

THE UNIVERSITY OF HULL

**Code Design and Analysis for Multiple Access
Communications**

being a Thesis submitted for the Degree of

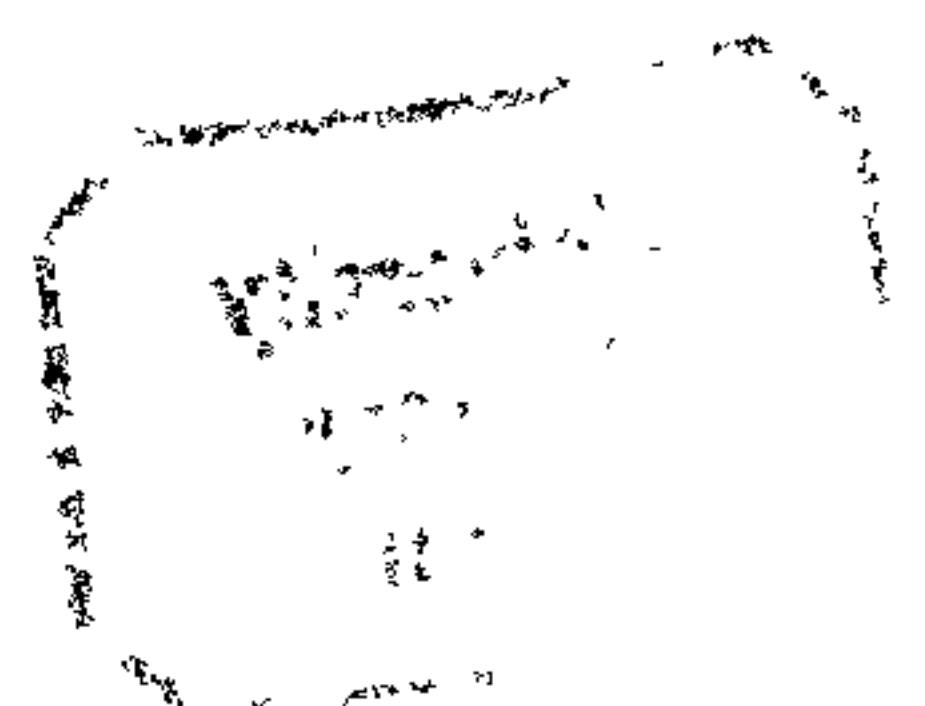
Doctor of Philosophy

in the University of Hull

by

Pingzhi Fan, M.Sc. (SWJU, China)

November 1994



To Xiaoping, who helped; also to Tina — who didn't !

Declaration

I, Pingzhi Fan, do declare that this work has not been submitted for any other degree at this University or any other Institution.

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Professor M. Darnell, for his keen guidance, encouragement, and valuable comments throughout this work.

I am deeply indebted to the Chinese Government and Hull-Lancaster Communication Research Group for supporting the research contained herein.

Thanks are also due to Professor B. Honary (Lancaster) and G. Markarian (Armenia) for their valuable advice and encouragement, Professor E. M. Gabidulin (Russia) for his advice and cooperation in part of the work of Chapter 7, Professor V. C. da Rocha Jr.(Brazil) for his advice and assistance in the work of Chapter 3, Dr. J. Gunson (Birmingham) and Professor W. K. Hayman (York) for their help in proving the inequality of Eqn B.23, and Professor F. Jin (PR of China) for his suggestions on the initial manuscript of the thesis. I am also indebted to all the members of the Hull-Lancaster Communications Research Group, for their encouragement, helpful comments and friendship.

Finally, I would like to take this opportunity to acknowledge my parents, my wife, my daughter and friends without whose encouragement, support and friendship I would not have been able to complete this work.

Abstract

This thesis explores various coding aspects of multiple access communications, mainly for spread spectrum multiaccess(SSMA) communications and collaborative coding multiaccess(CCMA) communications. Both the SSMA and CCMA techniques permit efficient simultaneous transmission by several users sharing a common channel, without subdivision in time or frequency. The general principle behind these two multiaccess schemes is that one can find sets of signals (codes) which can be combined together to form a composite signal; on reception, the individual signals in the set can each be recovered from the composite signal. For the CCMA scheme, the isolation between users is based on the code structure; for the SSMA scheme, on the other hand, the isolation between users is based on the autocorrelation functions(ACFs) and crosscorrelation functions(CCFs) of the code sequences. It is clear that, in either case, the code design is the key to the system design.

For the CCMA system with a multiaccess binary adder channel, a class of superimposed codes is analyzed. It is proved that every constant weight code of weight w and maximal correlation λ corresponds to a subclass of disjunctive codes of order $T < w/\lambda$. Results related to the decomposition of the disjunctive codes in the noiseless and noisy cases are derived. Decoding algorithms for both the noiseless and the noisy cases are proposed.

For the CCMA system operating over a multiaccess Q -ary adder channel, a class of cyclic uniquely decodable codes is proposed and analyzed by employing cyclic codes with symbols from an arbitrary finite integer rings. A very low complexity decoding procedure is presented.

For a synchronous SSMA system, a new approach employing orthogonal complementary sets is presented; the properties of such orthogonal complementary sets are studied in detail. Recursive formulas for constructing orthogonal complementary sets are given. Methods for synthesizing new orthogonal complementary sets from known ones with the same dimensions are also discussed.

For an asynchronous SSMA system, several new spreading codes are presented and studied:

1. A new class of polyphase codes with two-valued periodic ACF and CCF properties is derived. It is proved that, for a given prime length $L > 3$, the out-of-phase ACFs and CCFs of the codes are constant and equal to $\sqrt{L}$. In addition, all codes of the same length are mutually orthogonal.
2. Maximal length sequences (m-sequences) over Gaussian integers, suitable for use with QAM modulation, are considered. Two sub-classes of m-sequences with quasi-perfect periodic autocorrelations are obtained. The CCFs between the decimated m-sequences are studied. By applying a simple operation, it is shown that some m-sequences over rational and Gaussian integers can be transformed into perfect sequences with impulsive ACFs.
3. Frank codes and Chu codes have perfect periodic ACFs and optimum periodic CCFs. In addition, it is shown that they also have very favourable nonperiodic ACFs; some new results concerning the behaviour of the nonperiodic ACFs are derived. Further, it is proved that the sets of combined Frank/Chu codes, which contain a larger number of codes than either of the two constituent sets, also have very good periodic CCFs. Based on Frank codes and Chu codes, two interesting classes of real-valued codes with good correlation properties are defined. It is shown that these codes have periodic complementary properties and good periodic and nonperiodic ACF/CCFs.

Finally, a hybrid CCMA/SSMA coding scheme is proposed. This new hybrid coding scheme provides a very flexible and powerful multiple accessing capability and allows simple and efficient decoding. Given an SSMA system with K users and a CCMA system with N users, where at most T users are active at any time, then the hybrid system will have $K \cdot N$ users with at most $T \cdot K$ users active at any time. The hybrid CCMA/SSMA coding scheme is superior to the individual CCMA system or SSMA system in terms of information rate, number of users, decoding complexity and external interference rejection capability.

Contents

Declaration	ii
Acknowledgements	iii
Abstract	iv
List of Figures	xii
List of Tables	xiii
Glossary	xiv
Mathematical Symbols	xvi
1 Introduction	1
1.1 Outline of the Thesis	1
1.2 Single and Multiple Access Communications	3
1.3 Information Theory Approach	5
1.4 Spread Spectrum Approach	8
1.5 Collision Resolution Approach	12
1.6 Original Aspects of the Research Programme	13
2 Codes for the Multiaccess Binary Adder Channel	16
2.1 Introduction	16

2.2	Constant Weight Codes and Disjunctive Codes	19
2.3	Decomposition and Error Correction of the Codes	21
2.4	Decoding Algorithms for the Noiseless N-BAC	25
2.5	Decoding Algorithms for the Noisy Case	27
2.6	Concluding Remarks	28
3	Codes for the Multiaccess Q-ary Adder Channel	29
3.1	Introduction	29
3.2	Factorization of $x^n - 1$ over the Integer Ring Z_Q	30
3.3	Cyclic Codes over Z_Q for the N-QAC Channel	32
3.4	Encoding and Decoding Algorithms	34
3.5	Concluding Remarks	36
4	Codes for Synchronous SSMA Systems	38
4.1	Introduction	38
4.2	Complementarity, Uncorrelatedness and Orthogonality	39
4.3	Synthesis of Orthogonal Complementary Sets	41
4.4	Some Conjectures	47
4.5	Applications to Synchronous SSMA	47
4.6	Concluding Remarks	51
5	Codes for Asynchronous SSMA Systems–I	52
5.1	Introduction	52
5.2	Sequences with Two-valued ACFs and CCFs	54
5.3	Periodic Correlation Performance of the Sequences	56
5.4	Nonperiodic Correlation Performance of the Sequences	57
5.5	Concluding Remarks	61
6	Codes for Asynchronous SSMA Systems–II	62

6.1	Introduction	62
6.2	Gaussian Prime Residue Classes and Galois Fields	63
6.3	Properties of M-Sequences over Gaussian Integers	66
6.4	Complex M-Sequences with Good ACFs and CCFs	67
6.5	Perfect Sequences over Rational and Gaussian Integers	70
6.6	Concluding Remarks	73
7	Codes for Asynchronous SSMA Systems–III	74
7.1	Introduction	74
7.2	Periodic Correlations of Frank/Chu Sequences	75
7.3	Nonperiodic Correlations of Frank/Chu Sequences	77
7.4	Combined Frank/Chu Sequences and their Characteristics	82
7.5	Derived Real-valued Sequences and their Characteristics	85
7.6	Concluding Remarks	93
8	Hybrid CCMA/SSMA Coding Scheme	94
8.1	Introduction	94
8.2	Hybrid CCMA/SSMA System Model	95
8.3	Principle and Examples	97
8.4	Concluding Remarks	101
9	Conclusions and Recommendations for Further Work	103
9.1	Conclusions	103
9.2	Further Work	107
	References	109
A	Publications of the Author	122
A.1	Publications–After 1992	122

A.2	Publications–Before 1992	124
B	Proof of Various Lemmas, Theorems and Inequality	126
B.1	Proof 1	126
B.2	Proof 2	128
B.3	Proof 3	128
B.4	Proof 4	129
B.5	Proof 5	131
B.6	Proof 6	133
B.7	Proof 7	134
B.8	Proof 8	137
B.9	Proof 9	138
B.10	Proof 10	138

List of Figures

1.1	Single Access Communication System	3
1.2	Multiple Access Communication System	4
1.3	Classification of Multiaccess Communication Schemes	5
1.4	Capacity Region of 2-user MAC	6
1.5	Asynchronous Binary-phased DS SSMA System	10
2.1	Classification of Multiaccess Channel Models	17
2.2	Multiaccess Binary Adder Channel	18
4.1	Synchronous SSMA System Model Employing OCSS	48
4.2	Generalized Sliding Correlator Synchronization	50
5.1	Nonperiodic ACF of Sequence $a^{(0)}$	59
5.2	Nonperiodic ACF of Sequence $a^{(1)}$	59
5.3	Nonperiodic ACF of Sequence $a^{(99)}$	59
5.4	Nonperiodic CCF between $a^{(0)}$ and $a^{(1)}$	60
5.5	Nonperiodic CCF between $a^{(0)}$ and $a^{(99)}$	60
5.6	Nonperiodic CCF between $a^{(1)}$ and $a^{(99)}$	60
5.7	Periodic ACF of $a^{(0)}$	61
5.8	Periodic CCF bt. $a^{(0)}, a^{(1)}$	61
6.1	Signal Constellation for $\pi = 2 + i, 3 + 2i, 3i, 7i$ ($p = 5, 13, 3, 7$) .	64

7.1	PACF of $a^{(1)}$ -I	89
7.2	PACF of $b^{(1)}$ -I	89
7.3	PACF of $a^{(2)}$ -I	89
7.4	PACF of $b^{(2)}$ -I	89
7.5	PCCF of $a^{(1)}, a^{(2)}$ -I	89
7.6	PCCF of $b^{(1)}, b^{(2)}$ -I	89
7.7	PCCF $a^{(1)}, b^{(1)}$ -I	89
7.8	PCCF of $a^{(1)}, b^{(2)}$ -I	89
7.9	PACF of $a^{(1)}$ -II	90
7.10	PACF of $b^{(1)}$ -II	90
7.11	PACF of $a^{(2)}$ -II	90
7.12	PACF of $b^{(2)}$ -II	90
7.13	PCCF of $a^{(1)}, a^{(2)}$ -II	90
7.14	PCCF of $b^{(1)}, b^{(2)}$ -II	90
7.15	PCCF of $a^{(1)}, b^{(1)}$ -II	90
7.16	PCCF of $a^{(1)}, b^{(2)}$ -II	90
7.17	NACF of $a^{(1)}$ -I	91
7.18	NACF of $b^{(1)}$ -I	91
7.19	NACF of $a^{(2)}$ -I	91
7.20	NACF of $b^{(2)}$ -I	91
7.21	NCCF of $a^{(1)}, a^{(2)}$ -I	91
7.22	NCCF of $b^{(1)}, b^{(2)}$ -I	91
7.23	NCCF $a^{(1)}, b^{(1)}$ -I	91
7.24	NCCF of $a^{(1)}, b^{(2)}$ -I	91
7.25	NACF of $a^{(1)}$ -II	92
7.26	NACF of $b^{(1)}$ -II	92
7.27	NACF of $a^{(2)}$ -II	92

7.28	NACF of $b^{(2)}$ -II	92
7.29	NCCF of $a^{(1)}, a^{(2)}$ -II	92
7.30	NCCF of $b^{(1)}, b^{(2)}$ -II	92
7.31	NCCF of $a^{(1)}, b^{(1)}$ -II	92
7.32	NCCF of $a^{(1)}, b^{(2)}$ -II	92
8.1	Hybrid CCMA/SSMA System Model	96
B.1	Illustration of $C_F^{(r)}(uq + v) = A - B$	131

List of Tables

3.1	Examples of Factorization of $x^n - 1$ over Z_Q	32
5.1	Aperiodic ACFs/CCFs of New Sequences	58
5.2	Aperiodic ACFs/CCFs of Scholtz-Welch Sequences	58
6.1	Exponent Table of Field G_{3i}	65
6.2	Exponent Table of Field G_{2+i}	65
6.3	Exponent Table of Field G_{7i}	65
6.4	Exponent Table of Field G_{3+2i}	65
6.5	Examples of Primitive Polynomials $f(x)$ over G_π	67
7.1	Illustration of $b = f(r, L)$, $(r, L) = 1$, $L = ar + k$, $r \leq 20$, $k \leq \lfloor r/2 \rfloor$	81
7.2	Illustration of c , $B_C^{(r)} = L/c$, $(r, L) = 1$, $r \leq 20$, $k \leq \lfloor r/2 \rfloor$. . .	81
7.3	CCFs of Combined Frank/Chu Sequences($L=25$, $r=s \bmod 5$) . . .	85
8.1	Look-up Decoding Table for the 2-user CCMA system	101

Glossary

This section details all of the special abbreviations used in this thesis.

ACF Auto correlation function

CCF Cross correlation function

CCMA Collaborative coding multiple access

CDMA Code division multiple access

CR Collision resolution

CRC Cyclic redundancy check

CS Complementary sequence

CSMA Carrier sense multiple access

CW Constant weight code

DM-MAC Discrete memoryless MAC

DS SSMA Direct sequence SSMA

DSP Digital signal processor

FDMA Frequency division multiple access

FH SSMA Frequency hopping SSMA

FSR Feedback shift register

GCD Greatest common divisor

GWN Gaussian white noise

LAN Local area network

LCM Least common multiplier

MAC Multiple access channel

MOCSS Maximally OCSS

MUCSS Maximally UCSS

N-BAC N-user binary adder channel

N-QAC N-user Q-ary adder channel

NACF Nonperiodic ACF

NCCF Nonperiodic CCF

OCPS Orthogonal complementary pairs of sequences

OCSS Orthogonal complementary sets of sequences

PACF Periodic ACF

PCCF Periodic CCF

PRS Pseudo-random sequence

PSK Phase shift keying modulation

QAM Quadrature amplitude modulation

SAC Single access channel

SNR Signal to noise ratio

SSMA Spread spectrum multiple access

UCPS Uncorrelated complementary pairs of sequences

UCSS Uncorrelated complementary sets of sequences

TDMA Time division multiple access

Mathematical Symbols

This section details the common mathematical symbols used in this thesis.

$\rho_{i,i}(\tau)$ Continuous-time partial ACF

$\rho_{i,k}(\tau)$ Continuous-time partial CCF

B_F Asymptotic nonperiodic nontrivial ACF value of Sequence F

C_{MAC} Capacity region of MAC

C_{max} Maximum nontrivial value of nonperiodic ACF/CCF

$C_r(\tau)$ Non-periodic ACF

$C_{r,s}(\tau)$ Non-periodic CCF

$D(n, T, N)$ Disjunctive code of length n , order T and size N .

P_e Probability of error

$R_r(\tau)$ Periodic ACF

$R_{r,s}(\tau)$ Periodic CCF (Even CCF)

$\hat{R}_{r,s}(\tau)$ Odd CCF

R_{sum} Rate sum

R_{max} Maximum nontrivial value of periodic ACF/CCF

$S_{P,M}^N$ OCSS with N sets, each set has P sequences of length M

$Wt(z)$ Weight of z (sum of the z_i)

Z_Q Finite integer ring

Chapter 1

Introduction

1.1 Outline of the Thesis

This thesis deals with the code design and analysis for spread spectrum multi-access(SSMA) communications and collaborative coding multiaccess(CCMA) communications. The general idea behind these two multiaccess schemes is that one can find sets of signals (codes) which can be mixed together to form a composite signal but then the individual signals in the set can each be recovered from the composite signal. Obviously, in order to permit efficient simultaneous transmission by several users sharing a common channel, without subdivision in time or frequency, to obtain unique decodability, to facilitate system synchronization and to enhance the robustness to unwanted signals, code set design is the key element of both SSMA and CCMA systems.

The thesis opens with a brief introduction to multiple access communications. Three bodies of research on multiple-access channels, i.e. *multiple-access information theory*, *collision resolution*, and *spread spectrum*, each proceeding in virtual isolation from the others and each using totally different models, are reviewed. In particular, an overview of the coding aspects of CCMA and CDMA techniques is given. The chapter concludes with an outline of the original work contained within the thesis.

Chapters 2 and 3 give detailed accounts of the research undertaken in the area of CCMA. Chapter 2 investigates coding for the multiaccess binary adder channel. By giving some basic concepts concerning the superposition mechanism and superimposed codes, the relationship between the constant weight codes and disjunctive codes is analyzed. Then some important results related to the decomposition of the disjunctive codes in the noiseless and noisy cases are derived. Several efficient decoding algorithms for noiseless and noisy channel

are developed. In Chapter 3, coding for the multiaccess Q -ary adder channel is considered by employing cyclic codes with symbols taken from an arbitrary finite integer ring. The code construction is based on the factorization of $x^n - 1$ over the unit ring of an appropriate extension of a finite integer ring. A very low complexity decoding procedure is presented and it is shown that the maximum achievable sum rate is 1.

Chapter 4 deals with the design of orthogonal complementary sets of sequences for use in synchronous SSMA systems. After definition of the concepts of complementarity, uncorrelatedness and orthogonality, recursive formulas for constructing orthogonal complementary sets are proposed; methods for synthesizing new orthogonal complementary sets from known ones with the same dimensions are discussed. Conjectures relating to maximally orthogonal complementary sets are also given. Finally an application of orthogonal complementary sets to synchronous SSMA systems is described.

The work of Chapters 5,6 and 7 contributes to the code sequences used in asynchronous SSMA systems. In Chapter 5, a new class of code sequences is proposed. The proposed sequences have two-valued auto- and crosscorrelation functions (ACFs and CCFs) and any two sequences in this class are mutually orthogonal. In Chapter 6, a generalized class of maximal length sequences or m -sequences is defined over Gaussian integers. It is shown that there exist two sub-classes of sequences whose ACFs are quasi-perfect and which can be transformed to a perfect form by suitable operations. Chapter 7 is concerned with two classes of perfect codes, i.e. Frank codes and Chu codes. Apart from their periodic correlations, it is shown that they also have very favourable nonperiodic correlation properties. Some new results concerning the behaviour of the nonperiodic ACFs are obtained. It is also proved that sets of combined Frank/Chu codes, which contain a larger number of codes than either of the two constituent sets, also have very good periodic correlation properties, and hence can be used in asynchronous SSMA to provide more users. Based on Frank codes and Chu codes, two interesting classes of real-valued codes with good correlation properties are defined. It is shown that these codes have periodic complementary properties. From calculated ACF/CCF results, it is demonstrated that they also have good periodic and nonperiodic ACF/CCFs.

Chapter 8 presents a new hybrid CCMA/SSMA coding scheme. This scheme effectively comprises concatenated CCMA and SSMA systems. The hybrid system provides a very flexible and powerful multiple accessing method. Given an SSMA system with K users and, a CCMA system with N users, where at most T users are active at any time, then the hybrid system will have $K \cdot N$ users with at most $T \cdot K$ users active at any time. The hybrid system is superior to the individual CCMA system or SSMA system in terms of information rate, number of active users, synchronization ability and external interference

rejection capability.

Finally, Chapter 9 concludes the work contained within this thesis and details possible areas for further research. Several appendices are included that describe work which, whilst necessary for a complete description of the research, would detract from the flow of the thesis if included in the main body.

1.2 Single and Multiple Access Communications

The task of the communication system designer is to provide a cost-effective system for transmitting information from senders to recipients at the rate and level of accuracy that the users require.

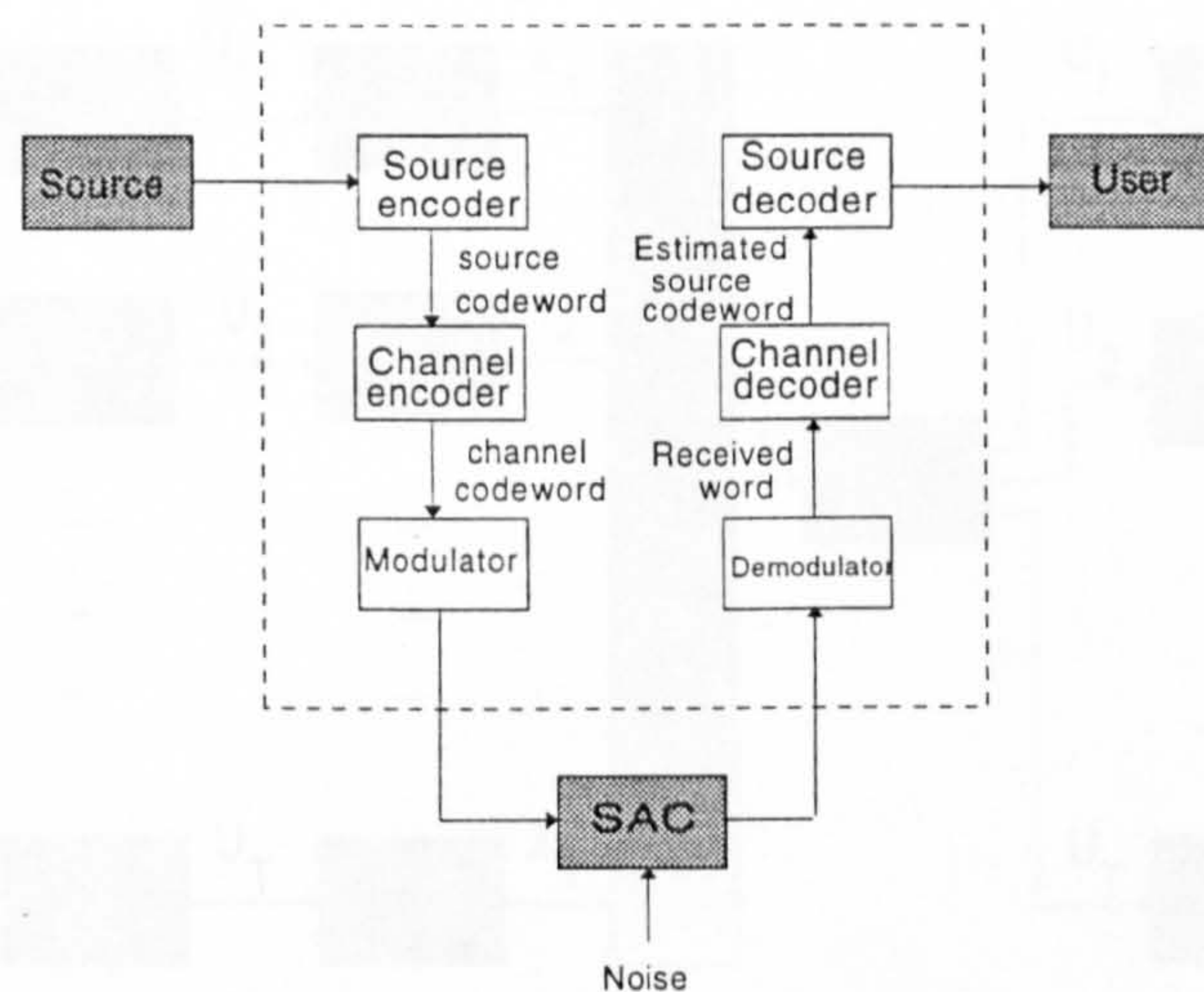


Figure 1.1: Single Access Communication System

The classical model of a single access communication system has a single transmitter sending information to a receiver through a single access channel (SAC) which in some way corrupts the transmitted information, as shown in Fig. 1.1. The source encoder is designed to represent the source data more compactly (i.e. to remove redundancy for rate). The channel encoder performs all the digital operations needed to prepare the source data for modulation, for example, error control coding (i.e. to add redundancy for accuracy), and binary-to-nonbinary conversion. The function of the modulator is to match the channel encoder output to the transmission channel. Because the channel is subject to various types of noise, distortion and interference, the channel output differs

from the channel input. The aim of demodulator, channel decoder and source decoder is to restore the original information at the receiver.

The most important and widely-used model of a multi-user communication is the multiple access communication channel (MAC) model (Gallager, 1985; Farrell, 1981; Wolf, 1981), as shown in Fig. 1.2. There are multiple transmitters and a single receiver. The received signal is corrupted both by noise and by mutual interference between the transmitters. Each of the transmitters is fed by an information source and each information source generates a sequence of messages, successive messages arriving at random instants of time. For a single access channel, one normally assumes an infinite reservoir of data to be transmitted. For multiaccess channels, most transmitters have nothing to send most of the time, with only a few being active. The problem is then to share the channel between the active users and this is often the central technical concern in multiaccess communication.

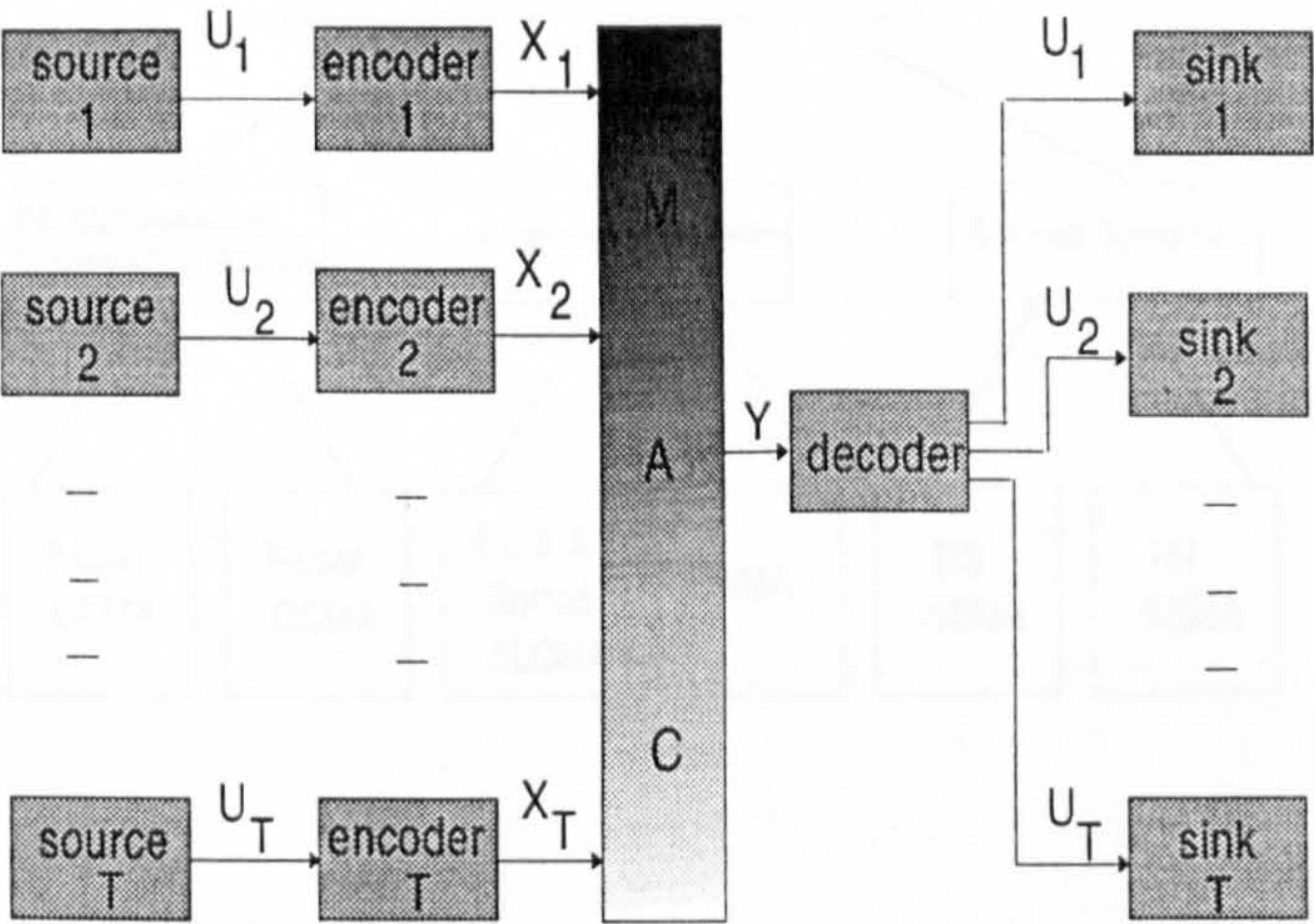


Figure 1.2: Multiple Access Communication System

This type of model is appropriate for the uplink of a satellite network, for a radio network where there is one central repeater and for the traffic to the central node on a multidrop telephone line. It is also adequate in most respects for studying networks where a common channel allows all nodes to hear all other nodes. Common examples are a cable connecting many nodes and a fully connected radio network.

Gallager (Gallager, 1985) points out that there are at least three bodies of research on multiple-access channels, each proceeding in virtual isolation from the others and each using totally different models. A classification of the three areas is shown in Fig. 1.3. The three areas can be described as *multiple-access*

information theory, collision resolution and spread spectrum.

The major issues that one has to deal with in multiple-access communication systems are interference between users, noise and the random (or bursty) arrivals of messages. The multiple-access information theory approach appropriately models the noise and interference of MACs but ignores the random arrival of messages. The collision resolution approach focuses on the random arrival of messages and on the transmission delays which are due to the interference between users, but generally ignores all other aspects of the underlying communication process. The traditional spread spectrum approach treats everybody else's transmissions as "jamming by the enemy", i.e. the interference from other users is treated as additional (potentially intelligent) noise.

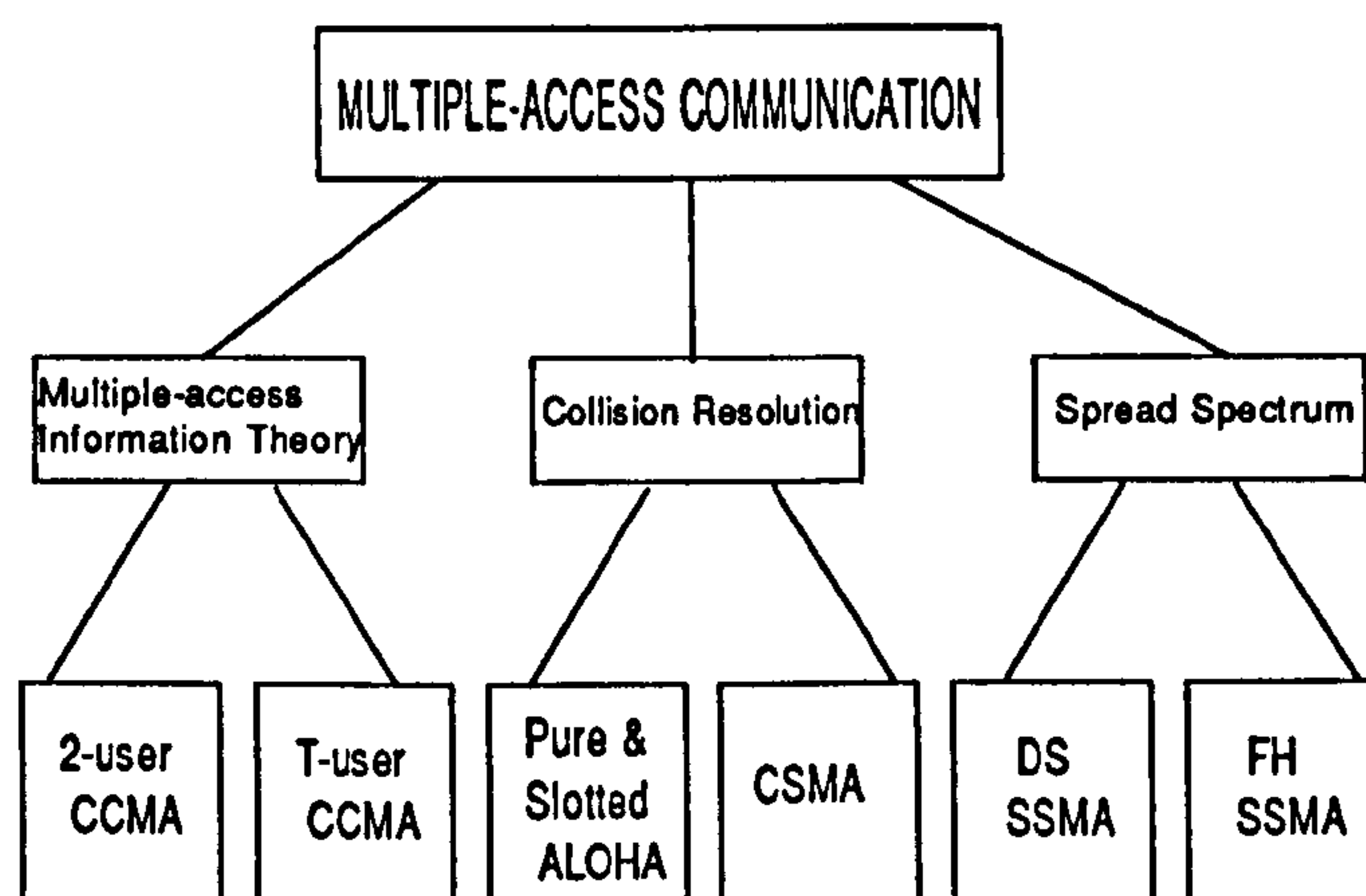


Figure 1.3: Classification of Multiaccess Communication Schemes

1.3 Information Theory Approach

The multiple access information theoretic approach was initiated in 1961 by Shannon in his fundamental paper (Shannon, 1961) and established in 1971 with a coding theorem developed by Ahlswede (Ahlswede, 1971) and Liao (Liao, 1972). This work has also been generalized in many ways and has given rise to a distinct area of research (Gamal & Cover, 1980; Meulen van der, 1977; Csiszar & Körner, 1981).

The coding theorems of information theory treat the question of how much data can be reliably communicated from one point, or set of points, to another point, or set of points. The main objective of the coding theorem is to characterize

the capacity region of a MAC for certain communication situations, that is to determine a set of simultaneously achievable rates which allow each user to communicate with the receiver with arbitrarily small error probability in the decoder output sequences. The highest rate at which reliable data can be transmitted over a channel is called the *capacity* of the channel. The set of rates at which simultaneous reliable transmission is possible is called the *capacity region* of a MAC, C_{MAC} .

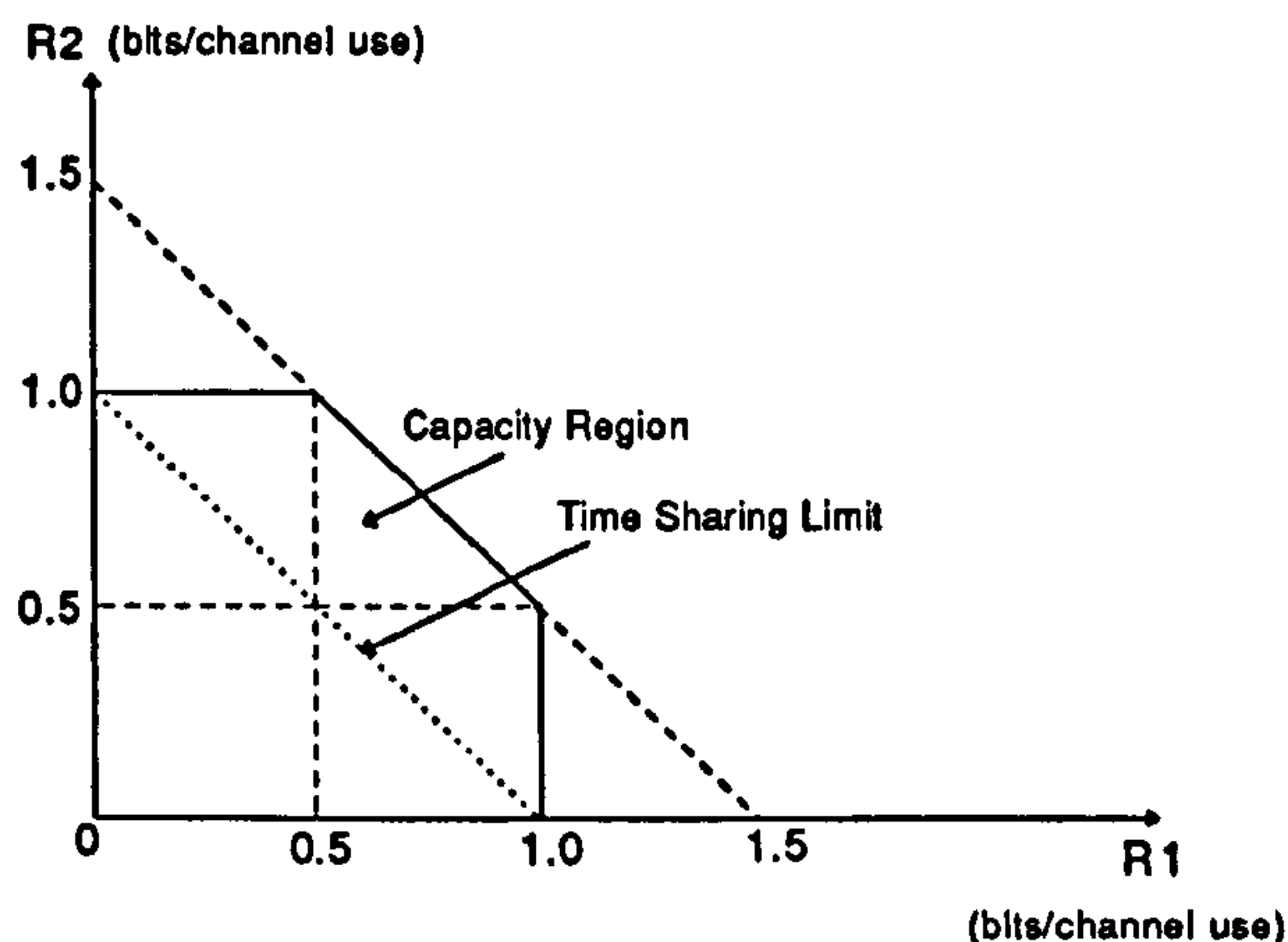


Figure 1.4: Capacity Region of 2-user MAC

The capacity regions for the 2-user and 3-user discrete memoryless(DM) MAC with independent sources have been determined by (Ahlsvede, 1971). van der Meulen (Meulen van der, 1971) put forward a limiting expression and simple inner and outer bounds on the sets of simultaneously achievable rates. Liao (Liao, 1972) studied the general T-user DM-MAC with independent sources. He determined a set of rates which allow each transmitter to communicate with the receiver with an arbitrarily small probability of error and showed that, for any set of rates outside the capacity region, the probability of error cannot be made arbitrarily small. In the case of 2-user adder MAC with binary inputs, the capacity region is shown in Fig. 1.4 (Ahlsvede, 1971; Liao, 1972). The basic assumption is that the encoders are to operate independently of each other. It was also assumed that the encoders utilized block codes and that the encoders produced codewords that were in block and bit synchronism. Besides this, it was assumed that the decoder was in block and bit synchronism with the encoders. Slepian and Wolf (Slepian & Wolf, 1973) later generalized this result by considering a third source that could be encoded jointly by both transmitters. The information capacity of a Gaussian MAC has been determined by Wyner (Wyner, 1974), Cover (Cover, 1975), Gamal et al (Gamal & Cover, 1980).

While the theoretical development of coding theorems for multiaccess is reason-

ably advanced, very little has been done with respect to general techniques for multiaccess collaborative coding (Gallager, 1985). Here a brief overview of the coding aspects of Collaborative Coding Multiple Access (CCMA) techniques is given.

The block code constructions for noiseless synchronous MAC model have followed three main approaches. The first one focused on achieving the bounds promised by multiple access information theory for the 2-user binary input adder MAC. Code constructions which belong to this class are given in (Kasami *et al.*, 1975a; Kasami & Lin, 1976; Kasami *et al.*, 1983; Weldon Jr., 1978; Khachatrian, 1982; Khachatrian, 1983; Braak & Tilborg, 1985; Lin & Wei, 1986). The search for codes in this case is complicated by the fact that at least one of the two codes must be nonlinear to achieve a nontrivial rate point anywhere near the boundary of the capacity region of the MAC. The second approach with the same philosophy is to construct codes for the T -user noiseless binary input adder MAC with the goal of achieving channel capacity asymptotically as T goes to infinity. In this case, each user usually gets two codewords and it is assumed that all T users are always active. Code constructions for this class of codes are given in (Chang & Weldon Jr., 1979; Ferguson, 1982; Chang, 1984; Wilson, 1988). As pointed out by (Gallager, 1985), what is needed is a coding technology that is applicable to a large set of transmitters of which a small, but variable, subset simultaneously use the channel; therefore, the third approach aims at the code construction for a T active users out of N multiple access system. In this case, the primary goal of code construction is not to achieve channel capacity (although this is of course always an enticing goal); the reason is that codes with highest possible sum rate may not be suitable for practical use if their decoders have a prohibitively high complexity. Therefore unique decodability and simple decoding algorithms are of great interest in this approach. Examples of this approach are given in (Mathys, 1990; da Rocha Jr., 1993b; da Rocha Jr., 1993a; da Rocha Jr. *et al.*, 1993; Fan *et al.*, 1994c; Fan *et al.*, 1995).

A code is said to be uniquely decodable if and only if all the received composite codewords, which result from the users' codeword transmissions, are distinct. A simple coding scheme for a 2-user uniquely decodable block length of $N = 2$ is constructed by Kasami and Lin (Kasami *et al.*, 1975a; Kasami & Lin, 1976), where user 1 has the codewords $C_1 = (00, 11)$ and user 2 the codewords $C_2 = (00, 01, 10)$. It is clear that (C_1, C_2) is a uniquely decodable code pair, in which all the received composite codewords are unique. Thus the decoder can unscramble the two messages without ambiguity. The overall rate sum achieved by this scheme is $R_{sum} = R_1 + R_2 = 1.293$ bits per channel use, which is higher than time-sharing. It is seen that, from Fig. 1.4, the maximum value R_{sum} of the 2-user binary adder MAC is 1.5 bits per channel use. This simple coding

scheme is extended later to block length L (Kasami & Lin, 1976). The rates are $(R_1, R_2) = (1/L, \lceil \log_2(2^L - 1) \rceil / L)$, and the rate sum decreases with increase in L , tending to unity. Thus $L = 2$ is both the simplest and the most efficient case. Obviously the T -user coding scheme will be much more complicated than that of the 2-user coding scheme.

For any T -user uniquely decodable coding scheme, the received vector can, in principle, be decoded by a look-up table using an exhaustive searching nearest-neighbour decoding algorithm, since there is a one-to-one correspondence between each received vector and the only possible set of T transmitted codewords. Thus, in noiseless conditions the decoder is capable of decoding every possible received vector, without ambiguity, into the T codewords that were transmitted by the T encoders. However, as the number of users and the length of codewords increase, the scheme obviously becomes impractical because of the prohibitively high complexity. Therefore it is very important to study other algorithms with low decoding complexity, such as the algorithms given by (Chang & Weldon Jr., 1979; Mathys, 1990; da Rocha Jr., 1993a; da Rocha Jr. *et al.*, 1993; Fan *et al.*, 1994c; Fan *et al.*, 1995).

1.4 Spread Spectrum Approach

Spread spectrum is a means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information; the band spread is accomplished by means of a code which is independent of the data, and the synchronized reception using a reference code at the receiver is used for despreading and subsequent data recovery. The large redundancy inherent in spread spectrum signals is required to overcome the severe levels of interference that are encountered in the transmission of digital information over some radio and satellite channels.

There are primarily two spread spectrum techniques, Direct Sequence (DS) spread spectrum and Frequency Hopping (FH) spread spectrum. The goal of both of these techniques is to take the power to be transmitted and spread it over a very wide bandwidth so that the power per unit bandwidth (watts per hertz) is small. FH spread spectrum occupies the large bandwidth provided for the spread spectrum systems by periodically changing the carrier frequency of the transmitted signal; the changing is called "hopping". DS spread spectrum achieves a spreading of the spectrum by using the data signal to modulate the very wide band spread spectrum sequence. This thesis will only deal with DS spread spectrum.

The multiple access system considered operates by spreading the bandwidth

of a user's signal over a wide range of frequencies prior to transmission. The multiple access capability achieved is termed Code Division Multiple Access (CDMA). As the data signals have been spectrally spread, this technique is also known as Spread Spectrum Multiple Access (SSMA) (Pickholtz *et al.*, 1982; Dixon, 1984; Simon *et al.*, 1985; Taylor & Omura, 1991; Scholtz, 1982; Schilling *et al.*, 1991).

In comparison, let us consider the two most common multiplexing techniques: Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA). In FDMA, all users transmit simultaneously, but use disjoint frequency subbands. Obviously the width of the subband, which corresponds to only a portion of its total system capacity for each user, is restricted. The need to allow "guard bands" between subbands also reduces system efficiency. In TDMA, all users occupy the complete system bandwidth, but transmit sequentially in uniquely defined time slots. When users are allowed to transmit simultaneously in time and occupy the complete system bandwidth as well, some other means of separating the signals at the receiver must be available; the above mentioned CCMA and SSMA techniques provide this necessary capability. In a perfectly linear, perfectly synchronous system, the number of orthogonal users for all three systems is the same, since this number only depends upon the dimensionality of the overall signal space. The differences between the three multiple access techniques become apparent when various real-world constraints are imposed upon the ideal situation described above.

1. SSMA does not require an external synchronization network, which is an essential feature of TDMA. That is to say, the SSMA system normally operates asynchronously, or the transition times of a user's data symbols do not have to coincide with those of the other users.
2. SSMA offers a gradual degradation in performance as the number of users is increased. It is therefore relatively easy to add new users to the system.
3. SSMA offers an external interference rejection capability (e.g. multipath rejection or resistance to deliberate jamming).
4. SSMA can be used in a frequency band that has existing narrowband users. Therefore, this means of communication represents an effective and efficient mode of frequency band utilization and sharing.

In DS SSMA, each user is given its own code, which is approximately uncorrelated (i.e., has low cross correlation) with the codes of the other users. While the code design problem in DS CDMA is very crucial in determining system performance, the power control strategy (referred to as "near-far problem" due

to different received powers from the geographically separated users) is also very important. However we will only focus on the code design problem in this thesis.

The asynchronous binary-phased DS SSMA system is shown in Fig. 1.5. The received signal is given by

$$r(t) = \sum_{k=1}^K \sqrt{2P} a_k(t - \tau_k) b_k(t - \tau_k) \cos(\omega_c t + \phi_k) + n(t) \quad (1.1)$$

where

$b_i(t)$ = binary message (± 1) of the i th user with bit duration T ;

$a_i(t)$ = spreading code waveform of the i th user, assuming that there are K active users;

$\sqrt{2P}, \omega_c, \phi_k$ = amplitude, frequency and phase of the i th user, $\phi_k = \theta_k - \omega_c \tau_k$;

τ_i = random time delay of the i th user distributed in $[0, T]$;

$n(t)$ = narrow-band interference and wideband channel noise.

