	110846	123138
4				123142	121986	109026	119846	122906	113794	129050	126450	125342	108894	114606	131322
8					132146	122426	132038	134594	113810	130826	128330	131502	129150	127550	127482
3						129134	131602	135670	121582	130966	133622	130042	129122	121954	133454
6							123370	116758	111158	118126	124654	128898	109890	124730	124430
12								127154	128114	128362	128762	131486	137286	130990	126746
9									129782	136198	137310	126362	120898	122290	140342
5										120998	115326	124482	130346	118570	125166
10											133726	133202	124690	124306	138126
7												121938	122186	121130	139798
14													121734	120670	131090
13														115382	120906
11															127538

CHAPTER 6

CONCLUSIONS

The asymptotic behavior of the aperiodic correlation parameters of random binary sequences has been studied and an accurate approximation of the average signal-to-noise ratio at the correlation receiver output was obtained. This result is very useful for preliminary system design. Those m-sequences that are best suited for synchronization as well as multiple-access were reported. The relationship between the third central moments of the odd correlation functions and the trinomial structure of m-sequences has been studied. Actual data showed, however, that the third central moment is not a very effective indication of good aperiodic correlation properties. A new method based on Gauss' products of cyclotomic cosets was presented and applied to obtain new subsets of sequences with better correlation properties.

The importance of the data presented in this thesis stems from its use in the selection of sequences for SSMA systems. This can be illustrated by a particular example. Suppose that there are $K=8$ users for a SSMA system and expression (2.29) indicates that for the system $\mathcal{E}_b/N_0$, the required sequence length is $p = 255$. One should select the eight AO/LSE m-sequences as given in Table 41 (p. 104) if the synchronization and anti-multipath requirements necessitate this. If, however, the peak cross-correlation parameters are of primary concern one should select eight AO/LSE Kasami sequences from Table 29 (p. 83) with $k \in \mathbb{F}_0, \mathbb{F}_5, \mathbb{F}_7$ and U . In the latter table up to sixteen users can be accommodated.

REFERENCES AND SELECTED BIBLIOGRAPHY

Abramson, N., and Kuo, F. F., (editors), Computer Communication Networks. Englewood Cliffs, New Jersey: Prentice-Hall, 1973.

Ackroyd, M. H., "Synthesis of efficient Huffman sequences," IEEE Transactions on Aerospace and Electronic Systems, vol. AES-8, pp. 2-6, January 1972.

Aein, J. M., "Multiple access to a hard-limiting communication satellite repeater," IEEE Transactions on Space Electronics and Telemetry, vol. SET-10, pp. 159-167, December 1964.

Aein, J. M., and Schwartz, J. M., (editors), "Multiple access to a communication satellite with a hard-limiting repeater--Volume II: Proceedings of the IDA multiple access summer study," Institute for Defense Analysis, Report R-108, January 1965.

Altman, F. J., et al., "Satellite communications reference data handbook," U.S. Department of Commerce, National Technical Information Service, Report AD-746 165, July 1972.

Anderson, D. R., "A new class of cyclic codes," SIAM Journal of Applied Mathematics, vol. 16, pp. 181-197, January 1968.

Anderson, D. R., and Wintz, P. A., "Analysis of a spread-spectrum multiple access system with a hard limiter," IEEE Transactions on Communication Technology, vol. COM-17, pp. 285-290, April 1969.

Arazi, B., "Decimation of m -sequences leading to any desired phase shift," Electronics Letters, vol. 13, pp. 213-215, March 1977.

Baier, W. P., "On parasitic correlation peaks in cross-correlation circuits for binary pseudorandom sequences," IEEE Transactions on Communications, vol. COM-24, pp. 1143-1148, October 1976.

Bajoga, B. G., and Walbesser, W. J., "Generation of irreducible polynomials from trinomials over $GF(2)$. I," Information and Control, vol. 30, pp. 396-407, April 1976.

Barker, R. H., "Group synchronizing of binary digital systems," in Communication Theory, (Jackson, W., editor). New York: Academic Press, 1953.

Bearce, L. S., and Ziffer, A. J., "Mean and variance of the correlation magnitude of random and pseudonoise sequences," Naval Research Laboratory, Washington, D.C., Report 8068, November 1976.

Berlekamp, E. R., Algebraic Coding Theory. New York: McGraw-Hill, 1968.

Bernfeld, M., "A property of binary sequences," Proceedings of the IEEE, vol. 52, p. 744, June 1964.

Blasbalg, H., "A comparison of pseudo-noise and conventional modulation for multiple-access satellite communications," IBM Journal, vol. 9, pp. 241-255, July 1965.

Blasblag, H., Najjar, H. F., D'Antonio, R. H., and Haddad, R. A., "Air-ground ground-air communications using pseudo-noise through satellite," IEEE Transactions on Aerospace and Electronic Systems, vol. AES-4, pp. 774-790, September 1968.

Boehmer, A. M., "Binary pulse compression codes," IEEE Transactions on Information Theory, vol. IT-13, pp. 156-167, April 1967.

Briggs, P. A. N., and Godfrey, K. R., "Design of uncorrelated signals," Electronics Letters, vol. 12, pp. 555-556, October 1976.

Calabro, D., and Paolillo, J., "Synthesis of cyclically orthogonal binary sequences of the same least period," IEEE Transactions on Information Theory, vol. IT-14, pp. 756-759, September 1968.

Calabro, D., and Wolf, J. K., "On the synthesis of two-dimensional arrays with desirable correlation properties," Information and Control, vol. 11, pp. 537-560, November 1968.

Cartier, D. E., "Partial correlation properties of pseudonoise (PN) codes in noncoherent synchronization/detection schemes," IEEE Transactions on Communications, vol. COM-24, pp. 899-903, August 1976.

Chakrabarti, N. B., and Tomlinson, M., "Design of sequences with specified autocorrelation and cross correlation," IEEE Transactions on Communications, vol. COM-24, pp. 1246-1252, November 1976.

Chang, J. A., "Ternary sequence with zero correlation," Proceedings of the IEEE, vol. 55, pp. 1211-1213, July 1967.

Chen, C. L., "Computer results on the minimum distance of some binary cyclic codes," IEEE Transactions on Information Theory, vol. IT-16, pp. 359-360, May 1970.

Chesler, D., "Performance of a multiple address RADA system," IEEE Transactions on Communication Technology, vol. COM-14, pp. 369-372, August 1966.

Chien, T., "A recursive formula for the correlations of Walsh functions," Journal of the Franklin Institute, vol. 301, pp. 371-377, April 1976.

Chu, D. C., "Polyphase codes with good periodic correlation properties," IEEE Transactions on Information Theory, vol. IT-18, pp. 531-532, July 1972.

Cohen, A. R., Heller, J. A., and Viterbi, A. J., "A new coding technique for asynchronous multiple access communication," IEEE Transactions on Communication Technology, vol. COM-19, pp. 849-855, October 1971.

Corr, F., Crutchfield, R., and Marchese, J., "A pulsed pseudo-noise VHF radio set," IBM Journal, vol. 9, pp. 256-263, July 1965.

Dixon, R. C., Spread Spectrum Systems, New York: Wiley, 1976.

Drouilhet, P. R., Jr., and Bernstein, S. L., "TATS - A bandspread modulation - demodulation system for multiple access tactical satellite communication," EASCON Convention Record, pp. 126-132, 1969.

Forney, G. D., Jr., "Coding and its application in space communications," IEEE Spectrum, vol. 7, pp. 47-58, June 1970.

Frank, R. L., "Polyphase codes with good nonperiodic correlation properties," IEEE Transactions on Information Theory, vol. IT-9, pp. 43-45, January 1963.

Frank, R. L., and Zadoff, S. A., "Phase shift pulse codes with good periodic correlation properties," IEEE Transactions on Information Theory, vol. IT-8, pp. 381-382, October 1962.

Fredricsson, S. A., "Pseudo-randomness properties of binary shift register sequences," IEEE Transactions on Information Theory, vol. IT-21, pp. 115-120, January 1975.

Gagliardi, R. M., "Rapid acquisition signal design in a multiple-access environment," IEEE Transactions on Aerospace and Electronic Systems, vol. AES-10, pp. 359-363, May 1974.

Gebhardt, F., and Weber, C. L., "Aperiodic correlation properties of pseudo-noise codes," Electronic Science Laboratory, University Southern California, USCEE Report 430, October 1972.

Geffe, P. R., "Open letter to communications engineers," Proceedings of the IEEE, vol. 55, pp. 2173, December 1967.

Gerhardt, L. A., (lecture series director), "Spread spectrum communications," AGARD Lecture Series No. 58, NATO, July 1973.

Gilson, R. P., "Some results of amplitude distribution experiments on shift register generated pseudo-random noise," IEEE Transactions on Electronic Computers, vol. EC-15, pp. 926-927, December 1966.