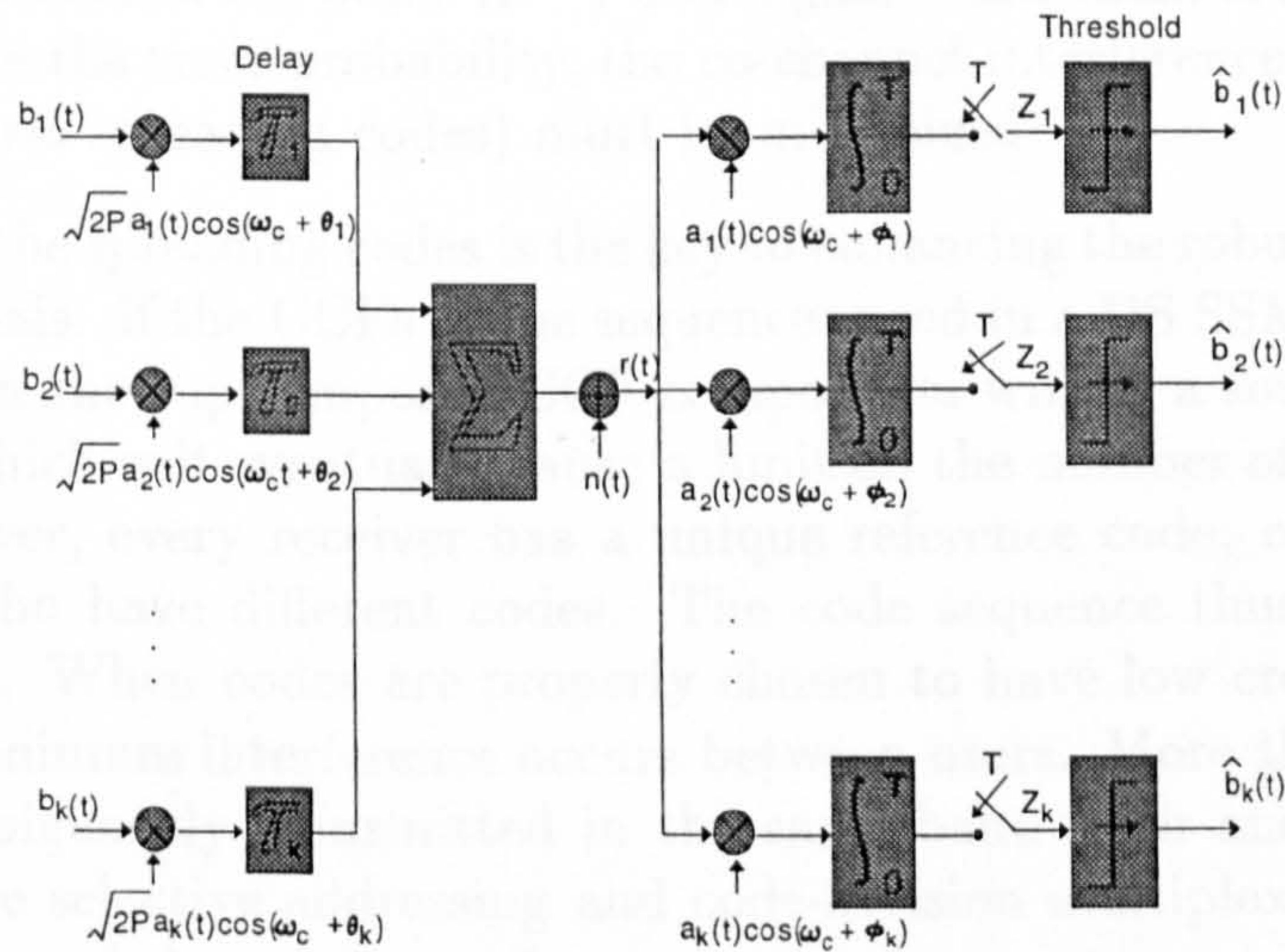


Figure 1.5: Asynchronous Binary-phased DS SSMA System

Assuming that the receiver is correctly synchronized to the i th signal, we can set ϕ_i to zero without losing any generality. If the received signal $r(t)$ is the input to a correlation receiver matched to the i th user's transmitted signal, the

output Z_i is given by

$$Z_i = \sqrt{\frac{P}{2}} b_{i,0} T + \sqrt{\frac{P}{2}} \sum_{\substack{k=1 \\ k \neq i}}^K [b_{k,-1} \rho_{k,i}(\tau_k) + b_{k,0} \hat{\rho}_{k,i}(\tau_k)] \cos \phi_k + n_0(t) \quad (1.2)$$

where $n_0(t) = \int_0^T n(t) a_i(t) \cos \omega_c t dt$, and the double frequency terms have been ignored. The $b_{k,-1}$, $b_{k,0}$ are consecutive data bits and $\rho_{k,i}$, $\hat{\rho}_{k,i}$ are the continuous-time partial crosscorrelation functions (CCFs) defined by

$$\rho_{k,i}(\tau) = \int_0^\tau a_k(t - \tau) a_i(t) dt, \quad \hat{\rho}_{k,i}(\tau) = \int_\tau^T a_k(t - \tau) a_i(t) dt \quad (1.3)$$

which can also be represented as discrete CCFs (Pursley, 1977; Pursley & Sarwate, 1977; Pursley & Roefs, 1977). In Eqn 1.2, the first, second and the last terms represent respectively the expected message, co-channel interference due to the existence of the other $K - 1$ user signals, and channel noise. Thus in order to reduce the error probability, the co-channel interference (or the CCFs between any two spreading codes) must be minimized.

The design of the spreading codes is the key to enhancing the robustness against unwanted signals. If the CCFs of the sequences used in a DS SSMA system are not small, then the superimposed CCF components will be a source of system "self noise" which will eventually cause a limit on the number of simultaneous users. Moreover, every receiver has a unique reference code, compared with other users who have different codes. The code sequence thus becomes the user's address. When codes are properly chosen to have low cross-correlation properties, minimum interference occurs between users. More than one signal can be unambiguously transmitted in the same bandwidth and at the same time; therefore selective addressing and code-division multiplexing are implemented by the coded modulation format.

For an ideal DS SSMA system, a set of completely uncorrelated sequences (CCF is zero everywhere) with ideal impulsive autocorrelation functions (ACFs) (which are zero everywhere except at zero time shift) should be used. However such sequences are impossible to find, although it is possible to find completely uncorrelated sequences with good ACFs (Darnell, 1989; Darnell, 1993b; Miller & Darnell, 1990; Miller, 1990), or to find good sequences with perfect ACFs and very low CCFs (Chu, 1972; Frank & Zadoff, 1962). In fact, for any set of sequences of size K and length L , there exist some fundamental restrictions on the values of ACF, CCF, K and L , as discussed below.

We now consider a set of K complex-valued sequences $\{(a_j^{(k)}) : 1 \leq k \leq K\}$ where $(a_j^{(k)})$ represents the code-sequence assigned to the k -th user in the DS SSMA system. The aperiodic CCF $C_{k,i}$ and periodic CCF $R_{k,i}$ for the complex-valued sequences $(a_j^{(k)})$ and $(a_j^{(i)})$ of period L are defined by

$$C_{k,i}(\tau) = \sum_{j=0}^{L-\tau-1} a_j^{(k)} [a_{j+\tau}^{(i)}]^*, \quad R_{k,i}(\tau) = \sum_{j=0}^{L-1} a_j^{(k)} [a_{j+\tau}^{(i)}]^*, \quad 0 \leq \tau < L \quad (1.4)$$

When $k = i$, the above definition becomes that of the ACF.

It is desirable to minimize the peak crosscorrelation magnitude and the out-of-phase autocorrelation magnitude, i.e. to minimize the maximum nontrivial value of R_{max} , C_{max} .

The results of Welch (Welch, 1974), Sidelnikov (Sidelnikov, 1971) and Sarwate (Sarwate, 1979) provide lower bounds on the minimum possible value of the parameter R_{max} and are commonly used to judge the merits of a particular sequence design. For large values of family size K and sequence length L the above lower bounds imply

$$R_{max} \geq L \sqrt{\frac{K-1}{LK-1}} \approx \sqrt{L} \quad (1.5)$$

There are also some similar bounds on the maximum nontrivial value of aperiodic correlation value $C_{k,i}$ (Welch, 1974; Sarwate & Pursley, 1980; Mow, 1994).

For synchronous DS SSMA, the basic requirement for the sequence design is that all the sequences used should be mutually orthogonal or nearly orthogonal.

In this thesis, we will concentrate on the design and analysis of orthogonal complementary codes and complex codes with two-valued or optimal ACFs/CCFs.

1.5 Collision Resolution Approach

The beginning of the collision resolution approach to multiaccess communication came in 1970 with Abramson's ALOHA network (Abramson, 1970). The idea here was that whenever a message (or packet) arrived at a transmitter, it would simply be transmitted, ignoring all other transmitters in the network. If another transmitter was transmitting in an overlapping interval,

interference would prevent the message from being correctly received, the cyclic redundancy check (CRC) would not check, no acknowledgment would be sent, and the transmitter would try again later; the later time would be pseudorandomly chosen to avoid the certainty of another collision which would occur if both transmitters waited the same time. Over the years, this basic strategy has been improved, generalized, and analyzed in many ways (Massey, 1985; Massey & Mathys, 1985; Abramson, 1985; Massey, 1986; Bertsekas & Gallager, 1992).

The collision resolution approach will not be discussed in any detail elsewhere in this thesis, but is briefly discussed here for completeness.

Collision resolution research has always focused on the bursty arrival of messages and the interference between transmitters, but has generally ignored any noise. More generally, this approach ignores the underlying communication process, assuming only that a message transmission is correctly received in the absence of collision and incorrectly received when a collision occurs.

The simplest form of collision resolution strategy using the assumptions above is slotted ALOHA. Slotted ALOHA is a variation of pure ALOHA (Abramson, 1970). In slotted ALOHA, whenever a packet arrives at one of the transmitters, that packet is transmitted in the next slot. Whenever a collision occurs in a slot, each packet involved in the collision is said to be backlogged and remains backlogged until it is successfully transmitted. Each such backlogged packet is transmitted in each subsequent slot with some fixed probability $p > 0$, independent of past slots and of other packets.

In many multiaccess systems such as local networks, each transmitter can hear whether or not the other transmitters are sending. In such a situation, a transmitter can start to send a packet in the middle of a data slot if no other transmitters are currently sending. Not only does this allow idle slots to be shortened, but it can also reduce the number of collisions. Carrier sense multiple access (CSMA) techniques were first developed by Kleinrock and Tobagi (Kleinrock & Tobagi, 1975). The terminology "carrier sense" does not necessarily imply the use of a carrier, but simply the ability to quickly detect use of the channel.

1.6 Original Aspects of the Research Programme

The major original contributions to knowledge resulting from the research programme described in this thesis are as follows:

1. For the CCMA system with a multiaccess binary adder channel, a class of superimposed codes are analyzed. The relationship between constant weight codes and disjunctive codes is analyzed. Some important results related to the decomposition of the disjunctive codes in the noiseless and noisy cases are derived. Several efficient decoding algorithms for both the noiseless and the noisy channel are developed.
2. For the CCMA system with a multiaccess Q -ary adder channel, a class of cyclic uniquely decodable codes is proposed and analyzed by employing cyclic codes with symbols from an arbitrary finite integer ring. A very low complexity decoding procedure is presented.
3. For the synchronous SSMA system, a new approach employing orthogonal complementary sets is presented. The properties of such orthogonal complementary sets are studied in detail. Recursive formulas for constructing orthogonal complementary sets are presented. Methods for synthesizing new orthogonal complementary sets from known ones with the same dimensions are also discussed.
4. For the asynchronous SSMA system, several new spreading codes are presented and studied:
 - (a) A new class of polyphase codes with two-valued periodic auto- and crosscorrelation properties is proposed. It is proved that, for a given prime length $L > 3$, the out-of-phase ACFs and CCFs of the codes are constant and equal to $\sqrt{L}$. In addition, all codes of the same length are mutually orthogonal.
 - (b) Maximal length codes over Gaussian integers that can be used with QAM modulation are considered. Two sub-classes of m-sequences with quasi-perfect periodic autocorrelations are obtained. The CCFs between the decimated m-sequences are studied. By applying a simple operation, multi-level and complex perfect sequences are obtained from some m-sequences over rational and Gaussian integers.
 - (c) Frank codes and Chu codes have perfect periodic ACFs and optimum periodic CCFs. It is also shown that they also have very favourable nonperiodic ACFs; some new results concerning the behaviour of the nonperiodic ACFs are derived. Further it is proved that the sets of combined Frank/Chu codes, which contain a larger number of codes than either of the two constituent sets, also have very good periodic CCFs. Based on the Frank codes and Chu codes, two interesting classes of real-valued codes with good correlation properties are defined. It is shown that these codes have periodic complementary properties and good periodic and nonperiodic ACF/CCFs.

5. Finally, a hybrid CCMA/SSMA coding scheme is proposed. The new hybrid coding scheme provides a very flexible and powerful multiple accessing capability and a simple, efficient decoding method. Given an SSMA system with K users, a CCMA system with N users where at most T users active at any time, then the hybrid system will have $K \cdot N$ users with at most $T \cdot K$ users are active at any time. The hybrid CCMA/SSMA coding scheme is superior to the individual CCMA system or SSMA system in terms of information rate, number of users, decoding complexity and external interference rejection capability.

Chapter 2

Codes for the Multiaccess Binary Adder Channel

2.1 Introduction

For multiaccess channels, most transmitters have nothing to send most of the time, and only a few are busy. Therefore the central technical problem in multiaccess communication is how to share the channel between the busy users, or how to assign codes to a set of N users where it is expected that no more than T of the users will be transmitting at any one time and where $T \ll N$. In a dynamic assignment strategy we would require only T codes. Then, as one user becomes inactive, its code can be reassigned to the next user requiring to transmit. However assignments should be made by a central reservation centre or by other means. A static assignment strategy is one where each of the N users is given its own code; thus we would require N distinct codes. In this case, it is essential to construct a set of N codes, any T of which can co-exist with each other during transmission over a given channel. This chapter and next chapter will study the static coding strategy only.

There are many channel models associated with the multiaccess coding (Farrell, 1981; Wolf, 1981; Gallager, 1985; Mathys, 1990). We restrict ourselves to memoryless discrete-time MACs with discrete input and output alphabets. Fig. 2.1 shows a classification of such MAC's according to the input combining function in the noiseless case (Mathys, 1990).

By far the most popular channel is the *real adder channel*, also known as erasure MAC or simply as the adder channel. The channel output symbol value is the arithmetic sum of the input symbol values, in the absence of noise. Code design for the noiseless and the noisy versions of this channel has been considered by

various authors (Chang & Weldon Jr., 1979; Chang, 1984; Braak & Tilborg, 1985; Farrell, 1981; Ferguson, 1982; Kasami *et al.*, 1975b; Kasami & Lin, 1976; Kasami *et al.*, 1983; Khachatrian, 1982; Khachatrian, 1983; Khachatrian, 1988; Lin & Wei, 1986; Weldon Jr., 1978; Wilson, 1988; Deaett & Wolf, 1978).

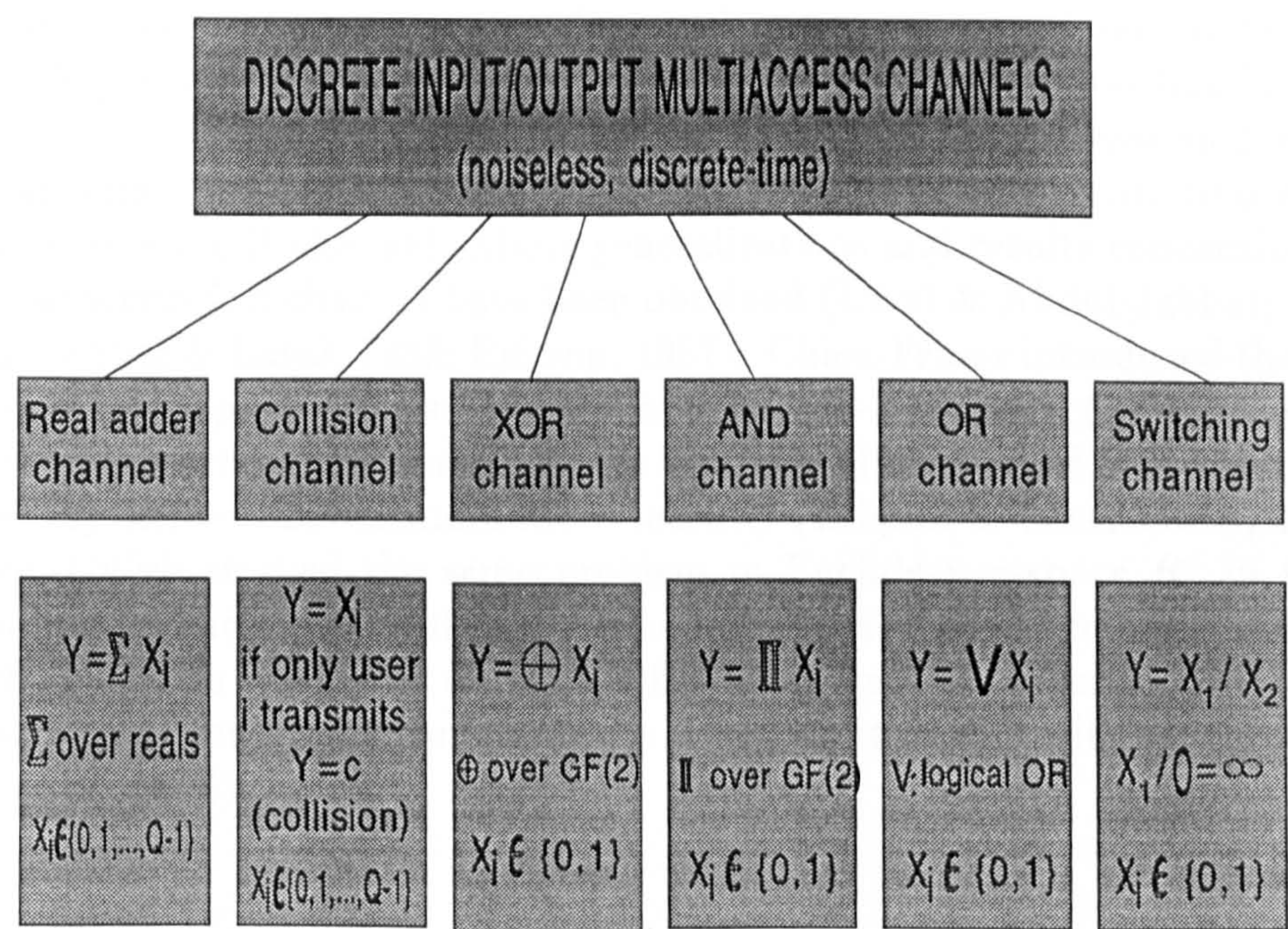


Figure 2.1: Classification of Multiaccess Channel Models

The collision channel is related to the collision resolution approach and is based on the assumption that whenever two or more users transmit simultaneously, the receiver can only detect that a collision took place. Channel discussions and code constructions for this channel are discussed in (Massey, 1985; Massey & Mathys, 1985; Massey, 1986; Gallager, 1985).

The OR channel, or pulse on-off channel, is used by various researchers in different communication situations. The output of the channel is zero if and only if all its inputs are zero, and one otherwise. Code design for this channel is treated in (Chang & Wolf, 1981; Wolf, 1981; Sommer, 1968; Cohen *et al.*, 1971; Viterbi, 1978; Gyorf, 1981; Laval & Abdul-Jabbar, 1988; Abdul-Jabbar & Laval, 1988; Ericson, 1987).

The XOR channel, or modulo 2 addition channel, is discussed in (Wolf, 1975; Farrell, 1981).

The AND channel, or binary multiplying channel, is considered in (Farrell, 1981; Meulen van der, 1977; Schalkwijk, 1982; Schalkwijk, 1983).

The switching channel is in some senses similar to the binary input real adder channel but exhibits a quite different behaviour in terms of its capacity region; its detailed description and related codes can be found in (Khachatrian, 1989; Vanroose & van der Meulen, 1987; Vanroose, 1988).

In this chapter, superimposed codes for the multiaccess binary adder channel are considered. The idea of superimposed codes was introduced in 1964 by Kautz-Singleton (Kautz & Singleton, 1964). The application they had in mind was information retrieval and the superposition mechanism assumed was a Boolean sum. The concept is, however, also useful in communications over the multiple access OR channel. Many generalizations and results concerning the multiple access OR channel have been obtained (Laval & Abdul-Jabbar, 1988; Abdul-Jabbar & Laval, 1988; Ericson, 1987). Chien-Frazer introduced the concept of superimposed codes by assuming modulo-2 addition (XOR Channel) as the superposition mechanism (Chien & Frazer, 1966), which was also reconsidered by Ericson-Levenshtein more recently (Ericson & Levenshtein, 1993). Ericson-Györfi studied the same problem in Euclidean n -space R^n in which all the inputs and the output of the channel are real-valued vectors (Ericson & Györfi, 1988). In this thesis we will further investigate the superimposed codes. The superposition mechanism used here is real addition, but with binary inputs (Fan *et al.*, 1995).

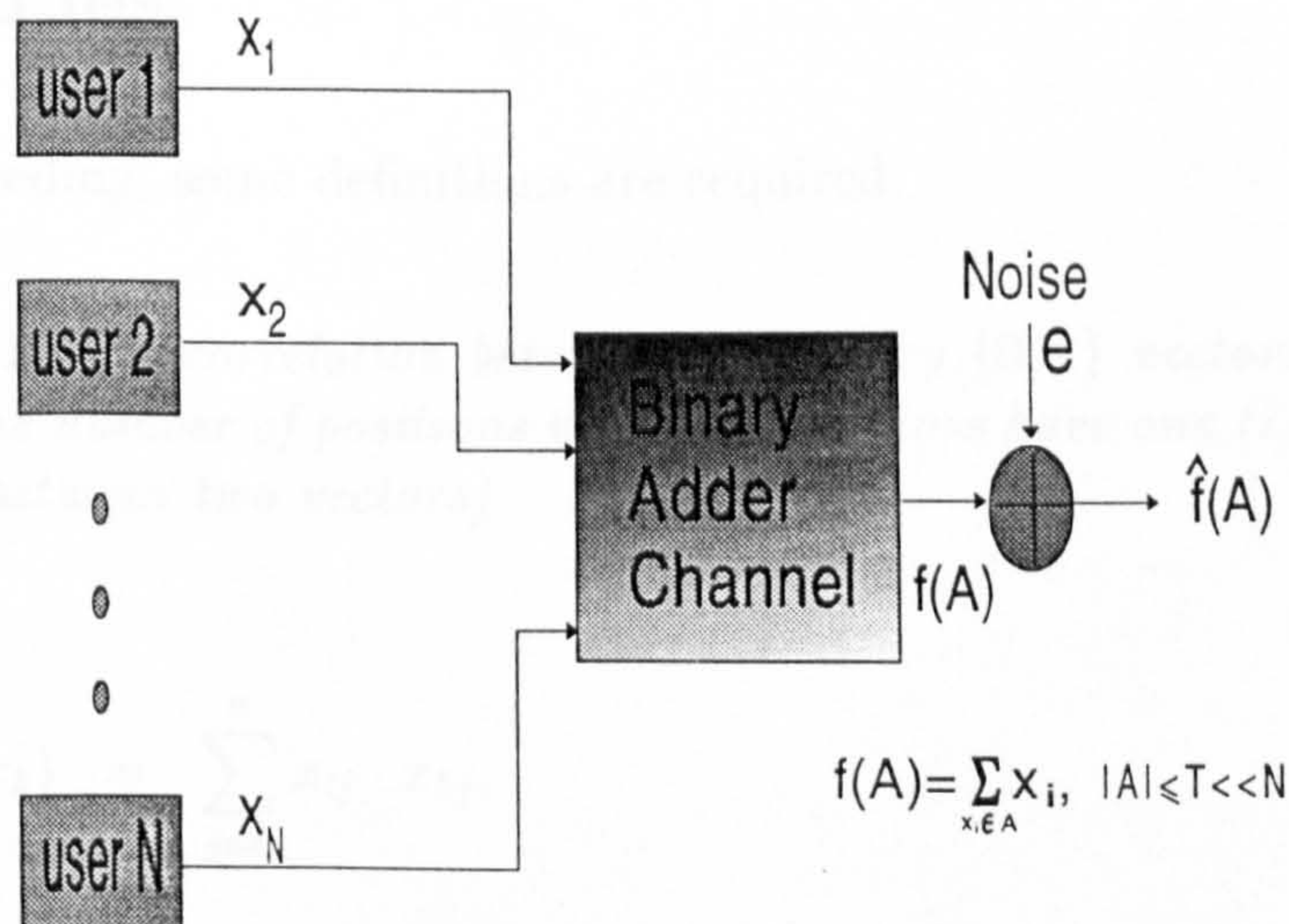


Figure 2.2: Multiaccess Binary Adder Channel

The multiaccess N -user binary adder channel (N -BAC) is shown in Fig. 2.2, where the summed output is the set of output codewords which results from the componentwise sum of codewords from a given superimposed code. The

superimposed codes are binary codes and are characterized by three parameters: the block length n , the order T and the size N . Identifying T out of N ($T \ll N$) users sharing a multiaccess adder channel can be done as follows: assign to each user one codeword from the superimposed code and the all-zero vector of length n . Those users who want to identify themselves (active users) send their respective codewords from the superimposed code. All others send the zero vector. It is assumed that both block and bit synchronization are maintained. The code guarantees unique identification of all active users as long as the number of active users does not exceed T . The decoder receives a sum vector, which is the superposition of the transmitted codewords, and it attempts to partition it into its component codewords.

In the following sections, some basic concepts concerning the superposition mechanism and superimposed codes are first given. Then the relationship between the constant weight codes and disjunctive codes is analyzed and some important results related to the decomposition of the disjunctive codes in the noiseless and noisy cases are derived. Lastly, several decoding algorithms for the noiseless channel and the noisy channel are developed.

2.2 Constant Weight Codes and Disjunctive Codes

Before proceeding, some definitions are required.

Definition 1 *The correlation between two binary $\{0,1\}$ vectors x_l and x_k of length n is the number of positions where both vectors have one (i.e., the number of overlaps between two vectors)*

$$\lambda(x_l, x_k) = \sum_{j=0}^n x_{lj} \cdot x_{kj}, \quad (2.1)$$

where the x_{lj}, x_{kj} are the j -th binary symbols of x_l and x_k respectively.

Given a binary code C , the maximum correlation λ is defined as

$$\lambda = \max_{x_l, x_k \in C, l \neq k} \lambda(x_l, x_k). \quad (2.2)$$

Definition 2 Consider a set $A = \{x_1, x_2, \dots, x_T\}$ consisting of T binary vectors of length n . The superposition of these vectors is a T -ary vector $z = f(A) = (z_1, z_2, \dots, z_n)$ of length n , where

$$z_j = \sum_{i=1}^T x_{ij} \quad j = 1, 2, \dots, n. \quad (2.3)$$

This superposition concept corresponds to the binary adder channel that operates on a set A of binary vectors and produces an output of a T -ary vector z equal to the ordinary sum of the input set.

Definition 3 The weight of a T -ary vector $z=f(A)=(z_1, z_2, \dots, z_n)$ is defined as $Wt(f(A)) = \sum_{j=1}^n |z_j|$. Let $x_i = \{x_{i1}, x_{i2}, \dots, x_{in}\}$ be a binary vector. The weight of the difference vector $f(A) - x_i$ is defined as

$$Wt(f(A) - x_i) = \sum_{j=1}^n |z_j - x_{ij}|, \quad (2.4)$$

where ' $-$ ' is normal subtraction.

Definition 4 A binary vector $x_i = (x_{i1}, x_{i2}, \dots, x_{in})$ is said to be included in a T -ary vector $z = (z_1, z_2, \dots, z_n)$ if and only if $z_j - x_{ij} \geq 0$, $j = 1, 2, \dots, n$.

Definition 5 The binary code C with codeword length n and size N is a disjunctive code of order T if each subset $A \subseteq C$ of size $|A| \leq T$ has the property that $z=f(A)$ includes only those codewords in C which are also in A . The set of all disjunctive codes with parameters n , T and N is denoted by $D(n, T, N)$.

The class of disjunctive codes is a subset of the class of superimposed codes.

Definition 6 A constant weight (CW) code is a binary code in which all codewords have the same weight. For a CW code with weight w , the correlation is related to the Hamming distance d_H by

$$d_H(x_l, x_k) = 2w - 2\lambda(x_l, x_k). \quad (2.5)$$

Denoting the minimum distance and maximum correlation by d_H and λ respectively, then

$$d_H = 2w - 2\lambda. \quad (2.6)$$

The set of all CW codes with length n , weight w , maximum correlation λ , and size N is denoted by $CW(n, w, \lambda, N)$.

2.3 Decomposition and Error Correction of the Codes

Theorem 1 *A binary constant weight code C with parameters (n, w, λ, N) is also a disjunctive code $D(n, T, N)$, where T satisfies*

$$T < \frac{w}{\lambda}. \quad (2.7)$$

Proof: Let $A \subseteq C$, $A = \{x_1, x_2, \dots, x_T\}$, and $x_c \in C$ be an arbitrary codeword not in A . Suppose $f(A)$ includes x_c , then $z_j - x_{cj} \geq 0, j = 1, 2, \dots, n$. Because the code C has a maximum correlation λ for all pairs of codewords, which means that each of the codewords $x_i \in A$ will overlap with x_c at most λ times, therefore there are at most λT positions in x_c which will overlap with all $x_1, x_2, \dots, x_T$. But from the conditions that the weight of x_c is a constant w and $\lambda T < w$ (or $T < w/\lambda$), it is obvious that there exist at least $w - \lambda T$ positions that do not overlap with any of the codewords $x_i \in A$. In other words, there exist some positions j such that $z_j - x_{cj} < 0$, which implies x_c cannot be included in $z = f(A)$ if $T < w/\lambda$. From definition 5, it can thus be concluded that a binary constant code C with parameters (n, w, λ, N) is also a disjunctive code $D(n, T, N)$.

In practice, the order T of a disjunctive code $D(n, T, N)$ should be an integer. In order to use Theorem 1, we can set

$$T = \lceil \frac{w}{\lambda} \rceil - 1 < \frac{w}{\lambda}, \quad (2.8)$$

where $\lceil x \rceil$ denotes the lowest integer greater than or equal to x . This relation is useful because it transforms the problem of designing disjunctive codes into problem of designing constant weight codes which have been fully studied in

the past (Best *et al.*, 1966; MacWilliams & Sloane, 1977). It should be pointed out that the constant weight codes only correspond to a subset of disjunctive codes. There might be some good disjunctive codes that are not constant weight codes.

Theorem 2 *If the binary code C is a disjunctive code $D(n, T, N)$ constructed from $CW(n, w, \lambda, N)$, then for each subset $A \subseteq C$ of size $|A| \leq T$, the equation $Wt(f(A) - x_i) = (|A| - 1)w$ holds when $x_i \in A$. But for all other codewords $x_c \in C \setminus A$, we have $Wt(z - x_c) > (|A| - 1)w$.*

Proof: If the binary code C is a constant weight code $CW(n, w, \lambda, N)$ then for $A \subseteq C$, it is simple to show that the weight of $z = f(A)$ is equal to

$$Wt(z) = \sum_{\{i|x_i \in A\}} \sum_{j=1}^n |x_{ij}| = |A|w. \quad (2.9)$$

Because $Wt(x_i) = w$, if $x_i \in A$ ($f(A)$ includes x_i) then

$$Wt(f(A) - x_i) = \sum_{j=1}^n |z_j - x_{ij}| = |A|w - w = (|A| - 1)w \quad (2.10)$$

which verifies the first part of the theorem.

If $x_c \in C \setminus A$ then $f(A)$ does not include x_c . It has been shown in the proof of Theorem 1 that there exist at least $w - \lambda T$ positions that do not overlap with any of the codewords $x_i \in A$, i.e. $z_j - x_{cj} < 0$ for some j . Let S denote the set of positions of nonzero elements in x_c which overlap with the other $x_i \in A$ and $\bar{S}$ denote the set of positions of the nonzero elements x_{cj} which do not overlap with any of $x_i \in A$. Because $(w - \lambda T) > 0$ and $|A| \leq T$, we have

$$\begin{aligned} Wt(f(A) - x_c) &= \sum_{j \in S} |z_j - x_{cj}| + \sum_{j \in \bar{S}} |z_j - x_{cj}| \\ &\geq (|A|w - \lambda|A|) + (w - \lambda|A|) \\ &= (|A| - 1)w + 2(w - \lambda|A|) \\ &> (|A| - 1)w, \end{aligned} \quad (2.11)$$

which concludes the theorem.

Theorem 3 *Let C be a binary disjunctive code $D(n, T, N)$ constructed from $CW(n, w, \lambda, N)$, then for each subset $A \subseteq C$ of size $|A| \leq T$ the receiver is able to distinguish how many codewords have been sent at transmitters if the weight of the error pattern $e = (e_1, e_2, \dots, e_n)$ satisfies $Wt(e) = \sum_{j=1}^n |e_j| < w/2$.*

Proof: From Theorem 1, if $|A| = m \leq T$, $Wt(f(A)) = mw$; if $|A| = m+1 \leq T$, then $Wt(f(A)) = (m+1)w$. Let $S = Wt(\hat{f}(A)) = Wt(f(A) + e)$, then

$$Wt(f(A)) - Wt(e) \leq S \leq Wt(f(A)) + Wt(e), \quad (2.12)$$

or

$$|A|w - Wt(e) \leq S \leq |A|w + Wt(e). \quad (2.13)$$

Now if $Wt(e) < w/2$, the number of codewords transmitted can be obtained by

$$|A| = \begin{cases} \lfloor \frac{S}{w} \rfloor & (S - \lfloor \frac{S}{w} \rfloor w) < \frac{w}{2} \\ \lfloor \frac{S}{w} \rfloor + 1 & (S - \lfloor \frac{S}{w} \rfloor w) > \frac{w}{2} \end{cases}, \quad (2.14)$$

where $\lfloor x \rfloor$ denotes the highest integer less than or equal to x , thus proving the theorem.

Theorem 4 Let C be a binary disjunctive code $D(n, T, N)$ constructed from $CW(n, w, \lambda, N)$, then for each subset $A \subseteq C$ of size $|A| \leq T$ the receiver is able to correct any error pattern $e = (e_1, e_2, \dots, e_n)$ whose weight satisfies $Wt(e) = \sum_{j=1}^n |e_j| < w - \lambda|A|$.

Proof: Suppose the received vector is $\hat{f}(A) = f(A) + e$. For each subset $A \subseteq C$ of size $|A| \leq T$, if the channel is noiseless, then $Wt(\hat{f}(A) - x_i) = (|A| - 1)w$, $x_i \in A$. If the channel is noisy and the weight of the error pattern satisfies $Wt(e) < w - \lambda|A|$; letting $x_i \in A$, then

$$\begin{aligned} Wt(\hat{f}(A) - x_i) &= Wt(f(A) + e - x_i) \\ &= \sum_{j \in S} |z_j + e_j - x_{ij}| + \sum_{j \in \bar{S}} |z_j + e_j - x_{ij}| \quad (2.15) \\ &\leq (|A|w - w) + Wt(e) \\ &< (|A| - 1)w + (w - \lambda|A|) \end{aligned}$$

But for all other codewords $x_c \in C \setminus A$ and $Wt(e) < w - \lambda|A|$, we have

$$\begin{aligned} Wt(\hat{f}(A) - x_c) &= Wt(f(A) + e - x_c) \\ &= \sum_{j \in S} |z_j + e_j - x_{cj}| + \sum_{j \in \bar{S}} |z_j + e_j - x_{cj}| \quad (2.16) \\ &\geq (|A|w - \lambda|A|) + (w - \lambda|A|) - Wt(e) \\ &= (|A| - 1)w + 2(w - \lambda|A|) - Wt(e) \\ &> (|A| - 1)w + (w - \lambda|A|). \end{aligned}$$

Therefore the correct codewords $x_i \in C$ can be distinguished from the codewords $x_c \in C \setminus A$.

It should be noted that the error-correcting ability of the disjunctive code constructed from a constant weight code is not constant, but is a function of size $|A|$. It can be seen from the condition, $Wt(e) < w - \lambda|A|$, that the maximum and minimum error weights that can be corrected are respectively $Wt_{max}(e) = w - \lambda = d_H/2$ (when $|A| = 1$) and $Wt_{min}(e) = w - \lambda|T|$ (when $|A| = T$), where $d_H = 2w - 2\lambda$ is the minimum Hamming distance of the constant weight code. It is clear that in order to use Theorem 4, the size of A should be known in advance. Although the $|A|$ can be obtained from Eqn. 2.14, Theorem 3 can however only guarantee the correctness of the $|A|$ computed by Eqn. 2.14 if $Wt(e) = \sum_{j=1}^n |e_j| < w/2$. This analysis directly leads to the following Theorem 5:

Theorem 5 *Let C be a binary disjunctive code $D(n, T, N)$ constructed from $CW(n, w, \lambda, N)$, then for each subset $A \subseteq C$ of size $|A| \leq T$ the receiver is able to distinguish how many codewords have been sent at the transmitter and, at the same time, can recover every codeword if the weight of the error pattern e satisfies*

$$Wt(e) = \sum_{j=1}^n |e_j| < \min \left\{ w - \lambda|A|, \frac{w}{2} \right\}. \quad (2.17)$$

An effective method for constructing good constant weight codes (and thereby disjunctive codes) is to use a concatenated code in which the inner code is a constant weight code. The KS code, which was first defined by W H Kautz and R S Singleton (Kautz & Singleton, 1964), is based on a maximum distance separable (MDS) outer code (e.g. Reed-Solomon code) and an orthogonal weight-one inner code $CW(q, 1, 0, q)$. Let C be a RS code over $GF(q)$ with length w and minimum distance d . The dimension will be $k = w - d + 1$. We now represent the inner $CW(q, 1, 0, q)$ code by mapping each symbol in $GF(q)$ to a binary vector of length q and weight one:

$$\begin{array}{ll} 0 & \longrightarrow 1000 \dots 0, \\ 1 & \longrightarrow 0100 \dots 0, \\ \cdot & \cdot \cdot \\ (q-1) & \longrightarrow 0000 \dots 1. \end{array}$$

We therefore obtain a constant weight code $CW(qw, w, \lambda, q^{\lambda+1})$ which corresponds to a disjunctive code $D(wq, \lceil \frac{w}{\lambda} \rceil - 1, q^{\lambda+1})$.

Example: Let C be the $RS(n, k, d) = RS(6, 2, 5)$ with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 6 & 5 & 4 & 3 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}. \quad (2.18)$$

With this RS code, a disjunctive code with parameters

$$D \left(6 \times 7, \left\lceil \frac{6}{6-5} \right\rceil - 1, 7^{6-5+1} \right) = D(42, 5, 49) \quad (2.19)$$

and Hamming distance $d_H = 2w - 2\lambda = 2 \times 6 - 2 \times 1 = 10$ can be constructed.

Any RS codeword $x_i = (x_{i1}, x_{i2}, \dots, x_{i6})$, $x_{ij} \in GF(7)$ can be calculated by multiplying the generator matrix by an information vector $m = (m_1, m_2)$, $m_j \in GF(7)$. For example, if $m \in \{(1, 2), (2, 2), (3, 2), (6, 6)\}$, then the codeword set A , $|A| \leq 5$, and the superposition of A , will be as follows:

$$\begin{aligned} A &= \{mG \mid m \in \{(1, 2), (2, 2), (3, 2), (6, 6)\}\} \\ &= \{(123456), (222222), (321065), (666666)\} \\ &= \left\{ \begin{pmatrix} 000000 \\ 100000 \\ 010000 \\ 001000 \\ 000100 \\ 000010 \\ 000001 \end{pmatrix}, \begin{pmatrix} 000000 \\ 000000 \\ 111111 \\ 000000 \\ 000000 \\ 000000 \\ 000000 \end{pmatrix}, \begin{pmatrix} 000100 \\ 001000 \\ 010000 \\ 100000 \\ 000000 \\ 000001 \\ 000010 \end{pmatrix}, \begin{pmatrix} 000000 \\ 000000 \\ 000000 \\ 000000 \\ 000000 \\ 000000 \\ 111111 \end{pmatrix} \right\}, \quad (2.20) \end{aligned}$$

$$z = f(A) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 3 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 2 \end{pmatrix}. \quad (2.21)$$

2.4 Decoding Algorithms for the Noiseless N-BAC

The aim of the decoder of a superimposed code is to reproduce the transmitted codewords of all the active users using the received vector. For the noiseless

N-BAC, the task is just to map from the received superimposed T -ary vector $f(A)$ formed by the noiseless N-BAC into a set of codewords $\hat{A}$ from the given superimposed code C . That is

$$f(A) \longrightarrow \hat{A}. \quad (2.22)$$

Decoding Algorithm 1

According to Theorem 2, if the binary code C is a binary disjunctive code $D(n, T, N)$ constructed from $CW(n, w, \lambda, N)$, then for each subset $A \subseteq C$ of size $|A| \leq T$, $Wt(f(A) - x_i) = (|A| - 1)w$ if and only if $x_i \in A$. Therefore an obvious way of decoding is an exhaustive search, i.e., for all codewords in $x_i \in C$, compute the $Wt(f(A) - x_i)$, and then output all the codewords which satisfy $Wt(f(A) - x_i) = (|A| - 1)w$. That is,

$$\hat{A} = \{x_i \in C \mid Wt(f(A) - x_i) = (|A| - 1)w\}, \quad (2.23)$$

where $|A|$ is obtained from Eqn. 2.14.

Decoding Algorithm 2

The exhaustive search decoder has a decoding complexity which is independent of the transmitted set of codewords and is equal to N . If we make use of the structure of the specific disjunctive code, the number of codewords x_i used in the test $Wt(f(A) - x_i) = (|A| - 1)w$, can be reduced greatly, thereby reducing decoding complexity. In the case of the KS code, it is simple to find the transmitted elements (symbols) from $GF(q)$ in the received vector. In the above example, from the first and second columns of the received superposition vector $z = f(A)$, it can readily be seen that the first and second positions of the transmitted RS codewords must be in the set $\{1, 2, 3, 6\}$ and $\{2, 6\}$ respectively. This means that the possible information vectors $m = (m_1, m_2)$ of the corresponding codewords are:

$$m \in \{(1, 2), (1, 6), (2, 2), (2, 6), (3, 2), (3, 6), (6, 2), (6, 6)\}. \quad (2.24)$$

Obviously, if we use the corresponding codeword set $\dot{C}$ as a candidate set in the decoding process, i.e.

$$\hat{A} = \{x_i \in \dot{C} \mid Wt(f(A) - x_i) = (|A| - 1)w\}, \quad (2.25)$$

the results will be the same as with Algorithm 1. However, because $|\dot{C}| \ll |C|$, the decoding complexity has been reduced greatly. For the example given above, $|C| = 49$, but $|\dot{C}| = 8$.

Based on the fact that the size of $|A|$ is constant for a given received vector $f(A)$ and can be calculated beforehand, the decoding complexity can be further reduced by counting the number of the decoded codewords. If the number of decoded codewords is equal to $|A|$, then there is no need to try the rest of the candidate codewords.

Therefore, the simplified algorithm can be summarized as follows:

1. Compute the size of $|A|$ using Eqn. 2.14.
2. Generate a relatively small candidate codeword set $\dot{C}$ by making use of the specific code structure.
3. Select a candidate codeword $x_i \in \dot{C}$ and test whether it satisfies the following condition:

$$Wt(f(A) - x_i) = (|A| - 1)w. \quad (2.26)$$

If it does, increase the decoded codeword counter by one.

4. If the counter is equal to $|A|$ then exit; otherwise go to step 3.

2.5 Decoding Algorithms for the Noisy Case

As is shown in Fig. 2.2, the received vector in the noisy case is given by $\hat{f}(A) = f(A) + e$. Based on Theorem 5, if C is a binary disjunctive code $D(n, T, N)$ constructed from $CW(n, w, \lambda, N)$ and the weight of the error pattern e satisfies $Wt(e) = \sum_{j=1}^n |e_j| < w_{err} = \min \{w - \lambda|A|, \frac{w}{2}\}$, $|A| \leq T$, then the codewords transmitted can be correctly recovered. Therefore, we have the following decoding algorithm:

Decoding Algorithm 3

$$\hat{A} = \left\{ x_i \in C \mid Wt(\hat{f}(A) - x_i) < (|A| - 1)w + w_{err} \right\}. \quad (2.27)$$

In order to reduce the decoding complexity, the same idea can be employed as in Algorithm 2; that is, to produce a relatively small set of candidate codewords

$\tilde{C}$ by making use of the structure of the specific disjunctive code and the known information $|A|$. For the KS code, however, the size of the candidate set $\tilde{C}$ and the process of producing candidate codewords will be slightly different, which will not be addressed here for simplicity. After generating the candidate set $\tilde{C}$, the decoding process is similar, i.e.:

Decoding Algorithm 4

$$\hat{A} = \left\{ x_i \in \tilde{C} \mid Wt \left(\hat{f}(A) - x_i \right) < (|A| - 1)w + w_{err} \right\}, \quad (2.28)$$

where the decoding process should be stopped if the decoded codeword counter is equal to $|A|$.

Finally it should be stressed that the error pattern e is not necessarily an integer vector; it can also be any real value vector as long as $Wt(e) < \min \left\{ w - \lambda|A|, \frac{w}{2} \right\}$. In other words, the proposed algorithms 3-4 are also soft-decision decoding algorithms which will give better error performance than hard-decision decoding.

2.6 Concluding Remarks

We have investigated in this chapter superimposed codes for N-BAC. The superposition mechanism used here is normal addition. The N-BAC system consists of a set of N users sharing a multiaccess binary adder channel. It has been proved that if the number of active users $|A| \leq T \ll N$, we can decompose the received word into its component codewords for the noiseless N-BAC. In the noisy case, the number of active users and the codewords can also be correctly recovered provided that the weight of the error pattern satisfies $Wt(e) = \sum_{j=1}^n |e_j| < \min \left\{ w - \lambda|A|, \frac{w}{2} \right\}$. The correctness of the decoding algorithms proposed has been tested by computer simulation.

In this study, each user is given only one codeword, which is simply used to identify the active users. However, if each user has available a set of codewords, information can be transmitted over the channel.

Chapter 3

Codes for the Multiaccess Q-ary Adder Channel

3.1 Introduction

In the previous chapter, it was mentioned that one central technical problem in multiaccess communication is how to share the channel between the busy users, or how to assign codes to a set of N users where it is expected that no more than $T \ll N$ of the users will be transmitting at any one time. However, in some practical situations, it is possible that all the N users or less are active simultaneously. It is therefore also required to construct a set of N codes, any $T \leq N$ of which can co-exist with each other for transmissions over a given channel.

By assuming that all N users are always simultaneously active (i.e. $N = T$), Chang and other researchers have constructed various codes for the T-user noiseless binary input adder MAC with the goal of achieving channel capacity asymptotically as T goes to infinity (Chang & Weldon Jr., 1979; Ferguson, 1982; Chang, 1984; Wilson, 1988). It is clear that the assumption is not reasonable. In a practical multiaccess communication system, the accessing time and transmitting duration of any user typically take random values. Hence, at any time, the number of active users in the system is variable; in this case, most of previously defined uniquely decodable CCMA codes are not absolutely decodable. For example, in a 3-user adder channel CCMA scheme proposed by Chang and Weldon (Chang & Weldon Jr., 1979), the codes used by the 3 users are $C_1 = \{00, 11\}$, $C_2 = \{00, 10\}$, $C_3 = \{01, 10\}$ respectively. It can be seen that each of the eight possible composite codewords – resulting from symbol-wise addition on the channel – is unique, and can therefore be unambiguously decoded into its constituent codewords, provided that all the three

users are simultaneously active. Let us now consider the 2-active user cases: if users 1 and 2 are active, the possible composite codewords are $\{00, 10, 11, 21\}$; if users 1 and 3 are active, the composite codewords are $\{01, 10, 21, 12\}$. If "10" and "21", which are common elements in these two composite codeword sets, are received, it would be impossible for the receiver to identify both the active users unambiguously (Ni & Honary, 1993).

Mathys has introduced another interesting class of codes for the synchronous noiseless discrete-time real adder channel (with gains and offset), without feedback, with N real or binary inputs (Mathys, 1990). Mathys' codes are uniquely decodable and have a sum rate that approaches 1 if the decoder is informed of which T or less users are active. The sum rate will be reduced to a value of at most $1/2$ if the decoder has to identify the subset of active users.

In this chapter, we will study a CCMA coding scheme with N users; any T ($T \leq N$) users can be simultaneously active at any time. The channel model used is the N -user noiseless Q -ary Adder Channel (N -QAC) which is similar to that of Fig. 2.2 except that the channel output symbol value is the arithmetic sum of the Q -ary input symbol values, in the absence of noise.

The CCMA code proposed here is a cyclic code over the integer ring Z_Q . It is shown that the class of codes can be identified uniquely. The maximum achievable sum rate is 1 when all users are active simultaneously. A remarkable advantage of this coding scheme is that it can be decoded by a very low complexity decoding algorithm (Fan *et al.*, 1994c).

3.2 Factorization of $x^n - 1$ over the Integer Ring Z_Q

In this section a brief summary of the theory needed to factor $x^n - 1$ and subsequently to construct cyclic codes over the integer ring Z_Q is given, following Shankar (Shankar, 1979).

Let Q be an arbitrary integer, with prime factorization $Q = \prod_{i=1}^l p_i^{k_i}$, where the p_i are distinct primes and the k_i are non-negative integers. Let $Z_{p_i^{k_i}}[y]$ denote the ring of polynomials in the variable y over $Z_{p_i^{k_i}}$ and let $\Phi_i(y)$ be a monic p_i -ary polynomial of degree r , irreducible over $\text{GF}(p_i)$, $i = 1, 2, \dots, l$. Let $R_i = GR(p_i^{k_i}, r) = Z_{p_i^{k_i}}[y] / \Phi_i(y)$ denote the *Galois ring*, i.e., the set of residue classes of polynomials in y over $Z_{p_i^{k_i}}$, modulo the polynomial $\Phi_i(y)$.

Suppose that $f(x) = \sum_{i=1}^n a_i x^i$ and let

$$R_Q(f(x)) = \sum_{i=1}^n R_Q(a_i) x^i, \quad (3.1)$$

where $R_Q(a_i)$ is the non-negative remainder when the integer a_i is divided by the integer Q . For $i = 1, 2, \dots, l$, let m_i be the smallest integer such that

$$R_{p_i, k_i}(m_i) = 1 \quad \text{and} \quad R_{p_j, k_j}(m_i) = 0, \quad \text{for } j \neq i, \quad 1 \leq j \leq l. \quad (3.2)$$

Then the polynomial

$$\Phi(y) = R_Q(m_1 \Phi_1(y) + m_2 \Phi_2(y) + \dots + m_l \Phi_l(y)) \quad (3.3)$$

is monic and irreducible over Z_Q and over $GF(p_i)$, $i = 1, 2, \dots, l$. Let $S(Q, r) = Z_Q[y]/\Phi(y)$. Now let R_i^* and S^* denote the group of units of R_i and $S(Q, r)$, respectively, let K_i denote $GF(p_i^r)$ and finally let K_i^* denote the multiplicative group of $GF(p_i^r)$. Let n be a divisor of the $\text{GCD}((p_1^r - 1), (p_2^r - 1), \dots, (p_l^r - 1))$ and let $H_{f,n}$ denote the cyclic subgroup of order n of S^* , generated by f , f is a generator of the cyclic subgroup. It follows that $H_{f,n}$ contains all the roots of $x^n - 1$ over S^* . Shankar therefore proved the following result (Shankar, 1979):

Theorem 6 *The polynomial $x^n - 1$ can be factored over S^* as*

$$x^n - 1 = (x - f)(x - f^2) \dots (x - f^n) \quad (3.4)$$

if and only if $\bar{\beta}_i = R_{p_i}(f)$ has order n in K_i^* , where n is coprime to p_i , i.e. $(n, p_i) = 1$, $i = 1, 2, \dots, l$.

Summarizing: the following are the main steps in the factorization of $x^n - 1$ over Z_Q .

a) Choose $\Phi_i(y)$ to be a monic p_i -ary polynomial of degree r , irreducible over $GF(p_i)$. Find m_i , $i = 1, 2, \dots, l$ as indicated above. Then

$$\Phi(y) = R_Q(m_1 \Phi_1(y) + m_2 \Phi_2(y) + \dots + m_l \Phi_l(y))$$

is monic and irreducible over Z_Q .

b) Let β_i be an element of order n in R_i , formed as $Z_{p_i, k_i}[y]/\Phi_i(y)$, $i = 1, 2, \dots, l$. Then

$$f = R_Q(m_1\beta_1 + m_2\beta_2 + \dots + m_l\beta_l) \quad (3.5)$$

generates the cyclic subgroup $H_{f,n}$ of the unit group of $Z_Q[y]/\Phi(y)$.

c) The factors of $x^n - 1$, irreducible over Z_Q , are defined by the cyclotomic cosets formed with the roots f^i , $1 \leq i \leq l$, of $x^n - 1$.

Table 3.1 gives some examples of factorization of $x^n - 1$ over Z_Q .

Table 3.1: Examples of Factorization of $x^n - 1$ over Z_Q

Factorization of $x^n - 1$	Z_Q
$x^6 - 1 = (x + 1)^2(x^2 + x + 1)^2$	Z_2
$x^6 - 1 = (x + 1)^3(x + 2)^3$	Z_3
$x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$	Z_2
$x^7 - 1 = (x - 1)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3)$	Z_4
$x^8 - 1 = (x + 1)(x + 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)$	Z_3
$x^8 - 1 = (x + 1)(x + 8)(x^2 + 1)(x^2 + 4x + 8)(x^2 + 5x + 8)$	Z_9
$x^{12} - 1 = (x + 1)(x + 2)(x + 3)(x + 4)(x^2 + x + 1)(x^2 + 2x + 4)$ $(x^2 + 3x + 4)(x^2 + 4x + 1)$	Z_5
$x^{15} - 1 = (x + 3)(x^5 + 3x^2 + 2x + 3)(x^5 + x^4 + 3x^3 + x + 3)$ $(x^5 + x^4 + 3x^3 + x^2 + 2x + 3)(x^5 + 2x^4 + x^3 + 3)$ $(x^5 + 2x^4 + 3x^3 + x^2 + 3x + 3)(x^5 + 3x^4 + x^2 + 3x + 3)$	Z_4
$x^{26} - 1 = (x + 1)(x + 2)(x^3 + 2x + 1)(x^3 + 2x + 2)(x^3 + x^2 + 2)$ $(x^3 + x^2 + x + 2)(x^3 + x^2 + 2x + 1)(x^3 + 2x^2 + 1)$ $(x^3 + 2x^2 + x + 1)(x^3 + 2x^2 + 2x + 2)$	Z_3

3.3 Cyclic Codes over Z_Q for the N-QAC Channel

In order to design the required codes and the corresponding decoding algorithm, we need to use the following Euclidean theorem and the Chinese Remainder theorem (Berlekamp, 1968).

Theorem 7 (Euclidean Theorem) Given any polynomials $a(x)$ and $b(x)$, there exist polynomials $A(x)$ and $B(x)$ such that

$$a(x)A(x) + b(x)B(x) = (a(x), b(x)) \quad (3.6)$$

where $(a(x), b(x))$ is the monic common factor of $a(x)$ and $b(x)$ with greatest degree. If $(a(x), b(x)) = 1$, then $a(x)$ and $b(x)$ have no factors in common.

Theorem 8 (Chinese Remainder Theorem) Given irreducible polynomials $g_1(x), g_2(x), \dots, g_T(x)$ and arbitrary polynomials $m_1(x), m_2(x), \dots, m_T(x)$, then the simultaneous congruences, $h(x) \equiv m_i(x) \pmod{g_i^{k_i}(x)}$, have a unique solution for $h(x) \pmod{\prod_{i=1}^T g_i^{k_i}(x)}$.

A blocklength n cyclic code over Z_Q is an ideal in the ring of polynomials with coefficients in Z_Q , reduced modulo $x^n - 1$, and is generated by a monic polynomial $g(x)$ which is a factor of $x^n - 1$. Let $g_1(x), g_2(x), \dots, g_N(x)$ be a set of N irreducible polynomials which are factors of $x^n - 1$ over Z_Q , i.e.,

$$x^n - 1 = \prod_{i=1}^N g_i^{k_i}(x), \quad (3.7)$$

where $\sum_{i=1}^N \deg [g_i^{k_i}(x)] = n$ and the k_i , $1 \leq i \leq N$, are positive integers. Since $h_i(x) = (x^n - 1)/g_i^{k_i}(x)$ has no factors in common with $g_i^{k_i}(x)$, the Euclidean algorithm can be used to find a polynomial $\beta_i(x)$ such that $\beta_i(x)h_i(x) \equiv 1 \pmod{g_i^{k_i}(x)}$, $1 \leq i \leq N$.

Let $m_i(x)$ denote the message polynomial for user i . Let $h_i(x)$ be the generator polynomial of the cyclic code allocated to user i . The codewords of user i are generated in the usual manner as an error-correcting code (Berlekamp, 1968; MacWilliams & Sloane, 1977). However, before being transmitted, each codeword is multiplied by $\beta_i(x)$ and reduced modulo $x^n - 1$. As is shown in the next section, the operations of encoding and multiplying by $\beta_i(x)$ can be done simultaneously.

We now prove the unique decodability of the codes proposed.

Theorem 9 Let $c_i(x) = m_i(x)h_i(x)\beta_i(x)$ be a Q -ary cyclic code with message polynomial $m_i(x)$ and generator polynomial $h_i(x)$. Then the T -tuple $(c_1(x), c_2(x), \dots, c_T(x))$, $1 \leq T \leq N$, is uniquely decodable over the synchronous noiseless T -user Q -ary adder channel and has a maximum sum rate of 1 achieved when $T = N$.

Proof: Consider the following sum $r(x)$, where addition is defined over the additive group of Z_Q

$$r(x) = \sum_{i=1}^T m_i(x)h_i(x)\beta_i(x), \quad 1 \leq T \leq N. \quad (3.8)$$

By the Chinese Remainder theorem for polynomials, it can be shown that the sum $r(x)$ is uniquely determined by $m_1(x), m_2(x), \dots, m_T(x)$. In fact, since $\beta_j(x)h_j(x)$ is a multiple of $g_i^{k_i}(x)$ if $j \neq i$, and $\beta_i(x)h_i(x) \equiv 1 \pmod{g_i^{k_i}(x)}$, it follows that $r(x) \equiv m_i(x) \pmod{g_i^{k_i}(x)}$ for all i . If $r'(x)$ also satisfies $r'(x) \equiv m_i(x) \pmod{g_i^{k_i}(x)}$ for all i , then $r'(x) - r(x)$ must be divisible by $g_i^{k_i}(x)$, $1 \leq i \leq T$; since both $r(x)$ and $r'(x)$ are polynomials of degree less than n , it follows that $r'(x) = r(x) \pmod{x^n - 1}$. Hence the sum $r(x)$ is uniquely determined by the arbitrary polynomials $m_i(x)$, $1 \leq i \leq T$, if $\deg[m_i(x)] < \deg[g_i^{k_i}(x)]$, i.e., $m_i(x) = r(x) \pmod{g_i^{k_i}(x)}$, $1 \leq i \leq T$. Further, when considered as a real sum of polynomials, $r(x)$ is also uniquely determined by $m_1(x), m_2(x), \dots, m_T(x)$.

Since each code $c_i(x)$ has $\deg[g_i^{k_i}(x)]$ information symbols and $\max \sum_i \deg[g_i^{k_i}(x)] = n$, it follows that the maximum sum rate is 1 when all users ($T = N$) are active.

3.4 Encoding and Decoding Algorithms

Based on the above analysis, a class of CCMA codes for the N-QAC over the integer ring Z_Q can be constructed. The encoding and decoding algorithms are as follows:

Encoding Algorithm

1. Given an integer ring Z_Q , choose a code length n as described in Section 3.2 and factor $x^n - 1$ into irreducible polynomials over Z_Q , $x^n - 1 = \prod_{i=1}^N g_i^{k_i}(x)$.
2. Assign each user a cyclic code with the generator polynomial $h_i(x) = (x^n - 1)/g_i^{k_i}(x)$. Compute the polynomials $\beta_i(x)$ which satisfy, $\beta_i(x)h_i(x) \equiv 1 \pmod{g_i^{k_i}(x)}$, $1 \leq i \leq N$.
3. For a given message polynomial $m_i(x) \neq 0$, the transmitted codewords $c_i(x)$ of each user are generated by computing $c_i(x) = h_i(x)\beta_i(x)m_i(x) \pmod{x^n - 1}$. In order to avoid ambiguity between zero messages ($m_i(x) = 0$) and the case where user i is not active, the message set is restricted to those $m_i(x) \neq 0$ in the encoding algorithm.

Decoding Algorithm

The received n -tuples are polynomials, denoted by $r'(x)$, which result from the componentwise real addition of the codewords of the active users. The first step in decoding is to reduce the coefficients of $r'(x)$ modulo Q . The result of this step is the polynomial $r(x)$. Once the polynomial $r(x) = \sum_{i=1}^T c_i(x)$ is obtained, the decoding algorithm is very simple and is given by the equation

$$\hat{m}_i(x) = r(x) \bmod g_i^{k_i}(x), 1 \leq i \leq N. \quad (3.9)$$

It should be noted that the above analysis and encoding/decoding algorithms are valid if $x^n - 1$ has repeated irreducible factors. Although the maximum number of users will be reduced if there are some repeated irreducible factors in $x^n - 1$, the maximum achievable sum rate remains the same.

Example 1: Construct a 3-user QAC system over Z_4 with code length $n = 7$. Employing the technique described above, the following factorization results:

$$x^7 - 1 = \prod_{i=1}^3 g_i(x) = (x - 1)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3). \quad (3.10)$$

Let $g_1(x) = x - 1$, $g_2(x) = x^3 + 2x^2 + x + 3$ and $g_3(x) = x^3 + 3x^2 + 2x + 3$. Using the Euclidean algorithm, the following are obtained:

$$h_1(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \quad \beta_1(x) = 3; \quad (3.11)$$

$$h_2(x) = x^4 + x^2 + x + 3, \quad \beta_2(x) = 1; \quad (3.12)$$

$$h_3(x) = x^4 + 3x^3 + 3x^2 + 3, \quad \beta_3(x) = x^3 + 2x^2 + 2. \quad (3.13)$$

Suppose the three users are all active, $m_1(x) = 3$, $m_2(x) = 2x + 3$, $m_3(x) = x$, then the transmitted codewords are:

$$\begin{aligned} c_1(x) &= m_1(x)h_1(x)\beta_1(x) \\ &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \bmod(x^7 - 1), \end{aligned} \quad (3.14)$$

$$\begin{aligned} c_2(x) &= m_2(x)h_2(x)\beta_2(x) \\ &= 2x^5 + 3x^4 + 2x^3 + x^2 + x + 1 \bmod(x^7 - 1), \end{aligned} \quad (3.15)$$

$$\begin{aligned} c_3(x) &= m_3(x)h_3(x)\beta_3(x) \\ &= x^6 + x^4 + 3x + 1 \bmod(x^7 - 1) \end{aligned} \quad (3.16)$$

At the receiver, the received sum codeword is

$$r'(x) = 2x^6 + 3x^5 + 5x^4 + 3x^3 + 2x^2 + 5x + 3 \quad (3.17)$$

which, after reduction modulo 4 at receiver, becomes

$$r(x) = \sum_{i=1}^3 c_i(x) = 2x^6 + 3x^5 + x^4 + 3x^3 + 2x^2 + x + 3. \quad (3.18)$$

The messages can be easily restored as: $\hat{m}_1(x) = 3 = r(x) \bmod g_1(x)$, $\hat{m}_2(x) = 2x + 3 = r(x) \bmod g_2(x)$, $\hat{m}_3(x) = x = r(x) \bmod g_3(x)$.

If only users 2 and 3 are active ($m_1(x) = 0$), then by the same process we will have $\hat{m}_1(x) = 0$.

Example 2: Let us consider another example with repeated irreducible factors in $x^n - 1$. Construct a 2-user QAC system over Z_2 with code length $n = 6$. From Table 3.1, we have $x^6 - 1 = (x + 1)^2(1 + x + x^2)^2$ over Z_2 . Let $g_1(x) = (1 + x)$, $g_2(x) = (1 + x + x^2)$, then

$$h_1(x) = (x^2 + x + 1)^2, \quad \beta_1(x) = 1; \quad (3.19)$$

$$h_2(x) = (x + 1)^2, \quad \beta_2(x) = x^2. \quad (3.20)$$

Suppose $m_1(x) = x$, $m_2(x) = x^3 + x + 1$, then the transmitted codewords are:

$$c_1(x) = m_1(x)h_1(x)\beta_1(x) = x^5 + x^3 + x \bmod(x^6 - 1), \quad (3.21)$$

$$c_2(x) = m_2(x)h_2(x)\beta_2(x) = x^4 + x^3 + x^2 + x \bmod(x^6 - 1). \quad (3.22)$$

The received sum codeword is $r'(x) = \sum_{i=1}^2 c_i(x) = x^5 + x^4 + 2x^3 + x^2 + 2x$ which, after reduction modulo 2 at receiver, becomes $r(x) = x^5 + x^4 + x^2$. The decoded messages are: $\hat{m}_1(x) = x = r(x) \bmod g_1^2(x)$, $\hat{m}_2(x) = x^3 + x + 1 = r(x) \bmod g_2^2(x)$.

3.5 Concluding Remarks

Uniquely decodable cyclic codes over the integer ring Z_Q for the N-QAC have been discussed in this chapter. The codes are attractive in practice because

the decoder can correctly identify any number of active users ($0 \leq T \leq N$, T is unknown in advance to the decoder), and correctly recover their respective messages. A very low complexity decoding algorithm is given and it is shown that the maximum achievable sum rate is 1.

Chapter 4

Codes for Synchronous SSMA Systems

4.1 Introduction

The SSMA technique is one of the important aspects of spread spectrum communications, as stated in Chapter 1. This chapter deals with the design of orthogonal complementary sets of sequences for use in synchronous SSMA systems. After the definition of the concepts of complementarity, uncorrelatedness and orthogonality, recursive formulas for constructing orthogonal complementary sets are proposed; methods for synthesizing new orthogonal complementary sets from known ones with the same dimensions are discussed. Then conjectures relating to maximally orthogonal complementary sets are given. Finally an application of orthogonal complementary sets to a synchronous SSMA system is described.

Complementary sequences (CS) are basically characterized by the property that their autocorrelation vector sum is zero everywhere, except at zero shift. Such sequences were originally considered by Golay in connection with his study of infrared spectrometry (Golay, 1961). Following Golay's work, the mathematical properties of CS and their relation to other types of codes, computer search for expected CSs, the existence problem for certain lengths, and the applications of CS were further investigated by various researchers (Welch, 1960; Turyn, 1963; Kruskal, 1961; Taki *et al.*, 1969; Griffin, 1977; Andres & Stanton, 1977; Schweitzer, 1971; Turyn, 1974; Eliahou *et al.*, 1990). For their research into acoustic surface-wave devices, Tseng and Liu studied generalized binary complementary sets of sequences with uncorrelated properties (Tseng & Liu, 1972). Another type of generalized complex-valued complementary code (or multiphase/polyphase code) was considered by Frank (Frank, 1980) and other

workers (Sivaswamy, 1978; Popovic, 1991b); this has found applications in the areas of radar and Loran-C etc.. Darnell and Budisin extended consideration of binary complementary sets to multilevel complementary sets which have further interesting properties, distinct from those of binary sets (Darnell & Kemp, 1989; Budisin, 1990a; Budisin, 1990b).

In more recent years, complementary pairs of sequences with orthogonal properties, as defined later in this chapter, have been studied for application in spread spectrum systems and in code division multiple access (CDMA) communications (Gutleber, 1982; Wen & Guangguo, 1987; Fan *et al.*, 1993a; Fan *et al.*, 1993b; Fan *et al.*, 1994a). The properties of orthogonal complementary pairs of sequences have been considered in detail (Fan *et al.*, 1993b). In this chapter, the properties of orthogonal binary complementary sets of sequences (OCSS) are studied (Fan *et al.*, 1994a).

4.2 Complementarity, Uncorrelatedness and Orthogonality

Definition 7 If $\{S_i, i = 1, 2, \dots, P\}$ is a set of sequences, each of length M , where $S_i = (s_{i,1}, s_{i,2}, \dots, s_{i,M})$, $s_{i,l} \in \{+1, -1\}$, then the aperiodic autocorrelation function of S_i is defined as

$$C_{S_i, S_i}(k) = \sum_{l=1}^{M-k} s_{i,l} s_{i,l+k}, \quad i = 1, 2, \dots, P. \quad (4.1)$$

Definition 8 A set of sequences $\{S_i, i = 1, 2, \dots, P\}$ each of length M is said to be a complementary set if and only if the P autocorrelation functions sum to zero at every shift, except the zero shift; that is

$$\sum_{i=1}^P C_{S_i, S_i}(k) = 0, \quad k \neq 0 \quad (4.2)$$

Definition 9 Two complementary sets $\{S_i, i = 1, 2, \dots, P\}$, $\{R_i, i = 1, 2, \dots, P\}$, each with equal numbers of sequences P and equal sequence lengths M , are termed uncorrelated complementary sets of sequences (UCSS) if the aperiodic crosscorrelation values for corresponding sequences in each set sum to

zero at all corresponding time shifts; that is

$$\sum_{i=1}^P C_{S_i, R_i}(k) = 0, \quad \forall k. \quad (4.3)$$

Definition 10 A class of mutually uncorrelated complementary sets is said to comprise maximally uncorrelated complementary sets of sequences (MUCSS) if the number of mutually uncorrelated complementary sets N is maximum for a given number of sequences P and length M .

Definition 11 Two complementary sets $\{S_i, i = 1, 2, \dots, P\}$, $\{R_i, i = 1, 2, \dots, P\}$, each with equal number of sequences P and equal sequence lengths M , are defined as orthogonal complementary sets of sequences (OCSS) if the aperiodic crosscorrelation values for corresponding sequences in each set sum to zero at in-phase time shifts; that is

$$\sum_{i=1}^P C_{S_i, R_i}(0) = 0. \quad (4.4)$$

Definition 12 A class of mutually orthogonal complementary sets is said to comprise maximally orthogonal complementary sets of sequences (MOCSS) if the number of mutually orthogonal complementary sets N is maximum for a given number of sequences P and length M .

It is obvious that the number of sets in a MOCSS will be larger than the number in the MUCSS with the same P and M . In fact, Schweitzer has proved that the maximum number of sets N in any MUCSS with parameters P and M is equal to P (Schweitzer, 1971). Taki and his colleagues proved the same result for Golay pairs ($P=2$) (Taki *et al.*, 1969). For orthogonal complementary pairs of sequences (OCPS, or orthogonal Golay pairs), it has been shown that the maximum number of orthogonal Golay pairs of length $2^k, 10 \cdot 2^k, 26 \cdot 2^k, 2(10 \cdot 2^k), 2(26 \cdot 2^k)$ is at least equal to $2^{k+1}, 4 \cdot 2^k, 4 \cdot 2^k, 16 \cdot 2^{k+1}$ respectively (Fan *et al.*, 1993b). In the following sections, generalized forms of CS will be considered.

4.3 Synthesis of Orthogonal Complementary Sets

Theorem 10 *Given a class of OCSS, $S_{P,M}^N$, which has N sets of CS each with P sequences and equal sequence lengths M , other OCSS $R_{P,M}^N$ with the same parameters N, P and M can be obtained by negating any number of sets in $S_{P,M}^N$.*

Proof: If $S^i \in S_{P,M}^N$ is a complementary set, $-S^i$ is also a complementary set (Tseng & Liu, 1972). Because $S^i, S^j \in S_{P,M}^N, i \neq j$, are orthogonal, then

$$\sum_{p=1}^P \sum_{m=1}^M (s_{p,m}^i)(-s_{p,m}^j) = - \sum_{p=1}^P \sum_{m=1}^M s_{p,m}^i s_{p,m}^j = 0, \quad (4.5)$$

which means $S_p^i, -S_p^j$ are also mutually orthogonal. Similarly $-S_p^i, -S_p^j$ are mutually orthogonal. Thus, the theorem is proved.

For example, given a class of OCSS $S_{4,4}^8$, if we negate the 1st, 2nd and 3rd sets, another OCSS of the same dimension can be obtained.

$$S_{4,4}^8 = \begin{bmatrix} - - + -, & + + + -, & - - + -, & + + + - \\ - + + +, & + - + +, & - + + +, & + - + + \\ - - - +, & + + - +, & - - - +, & + + - + \\ - + - -, & + - - -, & - + - -, & + - - - \\ - - + -, & - - - +, & - - + -, & - - - + \\ - + + +, & - + - -, & - + + +, & - + - - \\ - - - +, & - - + -, & - - - +, & - - + - \\ - + - -, & - + + +, & - + - -, & - + + + \end{bmatrix}$$

$$R_{4,4}^8 = \begin{bmatrix} + + - +, & - - - +, & + + - +, & - - - + \\ + - - -, & - + - -, & + - - -, & - + - - \\ + + + -, & - - + -, & + + + -, & - - + - \\ - + - -, & + - - -, & - + - -, & + - - - \\ - - + -, & - - - +, & - - + -, & - - - + \\ - + + +, & - + - -, & - + + +, & - + - - \\ - - - +, & - - + -, & - - - +, & - - + - \\ - + - -, & - + + +, & - + - -, & - + + + \end{bmatrix}$$

Theorem 11 *Let $S_{P,M}^N$ be a class of OCSS; other OCSS $R_{P,M}^N$ with the same parameters N, P and M can be obtained by 1) negating any number of sequences in all sets of $S_{P,M}^N$, 2) reversing any number of sequences in all sets of $S_{P,M}^N$, 3) interchanging any number of sequences in all sets of $S_{P,M}^N$, and 4) negating alternate elements in all sequences and all sets of $S_{P,M}^N$.*

The proof of this theorem is similar to that of Theorem 10 and is omitted here for brevity. As an example, let $S_{4,3}^8$ be an OCSS of length $M=3$, as shown below; if we negate the first sequence and reverse the last sequence of all sets, the result is still an OCSS.

$$S_{4,3}^8 = \begin{bmatrix} ---, & --+, & -+-, & +-- \\ ---, & -+-, & --+, & --+ \\ ---, & +--, & +--, & -+- \\ --+, & --+, & +-+, & +++ \\ --+, & +++-, & -+-, & +++ \\ -+-, & +++, & --+, & ++- \\ -++, & ---, & -++, & -+- \\ -++, & +-+, & ---, & --+ \end{bmatrix}$$

$$R_{4,3}^8 = \begin{bmatrix} +++, & --+, & -+-, & --+ \\ +++, & -+-, & --+, & +-- \\ +++, & +--, & +--, & -+- \\ ++-, & --+, & +-+, & +++ \\ ++-, & ++-, & -+-, & +++ \\ +-+, & +++, & --+, & -++ \\ +- -, & ---, & -++, & -+- \\ +- -, & +-+, & ---, & +-- \end{bmatrix}$$

Theorem 12 *Given a class of OCSS, $S_{P,M}^N$, then*

$$R_{PU,M}^N = \underbrace{[S_{P,M}^N, S_{P,M}^N, \dots, S_{P,M}^N]}_{U \text{ times}} \quad (4.6)$$

is also a class of OCSS which has N sets each with PU sequences and equal lengths M .

Proof: According to Definition 8, the PU autocorrelation functions will sum to zero at every shift (except the zero shift) in $R_{PU,M}^N$ because the P autocorrelation functions sum to zero at every shift (except the zero shift) in $S_{P,M}^N$; that is to say, every set in $R_{PU,M}^N$ is a complementary set. Note the fact that the orthogonality does not change in Eqn 4.6 and hence $R_{PU,M}^N$ is a class of OCSS.

The following is an illustrative example where $M = 2, P = 2, N = 4, U = 3$.

$$S_{2,2}^4 = \begin{bmatrix} --, & +- \\ -+, & ++ \\ --, & -+ \\ -+, & -- \end{bmatrix} R_{6,2}^4 = \begin{bmatrix} --, & +-, & --, & +-, & --, & +- \\ -+, & ++, & -+, & ++, & -+, & ++ \\ --, & -+, & --, & -+, & --, & -+ \\ -+, & --, & -+, & --, & -+, & -- \end{bmatrix}.$$

Theorem 13 Given a class of OCSS, $S_{P,M}^N$, then

$$R_{2P,M}^{2N} = \begin{bmatrix} S_{P,M}^N & S_{P,M}^N \\ S_{P,M}^N & -S_{P,M}^N \end{bmatrix} \quad (4.7)$$

is also a class of OCSS which has $2N$ sets, each with $2P$ sequences and equal lengths M .

Proof: From Theorem 12 it is clear that every set in $[S_{P,M}^N, S_{P,M}^N]$ is a complementary set and, therefore, every set in $[S_{P,M}^N, -S_{P,M}^N]$ is also a complementary set (Tseng & Liu, 1972).

We now prove that all the complementary sets in $R_{2P,M}^{2N}$ are also mutually orthogonal. First, all the complementary sets in $[S_{P,M}^N, S_{P,M}^N]$ or $[S_{P,M}^N, -S_{P,M}^N]$ are mutually orthogonal, according to Theorem 12 and Theorem 11. Secondly, for $R^i \in [S_{P,M}^N, S_{P,M}^N]$ and $R^j \in [S_{P,M}^N, -S_{P,M}^N]$, we have

$$\sum_{p=1}^P \sum_{m=1}^M (s_{p,m}^i)(s_{p,m}^j) + \sum_{p=1}^P \sum_{m=1}^M (s_{p,m}^i)(-s_{p,m}^j) = 0 \quad (4.8)$$

In other words, each complementary set in $[S_{P,M}^N, -S_{P,M}^N]$ is mutually orthogonal to every set in $[S_{P,M}^N, S_{P,M}^N]$. Therefore $R_{2P,M}^{2N}$ is a class of OCSS.

For example, given a class of OCSS $S_{2,2}^4$ of sequence length $M=2$, we can construct a larger class of OCSS $S_{4,2}^8$ of same sequence length, i.e.,

$$S_{2,2}^4 = \begin{bmatrix} --, & +- \\ -+, & ++ \\ --, & -+ \\ -+, & -- \end{bmatrix} \quad S_{4,2}^8 = \begin{bmatrix} --, & +-, & --, & +- \\ -+, & ++, & -+, & ++ \\ --, & -+, & --, & -+ \\ -+, & --, & -+, & -- \\ --, & +-, & ++, & -+ \\ -+, & ++, & +-, & -- \\ --, & -+, & ++, & +- \\ -+, & --, & +-, & ++ \end{bmatrix}$$

Theorem 14 Given a class of OCSS, $S_{2,M}^N = [X_M^N, Y_M^N]$, if $xy \in X_M^N Y_M^N$ is a concatenation of sequence x and sequence y , then

$$R_{2,2M}^{2N} = \begin{bmatrix} X_M^N Y_M^N, (-X_M^N) Y_M^N \\ X_M^N Y_M^N, X_M^N (-Y_M^N) \end{bmatrix} \quad (4.9)$$

is also a class of OCSS which has $2N$ sets each with 2 sequences and equal lengths $2M$.

Proof: Let $[x, y]$ be a complementary set in $S_{2,M}^N$, then by direct calculation it is simple to show that $[xy, -xy], [xy, -yx] \in S_{2,2M}^{2N}$ are complementary sets. Using the same method as in Theorem 13, all the complementary sets in $S_{2,2M}^{2N}$ are also mutually orthogonal.

As an example, given a class of mutually orthogonal pairs of CS of length 1, $s_{2,1}^2 = \begin{bmatrix} -1 & -1 \\ -1 & +1 \end{bmatrix}$, as a starting point, if the Theorem 14 is applied 3 times successively, the resulting OCSSs will be as follows:

$$S_{2,2}^4 = \begin{bmatrix} --, & +- \\ -+, & ++ \\ --, & -+ \\ -+, & -- \end{bmatrix} S_{2,4}^8 = \begin{bmatrix} --+-, & +++- \\ -+++, & +-++ \\ ---+, & ++-+ \\ -+--, & +--- \\ --+-, & ---+ \\ -+++, & -+-- \\ ---+, & --+- \\ -+--, & -+++ \end{bmatrix}$$

$$S_{2,8}^{16} = \begin{bmatrix} --+-+++-, & +-+---+- \\ -++++-++, & +----+-++ \\ ---+++-+, & +++-++-+ \\ -+-+---, & +-++++- \\ --+-+---+, & +-+---+-+ \\ -++++-+-, & +----+--- \\ ---+---+-, & +++-+---+ \\ -+-+---++, & +-++-++ \\ --+-+---+, & ---+---+-+ \\ -++++-+-, & -+++-+--- \\ ---+++-+, & ---+---+-+ \\ -+-+---, & -+-+---++ \\ --+-+---+, & ---+---+-+ \\ -++++-+-, & ---+++-++ \\ -+-+---++, & -+++-+--- \end{bmatrix}$$

Theorem 15 If $S_{P,M}^N$ is a class of OCSS, then $R_{2P,2M}^{4N}$ is also a class of OCSS with $4N$ sets each of $2P$ sequences and length $2M$, where

$$R_{2P,2M}^{4N} = \begin{bmatrix} S_{P,M}^N S_{P,M}^N, & -(S_{P,M}^N) S_{P,M}^N \\ S_{P,M}^N S_{P,M}^N, & S_{P,M}^N (-S_{P,M}^N) \\ (-S_{P,M}^N) S_{P,M}^N, & S_{P,M}^N S_{P,M}^N \\ S_{P,M}^N (-S_{P,M}^N), & S_{P,M}^N S_{P,M}^N \end{bmatrix}, \quad (4.10)$$

$(-S_{P,M}^N) S_{P,M}^N$ denote the matrix whose ij -th entry is the concatenation of the ij -th sequence of $-S_{P,M}^N$ and the ij -th sequence of $S_{P,M}^N$.

Proof: If $S^i \in S_{P,M}^N$ is complementary set with P sequences, $S_1^i, \dots, S_P^i$, then for any set $[S^i S^i, (-S^i) S^i] \in S_{2P,2M}^{4N}$, we have

$$C_{S_p^i S_p^i, S_p^i S_p^i}(\tau') = \begin{cases} 2M, & \tau' = 0 \\ 2C_{S_p^i, S_p^i}(\tau) + C_{S_p^i, S_p^i}(M - \tau), & \tau' = \tau = 1, \dots, M-1 \\ C_{S_p^i, S_p^i}(\tau), & \tau' = M, \dots, 2M-1, \\ & \tau = \tau' - M \end{cases} \quad (4.11)$$

$$C_{(-S_p^i) S_p^i, (-S_p^i) S_p^i}(\tau') = \begin{cases} 2M, & \tau' = 0 \\ 2C_{S_p^i, S_p^i}(\tau) - C_{S_p^i, S_p^i}(M - \tau), & \tau' = \tau = 1, \dots, M-1 \\ -C_{S_p^i, S_p^i}(\tau), & \tau' = M, \dots, 2M-1, \\ & \tau = \tau' - M \end{cases} \quad (4.12)$$

Thus

$$\sum_{p=1}^P C_{S_p^i S_p^i, S_p^i S_p^i}(\tau') + \sum_{p=1}^P C_{(-S_p^i) S_p^i, (-S_p^i) S_p^i}(\tau') = \begin{cases} 4PM, & \tau' = 0 \\ 0, & \tau' \neq 0 \end{cases} \quad (4.13)$$

It follows that each set $[S^i S^i, (-S^i) S^i] \in S_{2P,2M}^{4N}$ is a complementary set. Similarly any $[S^i S^i, S^i(-S^i)], [(-S^i) S^i, S^i S^i]$ and $[S^i(-S^i), S^i S^i] \in S_{2P,2M}^{4N}$, are all complementary sets.

Now considering orthogonality: because any $S^i, S^j \in S_{P,M}^N$ (or $-S_{P,M}^N$) $i \neq j$, are orthogonal, $R^i, R^j \in [S_{P,M}^N S_{P,M}^N, -(S_{P,M}^N) S_{P,M}^N]$, $i \neq j$, are also orthogonal. Furthermore, $R^i = [S^i S^i, (-S^i) S^i]$, $R^j = [S^j S^j, S^j(-S^j)] \in S_{2P,2M}^{4N}$ are orthogonal because

$$\begin{aligned} & \sum_{p=1}^P \sum_{m=1}^M s_{p,m}^i s_{p,m}^j + \sum_{p=1}^P \sum_{m=1}^M s_{p,m}^i s_{p,m}^j + \\ & \sum_{p=1}^P \sum_{m=1}^M s_{p,m}^i (-s_{p,m}^j) + \sum_{p=1}^P \sum_{m=1}^M (-s_{p,m}^i) s_{p,m}^j = 0 \end{aligned} \quad (4.14)$$

For all other cases, the results are similar. Therefore, $N_{2P,2M}^{4N}$ is a class of OCSS of length $2M$.

As an illustrative example, given an OCSS $S_{2,2}^4$ of length $M=2$, a new OCSS $R_{4,4}^{16}$ of sequence length $2M=4$ can be obtained as follows:

$$S_{2,2}^4 = \begin{bmatrix} --, & +- \\ -+, & ++ \\ --, & -+ \\ -+, & -- \end{bmatrix} R_{4,4}^{16} = \begin{bmatrix} ----, & +-+-, & ++--, & -++- \\ -+--, & +++, & +- --, & --++ \\ ----, & -+--, & ++--, & +- -- \\ -+--, & ----, & +- --, & ++-- \\ ----, & +-+-, & --++, & +- -- \\ -+--, & +++, & -++-, & ++-- \\ ----, & -+--, & --++, & -++- \\ -+--, & ----, & -++-, & --++ \\ ++--, & -++-, & ----, & +-+- \\ +- --, & --++, & -+--, & ++++ \\ ++--, & +- --, & ----, & -++- \\ +- --, & +++, & -+--, & ---- \\ --++, & +- --, & ----, & +-+- \\ -++-, & ++--, & -+--, & ++++ \\ --++, & -++-, & ----, & -++- \\ -++-, & --++, & -+--, & ---- \end{bmatrix}$$

Theorem 16 Suppose that S_{2T,M_1}^N is a class of OCSS of sequence length M_1 and $g = (g_1, g_2)$ is a Golay pair of length M_2 . Then $R_{2T,M_1M_2}^N$ is also a class of OCSS of length $M_1 \cdot M_2$, where

$$R_{2T,M_1M_2}^N = [R_1^N, R_2^N, \dots, R_{2T-1}^N, R_{2T}^N] \quad (4.15)$$

with $R_{2k-1}^N = S_{2k-1}^N \otimes \frac{g_1+g_2}{2} + S_{2k}^N \otimes \frac{g_1-g_2}{2}$, $R_{2k}^N = S_{2k-1}^N \otimes \frac{\tilde{g}_1-\tilde{g}_2}{2} - S_{2k}^N \otimes \frac{\tilde{g}_1+\tilde{g}_2}{2}$, $k = 1, \dots, T$; $\tilde{g}_j$ is the reverse of sequence g_j and $\otimes$ denotes the Kronecker product.

Proof: Using the same technique as Turyn, it has been proved that any set in $R_{2T,M_1M_2}^N$ is a complementary set (Turyn, 1974; Eliahou *et al.*, 1990). By noting the fact that S_{2T,M_1}^N is a class of OCSS, it can be shown by comprehensive verification that all the sets in $R_{2T,M_1M_2}^N$ are mutually orthogonal. Obviously, by selecting other Golay pairs of length M_2 , a larger OCSS can be synthesized.

For example, $S_{4,3}^8$ below is a class of OCSS of sequence length $M_1 = 3$ and $g = (++, -+)$ and $g' = (+-, --)$ are two uncorrelated Golay pairs of length $M_2 = 2$; by employing the above theorem twice, a new class of OCSS $R_{4,6}^{16}$ of length $M_1M_2 = 6$ can be synthesized as shown below:

$$S_{4,3}^8 = \begin{bmatrix} ---, & --+, & -+-, & +- - \\ ---, & -+-, & --+, & --+ \\ ---, & +--, & +--, & -+- \\ --+, & --+, & +--, & +++ \\ --+, & ++-, & -+-, & +++ \\ -+-, & +++, & --+, & ++- \\ -++, & ---, & -++, & -+- \\ -++, & +-+, & ---, & --+ \end{bmatrix}$$

$$R_{4,6}^{16} = \begin{bmatrix} ---+ , & +++-+ , & -+-+ , & +-+- \\ ---+- , & +++-+ , & --+-+ , & +-+-- \\ ---+- , & ++++- , & +-+-- , & -+++- \\ --+-+ , & ++-- , & +-++++ , & -+-+++ \\ --++++ , & ++-+- , & -+-++++ , & +-++++ \\ -+-++++ , & +-++++ , & --++++ , & +-+--+ \\ -++-- , & +-+-- , & -++-- , & +-+-- \\ -++++ , & +-+-- , & --+-- , & +++-- \\ ---+- , & ---+ , & -+-+ , & -+-+ \\ ---+- , & ---+ , & --++++ , & --+-+ \\ ---+- , & ---+ , & +-+-- , & +-+-- \\ ---+- , & ---+ , & +-+-- , & +-+-- \\ ---+- , & ---+ , & +-+-- , & +-+-- \\ ---+- , & ---+ , & +-+-- , & +-+-- \\ ---+- , & ---+ , & +-+-- , & +-+-- \\ ---+- , & ---+ , & +-+-- , & +-+-- \\ ---+- , & ---+ , & +-+-- , & +-+-- \\ ---+- , & ---+ , & +-+-- , & +-+-- \end{bmatrix}$$

4.4 Some Conjectures

In addition, we conjecture that the following statements are true:

Conjecture 1 *Let $S_{P,M}^N$ be an arbitrary MOCSS of sequence length M , then the parameters satisfy the following relation,*

$$N \leq P \cdot M. \quad (4.16)$$

Conjecture 2 *If $S_{P,M}^N$ is a MOCSS of sequence length M , then the OCSS $R_{2P,M}^{2N}$ of length M , given by Eqn 4.7, is also a MOCSS.*

Conjecture 3 *Given a class of MOCSS $S_{P,M}^N$ of sequence length M , then the $R_{2P,2M}^{4N}$ of length $2M$, given by Eqn 4.10, is also a class of MOCSS.*

Conjecture 4 *Given a class of MOCSS $S_{2T,M_1}^{N_1}$ of sequence length M_1 and a class of MOCSS $G_{2,M_2}^{N_2}$ of sequence length M_2 , then an MOCSS can be synthesized by using Theorem 16, $R_{2T,M_1M_2}^{\frac{N_1N_2}{2}}$, with sequence length $M_1 \cdot M_2$.*

4.5 Applications to Synchronous SSMA

In many multiaccess systems, such as local area networks(LANs), each transmitter can hear whether or not the other transmitters are sending. Here a

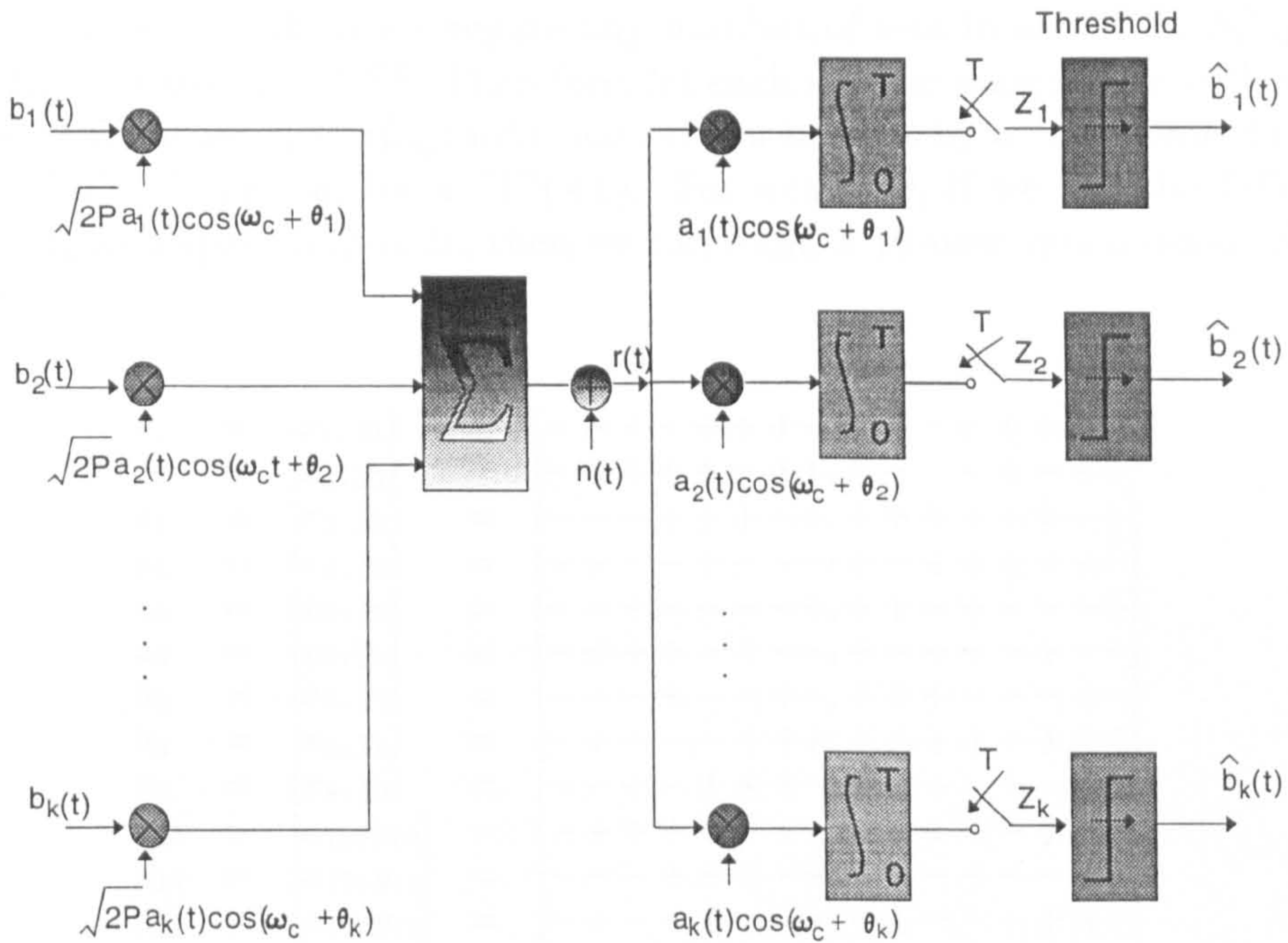


Figure 4.1: Synchronous SSMA System Model Employing OCSS

relatively new approach to eliminate system "self-noise" by using orthogonal complementary sets is proposed. The basic concept is to force the system to work in a quasi-synchronous mode by means of "carrier sensing". When the system works in such a quasi-synchronous mode, the interferences from other users' signals will be minimized by the use of orthogonal complementary sets which have zero CCF value at zero time shift.

The basic system model of synchronous SSMA based on the use of sets of complementary sequences is shown in Fig. 4.1. In the system shown, the individual transmitters can transmit data independently of the other transmitters. However, before transmitting, the user should listen to the channel; if the channel is idle, the transmission will start at once; if the channel is engaged, the channel signal should be received and processed to abstract the timing signal and the transmission started in a synchronized manner. Thus all relative time delays in Fig. 4.1 are integer multiples of the sequence period or the bit interval of duration T .

It should be noted that the purpose of carrier sensing in ALOHA CSMA is to avoid collision, while the purpose of "carrier sensing" in quasi-synchronous SSMA is to allow synchronous collisions in order to eliminate co-channel interference.