Golay, M. J. E., "A class of finite binary sequences with alternate autocorrelation values equal to zero," IEEE Transactions on Information Theory, vol. IT-18, pp. 449-450, May 1972.

Golay, M. J. E., "Sieves for low autocorrelation binary sequences," IEEE Transactions on Information Theory, vol. IT-23, pp. 43-51, January 1977.

Gold, R., and Kopitzke, E., "Study of correlation properties of binary sequences," Interis Technical Report Number 1, (AD 470696), Magnavox Research Laboratories, Torrance, California, August 1965.

Gold, R., "Characteristic linear sequences and their coset functions," SIAM Journal of Applied Mathematics, vol. 14, pp. 980-985, September 1966.

Gold, R., "Optimal binary sequences for spread spectrum multiplexing," IEEE Transactions on Information Theory, vol. IT-13, pp. 619-621, October 1967.

Gold, R., "Maximal recursive sequences with 3-valued recursive cross-correlation functions," IEEE Transactions on Information Theory, vol. IT-14, pp. 154-156, January 1968.

Gold, R., "Study of multi-state PN sequences and their application to communication systems," U.S. Department of Commerce, National Technical Information Service, Report AD-A025 137/1GA, Appendix F, March 1976.

Golomb, S. W., et al., Digital Communications with Space Applications. Englewood Cliffs, New Jersey: Prentice-Hall, 1964.

Golomb, S. W., Shift Register Sequences. San Francisco: Holden-Day, 1967.

Golomb, S. W., "Theory of transformation groups of polynomials over $GF(2)$ with applications to linear shift register sequences," Information Sciences, vol. 1, pp. 87-109, December 1968.

Golomb, S. W., "Irreducible polynomials, synchronization codes, primitive necklaces, and the cyclotomic algebra," in Combinatorial Mathematics and Its Applications, (Bose, R. C., and Dowling, T. A., editors). Chapel Hill, North Carolina: University of North Carolina Press, 1969.

Golomb, S. W., and Scholtz, R. A., "Generalized Barker sequences," IEEE Transactions on Information Theory vol. IT-11, pp. 533-537, October 1965.

Harmuth, H. F., Transmission of Information by Orthogonal Functions (2nd Edition). New York: Springer-Verlag, 1972.

Harris, R. L., "Introduction to spread-spectrum techniques," in "Spread spectrum communications," AGARD Lecture Series No. 58, NATO, July 1973.

Hartmann, C. R. P., Riek, J. P., Jr., and Longobardi, R. J., "Weight distributions of some classes of binary cyclic codes," IEEE Transactions on Information Theory, vol. IT-21, pp. 345-350, May 1975.

Heimiller, R. C., "Phase shift pulse codes with good periodic correlation properties," IRE Transactions on Information Theory, vol. IT-7, pp. 254-257, October 1961.

Helleseth, T., "Some two-weight codes with composite parity-check polynomials," IEEE Transactions on Information Theory, vol. IT-22, pp. 631-632, September 1976.

Huang, R. Y., and Hooten, P., "Communication satellite processing repeaters," Proceedings of the IEEE, vol. 59, pp. 238-252, February 1971.

Huber, J., "Simple asynchronous multiplex system for unidirectional low-data-rate transmission," IEEE Transactions on Communications, vol. COM-23, pp. 675-679, June 1975.

Kuffman, D. A., "The generation of impulse-equivalent pulse trains," IEEE Transactions on Information Theory, vol. IT-8, pp. 10-16, September 1962.

Jelinek, F., "Three signaling systems for double access to an active satellite," IEEE Transactions on Communication Technology, vol. COM-14, pp. 140-157, April 1966.

Jeruchim, M. C., "A survey of interference problems and applications to geostationary satellite networks," Proceedings of the IEEE, vol. 65, pp. 317-331, March 1977.

Jordan, H. F., and Wood, D. C. M., "On the distribution of sums of successive bits of shift-register sequences," IEEE Transactions on Computers, vol. C-22, pp. 400-408, April 1973.

Kaiser, J., Schwartz, J. W., and Aein, J. M., "Multiple access to a communication satellite with a hard-limiting repeater,--Volume I: Modulation techniques and their applications," Institute of Defense Analysis, Report R-108, January 1965.

Kasami, T., "Weight distribution formula for some class of cyclic codes," Coordinated Science Laboratory, University of Illinois, Report R-285, April 1966.

Kasami, T., "Some lower bounds on the minimum weight of cyclic codes of composite length," IEEE Transactions on Information Theory, vol. IT-14, pp. 814-818, November 1968.

Kendall, W. B., "A new algorithm for computing correlations," IEEE Transactions on Computers, vol. C-23, pp. 88-90, January 1974.

Lebow, I. L., Jordan, K. L., Jr., and Drouilhet, P. R., Jr., "Satellite communications to mobile platforms," Proceedings of the IEEE, vol. 59, pp. 139-159, February 1971.

Lee, J., and Smith, D. R., "Families of shift-register sequences with impulsive correlation properties," IEEE Transactions on Information Theory, vol. IT-20, pp. 255-261, March 1974.

Lempel, A., "Analysis and synthesis of polynomials and sequences over $GF(2)$," IEEE Transactions on Information Theory, vol. IT-17, pp. 297-303, May 1971.

Lempel, A., and Greenberger, H., "Families of sequences with optimal Hamming correlation properties," IEEE Transactions on Information Theory, vol. IT-20, pp. 90-94, January 1974.

Lempel, A., Cohn, M., and Eastman, W. L., "A class of balanced binary sequence with optimal autocorrelation properties," IEEE Transactions on Information Theory, vol. IT-23, pp. 38-42, January 1977.

Lerner, R. M., "Signals having good correlation functions," WESCON Convention Record, 1961.

Levitt, K. N., and Wolf, J. K., "On the interleaving of two-level periodic binary sequences," Proceedings of the N.E.C., pp. 644-649, 1965.

Lindholm, J. H., "An analysis of the pseudo-randomness properties of subsequences of long m-sequences," IEEE Transactions on Information Theory, vol. IT-14, pp. 569-576, July 1968.

Lindner, J., "Binary sequences up to length 40 with best possible autocorrelation function," Electronics Letters, vol. 11, p. 507, October 1975.

Lindsey, W., Synchronization Systems. Englewood Cliffs, New Jersey: Prentice-Hall, 1972.

Lint, J. H. van, Coding Theory. New York: Springer-Verlag, 1971.

MacWilliams, J., "An example of two cyclically orthogonal sequences with maximum period," IEEE Transactions on Information Theory, vol. IT-13, pp. 338-339, April 1967.

MacWilliams, F. J., and Sloane, N. J. A., "Pseudo-random sequences and arrays," Proceedings of the IEEE, vol. 64, pp. 1715-1730, December 1976.

Mann, H. B., (editor), Error Correcting Codes. New York: Wiley, 1969.

Massey, J. L., and Uhran, J. J., Jr., "Final report for multipath study," (Contract No. NAS 5-10786), Department of Electrical Engineering, University of Notre Dame, 1969.

Massey, J. L., and Uhran, J. J., Jr., "Sub-baud coding," Proceedings of the Thirteenth Annual Allerton Conference on Circuit and System Theory, pp. 539-547, October 1975.

Mattson, H. F., "A note on the ambiguity function," SIAM Journal of Applied Mathematics, vol. 11, pp. 732-736, September 1963.

McCalmont, A. M., "Multiple-access discrete-address communication systems," IEEE Spectrum, pp. 87-94, August 1967.

Meshkovskii, K. A., "A new class of pseudorandom sequences of binary signals," Problemy Peredachi Informatsii, Vol. 9, pp. 117-119, July 1973.

Milstein, L. B., "The use of combination sequences in a multiple access environment," Proceedings of the Thirteenth Annual Allerton Conference on Circuit and System Theory, pp. 21-27, October 1975.

Milstein, L. B., "Some statistical properties of combination sequences," IEEE Transactions on Information Theory, vol. COM-25, pp. 254-258, March 1977.

Milstein, L. B., and Ragonetti, R. R., "Combination sequences for spread spectrum communications," IEEE Transactions on Communications, vol. COM-25, pp. 691-696, July 1977.

Mohanty, N. C., "Signal design for asynchronous multiple access communications," Proceedings of the Twelfth Annual Allerton Conference on Circuit and System Theory, pp. 775-781, October 1974.

Mohanty, N. C., "Multiple Frank-Heimiller signals for multiple access systems," IEEE Transactions on Aerospace and Electronic Systems, vol. AES-11, pp. 622-628, July 1975.

Moharir, P. S., "Signal design", International Journal of Electronics, vol. 41, pp. 381-398, October 1976.