Based on Theorem 10, if we negate any number of sets in an OCSS $S_{P,M}^N$, the result $R_{P,M}^N$ is also an OCSS. Therefore, let each user be assigned an orthogonal complementary set $a_i \in S_{P,M}^N$; information can be sent by a complementary set a_i for a "0"(-1), or $-a_i$ for a "1"(+1). For example, if we use the following OCSS $S_{2,8}^{16}$ as a spreading code, then we can build a 16-user synchronous SSMA system:

$$\begin{aligned}
a_1 &= [x_1, y_1] = [- - + - + + + -, + + - + + + + -] \\
a_2 &= [x_2, y_2] = [- + + + + - + +, + - - - - + - + +] \\
a_3 &= [x_3, y_3] = [- - - + + + - +, + + + - + + - +] \\
a_4 &= [x_4, y_4] = [- + - - + - - -, + - + + + - - -] \\
a_5 &= [x_5, y_5] = [- - + - - - - +, + + - + - - - +] \\
a_6 &= [x_6, y_6] = [- + + + - + - -, + - - - - + - -] \\
a_7 &= [x_7, y_7] = [- - - + - - + -, + + + - - - + -] \\
a_8 &= [x_8, y_8] = [- + - - - + + +, + - + + - + + +] \\
a_9 &= [x_9, y_9] = [- - + - + + + -, - - + - - - - +] \\
a_{10} &= [x_{10}, y_{10}] = [- + + + + - + +, - + + + - + - -] \\
a_{11} &= [x_{11}, y_{11}] = [- - - + + + - +, - - - + - - + -] \\
a_{12} &= [x_{12}, y_{12}] = [- + - - + - - -, - + - - - + + +] \\
a_{13} &= [x_{13}, y_{13}] = [- - + - - - - +, - - + - + + + -] \\
a_{14} &= [x_{14}, y_{14}] = [- + + + - + - -, - + + + + - + +] \\
a_{15} &= [x_{15}, y_{15}] = [- - - + - - + -, - - - + + + - +] \\
a_{16} &= [x_{16}, y_{16}] = [- + - - - + + +, - + - - + - - -].
\end{aligned}$$

The receiver for each user is a correlation receiver matched to the user's code sequence, consisting in principle of a multiplier, to which is fed a local replica of the i -th user's complementary set, followed by an integrator which takes the integral over each bit period. The output of the integrator is then sampled every T seconds. The objective of the threshold detector is to compare the received samples with the optimum preset threshold value of zero. A data bit "1" is generated if the detector input Z_i exceeds zero, and a data bit "0" is output otherwise.

For the Gaussian white noise(GWN) channel, it is proved that the input of the detector Z_i is given by (Fan *et al.*, 1993a)

$$Z_i = \sqrt{\frac{P}{2}} T b_{i,0} + n_0(t) \quad (4.17)$$

where $b_{i,0}$, P , T are defined in Chapter 1, Section 1.4.

Obviously, because of the orthogonal properties of OCSS, the interference due to the co-channel effects of other user signals have been eliminated. The performance of the synchronous SSMA system is, therefore, the same as that of

the single-user, phase-coded, communication system, i.e.

$$P_e = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{E_b}{N_0}} \right) \quad (4.18)$$

where $\operatorname{erfc}(\cdot)$ is the complementary error function and $E_b = PT$ is the energy per data bit.

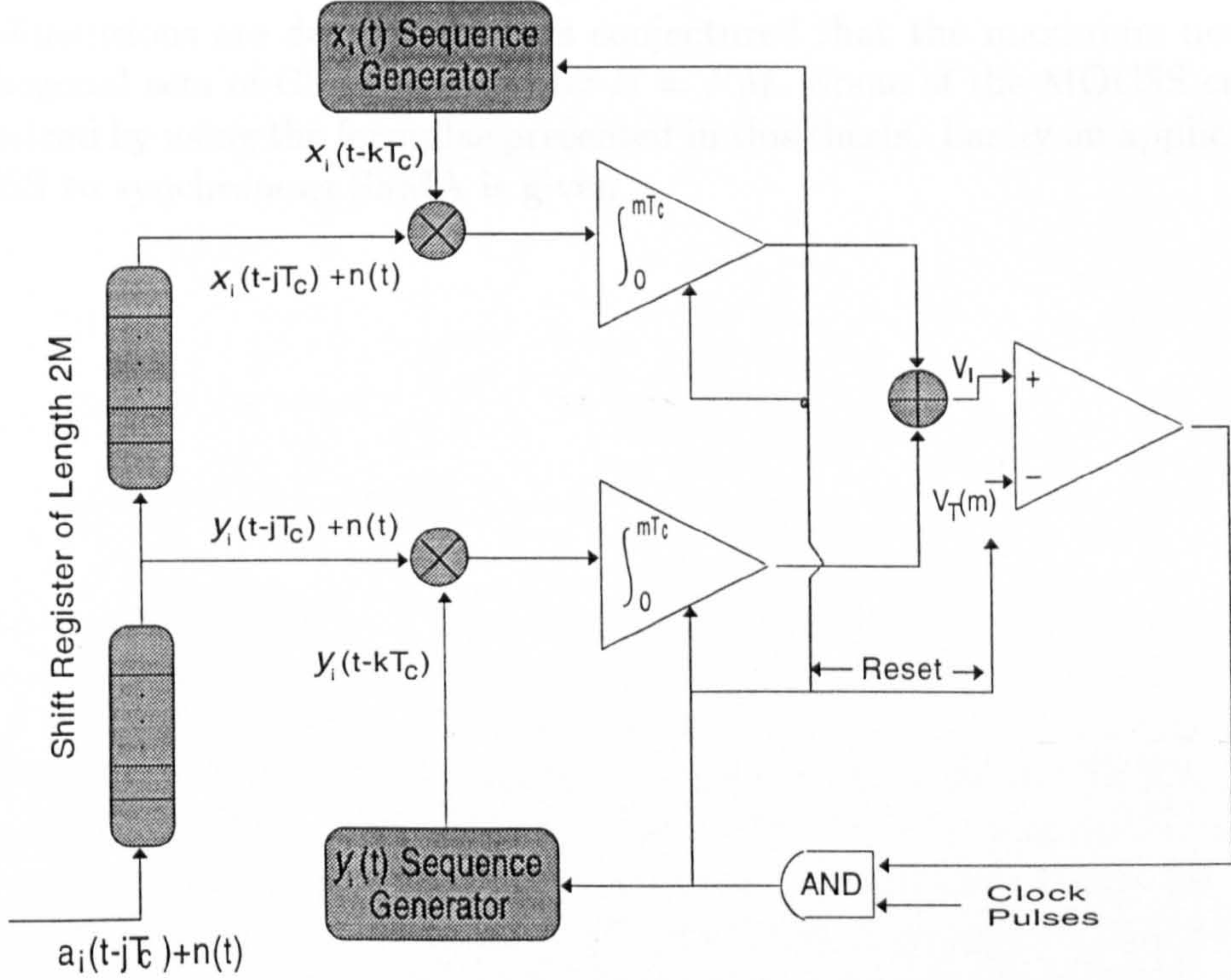


Figure 4.2: Generalized Sliding Correlator Synchronization

For synchronization, in order to make use of the summed impulsive ACF property, a generalized sliding correlator is proposed, as shown in Fig. 4.2. In this circuit, there are $P = 2$ shift registers, each of length M , which are used for storing a pair of complementary sequences. The first sequence in the received pair passes to the upper correlator while the second goes to the lower correlator. The locally generated sequences $x_i(t)$, $y_i(t)$ are available with synchronous delay stepped in increments of $1/2$ chip to ensure correlation. The output phase k of the local sequence generator is initially set to $k = 0$ and a partial correlation is performed by examining m chips. If the integrator output falls below the threshold and therefore is deemed too small, k is set to $k = 1$ and the procedure is repeated. If the summed output of the two correlators exceeds the threshold, then we have found the correct value of phase k of both local sequence generators.

4.6 Concluding Remarks

The concept of uncorrelated sets of CS has been extended to orthogonal sets of CS. It has been shown that the number of sets in an OCSS is much larger than the number of UCSS with the same parameters P and M . Recursive formulae for constructing orthogonal complementary sets are presented and examples are given. Methods for synthesizing new OCSS from known ones with the same dimensions are developed. It is conjectured that the maximum number of orthogonal sets of CS is bounded by $N = PM$. Some of the MOCSS can be synthesized by using the formulae presented in this thesis. Lastly an application of OCSS to synchronous SSMA is given.

Chapter 5

Codes for Asynchronous SSMA Systems—I

5.1 Introduction

Sets of sequences with good correlation properties have found application in radar, ranging and tracking, system identification, spread-spectrum communications and SSMA communications. The asynchronous SSMA communication system with PSK or QAM modulation provides multiple users with simultaneous access to the full communication channel bandwidth by assigning unique code sequences to each transmitter-receiver pair. Therefore, a large family of reliably distinguishable code sequences is required in an asynchronous SSMA system. Family size and maximum nontrivial correlation parameter C_{max} are commonly used to evaluate sequence designs. A large family size is required in order to support a large number of simultaneous users. Small values of C_{max} are required to permit unambiguous message synchronization and to minimize interference due to competing, simultaneous traffic across the channel.

To date, many very good sequences have been constructed. These sequences can be roughly classified into the following broad categories:

Binary Sequences with Optimal ACFs : M-sequences, quadratic residue sequences, Hall sequences, Twin prime sequences, Finite projective geometry sequences (Golomb, 1967; Everett, 1966), etc.. The ACF of these sequences is -1 (un-normalized) everywhere except at zero shift.

Binary Sequences with Good ACFs/CCFs : Gold sequences, Kasami sequences Gold-like and dual BCH sequences (Sarwate & Pursley, 1980); bent function sequences (Olsen *et al.*, 1982; Lempel & Cohn, 1982); GMW

sequences (Scholtz & Welch, 1984); No sequences (No & Kumar, 1989); Boztas-Kumar sequences (Boztas & Kumar, 1994), etc..

Real-valued Sequences with Good ACFs/CCFs : Visme sequences (de Visme, 1971); Bomer-Antweiler sequences (Bomer & Antweiler, 1991); Trajectory derived sequences (Darnell, 1993a); Frank-Chu like sequences (Fan & Darnell, 1994d), etc..

Perfect Sequences : Ternary sequences (Chang, 1967; Hoholdt & Justesen, 1983; Shedd & Sarwate, 1979); multi-level m-sequences (Darnell *et al.*, 1994); generalized bent sequences (Chung, 1972); Frank/Chu/Milewski sequences (Frank & Zadoff, 1962; Chu, 1972; Milewski, 1983; Zhang & Golomb, 1993; Fan *et al.*, 1994b); Nonpolyphase complex sequences (Darnell *et al.*, 1994); perfect array (Bömer & Antweiler, 1992), etc.. All these sequences have impulsive ACFs.

Polyphase Sequences with Two-valued ACFs/CCFs : Character sequences (Scholtz & Welch, 1978); Alltop sequences (Alltop, 1980); Luke sequences (Lüke, 92); triple product sequences (Fan *et al.*, 1994d), etc..

Polyphase Sequences with Good ACFs/CCFs : Quadriphase sequences (Krone & Sarwate, 1984; Boztas *et al.*, 1992; Novosad, 1993); Blake sequences (Blake & Mark, 1982); Helleseth sequences (Helleseth, 1976); Sidelnikov sequences (Sidelnikov, 1971); Kumar sequences (Kumar *et al.*, 1985; Kumar & Moreno, 1991), etc..

Nonpolyphase Complex Sequences with Optimal ACFs/CCFs : Maximal length sequences over Gaussian integers (Fan & Darnell, 1994c; Darnell *et al.*, 1994), etc..

In this chapter, and in the following two chapters, we will present some new constructions of polyphase and nonpolyphase sequences.

In this chapter, a new class of polyphase sequences with near-optimal two-valued ACFs and CCFs is proposed. It is proved that, for a given prime length $L > 3$, the out-of-phase ACFs and CCFs of the sequences are constant and equal to $\sqrt{L}$. An interesting and useful property of these sequences is that all the sequences of the same length L are mutually orthogonal. It is shown that the correlation values asymptotically reach the Sarwate bound.

5.2 Sequences with Two-valued ACFs and CCFs

Based upon the structure of Chu sequences (Chu, 1972) and Luke sequences (Lüke, 92), the intuitive extension described below can be formulated.

Definition 13 For any integers r, n and prime $L > 3$, where $0 \leq n, r < L$, a new class of polyphase sequences, $a^{(r)} = (a_0^{(r)}, a_1^{(r)}, \dots, a_{L-1}^{(r)})$, is defined as

$$a_n^{(r)} = \alpha^{n(n+1)(n+2)/6+rn}, \quad \alpha = e^{i2\pi v/L}, \quad (5.1)$$

where α is a primitive L -th root of unity and v is any integer relatively prime to L .

Obviously there exist L sequences each of length L for any prime $L > 3$.

We now show that the above sequences have the following ACF/CCF properties:

Theorem 17

$$|R_{r,r}(\tau)| = \begin{cases} L, & \tau = 0; \\ \sqrt{L}, & \tau \neq 0. \end{cases} \quad (5.2)$$

$$|R_{r,s}(\tau)| = \begin{cases} 0, & \tau = 0, r \neq s; \\ \sqrt{L}, & \tau \neq 0. \end{cases} \quad (5.3)$$

Proof: The squared absolute value of the periodic CCF $R_{r,s}(\tau)$ between sequence $a^{(r)}$ and sequence $a^{(s)}$ is defined as

$$|R_{r,s}(\tau)|^2 = \sum_{n=0}^{L-1} a_n^{(r)} a_{n+\tau}^{(s)*} \sum_{m=0}^{L-1} a_m^{(r)*} a_{m+\tau}^{(s)} \quad (5.4)$$

Substituting Eqn 5.1 into Eqn 5.4, we obtain

$$\begin{aligned}
|R_{r,s}(\tau)|^2 &= \sum_{n=0}^{L-1} \alpha^{n(n+1)(n+2)/6+rn-(n+\tau)(n+\tau+1)(n+\tau+2)/6-s(n+\tau)} \\
&\quad \sum_{m=0}^{L-1} \alpha^{-m(m+1)(m+2)/6-rm+(m+\tau)(m+\tau+1)(m+\tau+2)/6+s(m+\tau)} \\
&= \sum_{n=0}^{L-1} \alpha^{-\tau(2+6n+3n^2+3\tau+3n\tau+\tau^2)/6-(s-r)n-s\tau} \\
&\quad \sum_{m=0}^{L-1} \alpha^{\tau(2+6m+3m^2+3\tau+3m\tau+\tau^2)/6+(s-r)m+s\tau} \\
&= \sum_{n=0}^{L-1} \sum_{m=0}^{L-1} \alpha^{\tau[6(m-n)+3(m^2-n^2)+3\tau(m-n)]/6+(s-r)(m-n)} \\
&= \sum_{n=0}^{L-1} \sum_{m=0}^{L-1} \alpha^{(m-n)[\tau(\tau+m+n+2)/2+(s-r)]}
\end{aligned} \tag{5.5}$$

When $\tau = 0$, it is obvious that

$$|R_{r,s}(\tau)|^2 = \sum_{n=0}^{L-1} \sum_{m=0}^{L-1} \alpha^{(m-n)(s-r)} = \begin{cases} L^2, & \tau = 0, s = r; \\ 0, & \tau = 0, s \neq r. \end{cases} \tag{5.6}$$

When $\tau \neq 0$, we introduce the following change of variables:

$$n = m + l, \quad l = 0, 1, \dots, L-1. \tag{5.7}$$

Then the $|R_{r,s}(\tau)|^2$ can be rewritten as

$$\begin{aligned}
|R_{r,s}(\tau)|^2 &= \sum_{l=0}^{L-1} \sum_{m=0}^{L-1} \alpha^{-l[\tau(\tau+2m+l+2)/2+(s-r)]} \\
&= \sum_{l=0}^{L-1} \alpha^{-\tau l(\tau+l+2)/2-l(s-r)} \sum_{m=0}^{L-1} \alpha^{-\tau l m} = L,
\end{aligned} \tag{5.8}$$

where

$$\sum_{m=0}^{L-1} \alpha^{-\tau l m} = \begin{cases} 0, & l \neq 0, (\tau, L) = 1; \\ L, & l = 0. \end{cases} \tag{5.9}$$

It should be noted that for $\tau = 0, 1, \dots, L-1$, L must be a prime number in order to satisfy $(\tau, L) = 1$.

5.3 Periodic Correlation Performance of the Sequences

Let us now consider the asymptotic periodic correlation performance of the sequences. Sarwate (Sarwate, 1979) has shown that for a family of M uniform sequences, each of period L , the maximum magnitudes of the sidelobes Θ_a , Θ_c of periodic auto- and crosscorrelations respectively are lower bounded by

$$\frac{\Theta_c^2}{L} + \frac{L-1}{L(M-1)} \frac{\Theta_a^2}{L} \geq 1 \quad (5.10)$$

For the proposed sequences, $M = L$, $\Theta_a = \Theta_c = \sqrt{L}$, the Sarwate-bound yields

$$\frac{(\sqrt{L})^2}{L} + \frac{L-1}{L(L-1)} \frac{(\sqrt{L})^2}{L} = 1 + \frac{1}{L} \geq 1 \quad (5.11)$$

which approaches the bound for large L . Therefore

Theorem 18 *The proposed polyphase sequences are asymptotically optimal.*

An Example:

As a simple example, let $L = 7$; one obtains 7 distinct sequences

$$\begin{aligned} a^{(0)} &= (1, \alpha, \alpha^4, \alpha^3, \alpha^6, 1, 1) \\ a^{(1)} &= (1, \alpha^2, \alpha^6, \alpha^6, \alpha^3, \alpha^5, \alpha^6) \\ a^{(2)} &= (1, \alpha^3, \alpha, \alpha^2, 1, \alpha^3, \alpha^5) \\ a^{(3)} &= (1, \alpha^4, \alpha^3, \alpha^5, \alpha^4, \alpha, \alpha^4) \\ a^{(4)} &= (1, \alpha^5, \alpha^5, \alpha, \alpha, \alpha^6, \alpha^3) \\ a^{(5)} &= (1, \alpha^6, 1, \alpha^4, \alpha^5, \alpha^4, \alpha^2) \\ a^{(6)} &= (1, 1, \alpha^2, 1, \alpha^2, \alpha^2, \alpha) \end{aligned}$$

where $\alpha = e^{i2\pi/7}$. Their auto- and crosscorrelation functions are given by

$$\begin{aligned} |R_{r,r}(\tau)| &= (7, 2.6, 2.6, 2.6, 2.6, 2.6, 2.6) \\ |R_{r,s}(\tau)| &= (0, 2.6, 2.6, 2.6, 2.6, 2.6, 2.6) \end{aligned}$$

where $r \neq s$.

5.4 Nonperiodic Correlation Performance of the Sequences

From the periodic/nonperiodic correlation definition in Chapter 1, we have $R_{k,i}(\tau) = C_{k,i}(\tau) + C_{k,i}(\tau - L)$ and $R_{k,i}(-\tau) = [R_{i,k}(\tau)]^*$ (note that $C_{i,k}(\tau) = [C_{k,i}(-\tau)]^*$); the $R_{k,i}$ is called the even CCF. Similarly we have the odd CCF $\hat{R}_{k,i}$: $\hat{R}_{k,i}(\tau) = C_{k,i}(\tau) - C_{k,i}(\tau - L)$, where $\hat{R}_{i,k}(\tau) = -[\hat{R}_{k,i}(-\tau)]^*$. In the application of asynchronous SSMA, the odd correlation function represents the output of the correlator in the case where the data symbol changes during the integration of the correlation operation, whilst the even correlation function represents the output in the case where the data symbol remains constant over two consecutive symbols (Pursley, 1977; Sarwate & Pursley, 1980). Since the even and odd correlation functions appear with equal probability, both functions are of equal importance. It is clear that the nonperiodic correlations $C_i(\tau)$, $C_{k,i}(\tau)$ play an important role in reducing the maximal nontrivial even and odd correlation values.

Although many sequences have been found, little has been published concerning their nonperiodic correlation functions. This is because, generally speaking, the nonperiodic correlation is much more difficult to analyse than the periodic correlation.

For the sequences proposed above, a brief computer study for small length L has been carried out with attention being given to the maximum absolute value of nonperiodic correlation between pairs of sequences, as shown in Table 5.1. For comparison, similar results for Scholtz-Welch sequences with the same lengths are also given in Table 5.2. Scholtz-Welch sequences are constructed by employing characters of the group of units in the integer ring Z_L . It can be seen that for $L > 5$, the maximum nontrivial nonperiodic correlation values of the proposed sequences are lower than those of Scholtz-Welch sequences. Therefore the nonperiodic performance of the proposed sequences is better than that of Scholtz-Welch sequences.

In order to compare the periodic ACFs/CCFs and nonperiodic ACFs/CCFs of the new sequences, Figs. 5.1- 5.8 give a picture of the relative magnitudes of the two kinds of correlation for the length $L = 401$. It is seen that the two correlations have roughly the same peak magnitude.

Table 5.1: Aperiodic ACFs/CCFs of New Sequences

L	$ R_r(0) $	$\max_{r,\tau} R_r(\tau) $	$\min_{r,s} \max_{\tau} R_{r,s}(\tau) $	$\max_{r,s,\tau} R_{r,s}(\tau) $
5	5	1.62	1.54	3.24
7	7	2.98	1.97	3.21
11	11	4.48	2.73	4.48
13	13	5.09	2.98	5.18
17	17	4.90	4.19	6.36
19	19	6.67	3.82	6.67
23	23	6.69	4.24	7.44
29	29	8.24	5.05	8.24
31	31	8.30	5.42	8.48
37	37	10.03	5.59	10.15
41	41	9.90	6.77	10.98
43	43	9.35	7.35	9.54
47	47	10.26	7.44	10.58
53	53	10.88	8.19	10.88

Table 5.2: Aperiodic ACFs/CCFs of Scholtz-Welch Sequences

L	$ R_r(0) $	$\min_r \max_{\tau} R_r(\tau) $	$\min_{r,s} \max_{\tau} R_{r,s}(\tau) $	$\max_{r,s,\tau} R_{r,s}(\tau) $
5	4	1	2.24	2.24
7	6	2	2.65	3.46
11	10	1.62	3.32	5.02
13	12	2.73	3.61	6.03
17	16	2.86	4.12	7.21
19	18	2.35	4.36	6.36
23	22	3.23	4.80	8.30
29	28	3.12	5.39	10.16
31	30	3.62	5.57	10.59
37	36	4.00	6.37	12.44
41	40	3.95	6.40	13.20
43	42	4.82	6.77	13.15
47	46	5.00	6.86	14.48
53	52	5.32	7.66	14.40

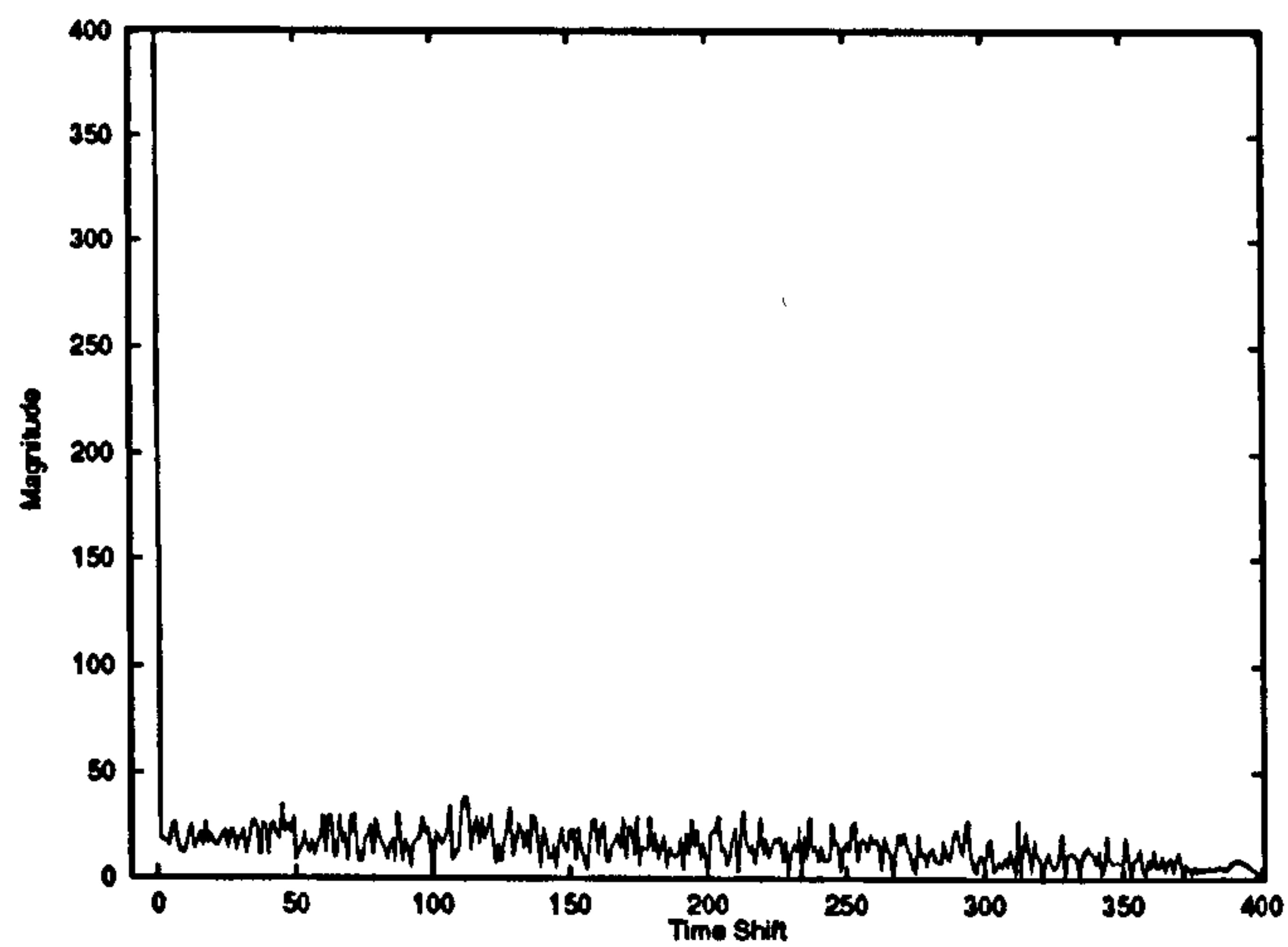


Figure 5.1: Nonperiodic ACF of Sequence $a^{(0)}$

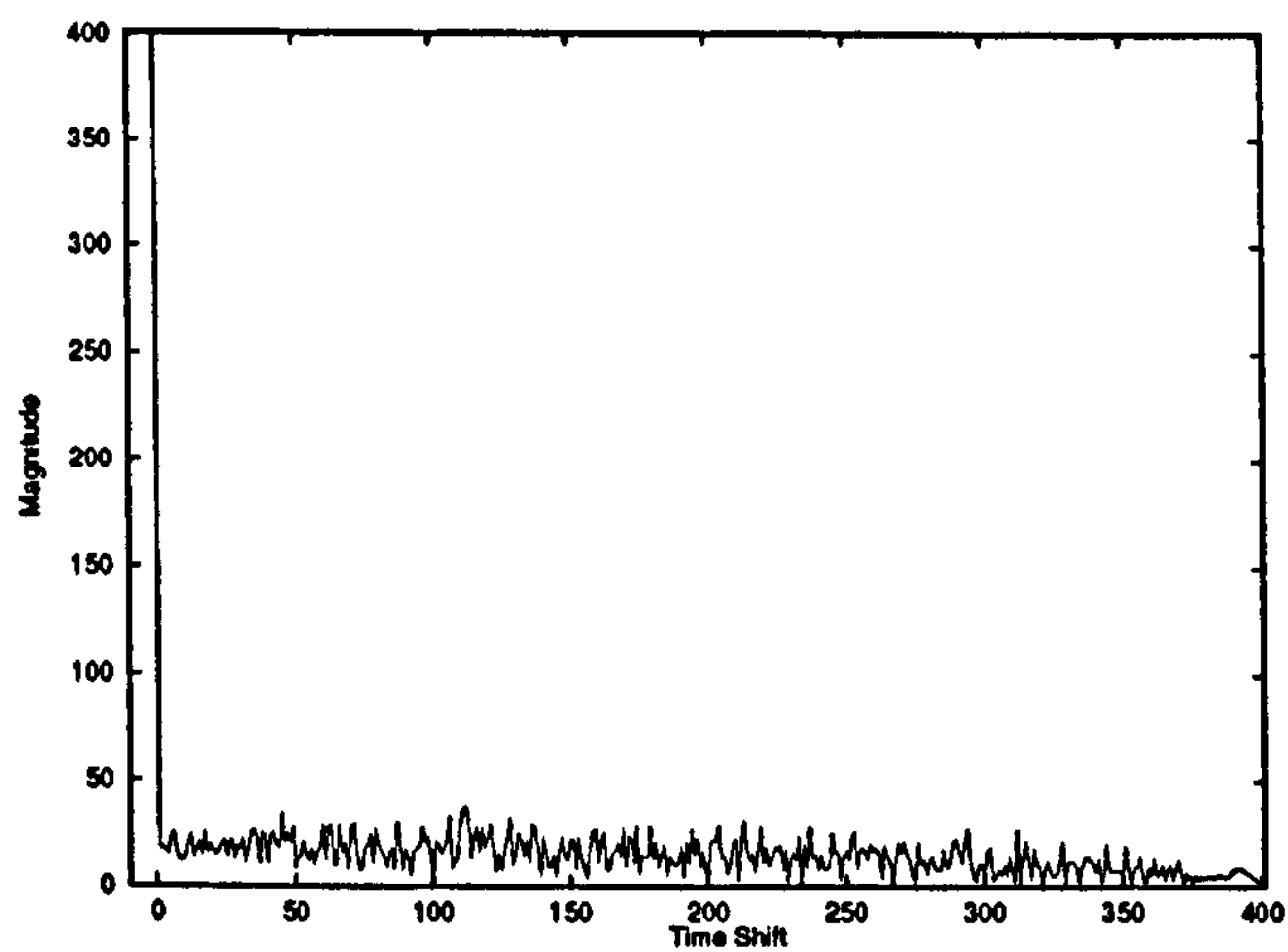


Figure 5.2: Nonperiodic ACF of Sequence $a^{(1)}$

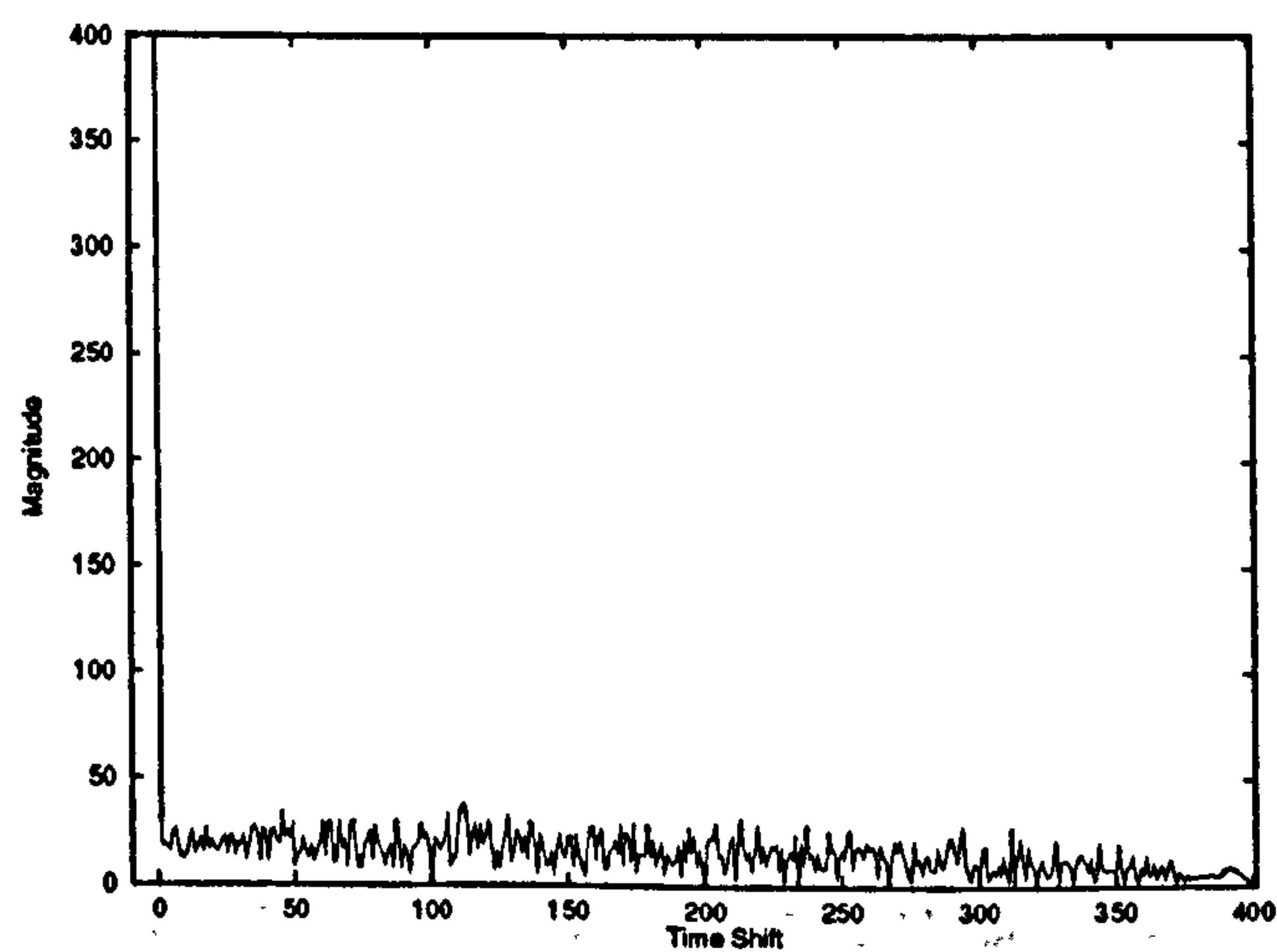


Figure 5.3: Nonperiodic ACF of Sequence $a^{(99)}$

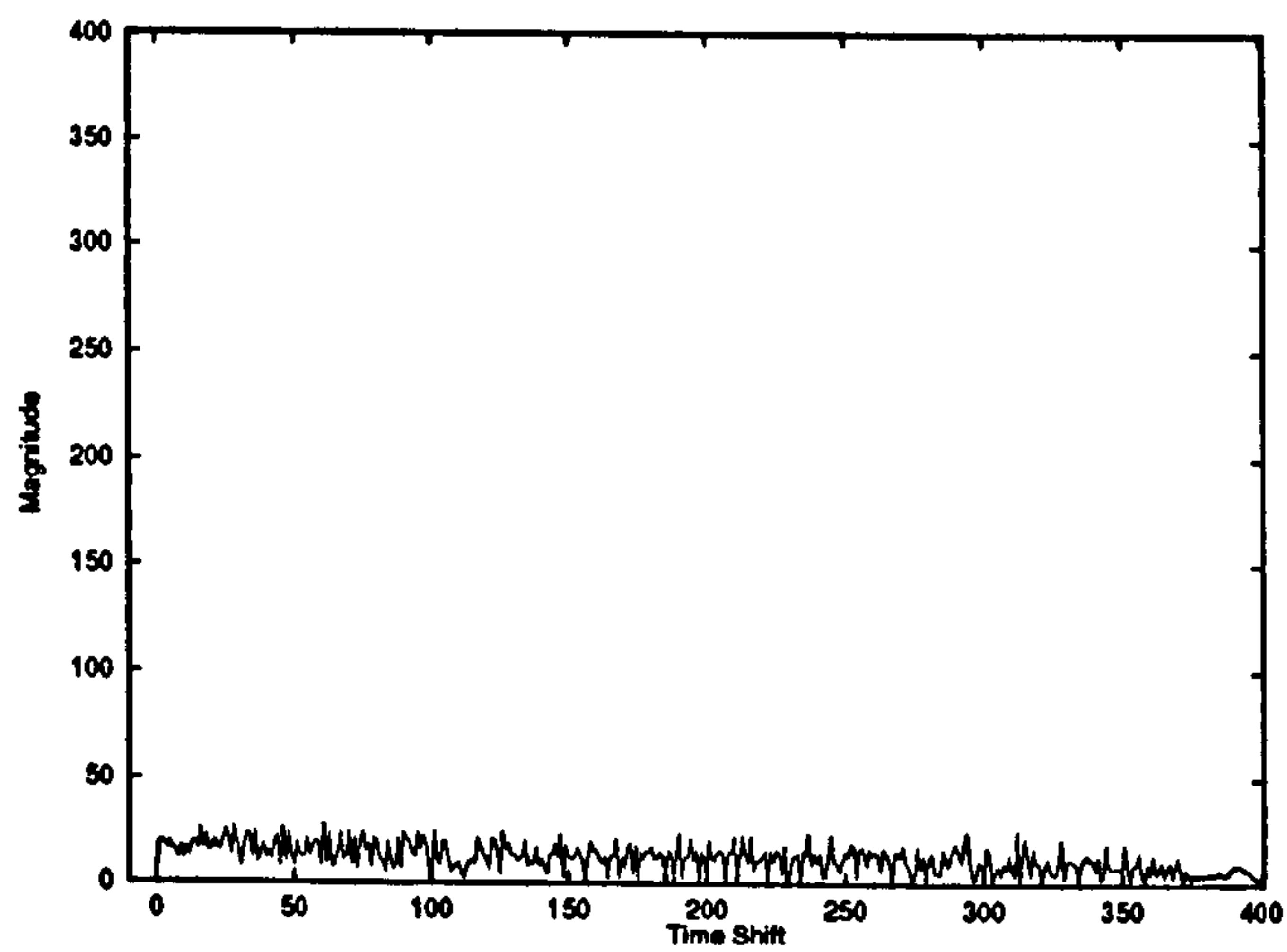


Figure 5.4: Nonperiodic CCF between $a^{(0)}$ and $a^{(1)}$

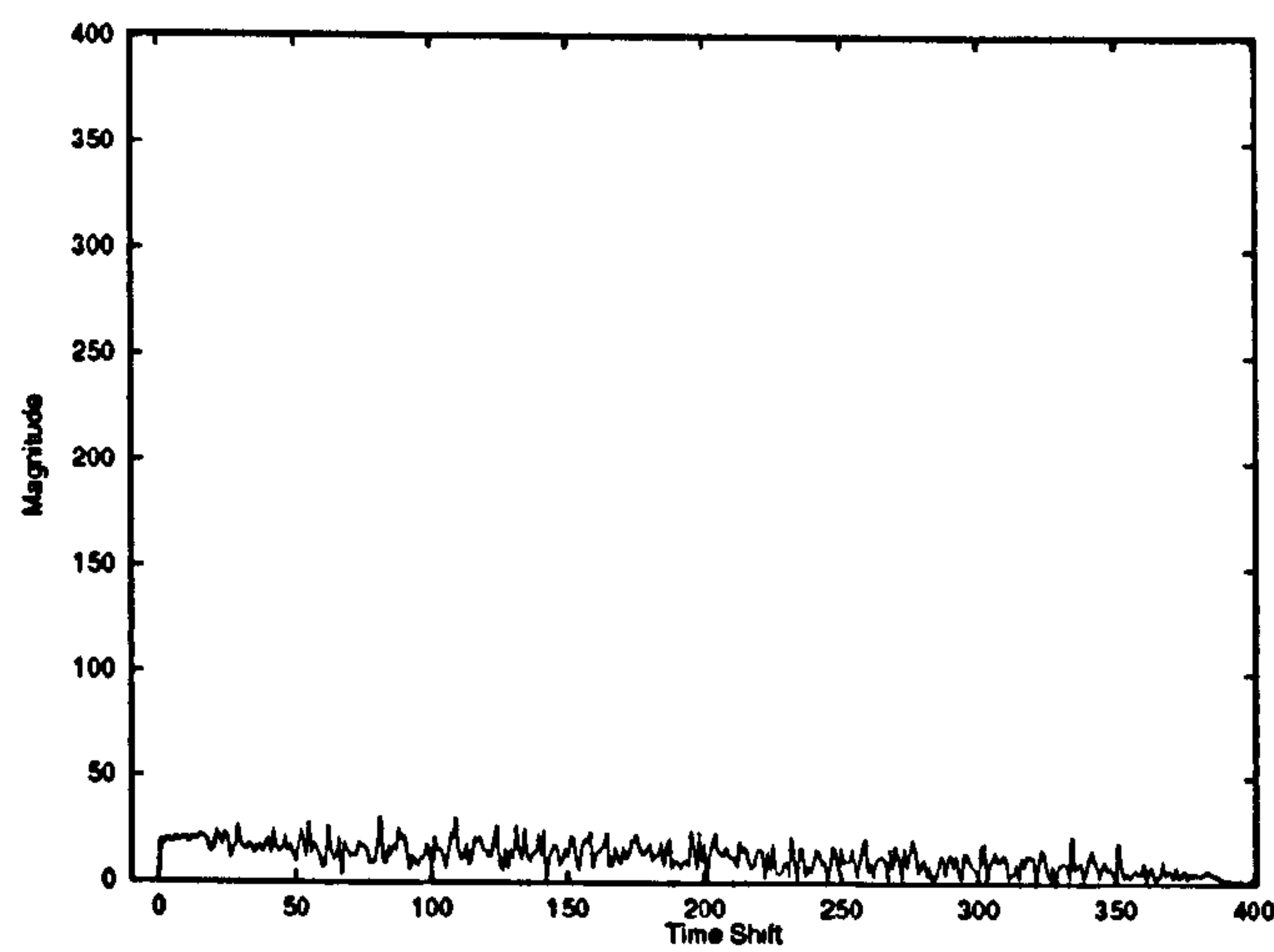


Figure 5.5: Nonperiodic CCF between $a^{(0)}$ and $a^{(99)}$

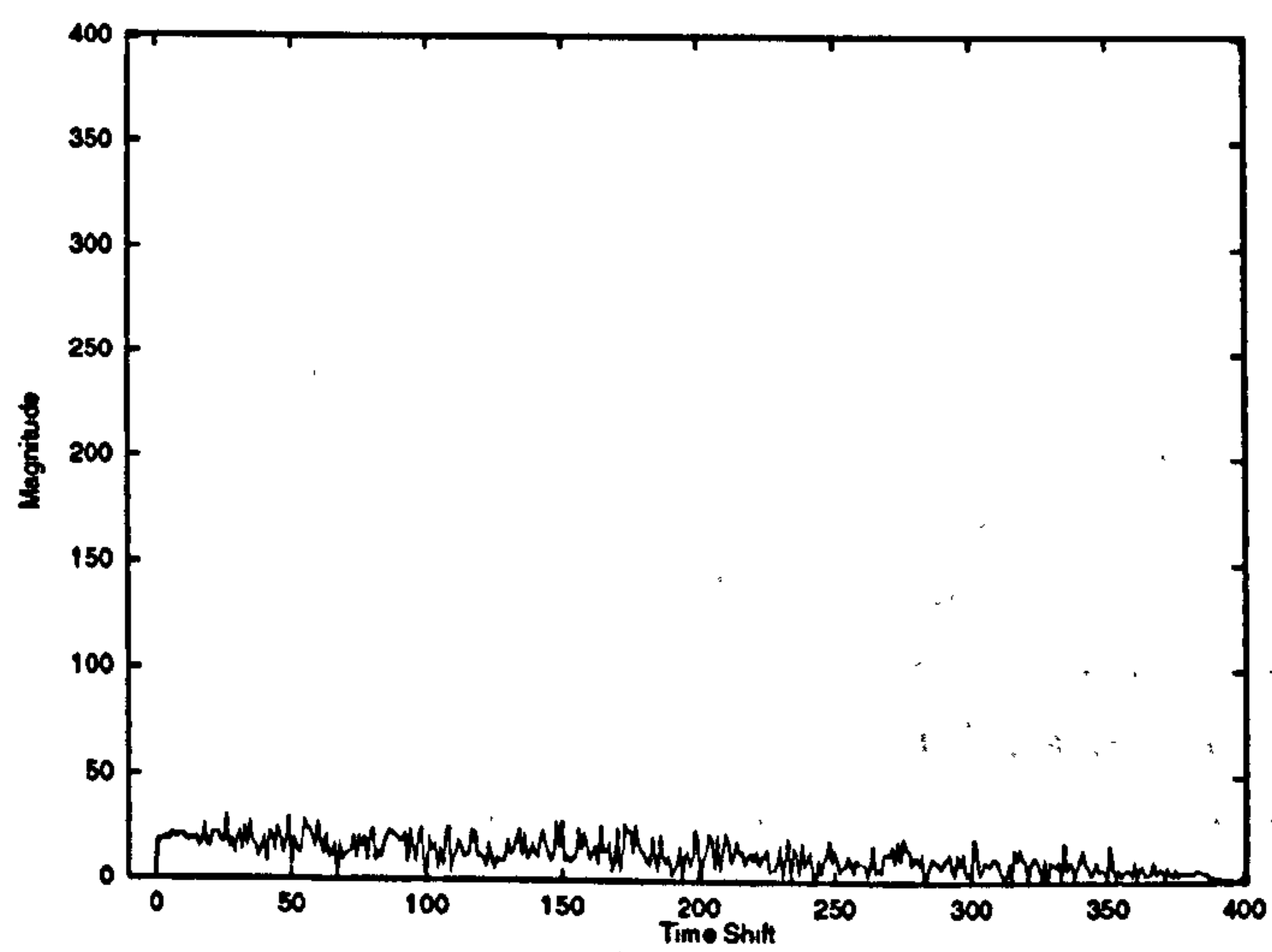


Figure 5.6: Nonperiodic CCF between $a^{(1)}$ and $a^{(99)}$

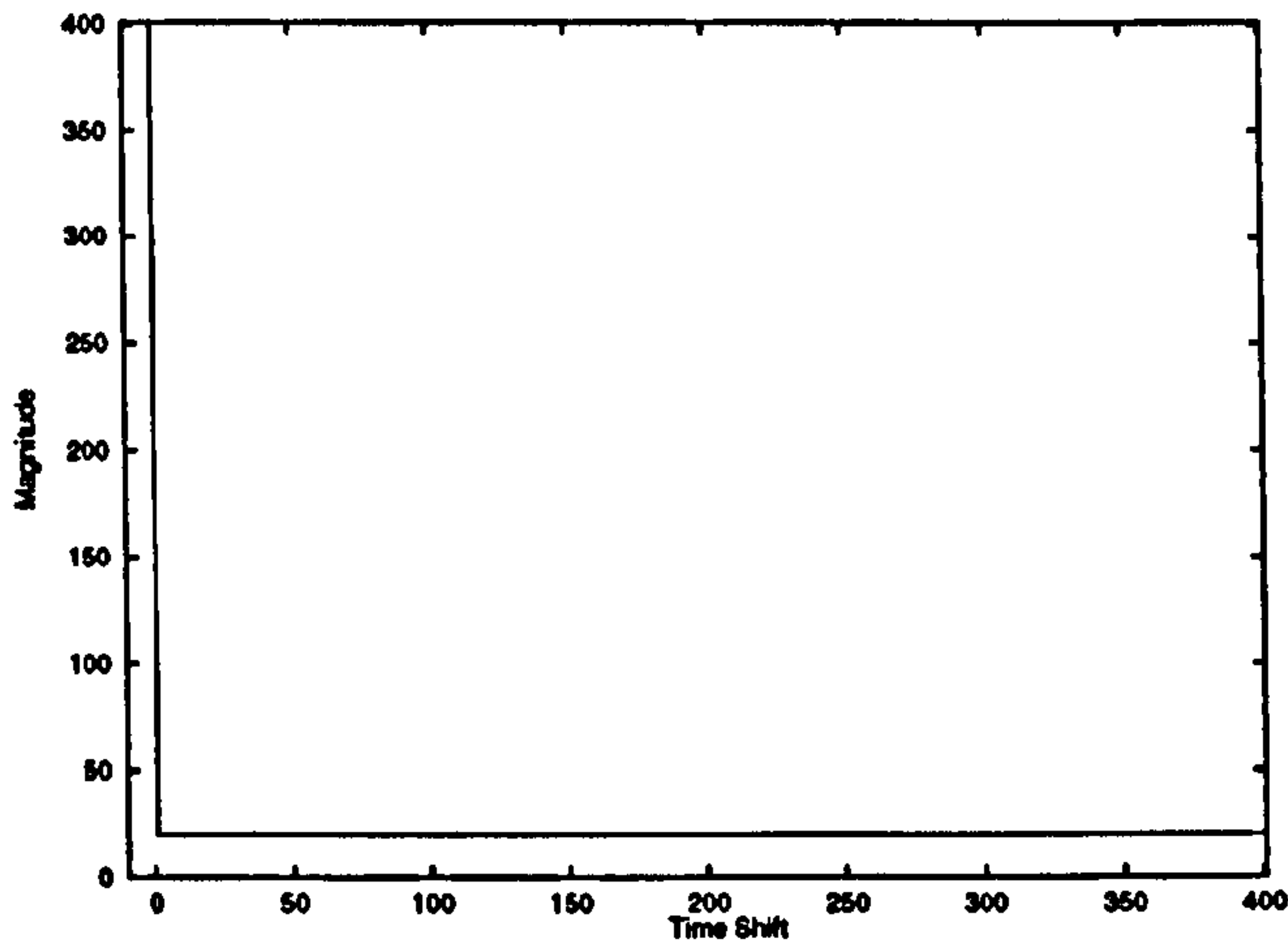


Figure 5.7: Periodic ACF of $a^{(0)}$

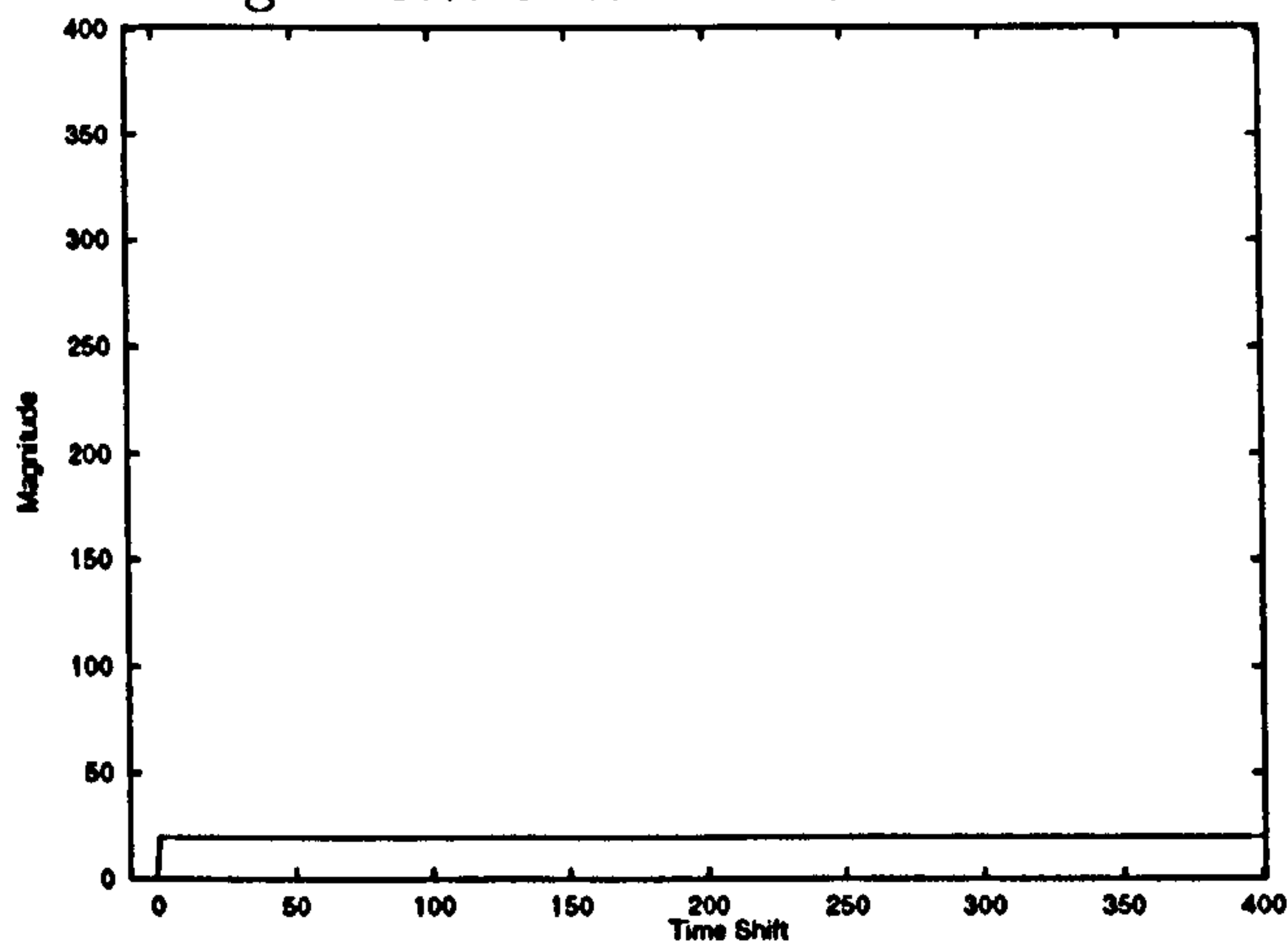


Figure 5.8: Periodic CCF bt. $a^{(0)}, a^{(1)}$

5.5 Concluding Remarks

A new class of polyphase sequences with nearly minimal periodic correlation magnitudes has been proposed in this chapter. For any given prime length $L > 3$, there are L polyphase sequences. It is proved that the out-of-phase periodic ACFs and CCFs of the sequences are constant and equal to $\sqrt{L}$. In addition, sequences of the same length are mutually orthogonal and the periodic correlation values asymptotically reach the Sarwate bound. It is also shown that the nonperiodic and periodic ACFs/CCFs of the new sequences have nearly the same peak magnitude. For $L > 5$, the maximum nontrivial correlation parameter C_{max} of the new sequences is lower than that of Scholtz-Welch sequences.