Moon, J. W., and Moser, L., "On the correlation function of random binary sequences," SIAM Journal of Applied Mathematics, vol. 16, pp. 340-343, March 1968.

Niho, Y., "Multi-valued cross-correlation functions between two maximal linear recursive sequences," Electronic Science Laboratory, University of Southern California, USCEE Report 409, January 1972.

O'Meara, T. R., "Binary autocorrelation computation and synthesis without multiplication," Proceedings of the IEEE, vol. 55, pp. 95-96, January 1967a.

O'Meara, T. R., "Ensemble correlation function computation by multiplication," Proceedings of the IEEE, vol. 55, January 1967b.

Pelekhatyi, M. I. and Golubev, E. A., "Autocorrelative properties of certain types of binary sequences," Problemy Peredachi Informatsii, vol. 8, pp. 52-99, January 1972.

Peterson, W. W., and Weldon, Jr., E. J., Error Correcting Codes (2nd Edition). Cambridge, Massachusetts: MIT Press, 1972.

Pritchard, W. L., "Satellite communication - an overview of the problems and programs," Proceedings of the IEEE, vol. 65, pp. 294-307, 1977.

Puente, J. G., Schmidt, W. G., and Werth, A. M., "Multiple-access techniques for commercial satellites," Proceedings of the IEEE, vol. 59, pp. 218-229, February 1971.

Pursley, M. B., "Evaluating performance of codes for spread spectrum multiple-access communications," Proceedings of the Twelfth Annual Allerton Conference on Circuit and System Theory, pp. 765-774, October 1974.

Pursley, M. B., "The role of coding in multiple-access satellite communication systems," Coordinated Science Laboratory, University of Illinois, Report R-724, April 1976a.

Pursley, M. B., "Recent advances in coding for multiple access communication systems," Proceedings of the International Telemetry Conference, Los Angeles, California, pp. 24-33, September 1976b.

Pursley, M. B., and Sarwate, D. V., "Correlation parameters for periodic sequences--properties, bounds and efficient computational methods," Coordinated Science Laboratory, University of Illinois, Report R-725, April 1976a.

Pursley, M. B., and Sarwate, D. V., "Bounds on aperiodic correlation for binary sequences," Electronics Letters, vol. 12, pp. 304-305, 1976b.

Roefs, H. F. A., and Pursley, M. B., "Correlation parameters of random and maximal length sequences for spread-spectrum multiple-access communication," Proceedings of the 1976 IEEE Canadian Communications and Power Conference pp. 141-143, October 1976.

Roefs, H. F. A., Sarwate, D. V., and Pursley, M. B., "Periodic correlation functions of sums of pairs of m-sequences," Proceedings of the 1977 Conference on Information Sciences and Systems, Johns Hopkins University, March 1977a.

Roefs, H. F. A., and Pursley, M. B., "Correlation parameters of random binary sequences," accepted for publication by Electronics Letters, August 1977b.

Sarwate, D. V., and Pursley, M. B., "Applications of coding theory to spread-spectrum multiple-access satellite communications," Proceedings of the 1976 IEEE Canadian Communications and Power Conference, October 1976.

Sarwate, D. V. and Pursley, M. B., "New correlation identities for periodic sequences," Electronics Letters, vol. 13, pp. 48-49, January 1977.

Savage, J. E., "Signal detection in the presence of multiple-access noise," IEEE Transactions on Information Theory, vol. IT-20, pp. 42-49, January 1974.

Schneider, K. S., and Orr, R. S., "Aperiodic correlation constraints on large binary sequence sets," IEEE Transactions on Information Theory, vol. IT-21, pp. 79-84, January 1975.

Schroeder, M. R., "Synthesis of low-peak-factor signals and binary sequences with low autocorrelation," IEEE Transactions on Information Theory, vol. IT-16, pp. 85-89, January 1970.

Seguin, G., "Binary sequences with specified correlation properties," Department of Electrical Engineering, University of Notre Dame, Technical Report No. 7103, August 1971.

Sidel'nikov, V. M., "Some k-valued pseudo-random sequences and nearly equidistant codes," Problemy Peredachi Informatsii, vol. 5, pp. 16-22, 1969.

Sidel'nikov, V. M., "On mutual correlation of sequences," Soviet Math. Dokl., vol. 12, pp. 197-201, 1971.

Simmons, G. J., "Two algorithms for the direct computation of binary correlation functions," Proceedings of the IEEE, vol. 55, pp. 1638-1639, September 1967.

Simon, M. K., "Noncoherent pseudonoise code tracking performance of spread spectrum receivers," IEEE Transactions on Communications, vol. COM-25, pp. 327-345, March 1977.

Smirnov, N. I., "Application of m-sequences in asynchronous radio systems," Telecommunications, vol. 24, pp. 26-34, 1970.

Smirnov, N. I., "Channel for rapid synchronization of a multiple-address system with code separation," Telecommunications, vol. 27, pp. 43-50, 1973.

Smirnov, N. I., and Golubkov, N. A., "Correlation properties of segments of m-sequences," Telecommunications, vol. 28, pp. 123-125, 1973.

Somaini, U., "Binary sequences with good correlation properties," Electronics Letters, vol. 11, pp. 278-279, June 1975.

Sommer, R. C., "High efficiency multiple access communications through a signal processing repeater," IEEE Transactions on Communication Technology, vol. COM-16, pp. 222-232, April 1968.

Stampfl, R. A., and Jones, A. E., "Tracking and data relay satellites," IEEE Transactions on Aerospace and Electronic Systems, vol. AES-6, pp. 276-289, May 1970.

Stiglitz, I. G., "Multiple-access considerations -- A satellite example," IEEE Transactions on Communications, vol. COM-21, pp. 577-582, May 1973.

Sywyk, M. R., "Sub-baud codes for code multiplexing," Department of Electrical Engineering, Royal Military College of Canada, May 1975.

Titworth, R. C., "Optimal ranging codes," IEEE Transactions on Space Electronics and Telemetry, vol. SET-10, pp. 19-30, March 1964.

Tomlinson, G. H., and Galvin, P., "Generation of Gaussian signals from summed m-sequences," Electronics Letters, vol. 11, pp. 521-522, October 1975.

Tretter, S. A., "Properties of PN^2 Sequences," IEEE Transactions on Information Theory, vol. IT-20, pp. 295-297, March 1974.

Turyn, R., "Sequences with small correlation," in Error Correcting Codes, (Mann, H. B., editor). New York: Wiley, 1968.

Turyn, R., and Storer, J., "On binary sequences," Proceedings of the American Mathematical Society, vol. 12, pp. 394-399, 1961.

Van Blerkom, R., Sears, R. E., and Freeman, D. G., "Analysis and simulation of a digital matched filter receiver of pseudo-noise signals," IBM Journal, vol. 9, pp. 264-273, July 1965.

Viterbi, A. J., and Jacobs, I. M., "Advances in coding and modulation for noncoherent channels affected by fading, partial band, and multiple-access interference," in Advances in Communication Systems, vol. 4 (A. J. Viterbi, editor). New York: Academic Press, 1975.

Wainberg, S., and Wolf, J. K., "Subsequences of pseudorandom sequences," IEEE Transactions on Communication Technology, vol. COM-18, pp. 606-612, October 1970.

Weathers, G. D., Graf, E. R., and Wallace, G. R., "The subsequence weight distribution of summed maximum length digital sequences," IEEE Transactions on Communications, vol. COM-22, pp. 997-1004, August 1974.

Welch, L. R., "Trace mappings in finite fields and shift register correlation properties," Electrical Engineering Department, University of Southern California, 1969.

Welch, L. R., "Lower bounds on the maximum cross correlation of signals," IEEE Transactions on Information Theory, vol. IT-20, pp. 397-399, May 1974.

Weng, L., "Decomposition of m-sequences and its applications," IEEE Transactions on Information Theory, vol. IT-17, pp. 457-463, July 1971.

White, W. D., "Theoretical aspects of asynchronous multiplexing," Proceedings of the IRE, vol. 38, pp. 270-275, March 1950.

Willett, M., "Characteristic m-sequences," Mathematics of Computation, vol. 30, pp. 306-311, April 1976.

Wittman, J. H., "Categorization of multiple-access/random-access modulation techniques," IEEE Transactions on Communication Technology, vol. COM-15, pp. 724-725, October 1967.

Wolf, J. K. and Elspas, B., "Mutual interference due to correlated constant-envelope signals," in "Multiple access to a communication satellite with a hard-limiting repeater--Volume II," (Aein, J. M., and Schwartz, J. W., editors), Institute of Defense Analysis, Report R-108, pp. 223-238, 1965.

Wu, W. W., "Coding for multiple-access communication satellites," Proceedings of the Thirteenth Annual Allerton Conference on Circuit and System Theory, pp. 548-559, October 1975.