Chapter 6

Codes for Asynchronous SSMA Systems—II

6.1 Introduction

In a p -ary PSK modulation format, the symbols can be represented by the complex p -th roots of unity, with the binary case ($p = 2$) being used most often in practice. Accordingly, the design of constant magnitude polyphase sequences has been extensively considered, e.g. (Frank & Zadoff, 1962; Chu, 1972; Milewski, 1983; Zhang & Golomb, 1993; Scholtz & Welch, 1978; Alltop, 1980; Lüke, 92; Kumar & Moreno, 1991; Fan *et al.*, 1994b; Fan *et al.*, 1994d). However, there is relatively little work on sequence design applicable to QAM signal formats. By introducing a two-dimensional modular distance, termed the Mannheim distance, Huber showed how block codes over Gaussian integers can be used for coding over a QAM signal space (Huber, 1994). Egri and Horrigan constructed a finite multiplicative group of complex integers and gave an application of the group to differential detection of 16 QAM signals (Egri & Horrigan, 1994).

In this chapter, we consider maximal length sequences (m-sequences) over Gaussian integers that can be used with QAM modulation; here the sequence symbols are also required to be complex numbers, but their magnitudes are not all constant. First, some general properties of m-sequences over Gaussian integers are discussed. Then two sub-classes of m-sequences with quasi-perfect periodic autocorrelations are obtained (Fan & Darnell, 1994c). The CCFs between decimated m-sequences over Gaussian integers are also studied. Finally, by applying a simple operation, some m-sequences over rational and Gaussian integers are transformed into perfect sequences with impulsive ACFs (Darnell *et al.*, 1994).

6.2 Gaussian Prime Residue Classes and Galois Fields

Gaussian integers are those complex numbers which have integer real and imaginary parts. Let G be the set of all Gaussian integers. If $\gamma = g_1 + ig_2 \in G$, where $i^2 = -1$, then $\gamma^* = g_1 - ig_2$ is the complex conjugate of γ . The norm of a Gaussian integer $\gamma = g_1 + ig_2$ is defined by $N(\gamma) = g_1^2 + g_2^2 = \gamma \cdot \gamma^*$. There are four *unities*, i.e., elements of G which have norm 1, namely $\pm 1, \pm i$. The elements $\pm\gamma, \pm i\gamma$ are called the *associates* of γ . A *Gaussian prime* is a Gaussian integer which is not 0 or a unity and is not divisible by any number except the unities and their associates. Thus $1 + i$ and its associates, the rational primes p with $p \equiv 3 \pmod{4}$ and their associates, and the factor $\pi = g_1 + ig_2$ of the rational primes $p = g_1^2 + g_2^2 = (g_1 + ig_2)(g_1 - ig_2) = \pi \cdot \pi^*$ with $p \equiv 1 \pmod{4}$ are all Gaussian primes. The fundamental theorem of number theory for the Gaussian integers takes the following form: any integer γ , not 0 or a unity, can be expressed uniquely as a product of Gaussian primes, apart from the order of the primes, the presence of unities, and ambiguities between associated primes (Hardy & Wright, 1979).

Let G_π be the residue class of G modulo π ; then the modulo function $\mu : G \rightarrow G_\pi$ is defined as

$$\mu(g) = g \bmod \pi = \gamma = g - \left\lfloor \frac{g \cdot \pi^*}{\pi \cdot \pi^*} \right\rfloor \cdot \pi; \quad g \in G, \gamma \in G_\pi. \quad (6.1)$$

Note that $[g] = [g_1 + ig_2] = [g_1] + i[g_2]$ denotes rounding of the complex number g . For example, for Gaussian primes $2 + i$ obtained from rational prime $5 \equiv 1 \pmod{4}$, and $3i$, obtained from rational prime $3 \equiv 3 \pmod{4}$, the corresponding Gaussian residue classes are given by $G_{2+i} = \{0, 1, i, -1, -i\}$, $G_{3i} = \{0, 1, 1 + i, -i, 1 - i, -1, -1 - i, i, -1 + i\}$.

Theorem 19 (Hardy & Wright, 1979) *For Gaussian primes π , obtained from rational primes $p \equiv 1 \pmod{4}$, the modulo function μ defines a bijective mapping from $GF(p)$ into a two-dimensional signal space $\mu : GF(p) \rightarrow G_\pi$*

$$\mu(k) = k \bmod \pi = \gamma = k - \left\lfloor \frac{k \cdot \pi^*}{p} \right\rfloor \cdot \pi, \quad (6.2)$$

$$k = \mu^{-1}(\gamma) \equiv \gamma \cdot (v\pi^*) + \gamma^* \cdot (u\pi) \bmod p, \quad (6.3)$$

where u, v fulfill $1 = u \cdot \pi + v \cdot \pi^*$, which can be calculated by using the extended Euclidean algorithm for Gaussian integers (Huber, 1994).

Theorem 20 (Hardy & Wright, 1979) *For Gaussian primes π , obtained from $p \equiv 3 \pmod{4}$, it can be shown that there is an isomorphism between $GF(p^2)$ and $G_{i\pi}$ where*

$$G_{i\pi} = \left\{ k + i l \mid k, l \in \left\{ -\frac{p-1}{2}, \dots, -1, 0, 1, \dots, \frac{p-1}{2} \right\} \right\}. \quad (6.4)$$

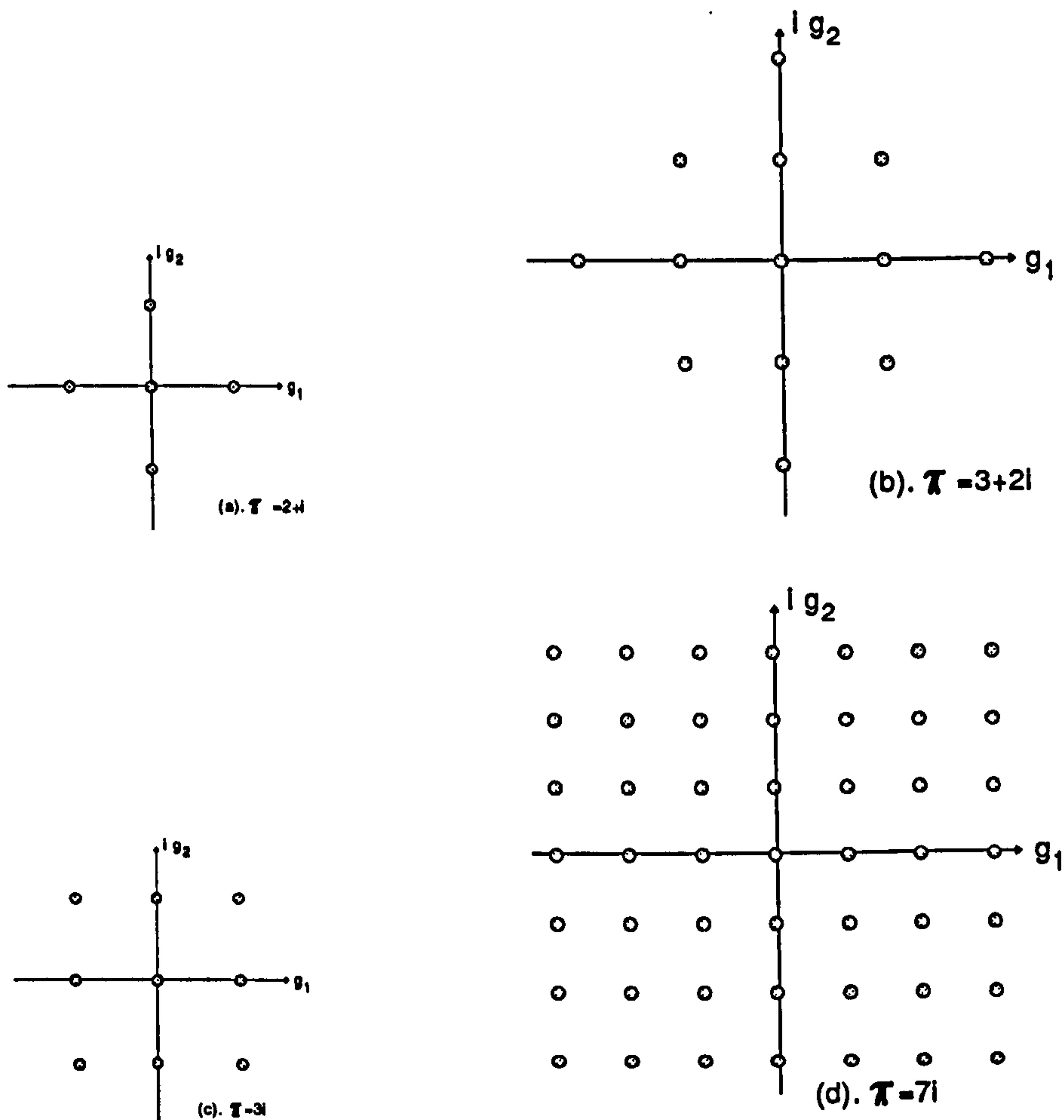


Figure 6.1: Signal Constellation for $\pi = 2 + i, 3 + 2i, 3i, 7i$ ($p = 5, 13, 3, 7$)

In Figure 6.1, the sets G_π obtained from the primes $\pi = 3i, 2 + i, i7, 3 + 2i$ ($p = 3, 5, 7, 13$) are displayed as points in the complex plane. With coding for communication over G_π channels in mind, these two-dimensional visualisations of G_π in communication terms are called signal constellations (Huber, 1994). In Table 6.1- 6.4, the exponent tables of corresponding fields are given.

Table 6.1: Exponent Table of Field G_{3i}

s	α^s	s	α^s	s	α^s	s	α^s
0	1	2	-i	4	-1	6	i
1	1+i	3	1-i	5	-1-i	7	-1+i

Table 6.2: Exponent Table of Field G_{2+i}

s	α^s	s	α^s	s	α^s	s	α^s
0	1	1	i	2	-1	3	-i

Table 6.3: Exponent Table of Field G_{7i}

s	α^s	s	α^s	s	α^s	s	α^s
0	1	12	-i	24	-1	36	i
1	1+2i	13	2-i	25	-1-2i	37	-2+i
2	-3-3i	14	-3+3i	26	3+3i	38	3-3i
3	3-2i	15	-2-3i	27	-3+2i	39	2+3i
4	-3i	16	-3	28	3i	40	3
5	-1-3i	17	-3+i	29	1+3i	41	3-i
6	-2+2i	18	2+2i	30	2-2i	42	-2-2i
7	1-2i	19	-2-i	31	-1+2i	43	2+i
8	-2	20	2i	32	2	44	-2i
9	-2+3i	21	3+2i	33	2-3i	45	-3-2i
10	-1-i	22	-1+i	34	1+i	46	1-i
11	1-3i	23	-3-i	35	-1+3i	47	3+i

Table 6.4: Exponent Table of Field G_{3+2i}

s	α^s	s	α^s	s	α^s	s	α^s
0	1	3	-i	6	-1	9	i
1	1+i	4	1-i	7	-1-i	10	-1+i
2	2i	5	2	8	-2i	11	-2

Although $GF(p)$ (or $GF(p^2)$) and G_π are mathematically equivalent, the two dimensional elements in G_π can be designed to match the signal constellation in QAM modulation directly; therefore significant signal design advantages can be obtained.

6.3 Properties of M-Sequences over Gaussian Integers

Definition 14 Let $h(x) = x^n + h_{n-1}x^{n-1} + \dots + h_1x + h_0$, $h_i \in G_\pi$, denote a primitive polynomial of degree n over G_π . An m -sequence $\mathbf{a} = \{a_i\}$ is defined over G_π by

$$a_{n-i} = -h_{n-1}a_{n-i-1} - \dots - h_1a_{i+1} - h_0a_i. \quad (6.5)$$

Here the subtraction and addition are carried out modulo Gaussian prime π . From this it follows that the sequence $\mathbf{a}$ can be generated, in a similar way to a conventional p -ary m -sequence, by an n -stage linear Feedback Shift Register (FSR) which has a feedback tap of weight h_i connected to the i th stage when $h_i \neq 0$.

From the relationship between $GF(p)$ (or $GF(p^2)$) and G_π , it can be shown that the above sequence has the following properties which are similar to those of an m -sequence over $GF(p)$ (or $GF(p^2)$) (MacWilliams & Sloane, 1976):

1. The period of $\mathbf{a}$ is $L = p^n - 1$ (or $p^{2n} - 1$).
2. There are exactly L nonzero sequences generated by $h(x)$, and they are simply the L different phases of $\mathbf{a}$.
3. A shift-and-add property: $T^i\mathbf{a} + T^j\mathbf{a} = T^k\mathbf{a}$, where T denotes an operator which shifts sequence cyclically to the left by one symbol; i, j, k are distinct integers and $0 \leq i, j, k < L$.
4. Each non-zero n -tuple appears exactly once in each period.
5. The number of occurrences of each non-zero element in each period is p^{n-1} (or $p^{2(n-1)}$); the number of zeros is $p^{n-1} - 1$ (or $p^{2(n-1)} - 1$).
6. Sampling $\mathbf{a} = \{a_i\}$ with each f in turn, $(f, L) = 1$, $1 \leq f \leq L - 1$, will produce all m -sequences of period L over G_π and no others. The number of different m -sequences of period L is $\frac{\Phi(L)}{n}$, where $\Phi(\cdot)$ is Euler's totient function.

In addition, we have the following particular properties of m -sequences over Gaussian integers:

1. Each period of sequence can be partitioned into four subsequences (their order may vary), i.e. $\mathbf{a} = (\alpha, -i\alpha, -\alpha, i\alpha)$, $\alpha = (a_0, \dots, a_{\frac{L}{4}-1})$. Thus $\sum_{k=0}^{L-1} a_k = 0$.
2. Each period of the periodic autocorrelation function can be partitioned into four parts (their order may vary), i.e. $\mathbf{R} = (\beta, i\beta, -\beta, -i\beta)$, $\beta = (R(0), \dots, R(\frac{L}{4}-1))$, $R(l) = \sum_{k=0}^{L-1} a_k a_{k+l}^*$, where the subscript addition is performed modulo L .
3. If $p \equiv 1 \pmod{4}$, $\frac{L}{4} \equiv d \pmod{p}$, then β has d nonzero elements at positions $k(p+1)$, $k = 0, 1, \dots, d-1$, and $\frac{L}{4} - d$ zero elements at the remaining positions.
4. If $p \equiv 3 \pmod{4}$, $\frac{L}{4} \equiv d' \pmod{p^2}$, then β has $d = \lceil \sqrt{d'} \rceil$ nonzero elements at positions $k\frac{L}{4d}$, $k = 0, 1, \dots, d-1$, and $\frac{L}{4} - d$ zero elements at the remaining positions.

Table 6.5: Examples of Primitive Polynomials $f(x)$ over G_π

Primitive Polynomial $f(x)$ over G_π	π	Length L
$f(x) = x^2 + x - i$	$2 + i$	24
$f(x) = x^3 + ix^2 + x - i$	$2 + i$	124
$f(x) = x^4 - x^3 - ix^2 - x - i$	$2 + i$	624
$f(x) = x^2 + x - (1 + i)$	$3i$	80
$f(x) = x^3 + x^2 - x - (1 + i)$	$3i$	728
$f(x) = x^2 + x + 2$	$3 + 2i$	168
$f(x) = x^2 + x - (1 + 2i)$	$4 + i$	288
$f(x) = x^2 + x - (2 + i)$	$7i$	2400
$f(x) = x^2 + x - (3 + 2i)$	$11i$	14640

In Table 6.5, some examples of primitive polynomials over G_π are obtained with the help of computer calculation.

6.4 Complex M-Sequences with Good ACFs and CCFs

Note the fact that when $p = 5 \equiv 1 \pmod{4}$, $\frac{5^n-1}{4} \equiv 1 \pmod{5}$, and when $p = 3 \equiv 3 \pmod{4}$, $\frac{3^{2n}-1}{4} \equiv 2 \pmod{3^2}$, $\lceil \sqrt{2} \rceil = 1$; hence, from above discussion,

A computer study shows that the size of maximal connected set is only 2 for any m-sequences of length L over G_{2+i} , G_{3i} .

Example 2: For primitive polynomial $f(x) = x^2 + x - i$ over G_{2+i} , there are $\frac{\phi(L)}{n} = \frac{8}{2} = 4$ m-sequences of length $L = 5^2 - 1 = 24$, which means the sampling sequences obtained by the sampling $f_i \in \{1, 5, 7, 11, 13, 17, 19, 23\}$, $(f_i, L) = 1$, can be partitioned into 4 equivalent classes: $\{1, 5\}, \{7, 11\}, \{13, 17\}, \{19, 23\}$.

$$\begin{aligned} a[1] : & \{0, 1, -1, -1, i, -1, 0, -i, i, i, 1, i, 0, -1, 1, 1, -i, 1, 0, i, -i, -i, -1, -i\} \\ a[7] : & \{1, i, 1, -1, -1, 0, i, -1, i, -i, -i, 0, -1, -i, -1, 1, 1, 0, -i, 1, -i, i, i, 0\} \\ a[13] : & \{1, 1, -1, -i, -1, 0, -i, -i, i, -1, i, 0, -1, -1, 1, i, 1, 0, i, i, -i, 1, -i, 0\} \\ a[19] : & \{1, -i, 1, 1, -1, 0, i, 1, i, i, -i, 0, -1, i, -1, -1, 1, 0, -i, -1, -i, -i, i, 0\} \end{aligned}$$

Their ACFs and CCFs are:

$$\begin{aligned} R_1 : & \{20, 0, 0, 0, 0, 0, 20i, 0, 0, 0, 0, 0, -20, 0, 0, 0, 0, 0, -20i, 0, 0, 0, 0, 0\} \\ R_7 : & \{20, 0, 0, 0, 0, 0, -20i, 0, 0, 0, 0, 0, -20, 0, 0, 0, 0, 0, 20i, 0, 0, 0, 0, 0\} \\ R_{13} : & \{20, 0, 0, 0, 0, 0, 20i, 0, 0, 0, 0, 0, -20, 0, 0, 0, 0, 0, -20i, 0, 0, 0, 0, 0\} \\ R_{19} : & \{20, 0, 0, 0, 0, 0, -20i, 0, 0, 0, 0, 0, -20, 0, 0, 0, 0, 0, 20i, 0, 0, 0, 0, 0\} \\ R_{1,7} : & \{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\} \\ R_{1,13} : & \{8 - 8i, -8i, 0, -8, 8 - 8i, 4i, 8 + 8i, 8, 0, -8i, 8 + 8i, -4, \\ & -8 + 8i, 8i, 0, 8, -8 + 8i, -4i, -8 - 8i, -8, 0, 8i, -8 - 8i, 4\} \\ R_{1,19} : & \{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\} \\ R_{7,13} : & \{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\} \\ R_{7,19} : & \{4, -8 - 8i, 8i, 0, -8, -8 - 8i, -4i, -8 + 8i, 8, 0, 8i, -8 + 8i, \\ & -4, 8 + 8i, -8i, 0, 8, 8 + 8i, 4i, 8 - 8i, -8, 0, -8i, 8 - 8i\} \\ R_{13,19} : & \{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\} \end{aligned}$$

The maximal connected sets are: $\{1, 7\}, \{1, 19\}, \{7, 13\}, \{13, 19\}$. Obviously the size of maximal connected sets are all 2.

Similarly it can be shown that for primitive polynomial $f(x) = x^2 + x - (1 + i)$ over G_{3i} , there are $\frac{\phi(L)}{n} = \frac{32}{2} = 16$ m-sequences of length $L = 9^2 - 1 = 80$. The sampling sequences obtained by sampler f_i , can be partitioned into 16 equivalent classes: $\{1, 9\}, \{3, 27\}, \{7, 63\}, \{11, 19\}, \{13, 37\}, \{17, 73\}, \{21, 29\}, \{23, 47\}, \{31, 39\}, \{33, 57\}, \{41, 49\}, \{43, 67\}, \{51, 59\}, \{53, 77\}, \{61, 69\}, \{71, 79\}$. The equivalent sampler set $\{1, 3, 7, 11, 13, 17, 21, 23, 31, 33, 41, 43, 51, 53, 61, 71\}$ is divided into two subsets: $A = \{1, 13, 17, 21, 33, 41, 53, 61\}$ and $B = \{3, 7, 11, 23, 31, 43, 51, 71\}$. Sequences within one subset are correlated with each other, $R_{i,j} \neq 0$, $i, j \in A$ or B ; also each sequence in one set is uncorrelated with all the sequences in another set, $R_{i,j} = 0$, $i \in A$, $j \in B$. Thus the size of the maximal connected set is $M_{80} = 2$, e.g. $\{1, 3\}, \{1, 7\}, \{13, 7\}, \{13, 11\}, \dots$.

6.5 Perfect Sequences over Rational and Gaussian Integers

The sequence synthesis technique proposed in this section derives new perfect sequences with zero out-of-phase ACF from previously known multi-level and complex m-sequences with quasi-perfect ACFs properties (Darnell *et al.*, 1994).

In their basic form, p -level m-sequences comprise the rational integers $0, 1, 2, \dots, (p-1)$, where p is a prime. To derive a practical bipolar sequence from such an m-sequence, a level transformation is necessary. Examples of two appropriate level transformations are given in (Darnell, 1993b), i.e. integer and sinusoidal; both these transformations yield bipolar signals with useful periodic ACF properties. For $p > 2$, the transformed sequences will be of even length $(p^n - 1)$, where n is the number of stages in the equivalent p -level FSR generator; they will also have an inverse-repeat (IR) format in which the last $(p^n - 1)/2$ digits of the transformed sequence period are the simple inverse of the first $(p^n - 1)/2$ digits. For $p = 3$ and 5 , the integer level transformation gives bipolar IR sequences $A = \{a_j\}$ of length $L = 2N$ with quasi-perfect periodic ACFs of the form:

$$\theta_A(l) = \begin{cases} P, & l = 0 \\ -P, & l = N, \\ 0, & \text{otherwise.} \end{cases} \quad (6.8)$$

where P is a positive real number which is dependent upon p , n and the level transformation employed.

In last section, two sub-classes of complex m-sequences of length $L = 4N$ with the following quasi-perfect autocorrelation function have been obtained by letting $\pi = 2 + i$ and $\pi = 3i$, which correspond to $p = 5$ and $p = 3$ respectively.

$$\theta_A(l) = \sum_{k=0}^{L-1} a_k a_{k+l}^* = \begin{cases} P, & l = 0 \\ i P, & l = N \\ -P, & l = 2N \\ -i P, & l = 3N \\ 0, & \text{otherwise.} \end{cases} \quad (6.9)$$

To allow the synthesis of sequences with ideal periodic ACFs from the m-sequences introduced above, it is necessary to use the following results for ACF combination.

Theorem 22 *If two component multi-level sequences $A = \{a_j\}$ of period $L = 2N$ and $B = \{(-1)^j\}$ of period 2 are combined using digit-by-digit multiplication, the periodic ACF of the resulting composite sequence C , $\theta_C(l)$, is given by*

$$\theta_C(l) = \begin{cases} \theta_A(l), & l = 0 \bmod 2 \\ -\theta_A(l), & l = 1 \bmod 2 \end{cases} \quad (6.10)$$

where $\theta_A(l)$ is the periodic ACF of sequence A .

Proof:

$$\theta_C(l) = \sum_{j=0}^{2N-1} c_j c_{j+l} = \sum_{j=0}^{2N-1} (-1)^j a_j (-1)^{j+l} a_{j+l} = \sum_{j=0}^{2N-1} (-1)^l a_j a_{j+l} \quad (6.11)$$

$$= (-1)^l \theta_A(l) = \begin{cases} \theta_A(l), & l = 0 \bmod 2 \\ -\theta_A(l), & l = 1 \bmod 2 \end{cases} \quad (6.12)$$

If sequence A is chosen as a transformed p -level m-sequence with quasi-perfect ACF, and the length of this sequence A is exactly divisible by 2 to give an odd integer N , then due to the IR format of A , the digit-by-digit multiplication process yields a multi-level perfect sequence C' of period N : $C' = (c_0, c_1, \dots, c_{N-1})$.

Theorem 23 *If the two component complex sequences $A = \{a_j\}$ of period $L = 4N$ and sequence $B = \{(i)^j\}$ of period 4 are combined using digit-by-digit multiplication, the periodic ACF of the resulting composite sequence C is given by*

$$\theta_C(l) = \begin{cases} \theta_A(l), & l = 0 \bmod 4 \\ -i\theta_A(l), & l = 1 \bmod 4 \\ -\theta_A(l), & l = 2 \bmod 4 \\ i\theta_A(l), & l = 3 \bmod 4 \end{cases} \quad (6.13)$$

where $\theta_C(l)$ and $\theta_A(l)$ are the periodic ACFs of sequences A and C respectively.

Proof:

$$\theta_C(l) = \sum_{j=0}^{4N-1} c_j c_{j+l}^* = \sum_{j=0}^{2N-1} (i)^j a_j (-i)^{j+l} a_{j+l}^* = \sum_{j=0}^{2N-1} (-i)^l a_j a_{j+l}^* \quad (6.14)$$

$$= (-i)^l \theta_A(l) = \begin{cases} \theta_A(l), & l = 0 \bmod 4 \\ -i\theta_A(l), & l = 1 \bmod 4 \\ -\theta_A(l), & l = 2 \bmod 4 \\ i\theta_A(l), & l = 3 \bmod 4 \end{cases} \quad (6.15)$$

Similarly, if the complex sequence A is a quasi-perfect sequence of period $L = 4N$, where N is an odd number, then the sequence C synthesised has a perfect ACF. Let $C' = (c_0, c_1, \dots, c_{N-1})$, then C' is a perfect sequence of period N .

It should be noted that if the ACF of a quasi-perfect sequence is of the form

$$\theta_A(l) = \sum_{k=0}^{L-1} a_k a_{k+l}^* = \begin{cases} P, & l = 0 \\ -iP, & l = N \\ -P, & l = 2N \\ iP, & l = 3N \\ 0, & \text{otherwise} \end{cases} \quad (6.16)$$

then the sequence B should be chosen as $B = \{(-i)^j\}$ and the ACF of sequence C is given by $\theta_C(l) = (i)^l \theta_A(l)$.

Examples of the application of the above method will now be presented. Firstly, consider the ternary m-sequence obtained using the integer level transformation where the original m-sequence elements 0, 1 and 2 are transformed to the bipolar elements 0, +1 and -1 respectively (Darnell, 1993b); the values $p = 3$, $n = 3$ and $p^n - 1 = 26$ are chosen. Here 26 is exactly divisible by 2 to give 13, and thus the digit-by-digit combination technique can be used as follows:

$$A = (0, 1, 1, 1, 0, 0, -1, 0, -1, 1, -1, -1, 1, 0, -1, -1, -1, 0, 0, 1, 0, 1, -1, 1, 1, -1)$$

$$B = (1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1)$$

$$C = (0, -1, 1, -1, 0, 0, -1, 0, -1, -1, -1, 1, 1, 0, -1, 1, -1, 0, 0, -1, 0, -1, -1, -1, 1, 1)$$

$$C' = (0, -1, 1, -1, 0, 0, -1, 0, -1, -1, -1, 1, 1)$$

$$\theta_{C'} = (9, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

Secondly, consider a complex m-sequence of length $L = 5^3 - 1 = 124$ generated by primitive polynomial $h(x) = x^3 + ix^2 + x - i$ over G_{2+i} . If the initial state of the FSR is 1, 0, 0, a new perfect sequence C' can then be derived as follows:

$$A = \begin{pmatrix} 0, 0, 1, -i, i, -i, -i, 1, 1, -i, 1, i, 1, -i, -i, 0, -1, -1, -1, 1, 0, 1, 0, -1, 1, i, -i, -1, 0, -i, 1, \\ 0, 0, i, 1, -1, 1, 1, i, i, 1, i, -1, i, 1, 1, 0, -i, -i, -i, i, 0, i, 0, -i, i, -1, 1, -i, 0, 1, i, \\ 0, 0, -1, i, -i, i, i, -1, -1, i, -1, -i, -1, i, i, 0, 1, 1, 1, -1, 0, -1, 0, 1, -1, -i, i, 1, 0, i, -1, \\ 0, 0, -i, -1, 1, -1, -1, -i, -i, -1, -i, 1, -i, -1, -1, 0, i, i, i, -i, 0, -i, 0, i, -i, 1, -1, i, 0, -1, -i \end{pmatrix}$$

Chapter 7

Codes for Asynchronous SSMA Systems–III

7.1 Introduction

This chapter studies two important classes of perfect sequences, Frank sequences and Chu sequences (Heimiller, 1961; Frank & Zadoff, 1962; Heimiller, 1962; Frank, 1963; Suehiro & Hatori, 1988; Chu, 1972; Frank, 1973; Ipatov, 1979; Lewis & Kretschmer, 1982; Kretschmer Jr. & Gerlach, 1991; Zhang & Golomb, 1993; Popović, 1992). Frank sequences and Chu sequences are two classes of sequences with perfect periodic ACFs and optimum CCFs.

Barker was the first to study sequences with good nonperiodic correlations (Barker, 1953). Golomb and Scholtz extended Barker's work from the binary to the polyphase case and found a larger family of generalized Barker sequences which satisfy the original Barker constraint on nonperiodic autocorrelation (Golomb & Scholtz, 1965). In the early 1960's, Frank showed that Frank sequences also have very good nonperiodic ACFs for small q . Specifically, it appears that the maximum out-of-phase nonperiodic ACF value is $O(q)$ for Frank sequences of length q^2 (Zhang & Golomb, 1993). Antweiler and Bömer found that, by computer search, the merit factor and peak-to-side-peak ratios of Frank sequences and Chu sequences grow linearly with the square root of the length L of the sequences; also, the parameters of Frank sequences are better than those of Chu sequences (Antweiler & Bömer, 1990; Popovic, 1991a). However, this conclusion cannot be generalized by merely using exhaustive computer search. In a recent paper, Zhang and Golomb proved the important result that the maximum out-of-phase nonperiodic ACF of Golomb sequences (which are equivalent to Chu sequences when L is odd and $r = 1$; this chapter will adopt Golomb's definition due to its simplicity) is bounded by

$\sqrt{L/4.348}$ as L tends to infinity (Zhang & Golomb, 1993). Mow and Li also obtained this result independently (Mow & Li, 1992). Subsequently Fan *et al.* (Fan *et al.*, 1994e) proved that there exist other Golomb sequences of length L whose maximum out-of-phase value is bounded by $\sqrt{L/2.174}$. In this thesis, many interesting and important new analytical results are derived (Fan *et al.*, 1994e; Fan & Darnell, 1994a; Gabidulin *et al.*, 1994).

Although the correlation properties of Frank and Chu sequences are very good, it is noted that the number of Frank sequences and Chu sequences available for a given length L is relatively small. As mentioned earlier, in order to permit unambiguous message synchronization, to minimize co-channel interference, and to support a large number of simultaneous users, large families of sequences with good ACFs and small CCF values, are required in an asynchronous SSMA system. To meet this requirement, sets of combined Frank/Chu sequences, which contain a larger number of sequences than either of the two constituent sets, are considered (Fan *et al.*, 1994b). It is shown analytically that the CCFs are similar to those of the original sets with one exception, whilst the ACFs remain perfectly impulsive.

Based on Frank and Chu sequences, two classes of real-valued sequences with good periodic autocorrelation and crosscorrelation properties are also proposed (Fan & Darnell, 1994d). It is proved that these sequences have a periodic complementary property. For each of these complementary pairs, there is an uncorrelated mate. The sequences are also shown to have many other symmetric properties. It is conjectured that, for a given length L , the out-of-phase ACFs and CCFs of the proposed real-valued sequences are bounded by $O(c\sqrt{L})$.

In the following sections, we will first briefly review the periodic properties of Frank and Chu sequences and their generalizations; next the asymptotic nonperiodic ACFs of Frank and Chu sequences are investigated in detail; then combined Frank/Chu sequences are studied; lastly derived real-valued sequences are presented.

7.2 Periodic Correlations of Frank/Chu Sequences

Frank sequences $F = \{f^{(1)}, \dots, f^{(r)}, \dots, f^{(q-1)}\}$ are a class of polyphase sequences of length $L = q^2$, in which the q th roots of unity are the elements of the sequence $f^{(r)} = (f_0^{(r)}, f_1^{(r)}, \dots, f_{L-1}^{(r)})$, i.e.

$$f_n^{(r)} = f_{jq+k}^{(r)} = e^{\frac{i2\pi}{q}rkj}, \quad 0 \leq k, j < q; \quad (r, q) = 1 \quad (7.1)$$

where $0 \leq n \leq q^2 - 1$ and q is any integer.

For Chu sequences $C = \{c^{(1)}, \dots, c^{(r)}, \dots, c^{(L-1)}\}$, the elements of the sequence $c^{(r)} = (c_0^{(r)}, c_1^{(r)}, \dots, c_{L-1}^{(r)})$ of length L are given by

$$c_n^{(r)} = e^{\frac{i\pi}{L}r(n+1)n}, \quad 0 \leq n < L; \quad (r, L) = 1. \quad (7.2)$$

It has been shown that the periodic ACFs and CCFs of Frank sequences and Chu sequences are given respectively by (Frank & Zadoff, 1962; Chu, 1972; Suehiro & Hatori, 1988; Popović, 1992):

$$R_{f^{(r)}}(\tau) = \sum_{n=0}^{L-1} f_n^{(r)} f_{n+\tau}^{*(r)} = \begin{cases} L, & \tau = 0 \pmod{L}, \\ 0, & \tau \neq 0 \pmod{L}, \end{cases} \quad (7.3)$$

$$\begin{aligned} R_{f^{(r)}, f^{(s)}}(\tau) &= \sum_{n=0}^{L-1} f_n^{(r)} f_{n+\tau}^{*(s)} \\ &= \sqrt{L}, \quad \forall \tau, r \neq s, (r-s, q) = 1, q \text{ is odd}, \end{aligned} \quad (7.4)$$

$$R_{c^{(r)}}(\tau) = \sum_{n=0}^{L-1} c_n^{(r)} c_{n+\tau}^{*(r)} = \begin{cases} L, & \tau = 0 \pmod{L}, \\ 0, & \tau \neq 0 \pmod{L}, \end{cases} \quad (7.5)$$

$$\begin{aligned} R_{c^{(r)}, c^{(s)}}(\tau) &= \sum_{n=0}^{L-1} c_n^{(r)} c_{n+\tau}^{*(s)} \\ &= \sqrt{L}, \quad \forall \tau, r \neq s, (r-s, L) = 1, L \text{ is odd}. \end{aligned} \quad (7.6)$$

In 1988, Suehiro and Hatori presented a new general class of Frank sequences with the same ideal periodic ACFs and optimum periodic CCFs (Suehiro & Hatori, 1988):

$$s_n^{(r)} = b_k^{(r)} f_{jq+k}^{(r)} = b_k^{(r)} e^{\frac{i2\pi}{q}rkj}, \quad 0 \leq k, j < q; \quad (r, q) = 1 \quad (7.7)$$

where $b_k^{(r)}$, $0 \leq k < q$, are arbitrary complex numbers with absolute values of 1. Later, Gabidulin proposed another similar generalization (Gabidulin, 1993).

In 1992, Popović derived another general class of Chu sequences which also has ideal periodic ACFs and optimum periodic CCFs (Popović, 1992; Popović, 1994b; Popović, 1994a):

$$s_n^{(r)} = b_{n \bmod m}^r c_n^{(r)} = b_{n \bmod m}^r e^{\frac{i\pi}{L}r(n+1)n}, \quad 0 \leq n < L; \quad (r, L) = 1. \quad (7.8)$$

where $b_k^{(r)}$, $0 \leq k < m$, are also arbitrary complex numbers with absolute values of 1.

Obviously the generalized Frank and Chu sequences can be considered as modulated sequences obtained by modulating one of the corresponding original Frank and Chu sequences with complex numbers (information) of absolute value 1. Because of the fact that the ACF/CCF properties are not changed by this modulation process, both generalized Frank and Chu sequences are called modulatable sequences.

7.3 Nonperiodic Correlations of Frank/Chu Sequences

For Frank sequences, we have

Lemma 1

$$C_F^{(r)}(uq + v) = \begin{cases} q^2, & u = v = 0; \\ 0, & 1 \leq u \leq q - 1, v = 0; \\ -e^{i\frac{2\pi r(u+1)}{q}}, & 0 \leq u \leq q - 1, v = 1; \\ e^{i\frac{2\pi ru}{q}}, & 0 \leq u \leq q - 1, v = q - 1; \\ \frac{e^{i\frac{2\pi rv}{q}} - 1}{e^{-i\frac{2\pi r}{q}} - 1}, & u = 0, u = q - 1, \\ & 2 \leq v \leq q - 2; \\ \frac{2(1 - \cos \frac{2\pi rv(u+1)}{q})}{(e^{-i\frac{2\pi rv}{q}} - 1)(e^{-i\frac{2\pi r(u+1)}{q}} - 1)}, & 1 \leq u \leq q - 2, \\ -\frac{2(1 - \cos \frac{2\pi ruv}{q})}{(e^{-i\frac{2\pi rv}{q}} - 1)(e^{-i\frac{2\pi ru}{q}} - 1)}, & 2 \leq v \leq q - 2. \end{cases} \quad (7.9)$$

The proof of this lemma is given in Appendix B.1.

Furthermore for any Chu sequence with $(r, L) = 1$, it can be proved that

Lemma 2

$$C_C^{(r)}(\tau) = -\frac{\sin \frac{\pi r}{L} \tau^2}{\sin \frac{\pi r}{L} \tau}. \quad (7.10)$$

The proof of this is given in Appendix B.2. Lemma 2 reveals that $C(\tau)$ is a real function.

Based on the above results, it can be proved that Frank and Chu sequences have the following symmetric properties:

Lemma 3

Chu sequences:

$$c_k^{(r)} = c_k^{(L-r)*} \quad (7.11)$$

$$|C_C^{(r)}(\tau)| = |C_C^{(r)}(L - \tau)| \leq \tau, \quad 0 < \tau \leq (L + 1)/2 \quad (7.12)$$

$$C_C^{(r)}(\tau) = C_C^{(L-r)}(\tau) \quad (7.13)$$

Frank sequences:

$$f_{k+jq}^{(r)} = f_{k+jq}^{(q-r)*} \quad (7.14)$$

$$|C_F^{(r)}(\tau)| = |C_F^{(r)}(L - \tau)| \leq \tau, \quad 0 < \tau \leq (L + 1)/2 \quad (7.15)$$

$$|C_F^{(r)}(uq + v)| = |C_F^{(r)}(uq + (q - v))| \quad (7.16)$$

$$C_F^{(r)}(\tau) = C_F^{(q-r)*}(\tau) \quad (7.17)$$

The proof of this lemma is given in Appendix B.3.

Let the time shift be $\tau = uq + v$, $0 \leq u, v \leq q - 1$. Due to Lemma 1 and Lemma 3, the problem of finding the nonperiodic ACF of Frank sequences reduces to that of finding

$$|C_F^{(r)}(\tau)| = |C_F^{(r)}(uq + v)|, \quad 0 \leq u, v, r \leq \lfloor \frac{q}{2} \rfloor, \quad (r, q) = 1. \quad (7.18)$$

For the case of $r = 1$, we have

Theorem 24

$$|C_F^{(1)}(uq + v)| \leq \sqrt{\frac{2}{1 - \cos \frac{2\pi}{q}}} \quad (7.19)$$

The proof is given in Appendix B.4. The case of $r = q - 1$ can be deduced immediately from Lemma 3.

The asymptotic maximum out-of-phase autocorrelation value of sequence $\mathbf{a}$ is defined as

$$B = \max_{L \rightarrow \infty} |C(\tau)| = |C(I_m(L))|, \quad \tau = 1, 2, \dots, L - 1, \quad (7.20)$$

where the $I_m(L)$ is the value of τ ($0 < \tau < L$) which maximizes $|C(\tau)|$.

Theorem 25 *As q goes to infinity, the asymptotic nonperiodic ACF of a Frank sequence with $r = 1$ is given by*¹

$$B_F^{(1)} = \frac{q}{\pi}, \quad I_m(L) = uq + \frac{q}{2}, \quad u = 0, q - 1. \quad (7.21)$$

Proof: From the symmetric properties of Frank sequences and the proof of Theorem 24, the maxima of the out-of-phase nonperiodic ACF amplitude occur at $u = 0, q - 1$, $v = q/2$, and

$$\begin{aligned} |C_F^{(1)}(uq + v)| &\leq \sqrt{\frac{2}{1 - \cos \frac{2\pi}{q}}} \\ &= \sqrt{\frac{2}{1 - (1 - \frac{1}{2}(\frac{2\pi}{q})^2 + \frac{1}{24}(\frac{2\pi}{q})^4 - \frac{1}{720}(\frac{2\pi}{q})^6 + \dots)}} \\ &= \sqrt{\frac{q^2}{\pi^2 - \frac{\pi^4}{3q^2} + \frac{8\pi^6}{45q^4} - \dots}} \end{aligned} \quad (7.22)$$

which leads to the asymptotic result that, as q goes to infinity,

$$B_F^{(1)} = \lim_{q \rightarrow \infty} \sqrt{\frac{q^2}{\pi^2 - \frac{\pi^4}{3q^2} + \frac{8\pi^6}{45q^4} - \dots}} = \sqrt{\frac{q^2}{\pi^2}} = \frac{q}{\pi}. \quad (7.23)$$

Let us now examine the nonperiodic ACF of Frank sequences of odd length L and $r = \frac{q-1}{2}, \frac{q+1}{2}$.

It is simple to show that for any odd integer q , $(\frac{q \pm 1}{2}, q) = 1$. Therefore Frank sequences with $r = \frac{q-1}{2}, \frac{q+1}{2}$ exist for every odd length q^2 . In this case we have the following important result:

¹From (Antweiler & Bömer, 1990; Popovic, 1991a; Zhang & Golomb, 1993), it appeared that this was an unsolved problem. We became aware of the prior work for $r = 1$ by Turyn (Turyn, 1967) after the initial preparation of this thesis. Turyn's proof is slightly different from that given here.

Theorem 26

$$|C_F^{(\frac{q-1}{2})}(uq+v)| < 2\sqrt{\frac{1}{1-\cos\frac{\pi}{q}}}. \quad (7.24)$$

Similarly we have

Theorem 27 *As q goes to infinity, the asymptotic nonperiodic ACF of a Frank sequence with $r = \frac{q-1}{2}$ is bounded by*

$$B_F^{(\frac{L-1}{2})} < 2\sqrt{2}\frac{q}{\pi}, \quad I_m(L) = uq + 2, \quad u = \begin{cases} \frac{q-1}{2}, & q = 4k + 1; \\ \frac{q-3}{2}, & q = 4k + 3. \end{cases} \quad (7.25)$$

It would appear that the exact asymptotic value should be $B_F^{(\frac{L-1}{2})} = 2\frac{q}{\pi}$; however, the proof would appear extremely complicated. In comparison, the following results indicate the worst case which occurs at $r = 2$ for the nonperiodic ACF of Frank sequences of odd length L .

Theorem 28

$$|C_F^{(2)}(uq+v)| \leq \sqrt{2(1+\cos\frac{2\pi}{q})} \left(\frac{1-\cos\pi(1+\frac{1}{q})}{1-\cos\frac{2\pi}{q}} \right) \quad (7.26)$$

$$B_F^{(2)} = 2\frac{q^2}{\pi^2}, \quad I_m(L) = uq + v, \quad v = u = \frac{L-1}{2}. \quad (7.27)$$

Due to Lemma 2 and Lemma 3, the problem of finding the nonperiodic ACFs of Chu sequences reduces to that of finding $C_C^{(r)}(\tau)$ in the range of $1 \leq \tau \leq \frac{L-1}{2}$ and $1 \leq r \leq \frac{L-1}{2}$. Based on Lemma 2, we have the following asymptotic bounds:

Theorem 29

$$B_C^{(r)}(b) = 0.48\sqrt{\frac{b}{r}}L, \quad I_m(L) = \frac{(Lb-1)s_0}{r}, \quad r \geq 2, \quad 0 \leq \frac{b}{r} \leq 0.37, \quad (7.28)$$

where $b = f(r, k)$, $k \equiv L \pmod{r}$, $s_0 = \sqrt{\frac{z_0 r}{\pi b}}$ and $z_0 = 1.1655$.