Yao, K., "Performance bounds on spread spectrum multiple access communication systems," Proceedings of the 1976 Conference on Information Sciences and Systems, Johns Hopkins University, March 1976a.

Yao, K., "Error probability of spread spectrum multiple access communication systems," Proceedings of the International Telemetering Conference, Los Angeles, California, September 1976b.

Yeh, L. P., "Multiple-access tradeoff study for intra South American satellite communication system," IEEE Transactions on Communication Technology, vol COM-16, pp 721-730, October 1968.

Zegers, L. E., "Common bandwidth transmission of information signals and pseudonoise synchronization waveforms," IEEE Transactions on Communication Technology, vol. COM-16, pp. 796-807, December 1968.

Zierler, N., "Linear recurring sequences," Journal of the Society of Industrial and Applied Mathematics, vol. 7, pp. 31-48, March 1959.

Zierler, N., "A note on the mean square weight for group codes," Information and Control, vol. 5, pp. 87-89, 1962.

Zierler, N., "Linear recurring sequences and error correcting codes," in Error Correcting Codes, (Mann, H. B., editor). New York: Wiley, 1968.

APPENDIX A
INTERFERENCE PARAMETER FOR BARKER SEQUENCES

In this Appendix we show that $r(u,v) = 2(p^2 + p - 1)$ in any set of Barker sequences of odd period p . For all known Barker sequences of odd period p ,

$$c_u(l) = \begin{cases} 0 & l \text{ odd} \\ (-1)^{\frac{p-1}{2}l} & l \text{ even} \end{cases} \quad (\text{A.1})$$

Each such a sequence gives rise to three others under the transformations (Turyn and Storer (1961))

$$v_j = \begin{cases} (-1)^j u_j & (\text{A.2a}) \\ (-1)^{j+1} u_j & (\text{A.2b}) \\ -u_j & (\text{A.2c}) \end{cases}$$

Substitution of (A.2a) or (A.2b) into (1.7) gives

$$c_{u,v}(l) = (-1)^l c_{u,v}(-l) \quad , \quad \forall l$$

hence

$$c_{u,v}(l)c_{u,v}(l+1) = -c_{u,v}(-l)c_{u,v}(-l-1) \quad , \quad \forall l$$

which implies

$$\sum_{l=1-p}^{p-1} c_{u,v}(l)c_{u,v}(l+1) = 0 \quad . \quad (\text{A.3})$$

Furthermore we have with (A.2c)

$$\sum_{\ell=1-p}^{p-1} C_{u,v}(\ell)C_{u,v}(\ell+1) = \sum_{\ell=1-p}^{p-1} C_u(\ell)C_u(\ell+1) . \quad (\text{A.4})$$

Substitution of (A.1) into (A.4) implies that (A.3) also holds for (A.2c)

hence, we conclude with (1.20) and (A.3) that for p odd

$$r(u,v) = 2 \sum_{\ell=1-p}^{p-1} C_{u,v}^2(\ell) . \quad (\text{A.5})$$

It was pointed out in Pursley and Sarvate (1976) that the sum in (A.5) equals $p^2 + p - 1$ for Barker sequences.

APPENDIX B

BOUNDS ON THE APERIODIC CROSS-CORRELATION FUNCTION

The number of sequence pairs (u, v) for which $C_{u,v}(\ell) = r$, with $0 \leq \ell \leq p-1$ and $|r| \leq p-\ell$, equals

$$h(\ell, p, r) = 2^p 2^{\ell} \binom{p-\ell}{\frac{1}{2}(p-\ell+r)}. \quad (\text{B.1})$$

To prove (2.4) we follow the procedure of Moon and Moser (1968). Let $f(p, G)$ denote the number of sequence pairs such that

$$\hat{C}_{\max}(u, v) = \max_{0 \leq \ell \leq p-1} |C_{u,v}(\ell)| \leq G = G(p).$$

Each sequence pair will be counted p times if $h(\ell, p, r)$ is summed over all ℓ and r such that $0 \leq \ell \leq p-1, |r| \leq G$. Therefore,

$$p \cdot f(p, G) \leq \sum_{\ell=0}^{p-1} \sum_{|r| \leq G} (2^p 2^{\ell} \binom{p-\ell}{\frac{1}{2}(p-\ell+r)})$$

or

$$\begin{aligned} p \cdot f(p, G) &\leq (2G+1) 2^{2p} \sum_{\ell=0}^{p-1} (p-\ell)^{-\frac{1}{2}} \\ &\leq (2G+1) 2^{2p} \{p^{-\frac{1}{2}} + 2(p-1)^{\frac{1}{2}}\}. \end{aligned}$$

Hence,

$$2^{-2p} f(p, G) \leq (2G+1) \{p^{-3/2} + 2p^{-1}(p-1)^{\frac{1}{2}}\}. \quad (\text{B.2})$$

The right hand side of (B.2) decreases to zero for $p \rightarrow \infty$, if $G(p) = p^{\frac{1}{2}-\tilde{\epsilon}}$, whereby $\tilde{\epsilon} > 0$.

Let $\tilde{f}(p, \ell, H)$ denote the number of sequence pairs such that $|C_{u,v}(\ell)| \geq H = H(p)$. Furthermore, let $\tilde{f}(p, H)$ denote the number of pairs such that

$$\hat{C}_{\max}(u, v) \geq H = H(p).$$

Clearly,

$$\begin{aligned} \tilde{f}(p, \ell, H) &= 2^p 2^\ell \sum_{|r| \geq H} \binom{p-\ell}{\frac{1}{2}(p-\ell+r)} \\ &= 2^{p+\ell} \sum_t \binom{p-\ell}{t} 2^{\ell-p} \end{aligned}$$

where the sum is over those integers t such that $|t - \frac{1}{2}(p-\ell)| > \frac{1}{2}H$.

Hence,

$$\tilde{f}(p, \ell, H) \leq 2^p \cdot 2^p 2 \exp\{- (4p)^{-1} H^2\}$$

or

$$\sum_{\ell=0}^{p-1} \tilde{f}(p, \ell, H) \leq 2p 2^{2p} \exp\{- (4p)^{-1} H^2\}.$$

Hence,

$$2^{-2p} \tilde{f}(p, H) \leq 2p \exp\{- (4p)^{-1} H^2\}. \quad (\text{B.3})$$

The right hand side of (B.2) decreases to zero for $p \rightarrow \infty$, if

$H(p) = (2+\epsilon')(p \log p)^{\frac{1}{2}}$, $\epsilon' > 0$ or $H(p) = p^{\frac{1}{2}+\tilde{\epsilon}}$, $\tilde{\epsilon} > 0$. This concludes the proof

Conclusion: If u and v are drawn at random from the set of all 2^{2p} pairs then

$$\Pr \left\{ \left| \frac{\log C_{\max}(u, v)}{\frac{1}{2} \log p} - 1 \right| \geq \epsilon \right\} \leq \tilde{\gamma}(p)$$

where $\lim_{p \rightarrow \infty} \tilde{\gamma}(p) = 0$.

APPENDIX C

CORRELATION PARAMETERS OF AO/LSE M-SEQUENCES

Table 32. AO/LSE m-sequences of length $p = 31$.

Poly.	Loading*	Poly.	Loading*	$\hat{\theta}_{\max}(u)$	$\hat{L}_a$	$S(u)$
045	11001	051	01001	7	2	107
067	00011	073	01101	7	2	123
075	11110	057	10010	7	2	91

Table 33. Correlation values for AO/LSE m-sequences; $p = 31$.

	0	0	0	0	0	0
	4	6	7	5	7	5
	5	7	5	1	3	7
045	7	11	15	15	15	19
067	9	7	15	15	19	15
075	9	9	7	19	15	15
051	11	9	9	7	11	15
073	9	11	9	9	7	15
057	9	9	11	9	9	7

Table 34. Interference parameter $r(u,v)$ for AO/LSE m-sequences; $p = 31$.

	045	067	075
045	2382	1846	1990
067		2318	1910
075			2206

Table 35. AO/LSE m-sequences of length $p = 63$.

Foly.	Loading*	Poly.	Loading*	$\hat{\theta}_{\max}(u)$	$\hat{L}_a$	$S(u)$
103	000010	141	011111	11	2	427
133	110001	155	011001	11	2	503
147	100011	163	110101	11	2	435

Table 36. Correlation values for AO/LSE m-sequences; $p = 63$.

	1	1	1	1	1	1
	0	3	4	4	5	6
	3	3	7	1	5	3
103	11	21	17	21	19	19
133	17	11	19	19	31	25
147	17	23	11	19	25	23
141	15	23	23	11	21	17
155	23	15	17	17	11	19
163	23	17	15	17	23	11

Table 37. Interference parameter $r(u,v)$ for AO/LSE m-sequences; $p = 63$.