The proof is given in Appendix B.7.

Theorem 30

$$B_C^{(r)} = \frac{L}{\pi} \left| \sin \left(\frac{\pi b}{r} \right) \right|, \quad I_m(L) = \frac{Lb - 1}{r}, \quad r \geq 2, \quad 0.5 \geq \frac{b}{r} \geq 0.37. \quad (7.29)$$

The proof is given in Appendix B.8.

Example: For any given integer $r \geq 2$, $(r, L) = 1$, L can be represented as $L = ar + k$, where a is an integer and $k \leq \lfloor \frac{r}{2} \rfloor$. If $2 \leq r \leq 20$, then $b = f(r, L) = f(r, k)$ can be obtained by using Euclid's algorithm as given in Table 7.1. Table 7.2 lists the bounds $B_C^{(r)} = \frac{L}{c}$ given by Theorems 29- 30. From the calculation of actual $B_C^{(r)}$ for large L , it is seen that the bounds obtained are quite tight.

Table 7.1: Illustration of $b = f(r, L)$, $(r, L) = 1$, $L = ar + k$, $r \leq 20$, $k \leq \lfloor r/2 \rfloor$

k	r																			
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
2				-2		-3		-4		-5		-6	-7		-8		-9			
3						-2	3		-3	4		-4	5		-5	6		-6	7	
4								-2		3		-3		4		-4		5		
5									-2	5		-5	3		-3	7	-7	4		
6											-2					3		-3		
7														-2	7	5	-5	-8	3	
8																-2		-7		
9																		-2	9	

Table 7.2: Illustration of c , $B_C^{(r)} = L/c$, $(r, L) = 1$, $r \leq 20$, $k \leq \lfloor r/2 \rfloor$

k	r																			
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
1	3.1	3.6	4.2	4.7	5.1	5.5	5.9	6.2	6.6	6.9	7.2	7.5	7.8	8.1	8.3	8.6	8.8	9.1	9.3	
2				3.3		3.2		3.2		3.2		3.2		3.2		3.2		3.2		
3						3.9	3.4		3.8	3.5		3.8	3.5		3.7	3.5		3.7	3.5	
4							4.4		4.0		4.3		4.0		4.3		4.1			
5									4.9	3.3	3.4	4.5			4.8	3.3	3.3	4.5		
6												5.3				5.0		5.2		
7														5.7	3.2	3.8	4.0	3.2	5.4	
8																6.1		3.4		
9																		6.4	3.2	

Note: The bound in bold face is computed by Eqn 7.29.

When $r = 1$, which is excluded from above derivation, we have the following result which is the same as in (Zhang & Golomb, 1993), but the derivation is simpler.

Theorem 31

$$B_C^{(1)} = \sqrt{L/4.34}, \quad I_m(L) = \sqrt{L/2.68}. \quad (7.30)$$

The proof is given in Appendix B.9. In addition, the following result (Fan *et al.*, 1994e) is proved in Appendix B.10.

Theorem 32 *If L is odd and $r = \frac{L-1}{2}$, then*

$$B_C^{(\frac{L-1}{2})} = \sqrt{L/2.17}, \quad I_m(L) = \sqrt{L/1.34}. \quad (7.31)$$

Furthermore, the maximum out-of-phase aperiodic ACF is bounded by $\sqrt{2}$ for all odd shifts in the range $0 < \tau \leq \frac{L-1}{2}$ and even shifts in the range $\frac{L+1}{2} \leq \tau < L-1$, as L tends to infinity.

Similar to Frank sequences, the worst case of Chu sequences occurs at $r = 2$:

Corollary 1

$$B_C^{(2)} = \frac{L}{\pi}, \quad I_m(L) = \frac{L \pm 1}{2}, \quad L = 2k + 1. \quad (7.32)$$

7.4 Combined Frank/Chu Sequences and their Characteristics

In order to obtain a larger set of sequences, we define the following combined sets of Frank/Chu sequences,

Definition 15 *The combined Frank/Chu sequences can be synthesised by the union of the sets of Frank sequences and Chu sequences of the same length:*

$$FC = \{ f^{(1)}, \dots, f^{(s)}, \dots, f^{(s')}, \dots, f^{(q-1)}; \\ c^{(1)}, \dots, c^{(r)}, \dots, c^{(r')}, \dots, c^{(L-1)} \}, \quad (7.33)$$

where $L = q^2$, $(s, q) = 1$, $(s', q) = 1$, $(s - s', q) = 1$, and $(r, L) = 1$, $(r', L) = 1$, $(r - r', L) = 1$.

Obviously the ACFs of the sequences in the set are exactly the same as those of the original Frank sequences and Chu sequences. The CCF is equal to $\sqrt{L}$ if both the sequences to be correlated are Frank sequences or both the sequences are Chu sequences. When one sequence is a Frank sequence and the other is a Chu sequence, we have.

Theorem 33 *The CCF between Frank sequence $f^{(s)}$ and Chu sequence $c^{(r)}$ of the same length $L = q^2$ is given by*

$$|R_{c^{(r)}, f^{(s)}}(\tau)| = \sqrt{L}, \quad r \neq s \pmod{q}; \quad (7.34)$$

$$|R_{c^{(s+hq)}, f^{(s)}}(\tau)| = \begin{cases} 0, & v \neq v_0 = \frac{q+1}{2}, \\ |g(h, s)|, & v = v_0 = \frac{q+1}{2}, \end{cases} \quad r = s \pmod{q}; \quad (7.35)$$

where $0 \leq h < q$, $\tau = uq + v$, and

$$g(h, s) = q \sum_{k=0}^{\frac{q-1}{2}-1} \alpha^{(s+hq)k(k+1)/2q - su(k+v_0)} + q \sum_{k=\frac{q-1}{2}}^{q-1} \alpha^{(s+hq)k(k+1)/2q - s(u+1)(k+v_0)}. \quad (7.36)$$

Proof: Let $n = jq + k$ and $\tau = uq + v$, $0 \leq j, k, u, v \leq q-1$, then the integer $n + \tau$ can be expressed as

$$n + \tau = (j + u + \epsilon)q + (k + v - \epsilon q) \quad (7.37)$$

where $\epsilon = 0$, if $k + v \leq q-1$, and $\epsilon = 1$, if $k + v \geq q-1$. Let $\alpha = e^{i2\pi/q}$, then $f_n^{(s)} = f_{jq+k}^{(s)} = \alpha^{skj}$, $c_n^{(r)} = \alpha^{r(n+1)n/2q}$. Thus

$$\begin{aligned} R_{c^{(r)}, f^{(s)}}(\tau) &= \sum_{n=0}^{L-1} c_n^{(r)} f_{n+\tau}^{*(s)} \\ &= \sum_{n=0}^{q^2-1} c_{jq+k}^{(r)} f_{(j+u+\epsilon)q+(k+v-\epsilon q)}^{*(s)} \\ &= \sum_{k=0}^{q-1} \sum_{j=0}^{q-1} \alpha^{r(jq+k)(jq+k+1)/2q} \alpha^{-s(j+u+\epsilon)(k+v-\epsilon q)} \\ &= \sum_{k=0}^{q-1} \alpha^{rk(k+1)/2q - s(u+\epsilon)(k+v-\epsilon q)} \sum_{j=0}^{q-1} \alpha^{jr(jq+2k+1)/2 - js(k+v-\epsilon q)} \\ &= \sum_{k=0}^{q-1} \alpha^{rk(k+1)/2q - s(u+\epsilon)(k+v)} \sum_{j=0}^{q-1} \alpha^{j(\frac{rq}{2} + rk + \frac{r}{2} - sk - sv)} \end{aligned} \quad (7.38)$$

The last equality is valid because $\alpha^{\pm cq} = 1$, c is any integer, and $\alpha^{j^2 r q/2} = e^{i\pi r j^2} = (-1)^{r j^2} = (-1)^{r j} = \alpha^{r j q/2}$. Let $l = \frac{r q}{2} + r k + \frac{r}{2} - s k - s v$, the above inner sum is equal to zero, if $l \neq 0$, and is equal to q , if $l = 0$. The equation $l = 0 \pmod{q}$ has a unique solution $k_0 = \frac{s v - r(1+q)/2}{r-s}$ if $r \neq s \pmod{q}$. That is

$$\sum_{j=0}^{q-1} \alpha^{j(\frac{r q}{2} + r k + \frac{r}{2} - s k - s v)} = \begin{cases} 0, & k \neq k_0 = \frac{s v - r(1+q)/2}{r-s} \\ q, & k = k_0 = \frac{s v - r(1+q)/2}{r-s}. \end{cases} \quad (7.39)$$

Therefore, if $r \neq s \pmod{q}$, we have

$$|R_{c(r), f(s)}(\tau)| = |\alpha^{r k_0 (k_0 + 1)/2q - s(u+c)(k_0+v)} q| = q = \sqrt{L}. \quad (7.40)$$

In the case of $r = s \pmod{q}$, the CCFs between Frank sequences and Chu sequences are given by

$$\begin{aligned} R_{c(s+hq), f(s)}(\tau) &= \sum_{n=0}^{L-1} c_n^{(s+hq)} f_{n+\tau}^{*(s)} \\ &= \sum_{k=0}^{q-1} \alpha^{(s+hq)k(k+1)/2q - s(u+c)(k+v)} \sum_{j=0}^{q-1} \alpha^{j s(\frac{q}{2} + \frac{1}{2} - v)}, \end{aligned} \quad (7.41)$$

where $h = 0, 1, \dots, q-1$ and

$$\sum_{j=0}^{q-1} \alpha^{j s(\frac{q}{2} + \frac{1}{2} - v)} = \begin{cases} 0, & v \neq v_0 = \frac{q+1}{2} \\ q, & v = v_0 = \frac{q+1}{2}. \end{cases} \quad (7.42)$$

Hence

$$\begin{aligned} R_{c(s+hq), f(s)}(\tau) &= \\ &= \begin{cases} 0, & v \neq v_0 = \frac{q+1}{2} \\ q \sum_{k=0}^{\frac{q-1}{2}-1} \alpha^{(s+hq)k(k+1)/2q - s u(k+v_0)} + \\ q \sum_{k=\frac{q-1}{2}}^{q-1} \alpha^{(s+hq)k(k+1)/2q - s(u+1)(k+v_0)}, & v = v_0 = \frac{q+1}{2}. \end{cases} \end{aligned} \quad (7.43)$$

As an example, the combined Frank/Chu sequences of length 25 are given below

$$FC = \{f^{(1)}, f^{(2)}, f^{(3)}, f^{(4)}; c^{(1)}, c^{(2)}, c^{(3)}, c^{(4)}\}. \quad (7.44)$$

The CCFs between any two sequences, $R_{c(r), c(s)}(\tau)$, $R_{f(r), f(s)}(\tau)$ and $R_{c(r), f(s)}(\tau)$ ($r \neq s \pmod{5}$), are constant and equal to 5. For the case of $r = s \pmod{5}$, the CCFs, $R_{c(s), f(s)}(\tau)$, are listed in Table 7.3.

Table 7.3: CCFs of Combined Frank/Chu Sequences(L=25, r=s mod 5)

τ	0	1	...																		23	24				
$ R_{c(1),f(1)}(\tau) $	0	0	0	24	0	0	0	0	4.4	0	0	0	0	1.8	0	0	0	0	1.8	0	0	0	0	4.4	0	0
$ R_{c(2),f(2)}(\tau) $	0	0	0	21	0	0	0	0	3.8	0	0	0	0	8.2	0	0	0	0	8.2	0	0	0	0	3.8	0	0
$ R_{c(3),f(3)}(\tau) $	0	0	0	18	0	0	0	0	6.2	0	0	0	0	11.	0	0	0	0	11.	0	0	0	0	6.2	0	0
$ R_{c(4),f(4)}(\tau) $	0	0	0	14	0	0	0	0	12.	0	0	0	0	8.8	0	0	0	0	8.8	0	0	0	0	12.	0	0

7.5 Derived Real-valued Sequences and their Characteristics

Definition 16 For any integers L, r and n , where $0 \leq n < L$, $(r, L) = 1$, L is an odd integer (the case of even L is omitted here for simplicity), the first class of real-valued sequences, $a^{(r)} = (a_0^{(r)}, a_1^{(r)}, \dots, a_{L-1}^{(r)})$ and $b^{(r)} = (b_0^{(r)}, b_1^{(r)}, \dots, b_{L-1}^{(r)})$, is defined as

$$a_n^{(r)} = \cos \frac{\pi r n(n+1)}{L} \quad \text{and} \quad b_n^{(r)} = \sin \frac{\pi r n(n+1)}{L}. \quad (7.45)$$

Definition 17 For any integers L, r, j and k , where $0 \leq n < L$, $0 \leq j, k < q$, $(r, q) = 1$ and $L = q^2$, the second class of real-valued sequences, $a^{(r)} = (a_0^{(r)}, a_1^{(r)}, \dots, a_{L-1}^{(r)})$ and $b^{(r)} = (b_0^{(r)}, b_1^{(r)}, \dots, b_{L-1}^{(r)})$, is defined as

$$a_n^{(r)} = a_{jq+k}^{(r)} = \cos \frac{2\pi r k j}{q}, \quad \text{and} \quad b_n^{(r)} = a_{jq+k}^{(r)} = \sin \frac{2\pi r k j}{q} \quad (7.46)$$

The above real-valued sequences have the following properties:

Lemma 4

$$a_n^{(r)} = a_n^{(L-r)}; \quad (7.47)$$

$$R_{a^{(r)}}(\tau) = R_{a^{(r)}}(L - \tau) \quad 0 < \tau \leq (L+1)/2. \quad (7.48)$$

$$R_{a^{(r)}a^{(s)}}(\tau) = R_{a^{(r)}a^{(s)}}(L - \tau) \quad 0 < \tau \leq (L+1)/2. \quad (7.49)$$

$$R_{a^{(r)}b^{(s)}}(\tau) = R_{a^{(r)}b^{(s)}}(L - \tau) \quad 0 < \tau \leq (L+1)/2. \quad (7.50)$$

The above symmetric properties also hold if $a^{(r)}$ is replaced with $b^{(r)}$.

Proof: For simplicity, we only prove the first two relations.

(1). Due to the fact that if $(r, L)=1$, then $(L-r, L)=1$; for the second class of real-valued sequences, we have

$$\begin{aligned} a_n^{(L-r)} &= \cos \frac{2\pi(q^2-r)kj}{q} = \cos \left[2\pi qkj - \frac{2\pi rkj}{q} \right] \\ &= \cos \frac{2\pi rkj}{q} = a_n^{(r)} \end{aligned} \quad (7.51)$$

Similarly, the relation is true for the first class of real-valued sequences.

(2). Note the fact that $R_{a^{(r)}}(\tau) = R_{a^{(r)}}(-\tau)$, then

$$\begin{aligned} R_{a^{(r)}}(L - \tau) &= R_{a^{(r)}}(\tau - L) \\ &= \sum_{n=0}^{L-1} a_n a_{n+(\tau-L)} \\ &= \sum_{n=0}^{L-1} \cos \frac{\pi r n(n+1)}{L} \cos \frac{\pi r (n+\tau-L)(n+\tau-L+1)}{L} \\ &= \sum_{n=0}^{L-1} \cos \frac{\pi r n(n+1)}{L} \cos \left[\frac{\pi r (n+\tau)(n+\tau+1)}{L} - \pi r (2n + 2\tau - L + 1) \right] \\ &= \sum_{n=0}^{L-1} \cos \frac{\pi r n(n+1)}{L} \cos \frac{\pi r (n+\tau)(n+\tau+1)}{L} \\ &= R_{a^{(r)}}(\tau) \end{aligned} \quad (7.52)$$

where $(2n + 2\tau - L + 1)$ is an even number because L is odd.

For the remainder of the relations, the proof is similar.

Definition 18 A pair of sequences $\{a, b\}$ of length L is said to be a periodic complementary pair if and only if their periodic autocorrelation functions sum to zero at every shift, except the zero shift; that is

$$R_a(\tau) + R_b(\tau) = \sum_{n=0}^{L-1} a_n a_{n+\tau} + \sum_{n=0}^{L-1} b_n b_{n+\tau} = \begin{cases} L', & \tau = 0, \\ 0, & \tau \neq 0. \end{cases} \quad (7.53)$$

Definition 19 Two complementary pairs, $\{a, b\}$ and $\{a', b'\}$, are termed uncorrelated mates if their periodic crosscorrelation values for corresponding sequences in each pair sum to zero at all corresponding time shifts; that is

$$R_{aa'}(\tau) + R_{bb'}(\tau) = \sum_{n=0}^{L-1} a_n a'_{n+\tau} + \sum_{n=0}^{L-1} b_n b'_{n+\tau} = 0 \quad (7.54)$$

The concept of binary complementary sequences was originally introduced by Golay (Golay, 1961). Here this concept is extended to include periodic complementary sequences. For the real-valued sequences defined above, it can be proved that

Theorem 34 $\{a^{(r)}, b^{(r)}\}$ is a pair of periodic complementary sequences, i.e.

$$R_a(\tau) + R_b(\tau) = \begin{cases} L, & \tau = 0, \\ 0, & \tau \neq 0. \end{cases} \quad (7.55)$$

Proof:

$$\begin{aligned} R_a(\tau) + R_b(\tau) &= \sum_{n=0}^{L-1} a_n a_{n+\tau} + \sum_{n=0}^{L-1} b_n b_{n+\tau} \\ &= \sum_{n=0}^{L-1} \cos \frac{\pi r n(n+1)}{L} \cos \frac{\pi r (n+\tau)(n+\tau+1)}{L} + \\ &\quad \sum_{n=0}^{L-1} \sin \frac{\pi r n(n+1)}{L} \sin \frac{\pi r (n+\tau)(n+\tau+1)}{L} \\ &= \sum_{n=0}^{L-1} \cos \frac{\pi r (2n\tau + \tau^2 + \tau)}{L} = \begin{cases} L, & \tau = 0, \\ 0, & \tau \neq 0. \end{cases} \end{aligned} \quad (7.56)$$

Furthermore, for every periodic complementary pair $\{a^{(r)}, b^{(r)}\}$, there is an uncorrelated mate $\{b^{(r)}, -a^{(r)}\}$; that is

Theorem 35

$$R_{ab}(\tau) + R_{b(-a)}(\tau) = 0 \quad (7.57)$$

Proof:

$$\begin{aligned}
 R_{ab}(\tau) + R_{b(-a)}(\tau) &= \sum_{n=0}^{L-1} a_n b_{n+\tau} - \sum_{n=0}^{L-1} b_n a_{n+\tau} \\
 &= \sum_{n=0}^{L-1} \cos \frac{\pi r n(n+1)}{L} \sin \frac{\pi r (n+\tau)(n+\tau+1)}{L} - \\
 &\quad \sum_{n=0}^{L-1} \sin \frac{\pi r n(n+1)}{L} \cos \frac{\pi r (n+\tau)(n+\tau+1)}{L} \\
 &= \sum_{n=0}^{L-1} \sin \frac{\pi r (2n\tau + \tau^2 + \tau)}{L} = 0
 \end{aligned} \tag{7.58}$$

In order to evaluate the practical usefulness of the real-valued sequences, many ACFs/CCFs for different sequence lengths were calculated. Specific examples are shown in Figs.(7.1- 7.32).

For the first class of real-valued sequences of length $L = 1001$, the periodic ACFs (PACFs) of $a^{(1)}$, $a^{(2)}$, $b^{(1)}$ and $b^{(2)}$ are shown in Figs.(7.1- 7.4); the periodic CCFs (PCCFs) between $a^{(1)}$ and $a^{(2)}$, $b^{(1)}$ and $b^{(2)}$, $a^{(1)}$ and $b^{(1)}$, $a^{(1)}$ and $b^{(2)}$, are shown in Figs.(7.5- 7.8). It is seen that the maximum periodic out-of-phase ACF is bounded by 15.9 and the maximum periodic CCF is bounded by 29.8. Figs.(7.9- 7.16) show the same periodic ACFs and CCFs for the second class of real-valued sequences of length $L = 31^2 = 961$. The maximum periodic out-of-phase ACF is bounded by 15.5 and the maximum periodic CCF is bounded by 30.9. An interesting phenomenon is that the maximum CCF between $a^{(r)}$ and $b^{(r)}$ has the same magnitude as the maximum out-of-phase ACF of $a^{(r)}$ or $b^{(r)}$. Obviously, the periodic ACFs/CCFs of the real-valued sequences discussed here are favourable.

Although it is extremely difficult to obtain the closed analytical form of the periodic ACFs/CCFs for the above real-valued sequences, based on our comprehensive computer simulations it can be conjectured that:

Conjecture 5 *For the real-valued sequences of length L , the maximum out-of-phase periodic ACF is asymptotic to $O(c_1\sqrt{L})$.*

Conjecture 6 *For the real-valued sequences of length L , the maximum magnitude of periodic CCF is asymptotic to $O(c_2\sqrt{L})$, $c_2 \leq 2c_1$.*

As is shown in Figs.(7.17- 7.32), their nonperiodic ACFs/CCFs (NACFs/NCCFs) are very similar to those of the original Frank and Chu sequences. The best NACF occurs when $r = 1$ and the worst NACF occurs when $r = 2$. However their NCCFs are normally good.

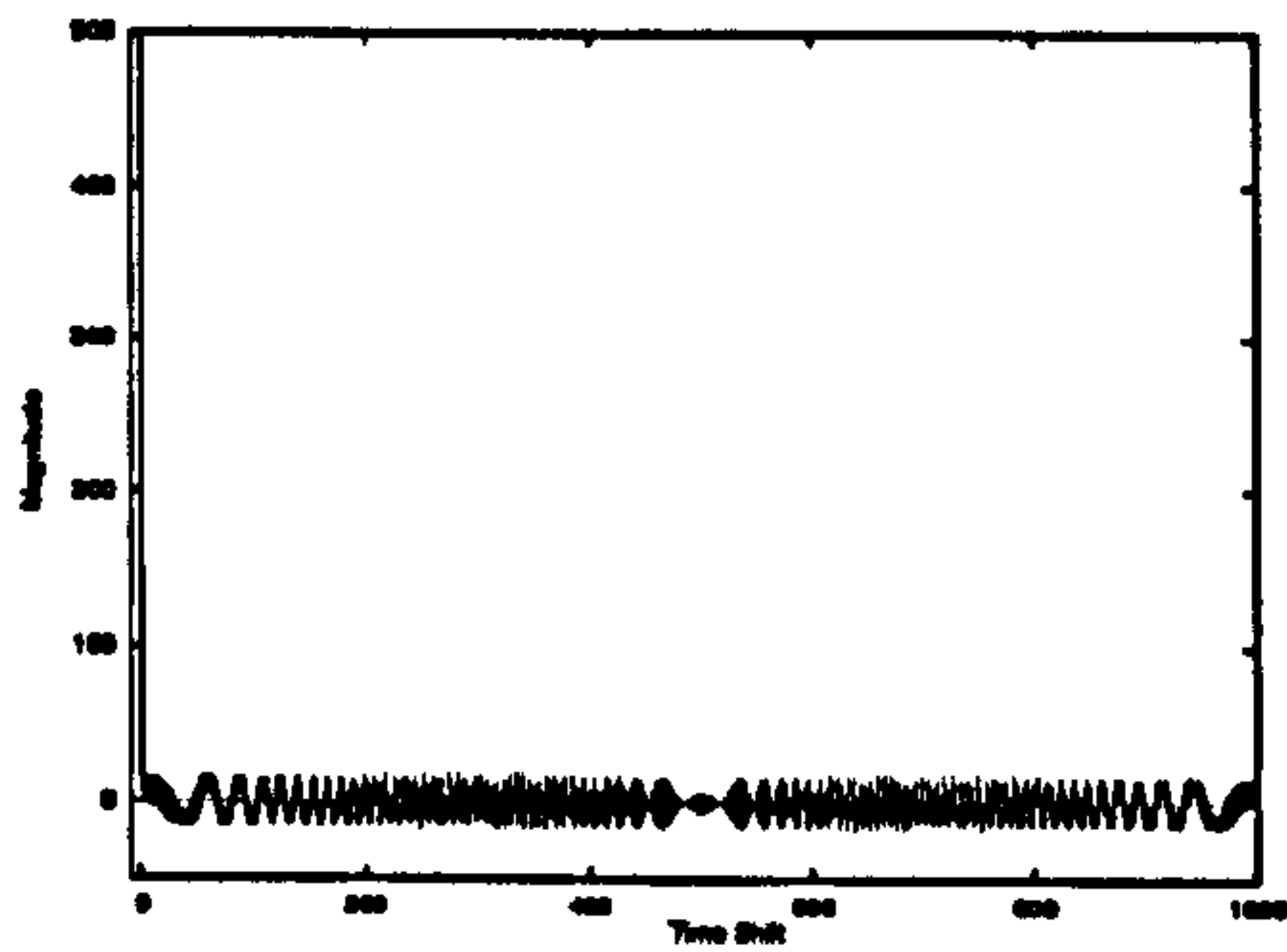


Figure 7.1: PACF of $a^{(1)}-I$

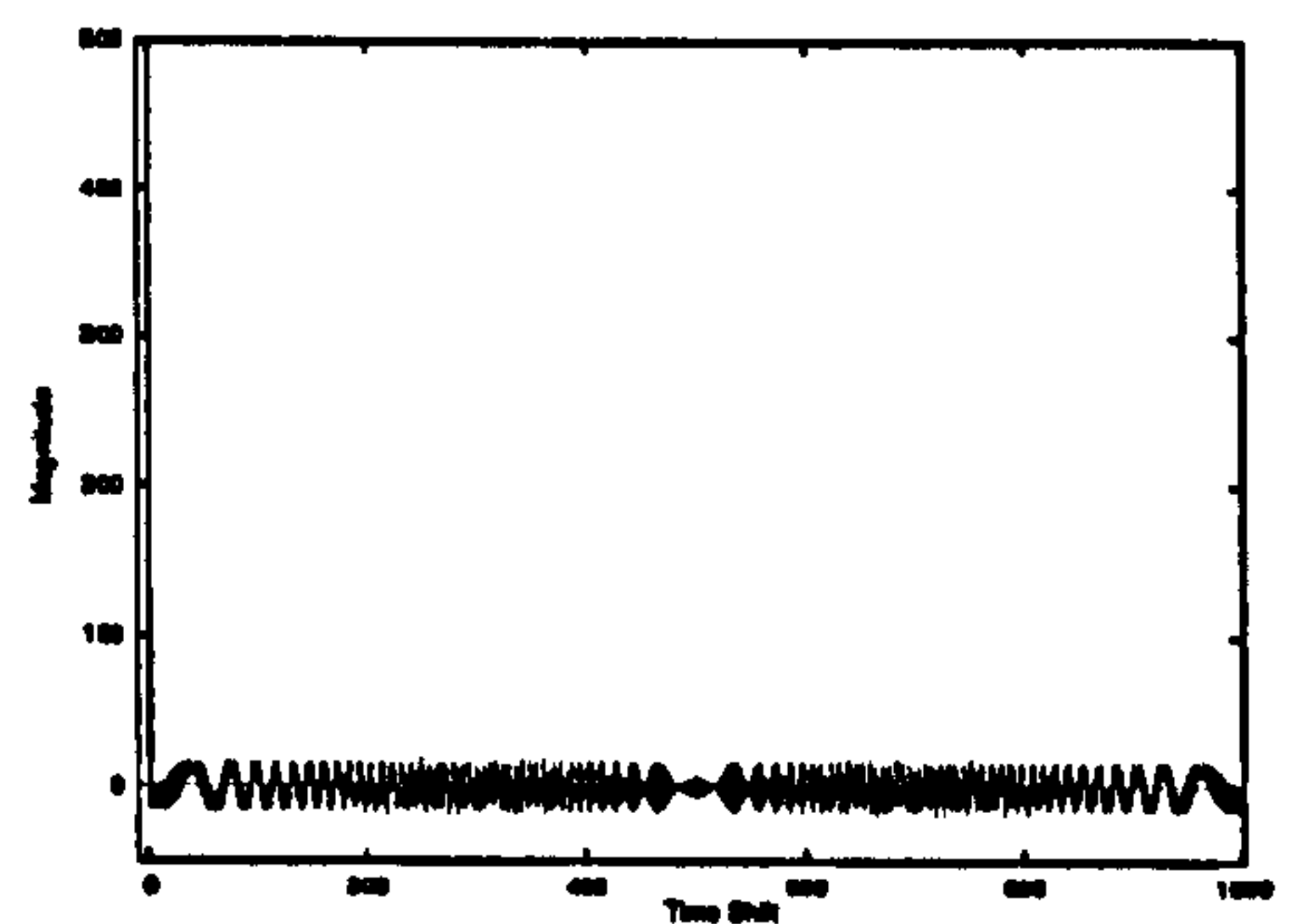


Figure 7.2: PACF of $b^{(1)}-I$

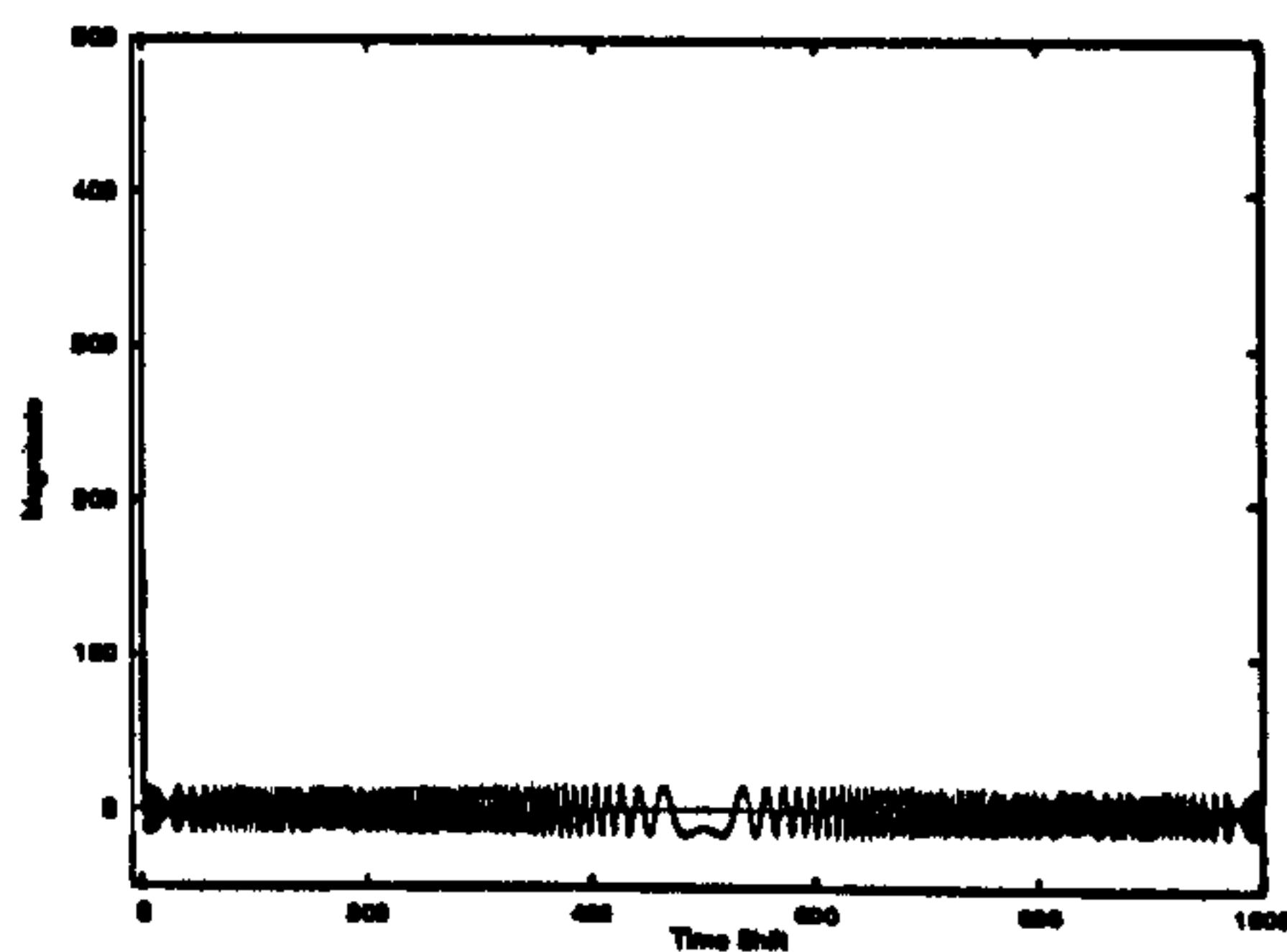


Figure 7.3: PACF of $a^{(2)}-I$

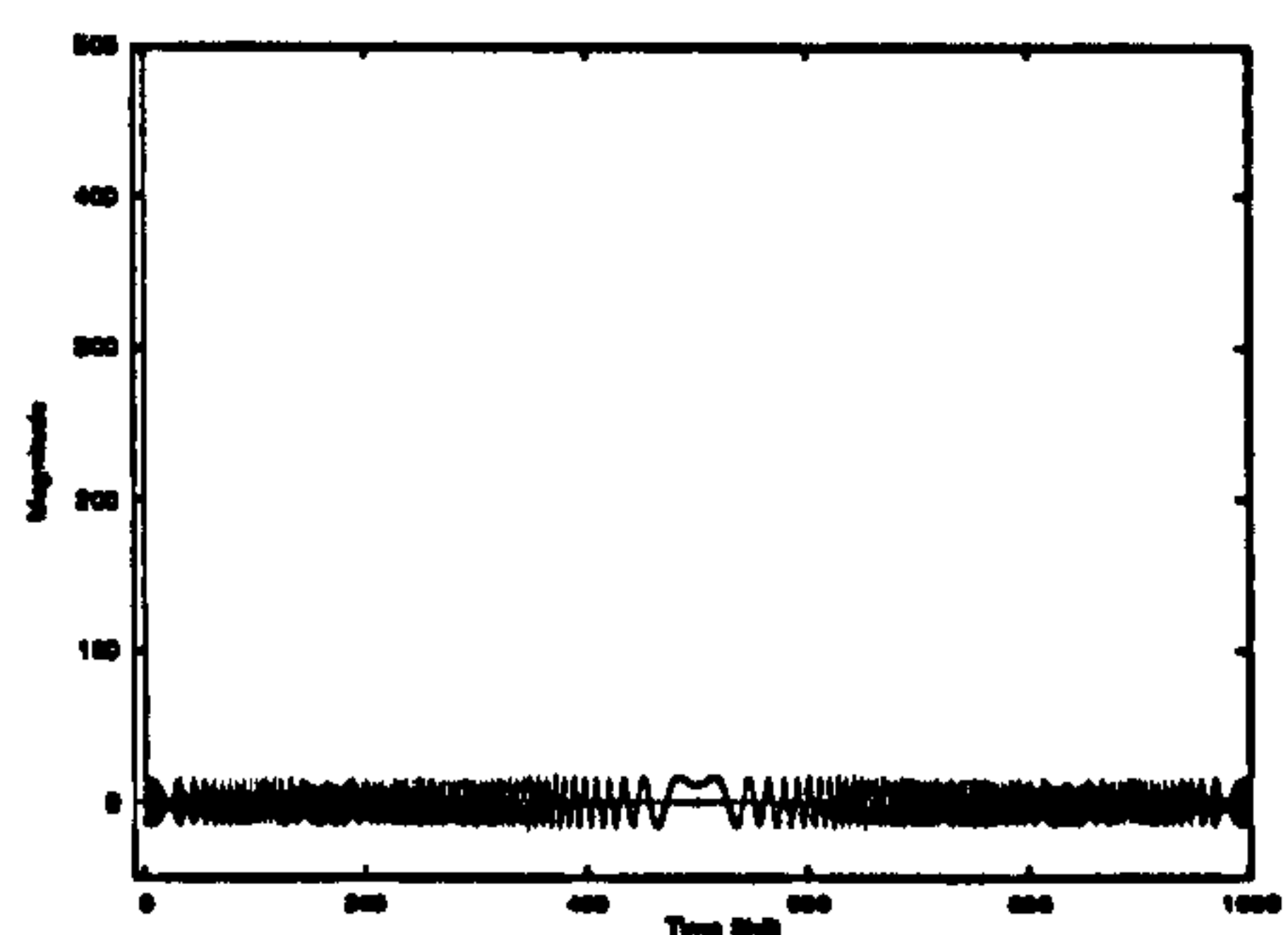


Figure 7.4: PACF of $b^{(2)}-I$

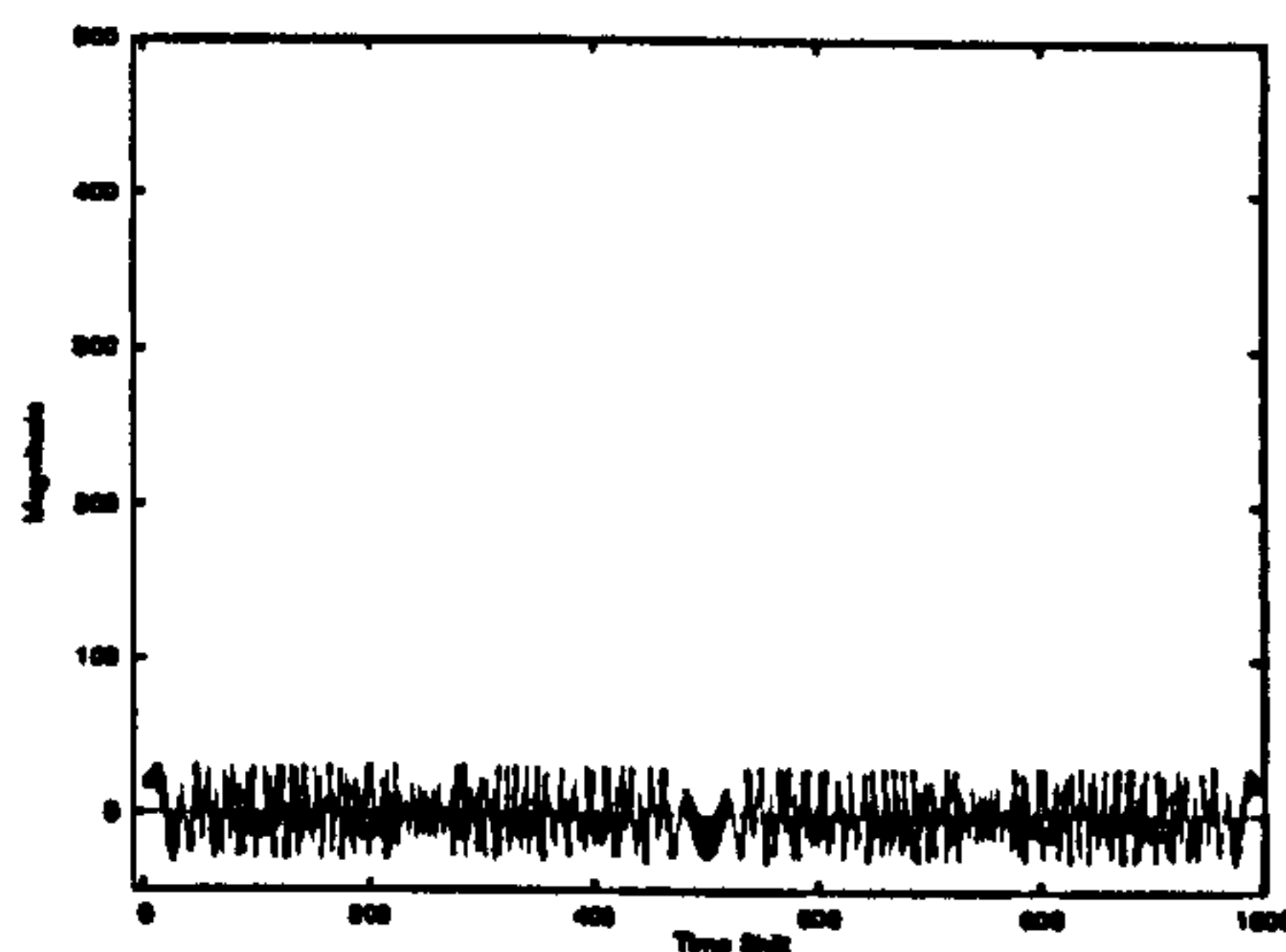


Figure 7.5: PCCF of $a^{(1)}, a^{(2)}-I$

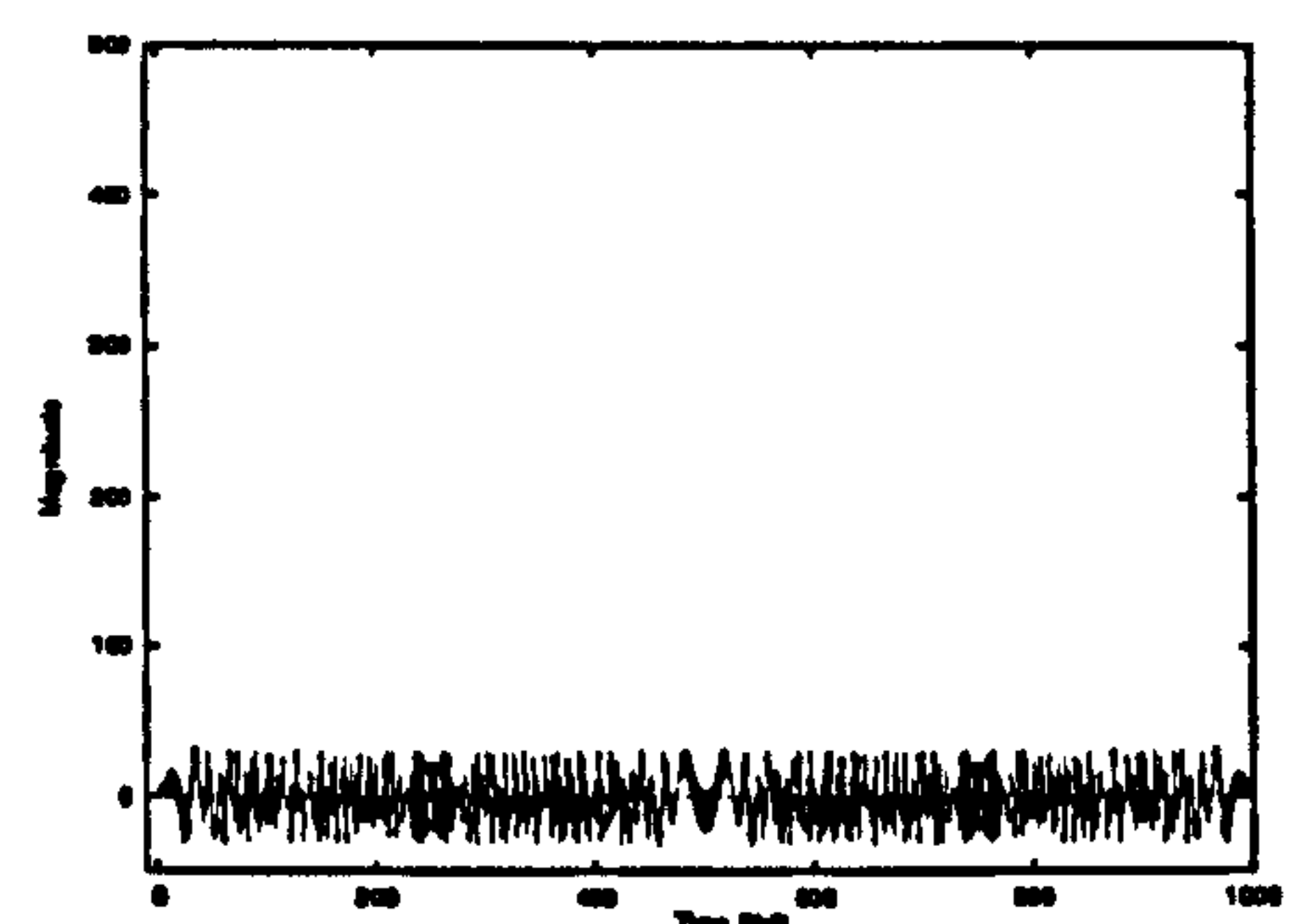


Figure 7.6: PCCF of $b^{(1)}, b^{(2)}-I$

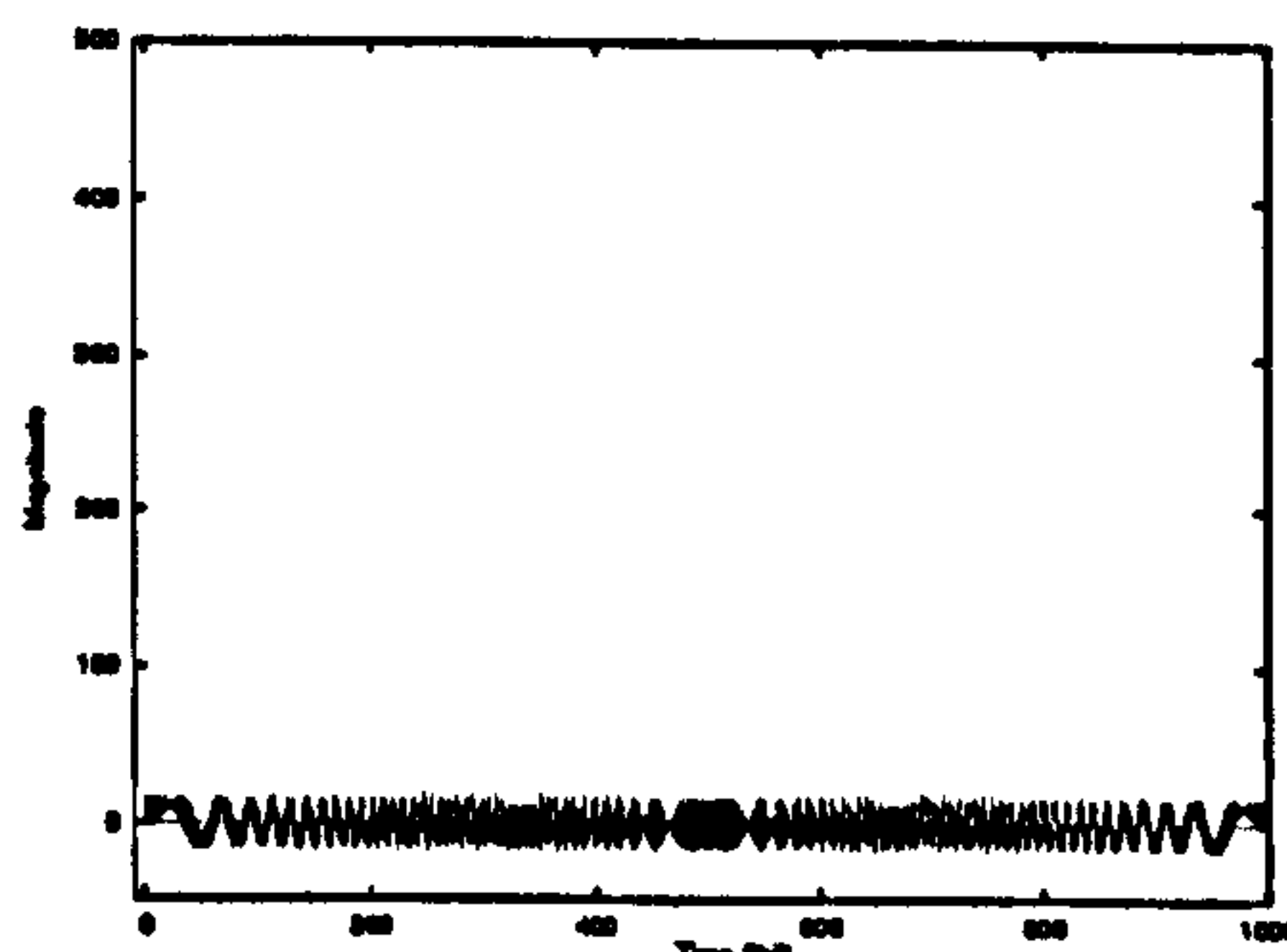


Figure 7.7: PCCF $a^{(1)}, b^{(1)}-I$

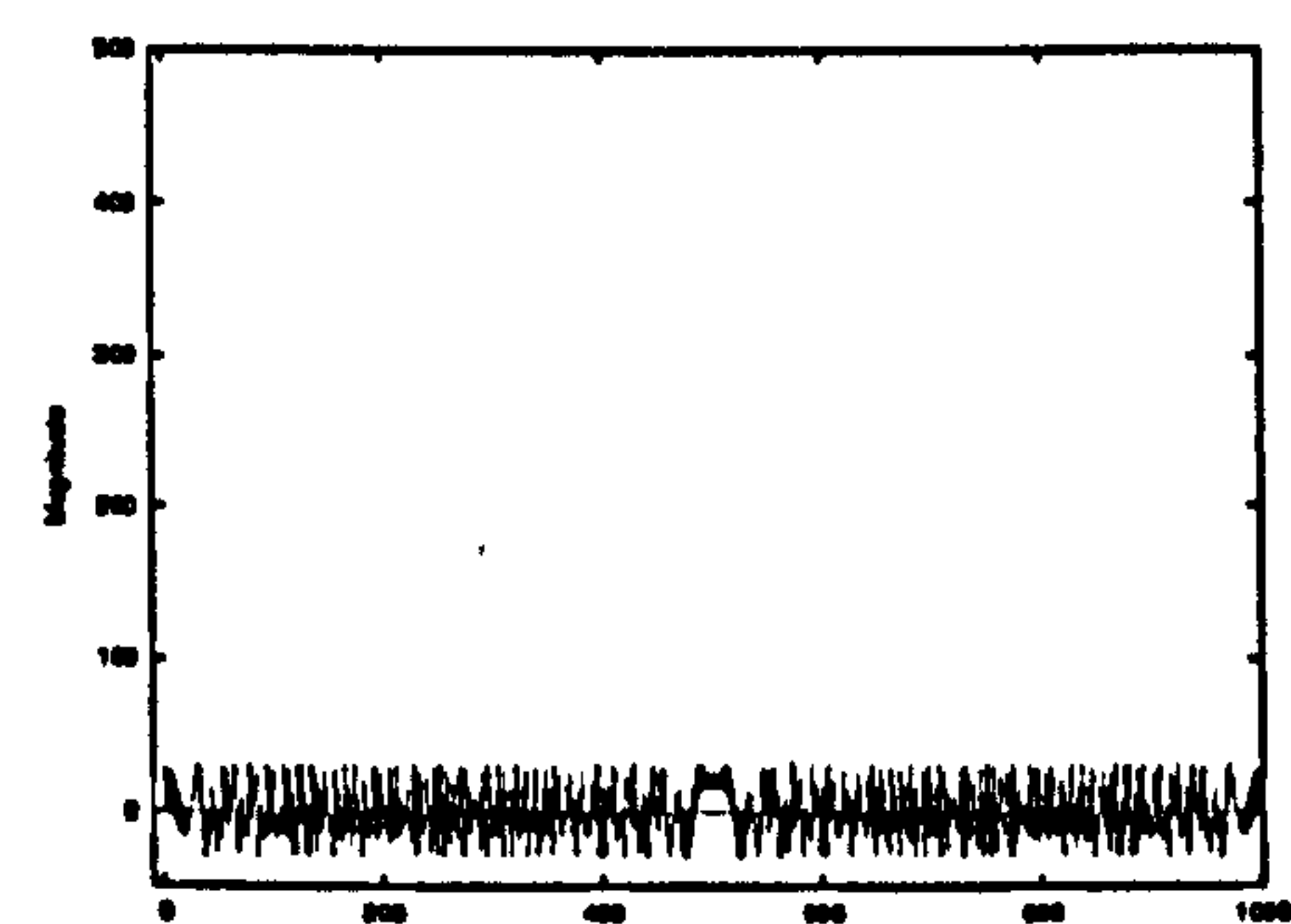


Figure 7.8: PCCF of $a^{(1)}, b^{(2)}-I$

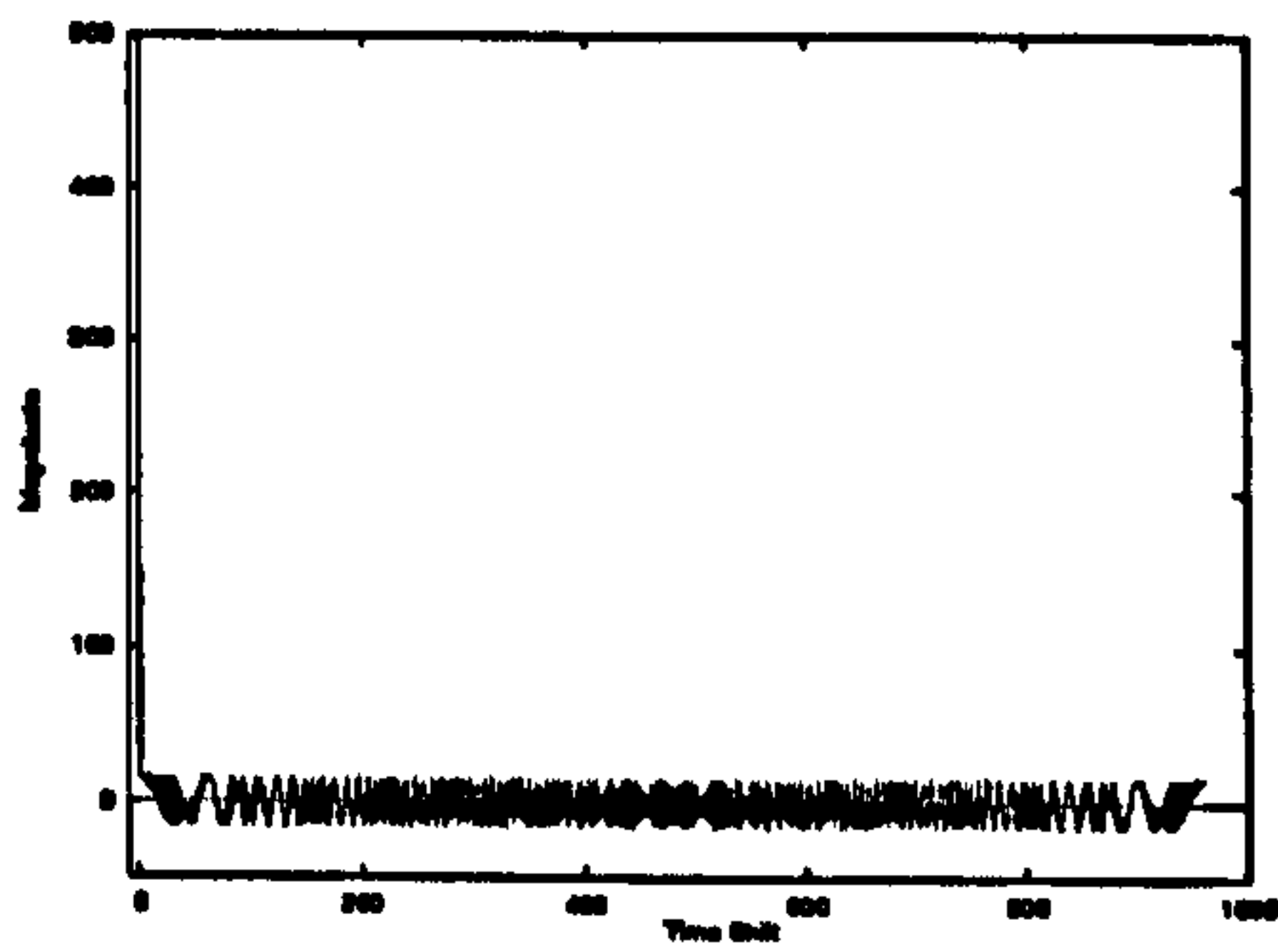


Figure 7.9: PACF of $a^{(1)}$ -II

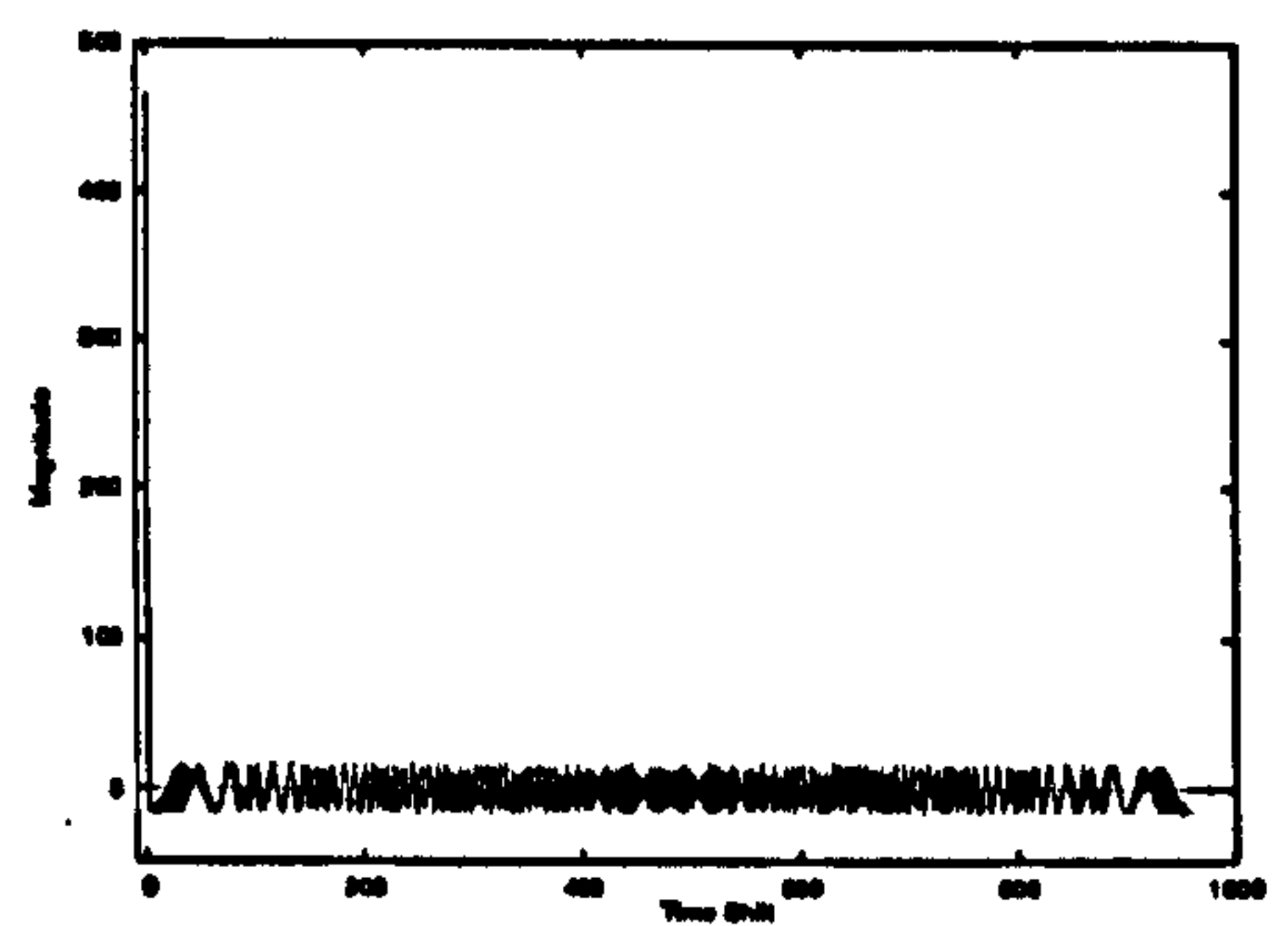


Figure 7.10: PACF of $b^{(1)}$ -II

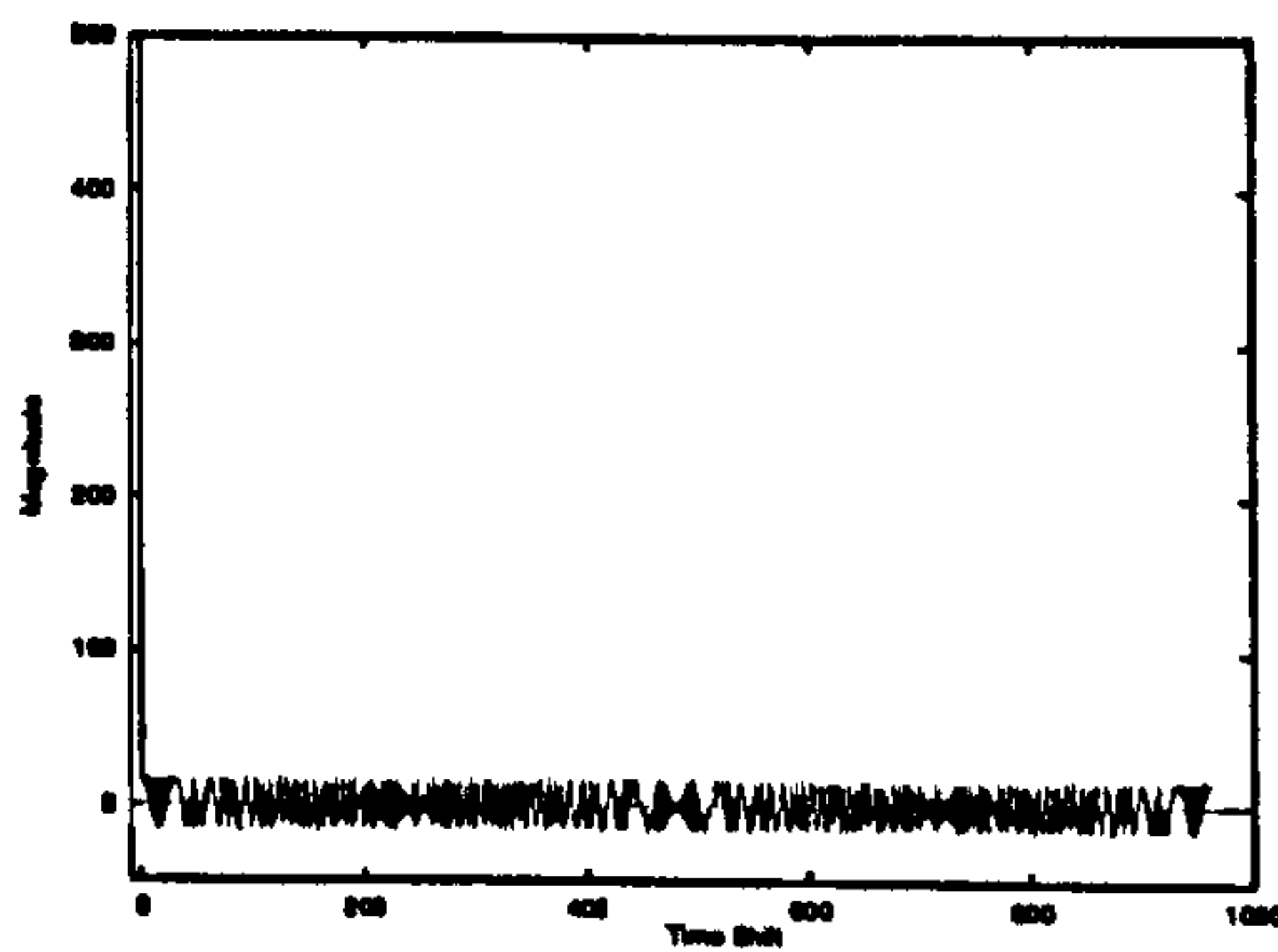


Figure 7.11: PACF of $a^{(2)}$ -II

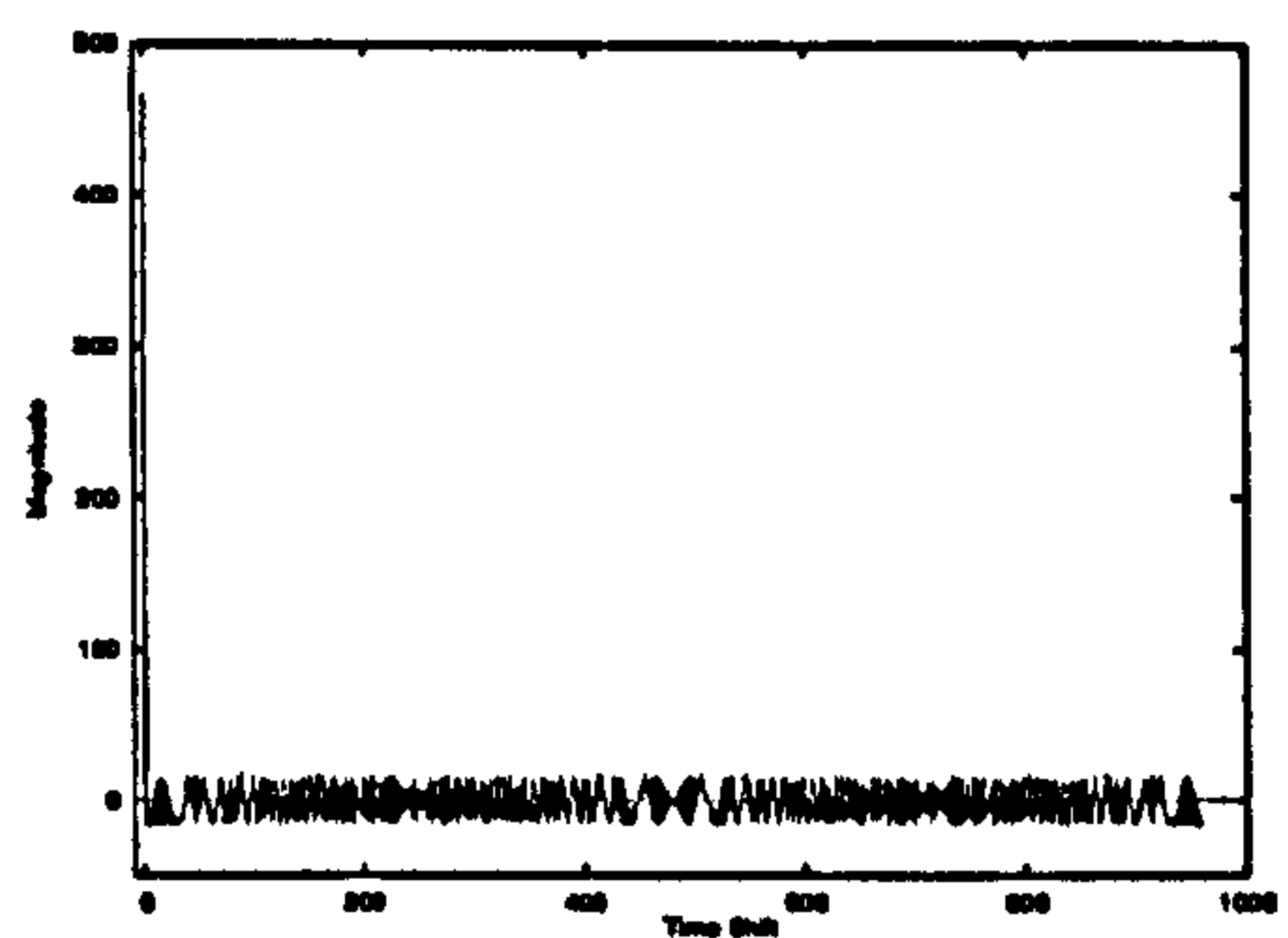


Figure 7.12: PACF of $b^{(2)}$ -II

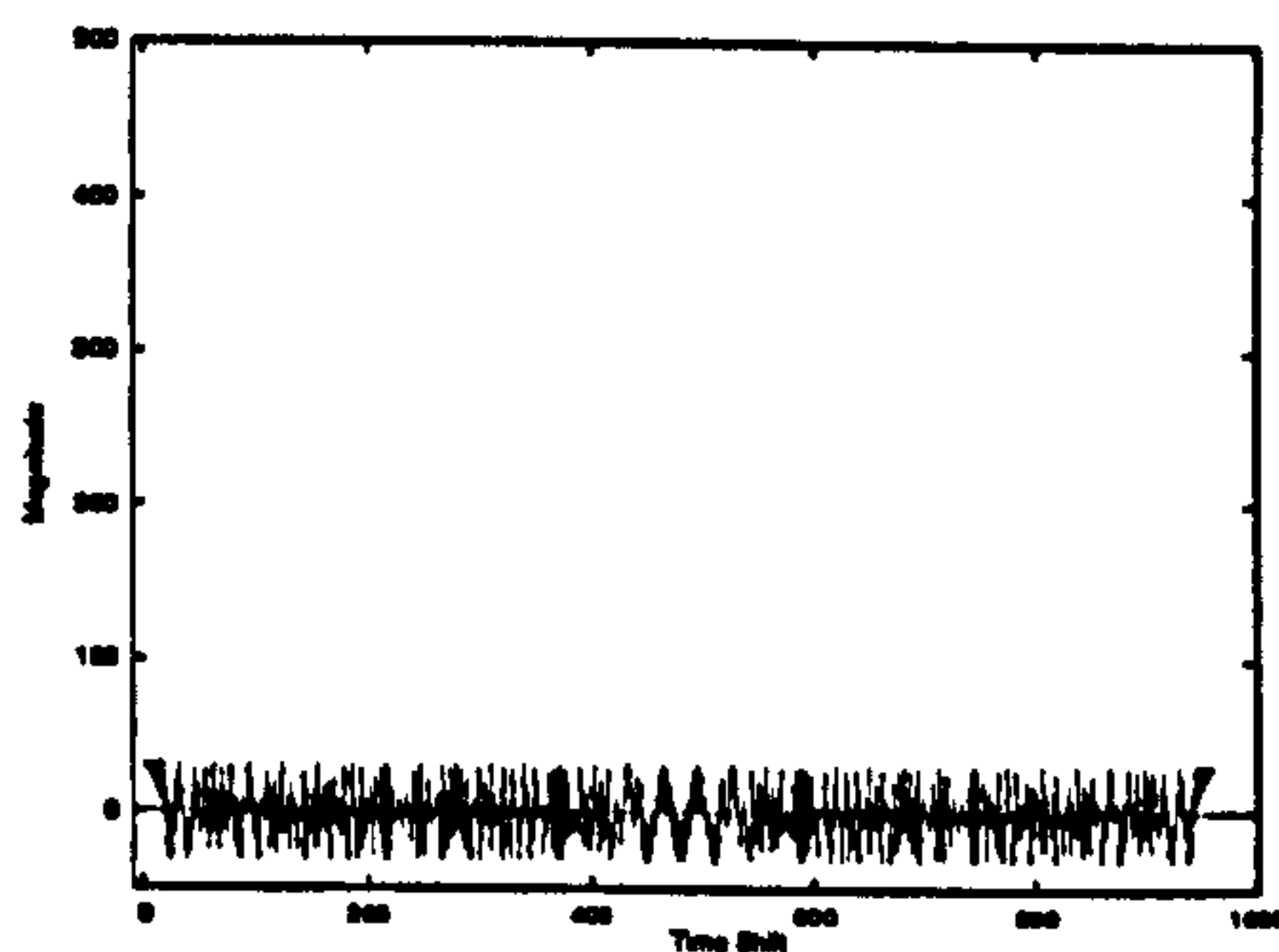


Figure 7.13: PCCF of $a^{(1)}, a^{(2)}$ -II

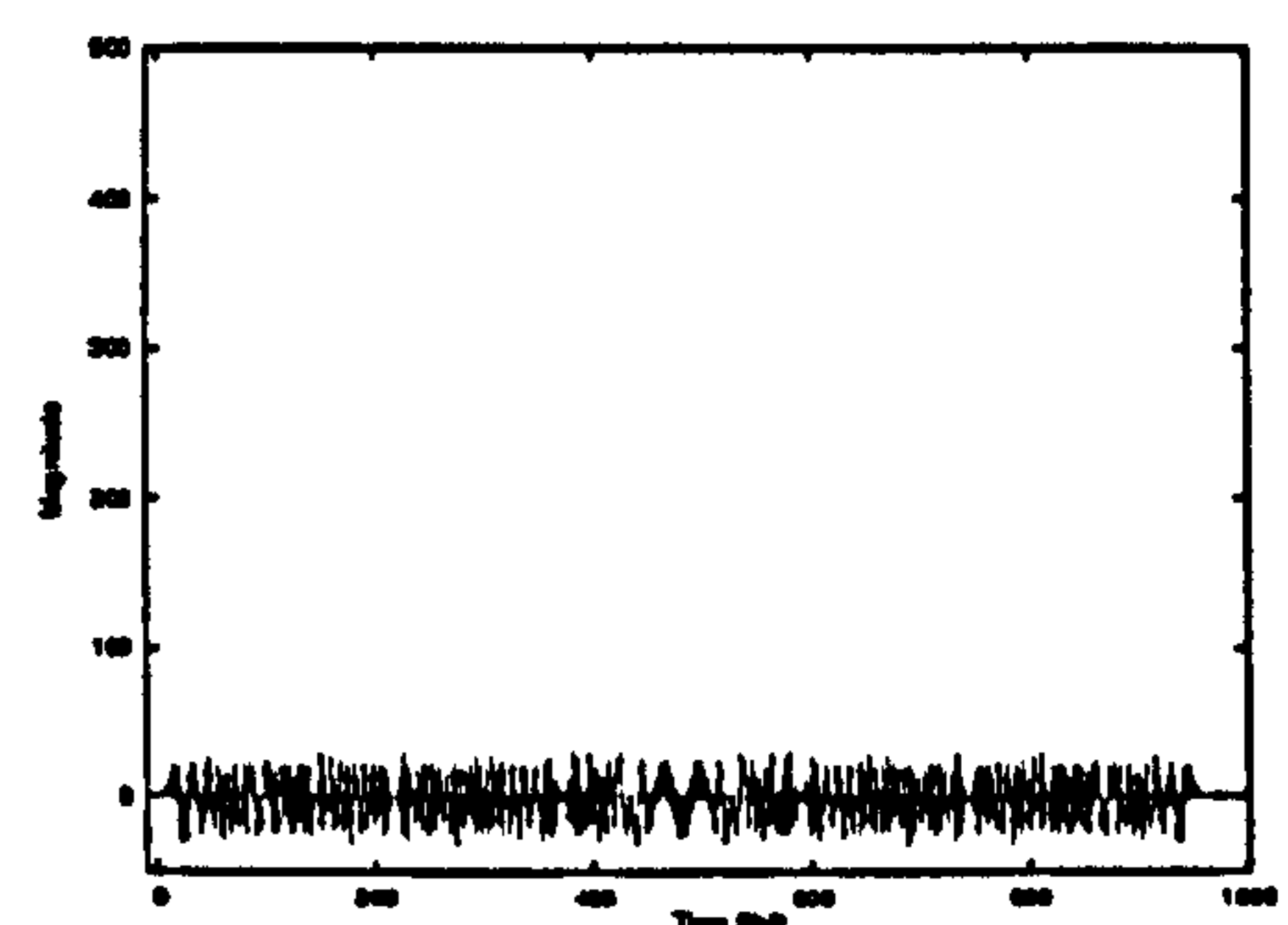


Figure 7.14: PCCF of $b^{(1)}, b^{(2)}$ -II

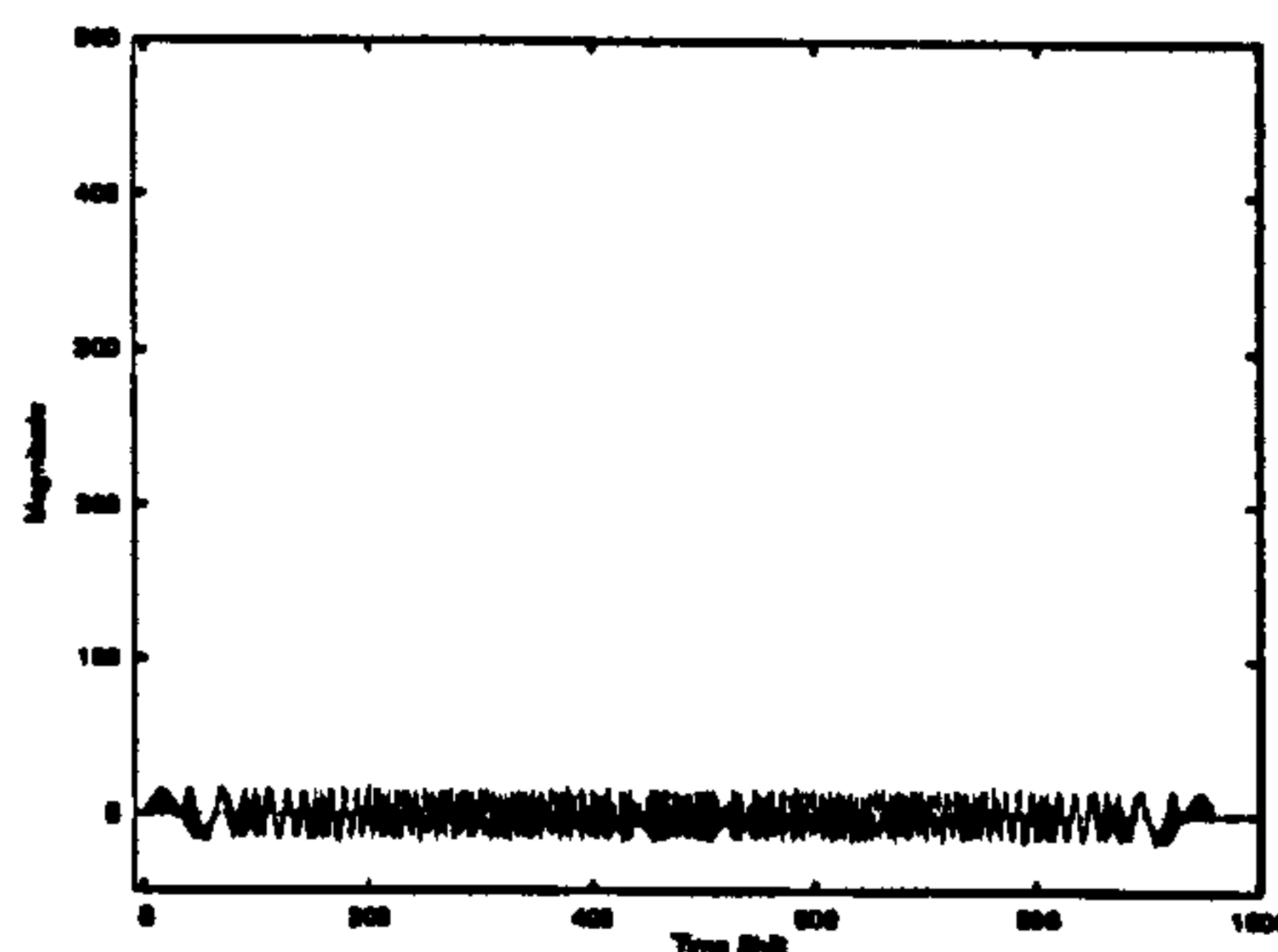


Figure 7.15: PCCF of $a^{(1)}, b^{(1)}$ -II

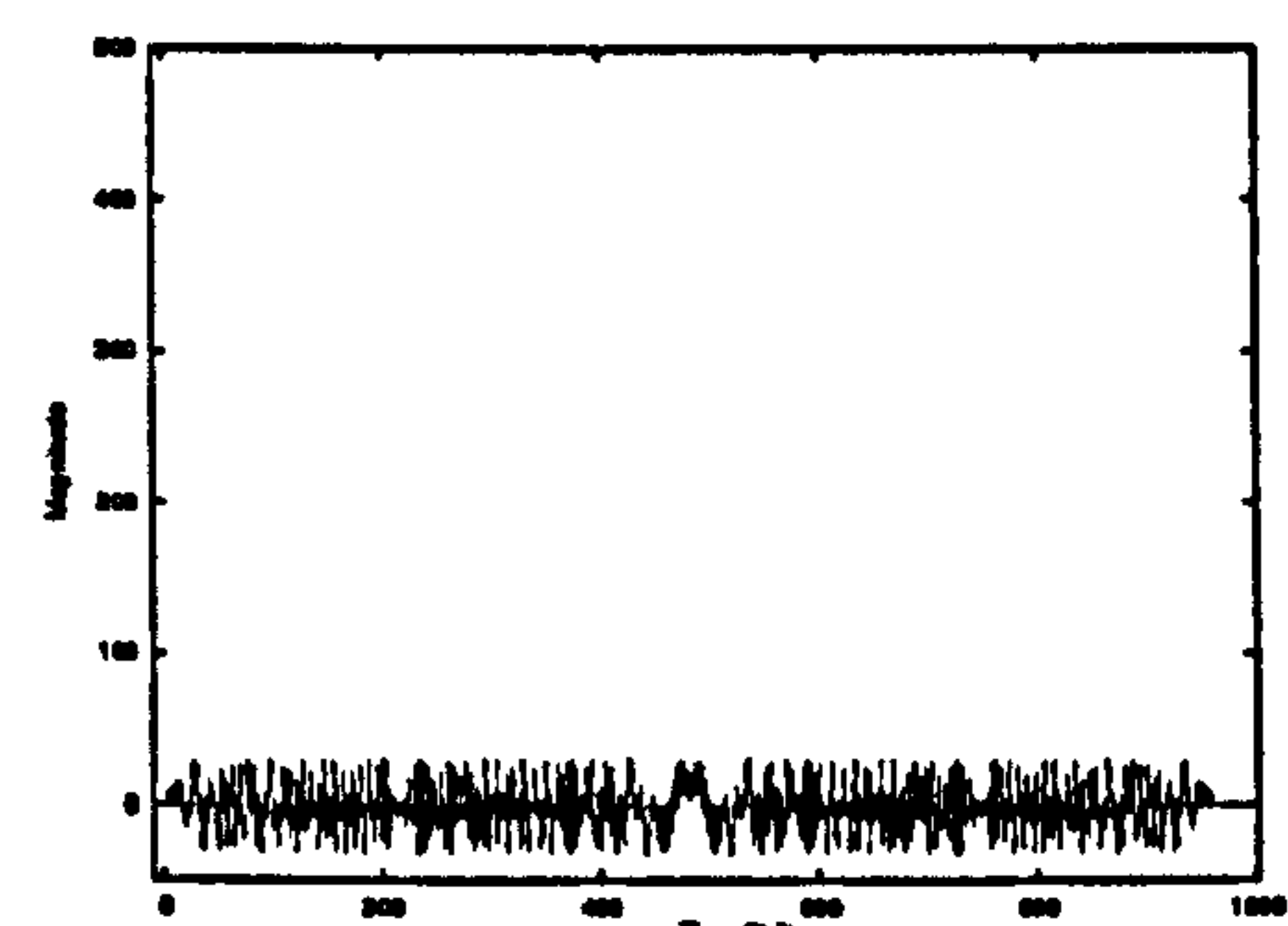


Figure 7.16: PCCF of $a^{(1)}, b^{(2)}$ -II

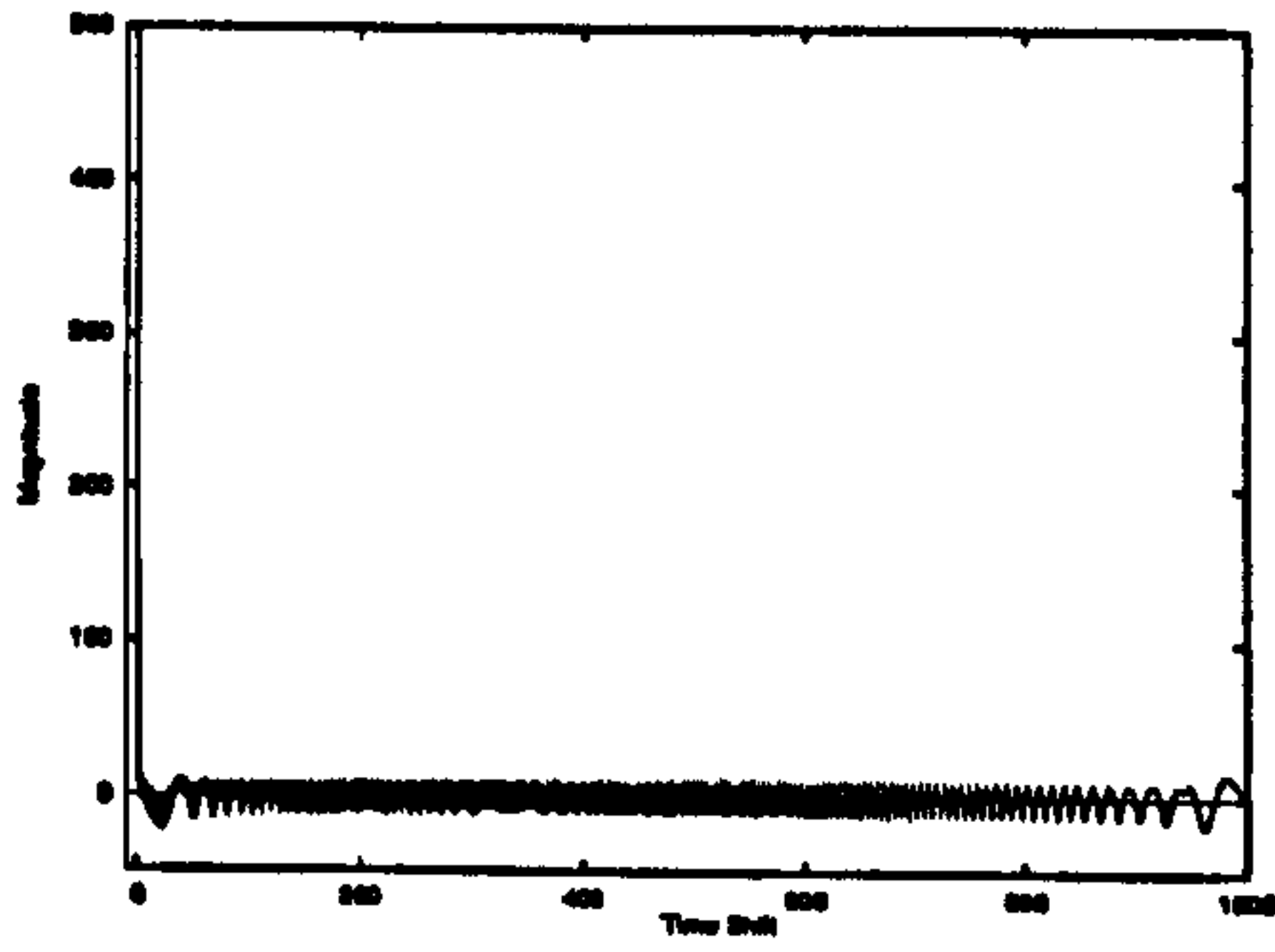


Figure 7.17: NACF of $a^{(1)}$ -I

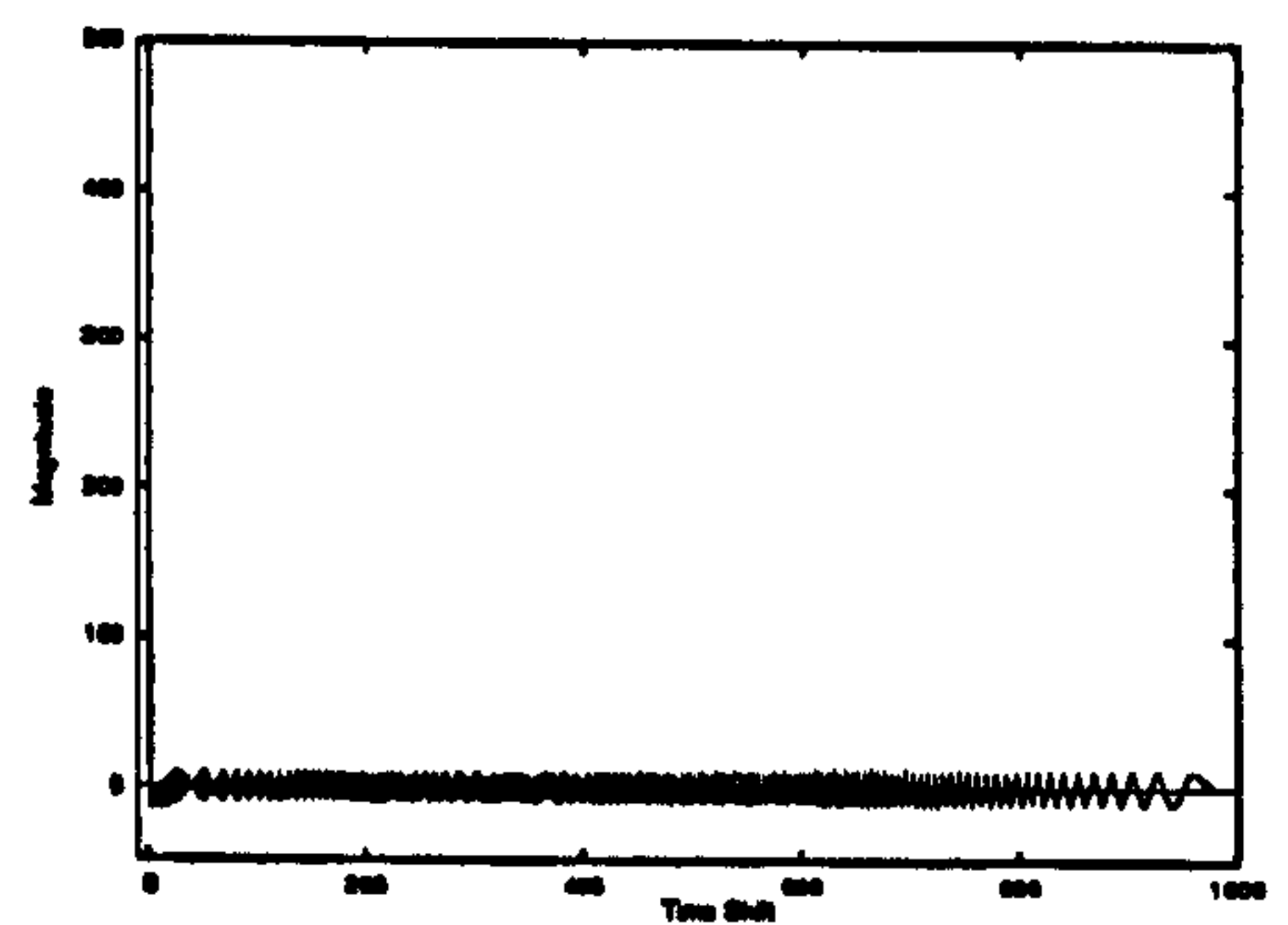


Figure 7.18: NACF of $b^{(1)}$ -I

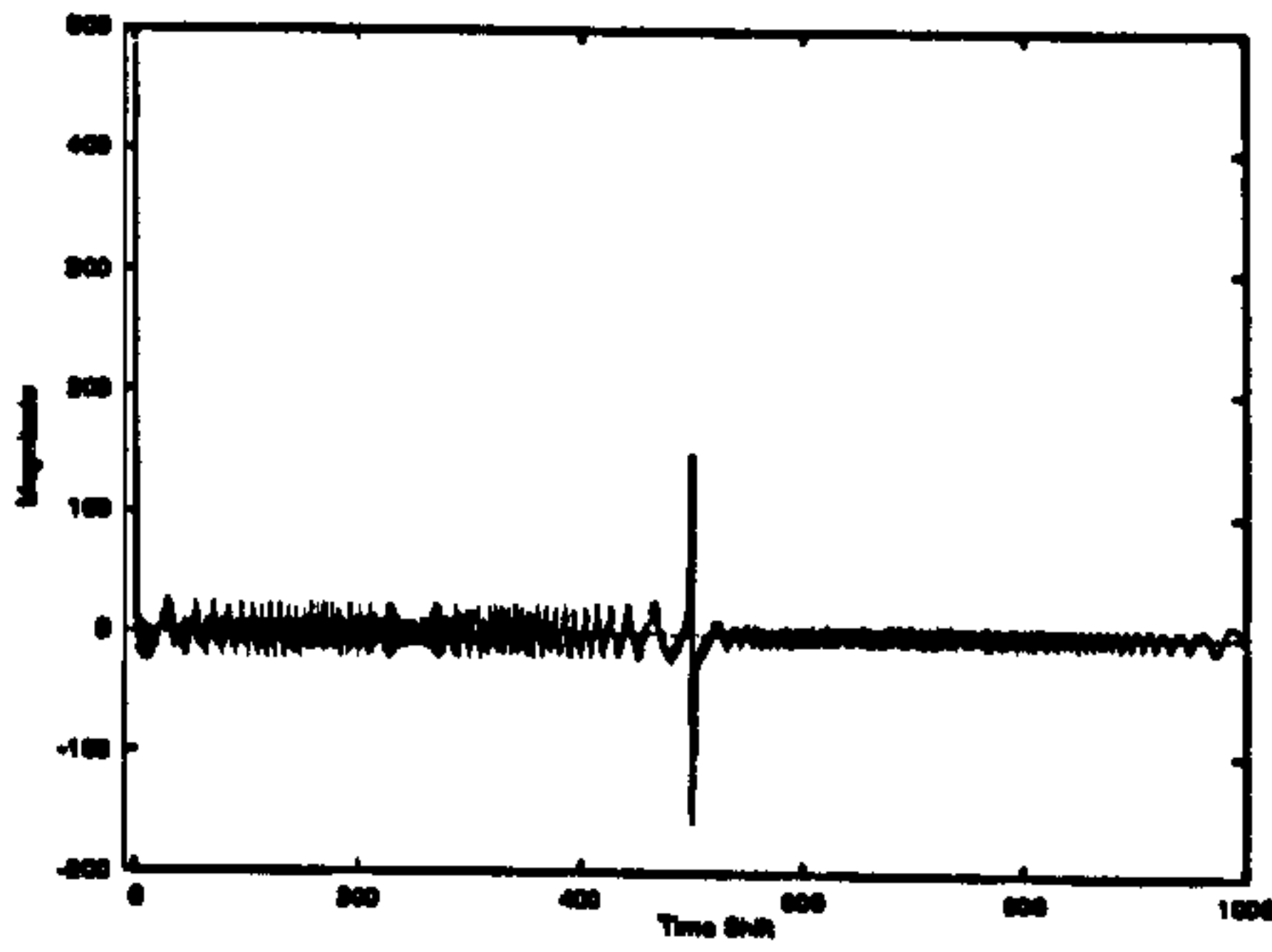


Figure 7.19: NACF of $a^{(2)}$ -I

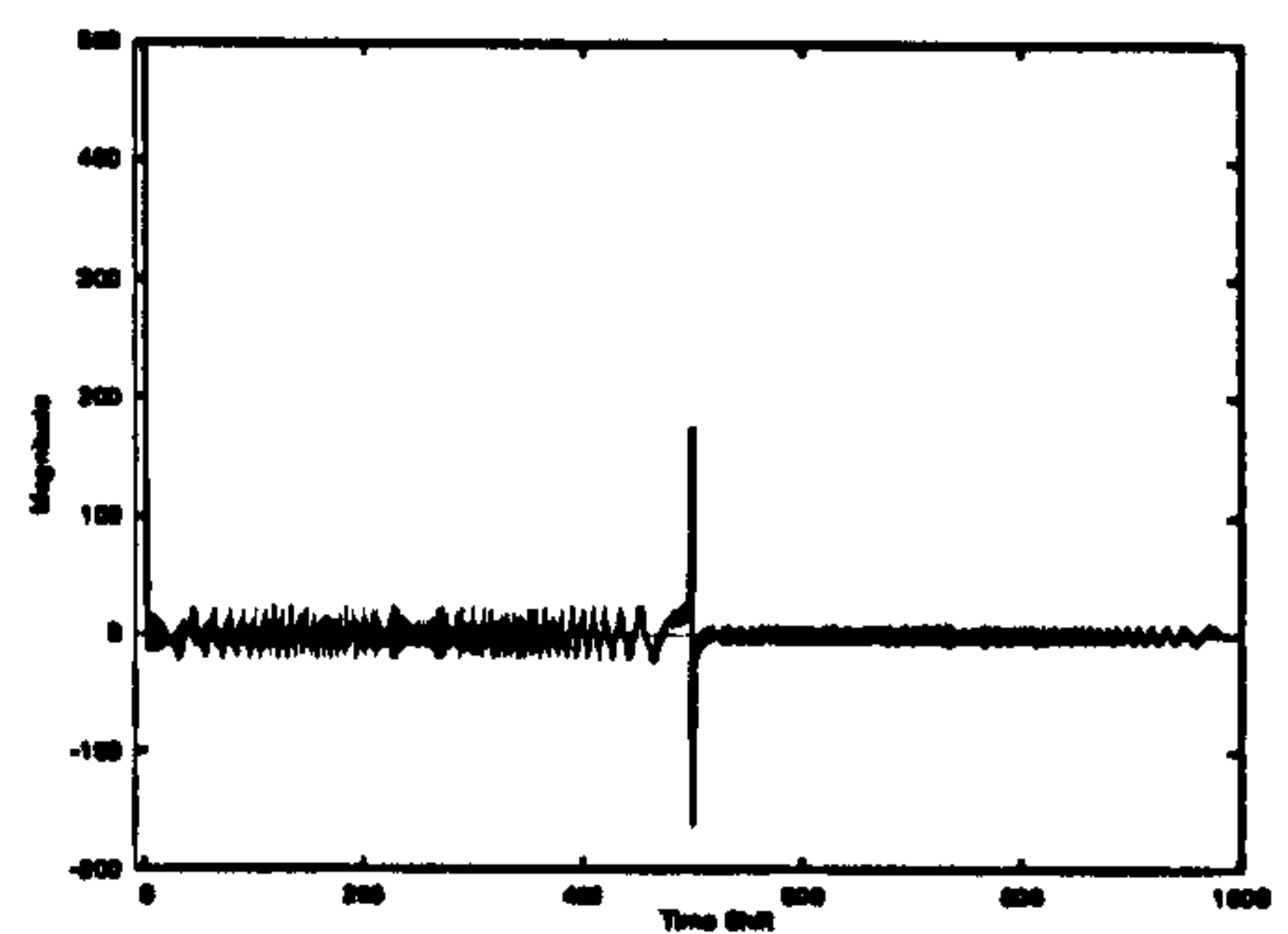


Figure 7.20: NACF of $b^{(2)}$ -I

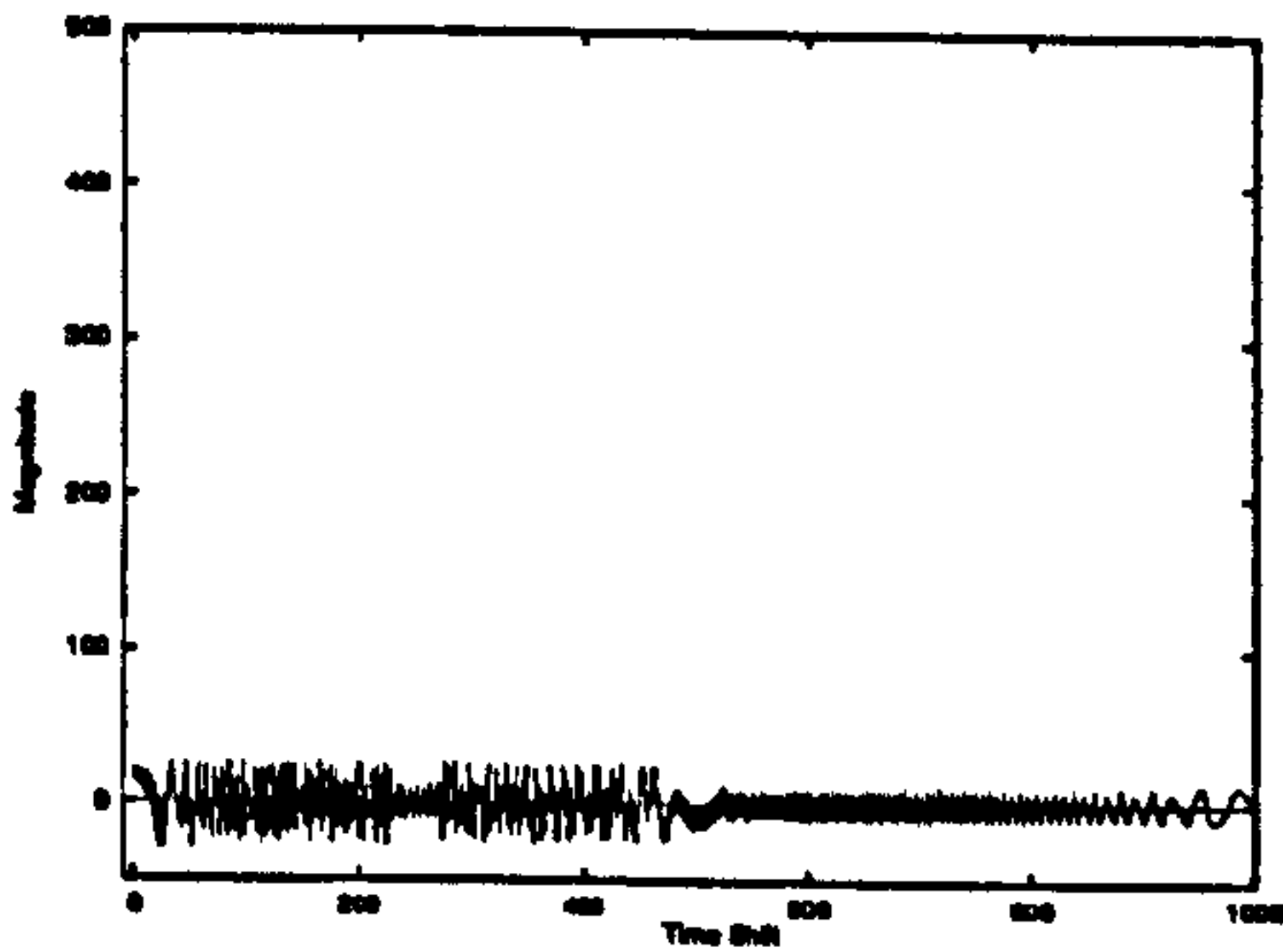


Figure 7.21: NCCF of $a^{(1)}, a^{(2)}$ -I

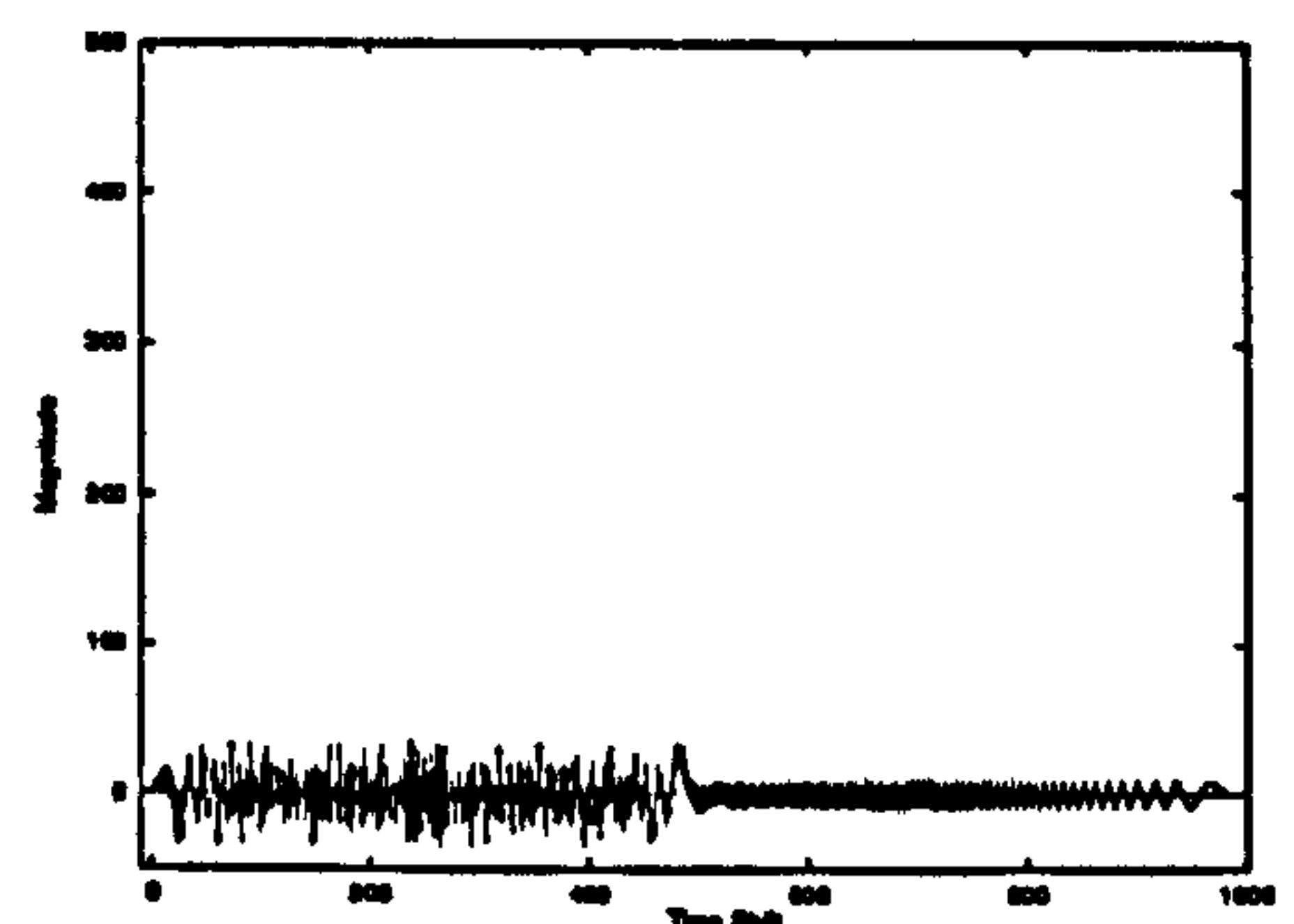


Figure 7.22: NCCF of $b^{(1)}, b^{(2)}$ -I

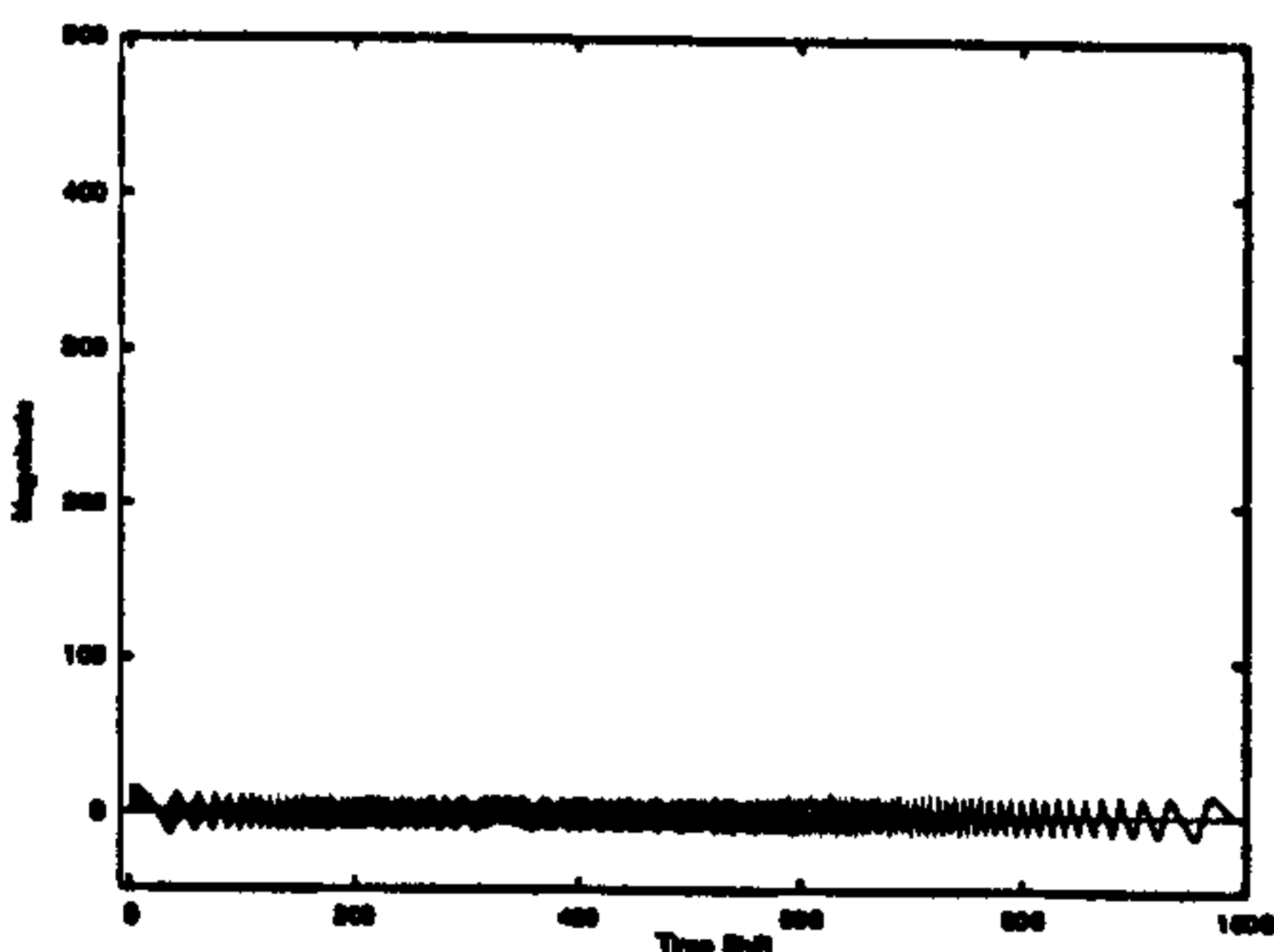


Figure 7.23: NCCF $a^{(1)}, b^{(1)}$ -I

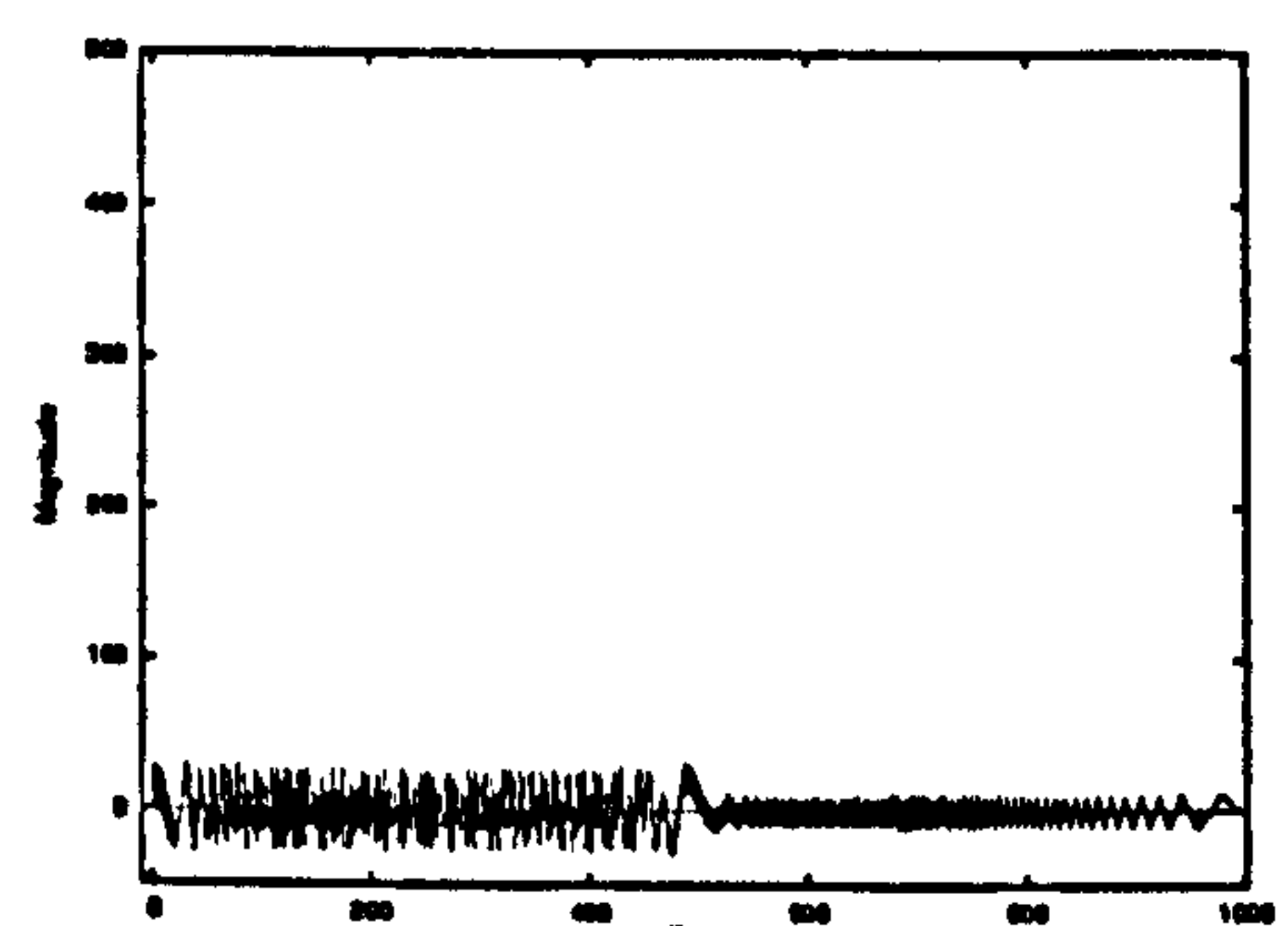