	103	133	147
103	9574	7954	6958
133		10006	8138
147			9414

APPENDIX D

MOMENTS OF APERIODIC CORRELATION FUNCTIONS OF M-SEQUENCES

In this Appendix, various moments of the aperiodic cross-correlation and autocorrelation functions are calculated. Let $\tilde{u} = T^x u$ and $\tilde{v} = T^y v$, where u and v are m -sequences in their characteristic form. Assume that x and y are independent random variables both uniformly distributed over the integers in the range $[0, p-1]$. With the aperiodic cross-correlation for m -sequences $\tilde{u}$ and $\tilde{v}$ defined as in (1.7), the higher moments of $C_{\tilde{u}, \tilde{v}}(l)$ can be calculated in a straightforward manner. Similarly, the moments of $C_{\tilde{u}}(l)$, $l \neq 0$ can be obtained. The latter are identical to Lindholm's (1968) moments of M -tuples when the substitution $p - |l| = M$ is used.

D.1. First moments of the aperiodic correlation functions

The conditional expectation of $C_{\tilde{u}, \tilde{v}}(l)$ given $1-p \leq l < 0$, equals

$$\begin{aligned} E\{C_{\tilde{u}, \tilde{v}}(l) / 1-p \leq l < 0\} &= E\left\{\sum_{j=0}^{p-1+l} u_{j-l+x} v_{j+y}\right\} \\ &= \sum_{j=0}^{p-1+l} p^{-2} \left(\sum_{x=0}^{p-1} u_{j-l+x}\right) \left(\sum_{y=0}^{p-1} v_{j+y}\right) \\ &= p^{-2} (p+l) \end{aligned} \tag{D.1}$$

which follows from the property that $\sum_{j=0}^{p-1} u_j = -1$ for any m -sequence u .

Similarly it follows that

$$E\{C_{\tilde{u},\tilde{v}}(l)/0 \leq l \leq p-1\} = p^{-2}(p-l) . \quad (D.2)$$

Hence, from (D.1) and (D.2), for all l

$$E\{C_{\tilde{u},\tilde{v}}(l)\} = p^{-2}(p - |l|) . \quad (D.3)$$

For the conditional expectation of $C_{\tilde{u}}(l)$, given $1-p \leq l < 0$, we have

$$E\{C_{\tilde{u}}(l)/1-p \leq l < 0\} = \sum_{j=0}^{p-1+l} p^{-1} \sum_{x=0}^{p-1} u_{j-l+x} u_{j+x} .$$

From the shift- and-multiply property of m-sequences (see Section 3.2)

whereby $u_{j-r+x} = u_{j-l+x} u_{j+x}$, $\forall x$, for some r and $l \neq 0$, one obtains simply

$$E\{C_{\tilde{u}}(l)/1-p \leq l < 0\} = \sum_{j=0}^{p-1+l} p^{-1} \sum_{x=0}^{p-1} u_{j-r+x} = -p^{-1}(p+l) .$$

Therefore, for all $l \neq 0$

$$E\{C_{\tilde{u}}(l)\} = p^{-1}(|l| - p) . \quad (D.4)$$

D.2. Second moments of the aperiodic correlation functions

The conditional expectation of $C_{\tilde{u},\tilde{v}}^2(l)$, given $1-p \leq l < 0$

$$\begin{aligned} E\{C_{\tilde{u},\tilde{v}}^2(l)/1-p \leq l < 0\} &= E\left\{\sum_{j=0}^{p-1+l} (u_{j-l+x} v_{j+y})^2\right\} + \\ &+ 2p^{-2} \sum_{j=0}^{p-2+l} \sum_{m=j+1}^{p-1+l} \left(\sum_{x=0}^{p-1} u_{j-l+x} u_{m-l+x}\right) \left(\sum_{y=0}^{p-1} v_{j+y} v_{m+y}\right) . \end{aligned}$$

Again from the shift-and-multiply property of m-sequences

$$\begin{aligned} E\{C_{u,\tilde{v}}^2(l)/1-p \leq l < 0\} &= p+l+2p^{-2} \sum_{j=0}^{p-2+l} \sum_{m=j+1}^{p-1+l} 1 \\ &= (p+l)[1+p^{-2}(p+l-1)] . \end{aligned}$$

Hence, for all l ,

$$E\{C_{u,\tilde{v}}^2(l)\} = (p - |l|)[1+p^{-2}(p - |l| - 1)] . \quad (D.5)$$

For the conditional expectation of $C_u^2(l)$, given $1-p \leq l < 0$, we have

$$E\{C_u^2(l)/1-p \leq l < 0\} = p+l+2p^{-1} \sum_{j=0}^{p-2+l} \sum_{m=j+1}^{p-1+l} \sum_{x=0}^{p-1} u_{j-l+x} u_{m-l+x} u_{j+x} u_{m+x} .$$

With $l \neq 0$ and some $r \neq 0$ and $s \neq 0$, one can write

$$u_{j-l+x} u_{j+x} u_{m-l+x} u_{m+x} = u_{r+x} u_{s+x} , \quad \forall x .$$

Then, $u_{r+x} u_{s+x} = u_{t+x}$, $\forall x$, for some t because $r \neq s$. Therefore

$$\begin{aligned} E\{C_u^2(l)/1-p \leq l < 0\} &= p+l+2p^{-1} \sum_{j=0}^{p-2+l} \sum_{m=j+1}^{p-1+l} (-1) \\ &= (p+l)[1-p^{-1}(p+l-1)] . \end{aligned}$$

Hence, for all $l \neq 0$,

$$E\{C_u^2(l)\} = (p - |l|)[1-p^{-1}(p - |l| - 1)] . \quad (D.6)$$

D.3. Expectation of the interference parameter $r(u,v)$

Consider the product of $C_{\tilde{u},\tilde{v}}(l)$ and $C_{\tilde{u},\tilde{v}}(l+1)$.

$$\begin{aligned}
 E\{C_{\tilde{u},\tilde{v}}(l) C_{\tilde{u},\tilde{v}}(l+1)/1-p \leq l < -1\} &= \\
 &= p^{-2} \sum_{j=0}^{p-1+l} \sum_{m=0}^{p+l} \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} u_{j-l+x} u_{m-l+x} v_{j+y} v_{m+y} \\
 &= -2p^{-1} \sum_{j=0}^{p-1+l} \sum_{m=0}^{p+l} \sum_{\substack{j \neq m, \\ j \neq m-1}}^{p-1+l} \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} u_{j-l+x} u_{m-l-1+x} v_{j+y} v_{m+y} \Bigg|_{1-p \leq l < -1}.
 \end{aligned}$$

Hence,

$$E\{C_{\tilde{u},\tilde{v}}(l) C_{\tilde{u},\tilde{v}}(l+1)/1-p \leq l < -1\} = (p+l) p^{-2} (-p+l-1).$$

For all l one finds

$$E\{C_{\tilde{u},\tilde{v}}(l) C_{\tilde{u},\tilde{v}}(l+1)\} = \begin{cases} (p-l-1)p^{-2}(-p-l-2) & 0 \leq l \leq p-1 \\ (p+l) p^{-2}(-p+l-1) & 1-p \leq l \leq -1 \end{cases} \quad (D.7)$$

Substitution of (D.5) and (D.7) in the expression of the interference parameter $r(u,v)$ defined in (1.20) gives

$$\begin{aligned}
 E\{r(\tilde{u},\tilde{v})\} &= \sum_{l=1-p}^{p-1} \{2E\{C_{\tilde{u},\tilde{v}}^2(l)\} + E\{C_{\tilde{u},\tilde{v}}(l) C_{\tilde{u},\tilde{v}}(l+1)\}\} \\
 &= 2(p^2 + \frac{2}{3}p - 1 + (3p)^{-1}) + 2 \sum_{l=1}^{p-1} l p^{-2} (l - 2p - 1).
 \end{aligned}$$

Hence,

$$E\{r(\tilde{u},\tilde{v})\} = 2(p^2 - 1 + p^{-1}). \quad (D.8)$$

Also of interest is the product of $C_{\tilde{u}, \tilde{v}}(l)$ and $C_{\tilde{u}, \tilde{v}}(l-p)$ whereby $0 \leq l \leq p-1$.

$$\begin{aligned} E\{C_{\tilde{u}, \tilde{v}}(l-p) C_{\tilde{u}, \tilde{v}}(l) / 0 < l \leq p-1\} = \\ = p^{-2} \sum_{j=0}^{l-1} \sum_{m=0}^{p-1-l} \left(\sum_{x=0}^{p-1} u_{j-l+x} u_{m+x} \right) \left(\sum_{y=0}^{p-1} v_{j+y} v_{m+l+y} \right) \end{aligned}$$

because, indeed $j \neq l+m$ whenever $0 \leq j \leq l-1$ and $0 \leq m \leq p-1-l$.

Therefore, with $C_{\tilde{u}, \tilde{v}}(-p) = 0$,

$$E\{C_{\tilde{u}, \tilde{v}}(l-p) C_{\tilde{u}, \tilde{v}}(l) / 0 \leq l \leq p-1\} = p^{-2} l(p-l). \quad (D.9)$$

In a similar manner, it follows that

$$E\{C_{\tilde{u}}(l-p) C_{\tilde{u}}(l) / 0 < l \leq p-1\} = p^{-1} l(l-p). \quad (D.10)$$

D.4. Third moments of the aperiodic correlation functions

Of most interest is the third moment of $C_{\tilde{u}, \tilde{v}}(l)$.

$$E\{C_{\tilde{u}, \tilde{v}}^3(l) / 1-p \leq l < 0\} =$$

$$\begin{aligned} &= E\left\{ \sum_{j=0}^{p-1+l} (\tilde{u}_{j-l} \tilde{v}_j)^3 \right\} + 3(p+l) E\left\{ \sum_{j=0}^{p-1+l} \tilde{u}_{j-l} \tilde{v}_j \right\} \\ &- 3E\left\{ \sum_{j=0}^{p-1+l} \tilde{u}_{j-l} \tilde{v}_j \right\} + 3! E\left\{ \sum_{j=0}^{p-3+l} \sum_{m=j+1}^{p-2+l} \sum_{n=m+1}^{p-1+l} \tilde{u}_{j-l} \tilde{u}_{m-l} \tilde{u}_{n-l} \tilde{v}_j \tilde{v}_m \tilde{v}_n \right\} \\ &= p^{-2} (p+l) [3(p+l) - 2] + \end{aligned}$$

$$+ 6p^{-2} \left[\sum_{j=0}^{p-3+l} \sum_{m=j+1}^{p-2+l} \sum_{n=m+1}^{p-1+l} \sum_{x=0}^{p-1} u_{j-l+x} u_{m-l+x} u_{n-l+x} \right]$$

$$\left[\sum_{j=0}^{p-3+l} \sum_{m=j+1}^{p-2+l} \sum_{n=m+1}^{p-1+l} \sum_{y=0}^{p-1} v_{j+y} v_{m+y} v_{n+y} \right].$$

Let $1-p \leq l < 0$. Whenever there exist a three-tuple (j, m, n) such that

$$u_{j-l+x} u_{m-l+x} = u_{n-l+x}, \quad \forall x \quad (D.11)$$

and

$$0 \leq j < m < n \leq p-1+l \quad (D.12)$$

the sum $\sum_{x=0}^{p-1} u_{j-l+x} u_{m-l+x} u_{n-l+x} = p$. Whenever such a three-tuple does not exist, i.e., $u_{j-l+x} u_{m-l+x} u_{n-l+x} = u_{h-l+x}$, some h , the sum $\sum_{x=0}^{p-1} u_{j-l+x} u_{m-l+x} u_{n-l+x} = -1$. Of the $\binom{p+l}{3}$ possible three-tuples (j, m, n) for which (D.12) holds, there are $B_3^u(p+l)$ three-tuples for which (D.11) holds for u -sequence u . Hence,

$$E\{C_{u,v}^3(l) / 1-p \leq l < 0\} = p^{-2} [3(p+l) - 2](p+l) +$$

$$+ 6p^{-2} \left[-\binom{p+l}{3} + (p+1)B_3^u(p+l) \right] \left[-\binom{p+l}{3} + (p+1)B_3^v(p+l) \right].$$

For all l one obtains

$$E\{C_{u,v}^3(l)\} = p^{-2} \{ 3(p - |l|)^2 - 2(p - |l|) + 6\binom{p-|l|}{3} \} -$$

$$6p^{-2}(p+1) \binom{p-|l|}{3} [B_3^u(p-|l|) + B_3^v(p-|l|)]$$

$$+ 6p^{-2}(p+1)^2 B_3^u(p-|l|) B_3^v(p-|l|). \quad (D.13)$$

A similar procedure for the autocorrelation function gives,

for $l \neq 0$,

$$E\{C_u^3(l)\} = p^{-1}(|l| - p)^3 + 6p^{-1}(p+1)B_3^u(p - |l|) \quad (D.14)$$

as previously derived by Lindholm (1968).

D.5. Expectation of a product of aperiodic correlation functions

Finally we derive the expectation of the product of $C_{\tilde{u},\tilde{v}}^2(l-p)$ and $C_{\tilde{u},\tilde{v}}(l)$.

$$E\{C_{\tilde{u},\tilde{v}}^2(l-p) C_{\tilde{u},\tilde{v}}(l) / 0 < l \leq p-1\} = E\left\{ \sum_{j=0}^{l-1} (\tilde{u}_{j-l} \tilde{v}_j)^2 \sum_{j=0}^{p-1-l} \tilde{u}_n \tilde{v}_{n+l} \right\} + \\ + 2p^{-2} \sum_{j=0}^{l-2} \sum_{m=j+1}^{l-1} \sum_{n=l}^{p-1} \left(\sum_{x=0}^{p-1} u_{j-l+x} u_{m-l+x} u_{n-l+x} \right) \sum_{j=0}^{l-2} \sum_{m=j+1}^{l-1} \left(\sum_{n=l}^{p-1} \sum_{y=0}^{p-1} v_{j+y} v_{m+y} v_{n+y} \right).$$

Let $0 < l \leq p-1$. Whenever there exists a three-tuple (j,m,n) such that

$$u_{j-l+x} u_{m-l+x} = u_{n-l+x}, \quad \forall x \quad (D.15)$$

and

$$0 \leq j < m \leq l-1; \quad l \leq n \leq p-1 \quad (D.16)$$

the sum $\sum_{x=0}^{p-1} u_{j-l+x} u_{m-l+x} u_{n-l+x} = p$. In the other cases this sum equals -1. Of the $\binom{l}{2}(p-l)$ possible three-tuple (j,m,n) for which (D.16) holds, there are $C_3^u(l)$ three-tuples for which (D.15) holds.

With $C_{\tilde{u},\tilde{v}}(-p) = 0$, one obtains

$$E\{C_{\tilde{u},\tilde{v}}^2(l-p) C_{\tilde{u},\tilde{v}}(l) / 0 \leq l \leq p-1\} = p^{-2} l(p-l) + \\ + 2p^{-2} \left[-\binom{l}{2}(p-l) + (p+1)C_3^u(l) \right] \left[-\binom{l}{2}(p-l) + (p+1)C_3^v(l) \right]. \quad (D.17)$$

A similar procedure for the auto-correlation gives

$$E\{C_u^2(l-p) C_u(l) / 0 < l \leq p-1\} = -p^{-1} l(p-l) + 2p^{-1} \left[-\binom{l}{2} (p-l) + (p+1) C_3^u(l)\right]. \quad (D.18)$$

D.6. Relationship between $B_3^u(l)$ and $C_3^u(l)$

For any m-sequence u one has the relation

$$C_u(l-p) + C_u(l) = A_u(l) = -1, \quad 0 < l \leq p-1.$$

Hence, the left-hand side of (D.18) can be written as

$$E\{C_u^2(l-p) C_u(l) / 0 < l \leq p-1\} = E\{-C_u^3(l-p) / 0 < l \leq p-1\} - E\{C_u^2(l-p) / 0 < l \leq p-1\}.$$

Substituting (D.14) and (D.6) results in

$$E\{C_u^2(l-p) C_u(l) / 0 < l \leq p-1\} = p^{-1} [l(l^2 - p + l - 1) - 6(p+1) B_3^u(l)]. \quad (D.19)$$

A comparison between (D.18) and (D.19) gives

$$3B_3^u(l) + C_3^u(l) = \binom{l}{2}. \quad (D.20)$$

Indeed, this relationship can be obtained from the conditions (D.11), (D.12) and (D.16) immediately, as follows. Again $0 < l \leq p-1$. Whenever (D.11) holds for $B_3^u(l)$ three-tuples, i.e., whereby $0 \leq j < m < n \leq l-1$, there will be $3B_3^u(l)$ three-tuples (j, m, n) such that (D.15) holds whereby $0 \leq j < m \leq l-1$, $0 \leq n \leq l-1$. Notice that there are $\binom{l}{2}$ possible choices for the pair (j, m) such that $0 \leq j < m \leq l-1$ and thus one concludes with condition (D.16) that (D.20) must hold.

D.7. Fourth moments of the aperiodic correlation functions

Equally straightforward as the derivations of the third moment of $C_{\tilde{u},\tilde{v}}(\ell)$ in Section D.4, it is not difficult to show that

$$\begin{aligned} E\{C_{\tilde{u},\tilde{v}}^4(\ell)\} &= \underline{(p - |\ell|)\{3(p - |\ell|) - 2 + 2p^{-2}\{3(p - |\ell|) - 4\}(p - |\ell| - 1)\}} \\ &\quad + 24p^{-2}(p - |\ell|)^2 - 24p^{-2}(p + 1)(p - |\ell|)(B_4^u(p - |\ell|) + B_4^v(p - |\ell|)) \\ &\quad + 24p^{-2}(p + 1)^2 B_4^u(p - |\ell|) B_4^v(p - |\ell|) . \end{aligned}$$

where $B_4^u(p - |\ell|)$ denotes the number of four-tuples (j, m, n, t) such that

$$u_{j-x} u_{m-x} u_{n-x} = u_{t-x} , \quad \forall x$$

and

$$0 \leq j < m < n < t \leq p - |\ell| - 1 .$$

Notice that the underlined part of $E\{C_{\tilde{u},\tilde{v}}^4(\ell)\}$ equals the fourth moment of $C_{\tilde{u},\tilde{v}}(\ell)$ for random binary sequences (see Chapter 2).

The fourth moment of $C_{\tilde{u}}(\ell)$, $\ell \neq 0$, is given by Lindholm (1968).

APPENDIX E

CORRELATION PARAMETERS OF SUMS OF PAIRS OF M-SEQUENCES

Table 44. AO/LSE sequences $W = T^y(u \cdot T^k v)$; $u:045$, $v:075$; $p = 31$.

$\theta_{\max}(w)$	L_a	$M(w)$	k	Loading	y	$\hat{\theta}_{\max}(w)$	$\hat{L}_a$	$S(w)$	$\hat{M}(w)$
7	10	510	0	7150	20	5	8	203	302
9	2	766	5	3446	4	9	2	323	526
			10	1764	8	7	6	339	590
			20	4377	15	7	2	271	318
			9	7017	28	7	2	291	398
			18	3354	10	7	10	355	654
9	4	830	11	3007	30	5	8	291	334
			22	7112	23	7	2	303	382
			13	3125	8	7	6	319	446
			26	1602	16	5	12	311	414
			21	0750	1	7	6	379	686
9	6	798	15	2776	27	7	2	267	270
			30	3440	9	7	2	291	366
			29	6651	16	7	2	283	334
			27	7046	7	7	4	319	478
			23	4503	3	7	6	355	622
9	6	1086	7	4552	22	7	4	399	510
			14	4421	26	7	2	375	414
			28	5151	13	7	2	379	430
			25a	2221	10	5	10	359	350
			b	1110	9				
9	8	1054	19	4060	22	7	4	399	510
			1	3631	19	9	2	363	398
			2	6741	28	5	6	331	270
			4	3043	14	5	8	335	286
			8	1262	6	9	2	419	622
9	10	1310	16	0655	2	9	4	479	862
			3	5272	10	7	10	475	590
			6	1646	30	7	6	471	574
			12	7072	17	7	4	439	446
			24	7613	4	7	2	423	382
			17	7002	14	7	4	439	446

Table 45. AO/LSE sequences $W = T^y(u \cdot T^k v)$; $u:045$, $v:067$; $p = 31$.

$\theta_{\max}(w)$	La	M(w)	k	Loading	y	$\hat{\theta}_{\max}(w)$	$\hat{La}$	S(w)	$\hat{M}(w)$	
7	10	510	0	1723	13	7	2	235	430	
9	2	766	{	7	6522	26	7	2	323	526
				14	5730	2	7	2	275	334
				28	5333	2	7	2	283	366
				25	3427	17	7	2	307	462
				19	1347	12	5	10	279	350
9	4	830	{	11	4427	6	7	2	291	334
				22	3053	24	5	12	311	414
				13	1021	22	7	2	291	334
				26	3044	26	7	2	323	462
				21	4103	3	7	2	295	350
9	6	798	{	1	5354	9	7	2	319	478
				2	4641	30	5	10	287	350
				4	4440	7	5	2	247	190
				8	7553	9	7	2	295	382
				16	6774	15	7	4	311	446
9	6	1086	{	5	2102	15	7	2	355	334
				10	4014	1	7	4	427	622
				20	1071	25	7	2	355	334
				9	0336	26	9	2	411	558
				18	5214	6	7	2	367	382
9	8	1054	{	3	3202	7	7	2	327	254
				6	7321	11	7	4	391	510
				12	6634	23	9	2	415	606
				24	3242	11	7	4	391	510
				17a	6367	0	9	2	415	606
	b	4601	20							
9	10	1310	{	15	4741	10	7	6	455	510
				30	3235	19	7	2	419	366
				29	4417	12	7	2	435	430
				27	2224	26	7	2	447	478
				23	5451	5	7	2	451	494

Table 46. AO/LSE sequences $W = T^y(u \cdot T^k v)$; $u:067$, $v:075$; $p = 31$.

$\theta_{\max}(w)$	La	$M(w)$	k	Loading	y	$\hat{\theta}_{\max}(w)$	$\hat{La}$	$S(w)$	$\hat{M}(w)$
7	10	510	0	6537	14	7	4	263	542
9	2	766	7	5773	5	7	6	351	638
			14	5624	1	5	4	243	206
			28	3551	15	5	8	275	334
			25	3530	13	7	2	279	350
			19	4376	14	5	6	251	238
9	4	830	3	1401	12	5	10	295	350
			6	5224	21	7	6	335	510
			12	4621	8	7	2	299	366
			24	5424	7	9	2	375	670
			17	1014	5	9	2	315	430
9	6	798	11	3676	27	7	2	275	202
			22	0227	18	7	2	315	202
			13	6271	12	7	8	343	574
			26	4317	27	9	2	303	414
			21	7615	30	5	8	271	286
9	6	1086	1	7000	6	7	2	351	318
			2	0200	23	7	4	395	494
			4	1201	30	7	4	367	382
			8	5773	5	7	6	351	318
			16	6056	3	7	2	379	430
9	8	1054	5	3602	18	7	2	367	414
			10	6552	8	7	4	375	446
			20	4025	5	5	8	335	286
			9	2024	12	5	8	347	334
			18	6052	25	7	4	359	382
9	10	1310	15	7057	9	7	2	407	318
			30	2312	26	7	4	455	510
			29	3140	17	5	6	395	270
			27	3225	11	7	4	459	526
			23	4334	5	9	2	467	558

Table 47. Correlation values for the A0/LSE sequences U, V and

$$W = T^Y(u \cdot T^k v); u:045, v:075; k \in \eta_0 \text{ and } \eta_5; p = 31.$$

k	0	5	10	20	9	18	U	V
0	5	17	15	11	11	11	11	13
5	9	9	15	11	11	13	13	15
10	9	7	7	13	11	17	15	11
20	9	9	7	7	13	11	13	13
9	9	9	9	7	7	11	11	15
18	9	7	9	9	7	7	13	13
U	9	9	9	9	9	9	7	15
V	9	9	9	9	9	9	9	7

Table 48. Interference parameter $r(w, z)$ for the A0/LSE sequences U, V and

$$W = T^Y(u \cdot T^k v); u:045, v:075; k \in \eta_0 \text{ and } \eta_5; p = 31.$$

k	5	10	20	9	18	U	V
0	2006	1942	2050	1846	1830	1742	1702
5		1854	2578	2470	1918	2190	2142
10			1898	2406	1830	1846	1790
20				2106	2146	2090	1858
9					1582	2206	2054
18						1678	1526
U							1990

Table 49. AO/ISE sequences $W = T^Y(u \cdot T^k v)$; $u:103$, $v:147$; $p = 53$.

$\theta_{\max}(w)$	L_a	$M(w)$	k	Loading	y	$\theta_{\max}(w)$	$\hat{\theta}_{\max}(w)$	$\hat{L}_a$	$s(w)$	$\hat{M}(w)$
15	14	3198	0	2172	59	13	2	2	1199	1598
			11	5126	54	11	2	2	1195	1582
			22	5044	3	13	2	2	1243	1774
			44	0475	49	13	4	4	1551	3006
15	14	3198	25	0502	26	13	2	2	1395	2382
			50	2565	13	11	6	6	1343	2174
			37	2050	47	12	4	4	1331	2126
			27	4113	59	9	10	10	1215	1662
15	14	3198	54	0425	30	11	4	4	1275	1902
			45	0023	4	11	6	6	1239	1758
			31	4037	39	15	2	2	1927	2590
			62	6450	12	15	2	2	1959	2718
			61	3347	2	15	2	2	1923	2574
17	2	5110	59	6836	62	11	8	8	1731	1806
			55	7436	60	13	4	4	1751	1886
			47	7267	32	13	2	2	1935	2622
			15	5706	52	15	2	2	1135	2430
			30	3116	13	11	6	6	1143	2462
			60	2715	56	11	2	2	891	1454
17	4	2110	57	0424	35	11	2	2	959	1726
			51	1457	22	9	10	10	939	1646
			39	5657	39	15	2	2	991	1854
			13	3172	42	13	4	4	1447	3678
			26	7234	26	13	2	2	1071	2174
			52	3646	10	11	6	6	1067	2158
17	4	2110	41	0313	46	13	2	2	951	1694
			19	4146	59	11	4	4	939	1646
			36	0363	29	11	14	14	1263	2942
			23	0543	42	13	2	2	1051	2094
			46	4345	49	13	2	2	859	1326
			29	1240	41	11	2	2	999	1886
17	4	2110	58	2474	37	11	4	4	1051	2094
			53	5274	34	11	4	4	1175	2590
			43	6322	54	15	2	2	983	1822

Table 55. AO/LSE sequences $W = T^y(u \cdot T^k v)$; $u:103$, $v:141$; $k \in \eta_{21}, \eta_{13}, \eta_{11}$, and η_{27} ; $p = 63$.

$\theta_{\max}(w)$	L_a	$M(w)$	k	Loading	y	$\hat{\theta}_{\max}(w)$	$\hat{L}_a$	$S(w)$	$\hat{M}(w)$
13	6	3182	21a	2223	41	13	2	1339	2174
			b	6053	2				
			42a	6463	57	11	2	1207	1646
			b	1103	28				
13	6	3502	13a	3745	41	11	4	1247	1486
			b	0564	10				
			26a	7514	29	13	2	1339	1854
			b	3520	9				
			52a	3262	48	13	2	1375	1998
			b	7110	27				
			41a	5341	59	13	2	1431	2222
			b	7313	27				
			19a	4571	37	13	2	1475	2398
			b	0545	8				
			38a	0367	56	11	2	1283	1630
			b	7172	33				
15	2	3742	11a	5062	44	13	2	1551	2462
			b	5615	9				
			22a	3320	0	11	6	1635	2798
			b	0430	42				
			44a	4026	58	11	2	1311	1502
			b	1127	25				
			25a	4203	37	13	2	1463	2110
			b	1575	2				
			50a	7246	56	11	2	1327	1566
			b	2103	21				
15	6	5022	37a	4326	57	13	2	1467	2126
			b	0721	33				
			27a	0431	62	13	2	1775	2078
			b	4507	38				
			54a	1601	56	13	4	1863	2430
			b	1445	17				
			45a	3412	54	11	8	1843	2350
			b	6022	28				

Table 56. Correlation values for the AO/LSE sequences $W = T^y(u \cdot T^k v)$; $u:103, v:141; k \in \eta_{11a}, \eta_{27a}; p = 63.$

k	11	22	44	25	50	37	27	54	45
11	13	23	21	15	23	27	21	21	19
22	15	11	19	21	19	23	27	17	21
44	13	15	11	17	23	21	21	23	19
25	15	13	15	13	23	19	15	17	29
50	13	15	13	15	11	23	19	21	21
37	15	13	15	13	15	13	21	25	19
27	13	13	15	13	13	15	13	19	17
54	15	13	13	15	13	13	15	13	17
45	13	15	13	13	15	13	15	15	11

Table 57. Interference parameter $r(w, z)$ for the AO/LSE sequences $W = T^y(u \cdot T^k v); u:103, v:141; k \in \eta_{11a}, \eta_{27a}; p = 63.$

k	22	44	25	50	37	27	54	45
11	8154	6366	5638	6014	7650	6110	9190	5962
22		8730	7538	7650	6590	7322	7034	8022
44			8366	6150	6738	9230	7694	6666
25				7734	6858	6766	9254	6658
50					7970	6406	6966	7946
37						7570	8122	6934
27							8550	6866
54								7946

Table 58. AO/LSE sequences $W = T^Y(u \cdot T^k v)$; $u:211$, $v:217$; $k \in \eta_0, \eta_7, \eta_3$ and η_5 ; $p = 127$.

$\theta_{\max}(w)$	$L\epsilon$	$M(w)$	k	Loading	y	$\hat{\theta}_{\max}(w)$	$\hat{L}\alpha$	$S(w)$	$\hat{M}(w)$
17	14	10430	0	03121	103	21	2	5447	11358
17	18	13374	7	32357	78	19	2	5563	8878
			14	36341	29	19	2	5463	8478
			28	66225	11	19	2	5571	8910
			56	73375	103	19	2	5651	9230
			112	13367	85	21	4	6535	12766
			97	07553	109	19	6	6307	11854
			67	33553	32	13	8	4815	5886
17	22	14526	3	54364	55	17	6	5839	8830
			6	20430	60	17	8	5863	8926
			12	60012	46	19	2	6291	10638
			24	25226	47	19	4	6235	10414
			48	04210	75	19	2	5695	8254
			96a	51060	55	21	2	6407	11102
			b	24430	54				
			65	11654	108	19	4	6739	12430
17	38	19582	5	60763	12	19	2	7527	10526
			10	12732	34	21	2	7775	11518
			20	10774	98	21	4	8327	13726
			40	57743	100	17	8	6987	8366
			80	73550	83	19	2	7747	11406
			33	73731	33	19	4	7823	11710
			66	61443	29	19	4	7279	9534

Table 59. Correlation values for the AO/LSE sequences U, V and

$$W = T^Y(u \cdot T^k v); u:211, v:217; k \in \pi_0 \text{ and } \pi_7; p = 127.$$

k	0	7	14	28	56	112	97	67	U	V
0	21	27	27	31	31	43	35	31	31	41
7	17	19	27	35	27	31	29	29	35	41
14	17	17	19	31	37	31	33	31	31	37
28	17	17	17	19	31	27	25	31	31	31
56	17	17	17	17	19	27	35	25	29	23
112	17	17	17	17	17	21	27	29	27	33
97	17	17	17	17	17	17	19	31	37	39
67	17	17	17	17	17	17	17	13	29	29
U	17	17	17	17	17	17	17	17	17	33
V	17	17	17	17	17	17	17	17	17	15

Table 60. Interference parameter $r(w, z)$ for the AO/LSE sequences U, V and

$$W = T^Y(u \cdot T^k v); u:211, v:217; k \in \pi_0 \text{ and } \pi_7; p = 127.$$

	7	14	28	56	112	97	67	U	V
0	31746	31078	30090	29106	33878	34338	30942	31350	28798
7		32474	30750	30030	32082	32942	31626	33034	32042
14			35018	30586	34670	34978	34998	32158	34166
28				29022	31866	32542	31026	32394	33522
56					31258	30854	29946	30482	28882
112						31450	33206	32982	32918
97							34282	33226	35002
67								31670	31886
U									33622

Table 61. Cardinality L_c for (k, m) of sequence pairs

$$(w = u \cdot T^k v, z = u \cdot T^m v); u:211, v:217; p = 127.$$

(k, m)	L_c
$G(0, 7)$	37
$G(7, 14)$	20
$G(7, 28)$	18
$G(7, 56)$	19

VITA

Henricus Franciscus Albertus Roefs was born in Utrecht, The Netherlands on May 15, 1946. From September 1964 to October 1970 he attended the Delft University of Technology, Delft, The Netherlands where he received a B.Sc. degree in electrical engineering in January 1968 and a M.Sc. degree in electrical engineering in October 1970. From November 1970 to August 1974 he joined the Department of Electrical Engineering of the Delft University of Technology as a research engineer, where he was active in a research cooperation project -- sponsored by the Netherlands University Foundation for International Cooperation -- with the Institut Teknologi Bandung, Bandung, Indonesia.

Since September 1974 he has been a graduate student at the University of Illinois at Urbana-Champaign. He was a graduate teaching assistant in the Department of Electrical Engineering during the 1974-1975 academic year and a graduate research assistant in the Coordinated Science Laboratory for the remainder of the time he attended the University of Illinois.

Henricus F. A. Roefs is co-author of the papers

- I. Roefs, H. F. A., and Pursley, M. B., "Correlation parameters of random and maximal length sequences for spread-spectrum multiple-access communication," Proceedings of the 1976 IEEE Canadian Communications and Power Conference, October 1976.

- II. Roefs, H. F. A., Sarwate, D. V., and Pursley, M. B., "Periodic correlation functions of sums of pairs of m-sequences," Proceedings of the 1977 Conference on Information Sciences and Systems, Johns Hopkins University, March 1977.
- III. Roefs, H. F. A., and Pursley, M. B., "Correlation parameters of random binary sequences," accepted for publication by Electronics Letters, August 1977.

Henricus F. A. Roefs was elected to the Phi Kappa Phi honor society in 1975. He is a member of the Royal Dutch Institute of Engineers and a student member of the Institute of Electrical and Electronics Engineers.