Figure 7.24: NCCF of $a^{(1)}, b^{(2)}$ -I

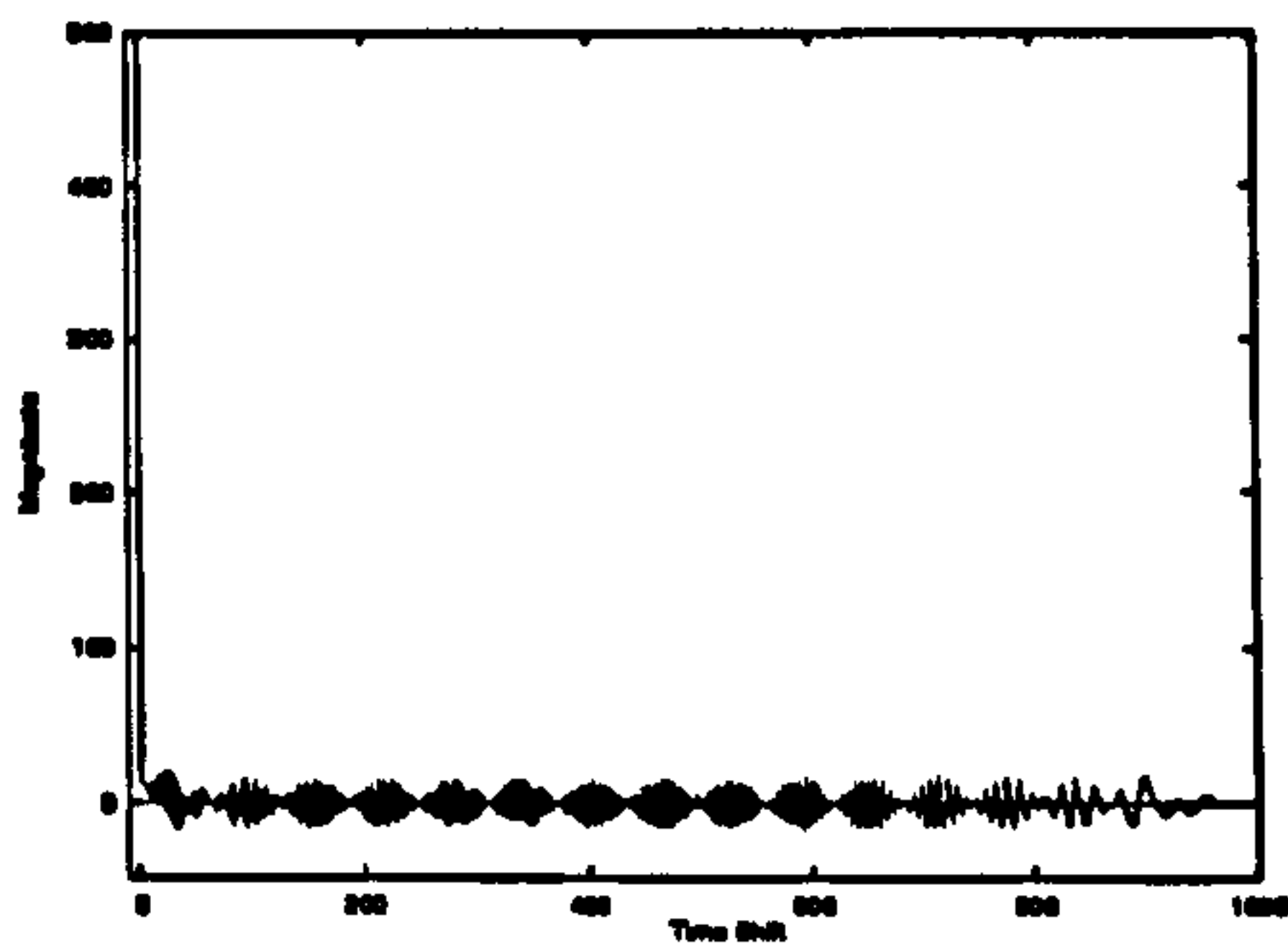


Figure 7.25: NACF of $a^{(1)}$ -II

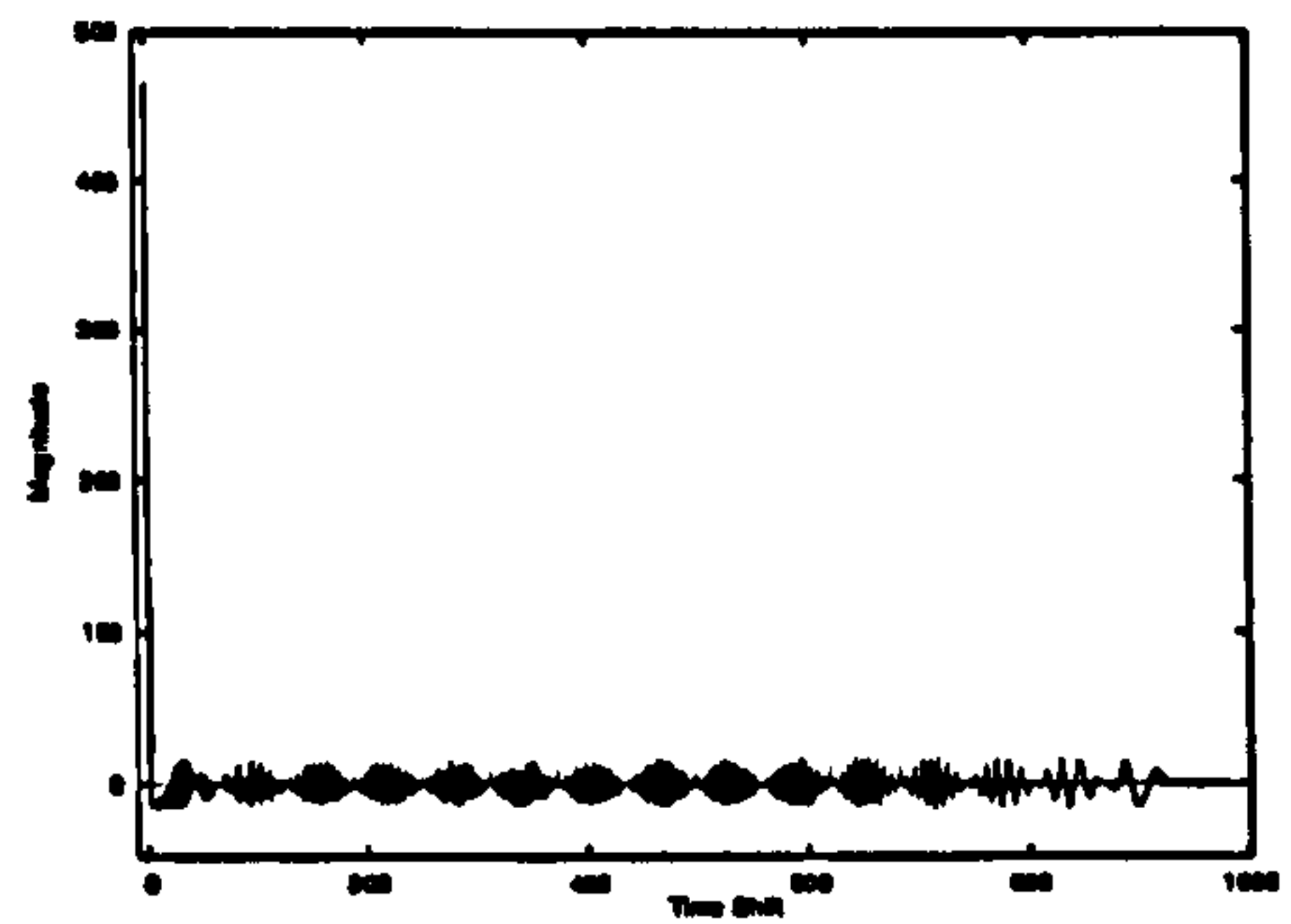


Figure 7.26: NACF of $b^{(1)}$ -II

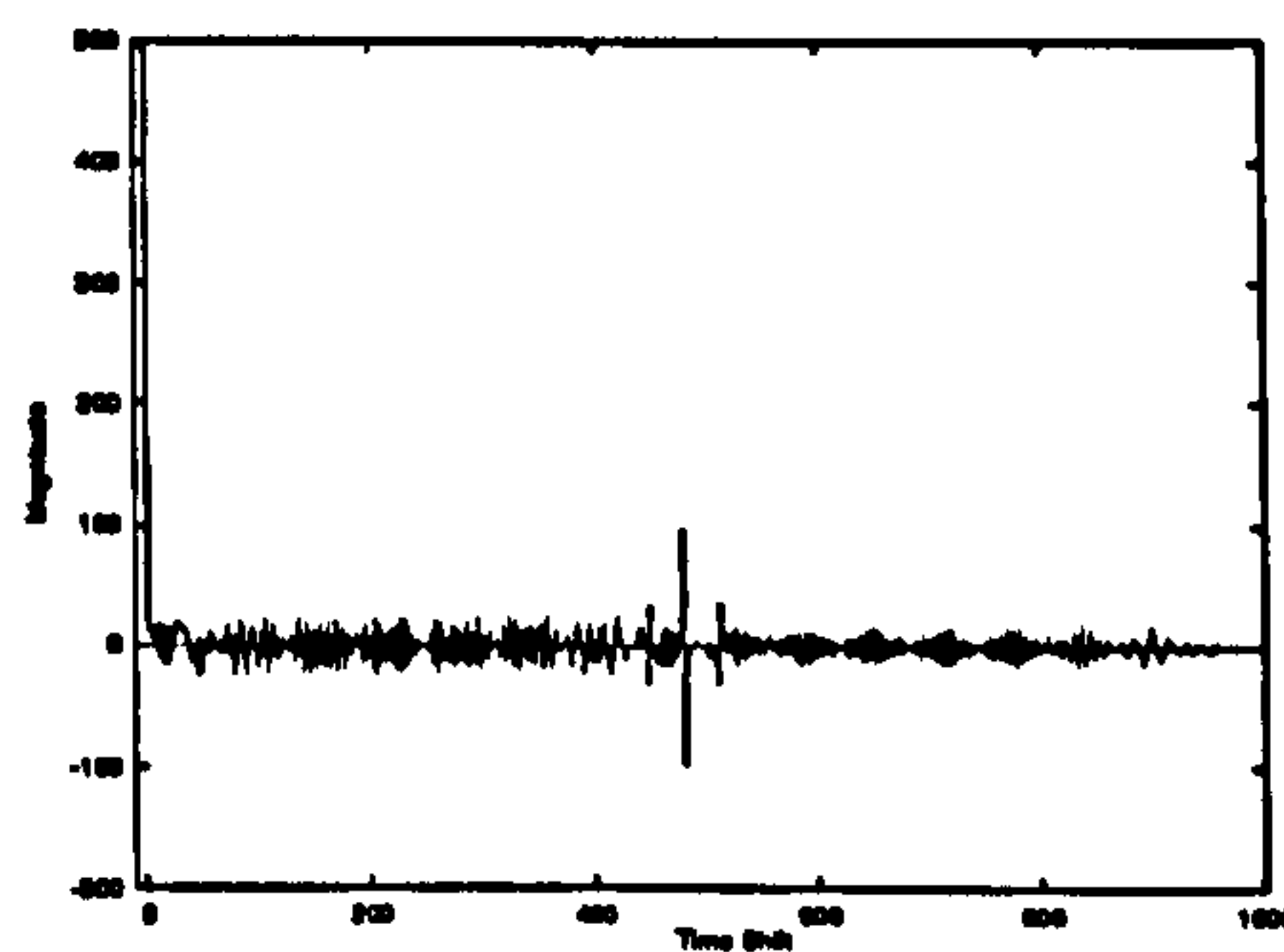


Figure 7.27: NACF of $a^{(2)}$ -II

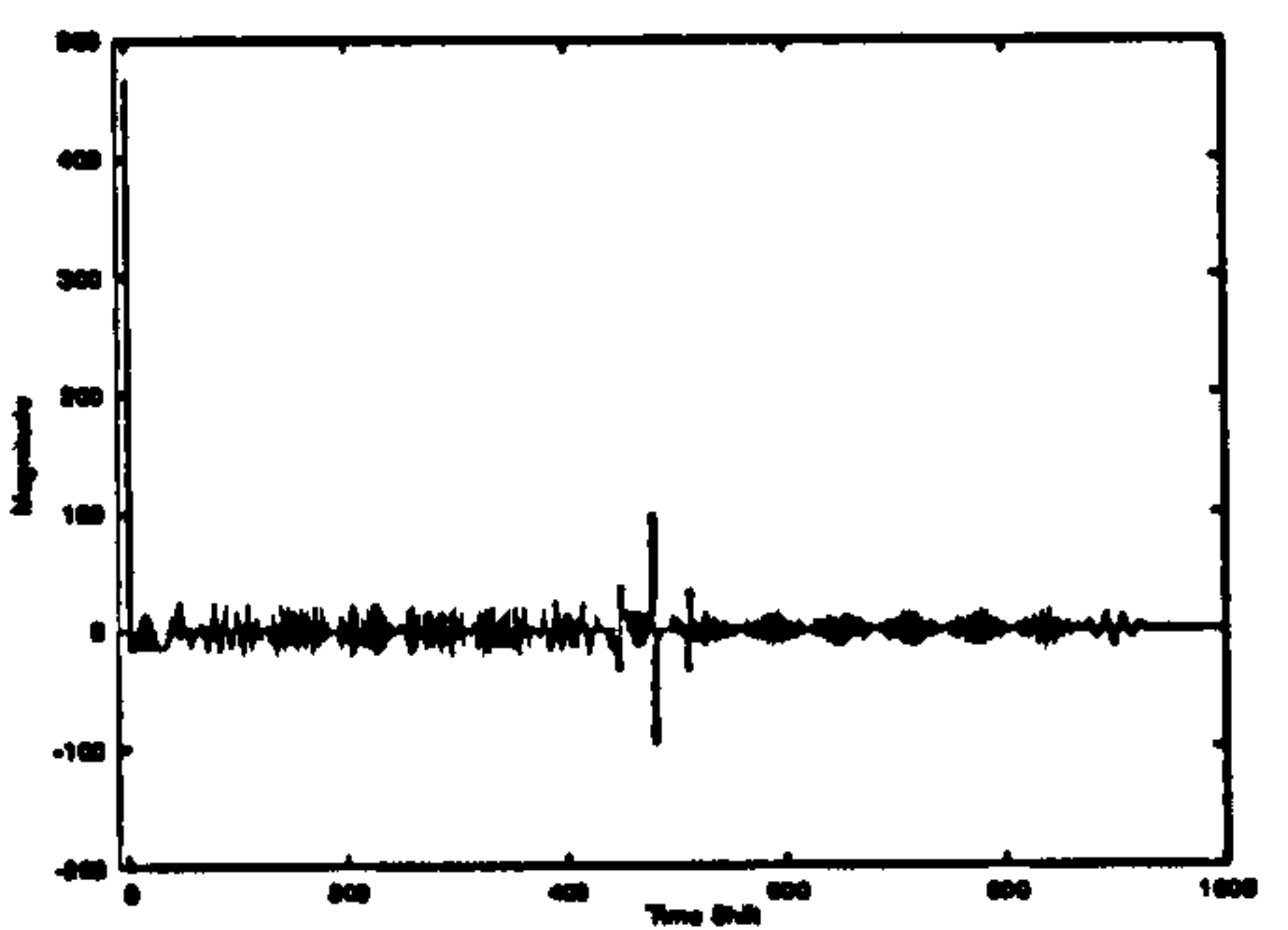


Figure 7.28: NACF of $b^{(2)}$ -II

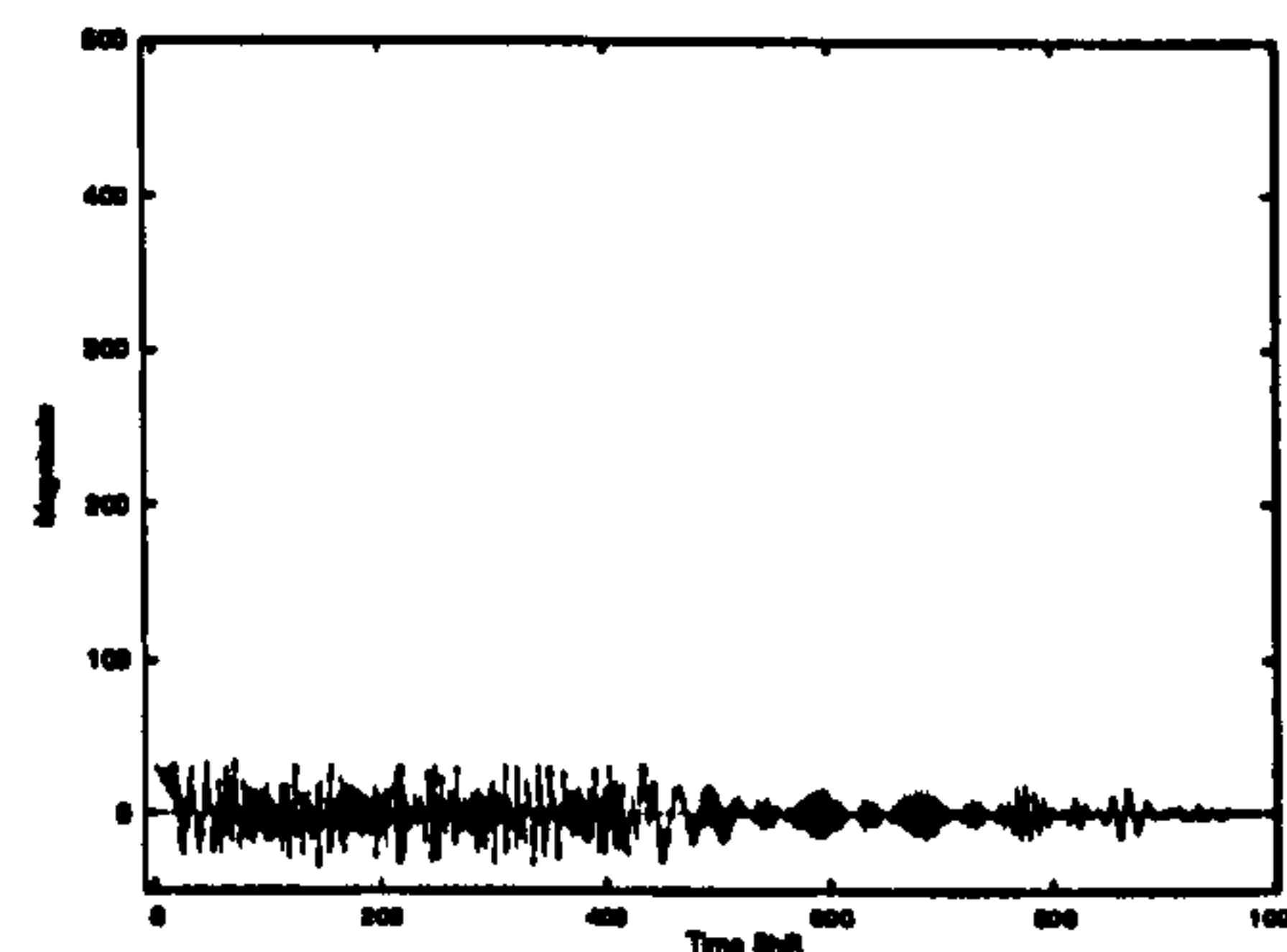


Figure 7.29: NCCF of $a^{(1)}, a^{(2)}$ -II

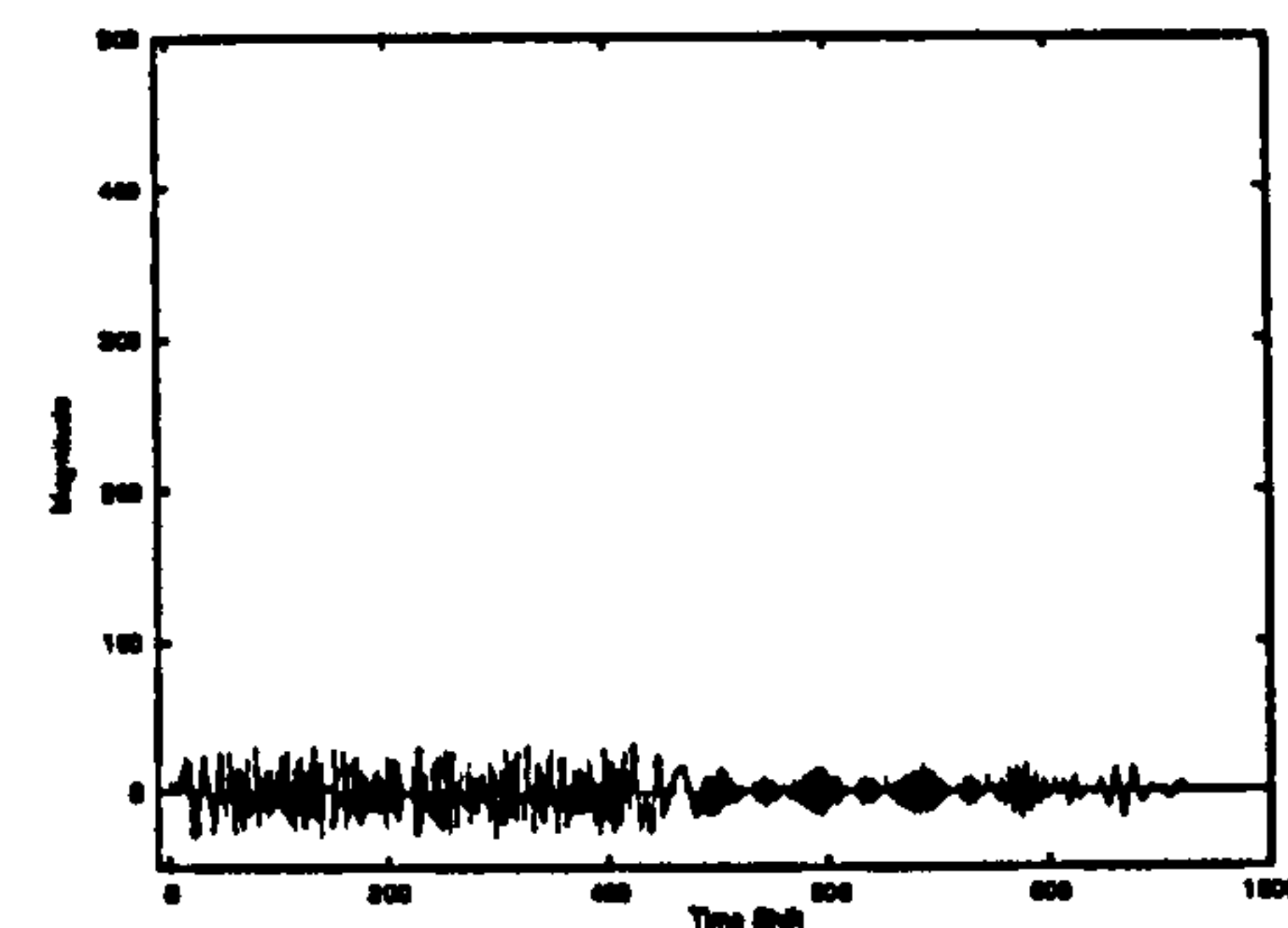


Figure 7.30: NCCF of $b^{(1)}, b^{(2)}$ -II

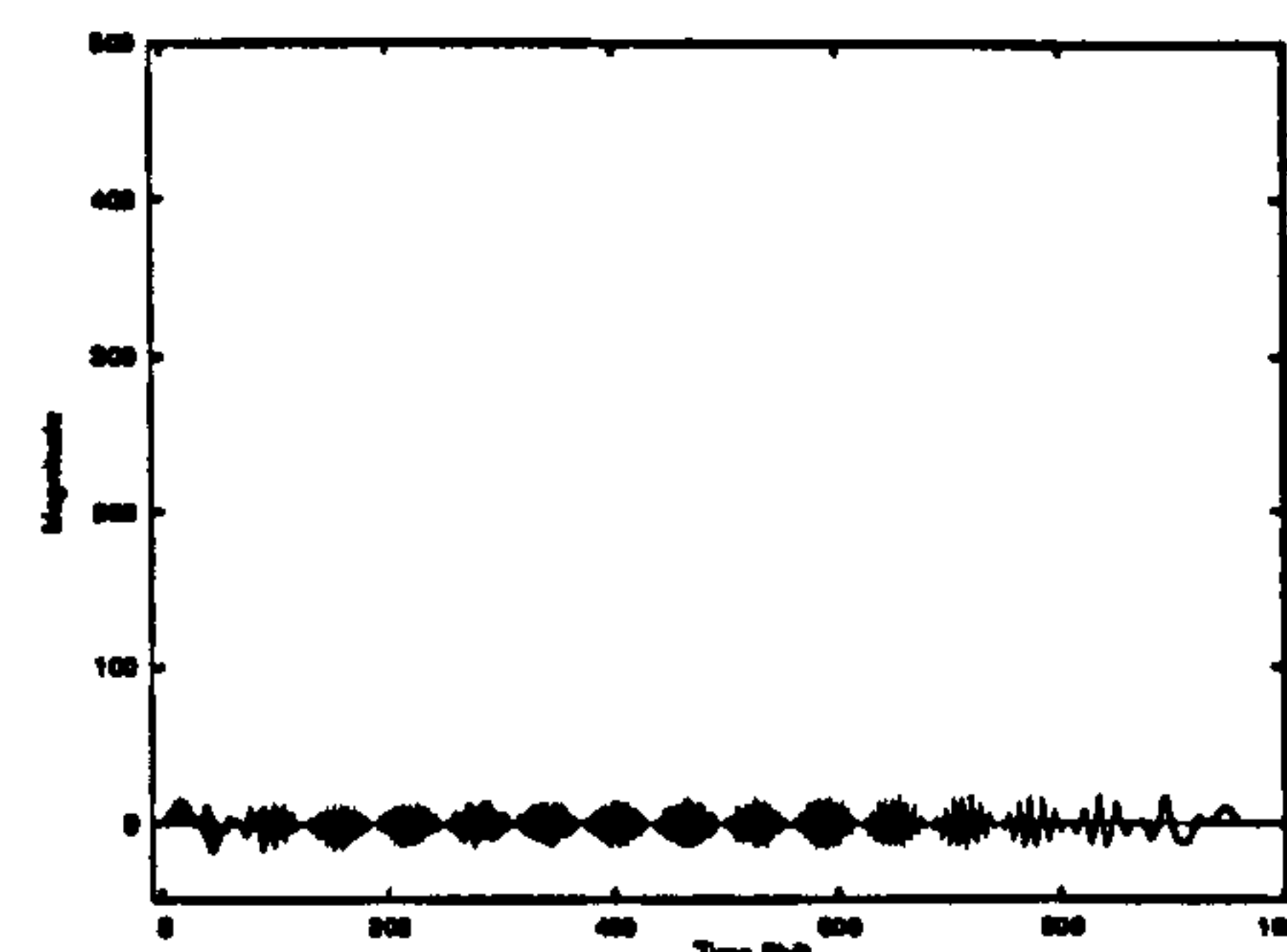


Figure 7.31: NCCF of $a^{(1)}, b^{(1)}$ -II

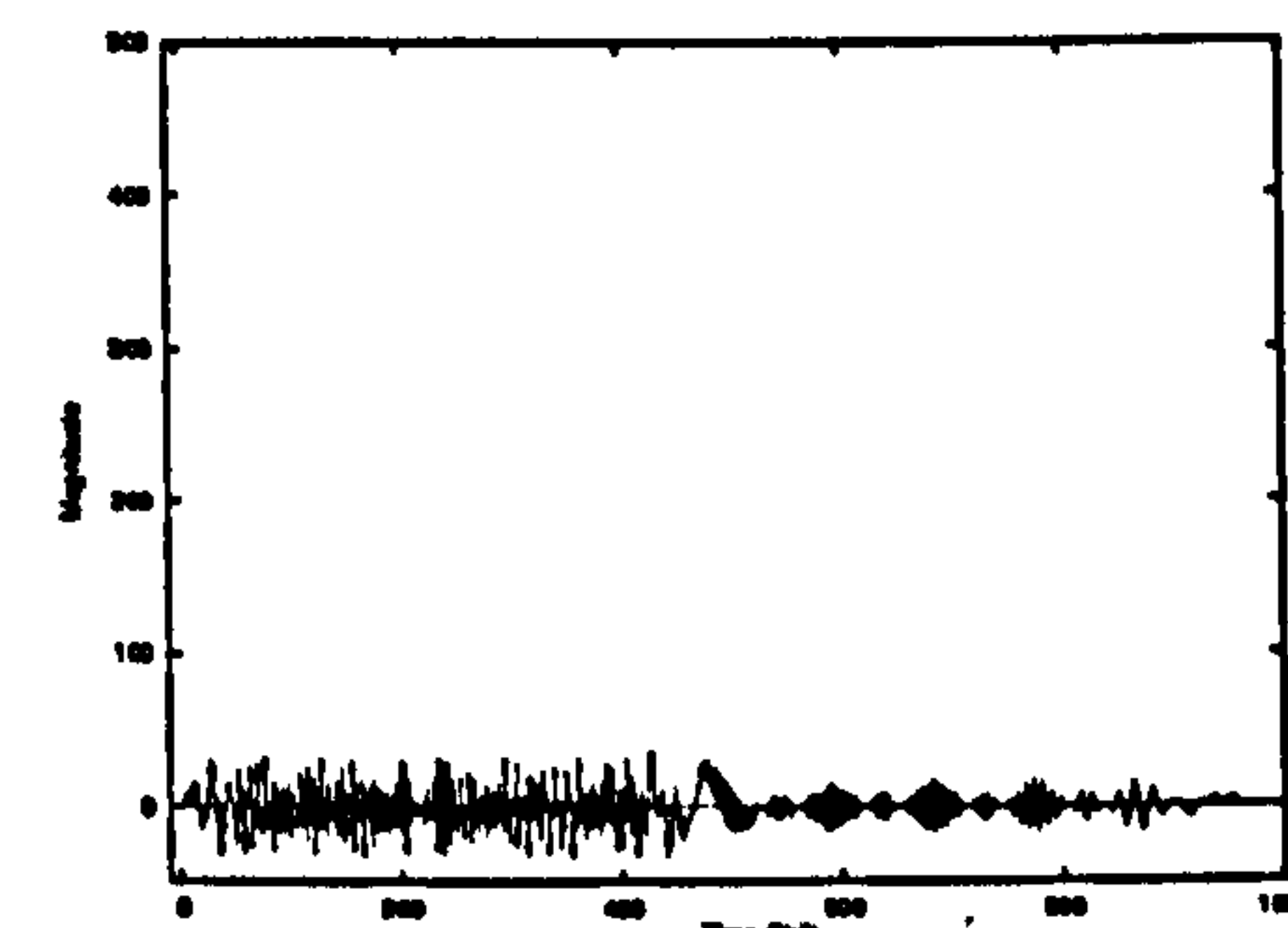


Figure 7.32: NCCF of $a^{(1)}, b^{(2)}$ -II

7.6 Concluding Remarks

In conclusion, we have considered the asymptotic maximum out-of-phase ACFs of Frank and Chu sequences of length L and order r . For Chu sequences, it is shown that the B_C^r is bounded by $\sqrt{L/4.34}$, if $r = 1$; or $0.48\sqrt{b/r}L$, if $r \geq 2$, $b/r \leq 0.37$; or $L/\pi \sin \pi b/r$, if $r \geq 2$, $b/r > 0.37$. For Frank sequences, it is shown that the B_F^1 , B_F^{q-1} , are asymptotic to q/π as q tends to infinity; when L is odd, $B_F^{\frac{L-1}{2}}$, $B_F^{\frac{L+1}{2}}$, are bounded by $2\sqrt{2}\frac{q}{\pi}$. In comparison, Chu sequences exist for every integer length $L > 1$, rather than solely at lengths which are perfect squares, as is the case with Frank sequences. However, Frank sequences have more symmetrical structures and more favourable nonperiodic ACFs. Specifically, we have $B_C^{(1)}/B_F^{(1)} = 1.507$, $B_C^{(\frac{L-1}{2})}/B_F^{(\frac{L-1}{2})} = 1.065$, $B_C^{(2)}/B_F^{(2)} = 1.571$.

For the combined Frank/Chu sequences, it is proved that $R_{f(r),c(s)}(\tau) = \sqrt{L}$ when $r \neq s \pmod{q}$. Although there exist some time shifts where the CCF values are relatively large (when $r = s \pmod{q}$), in this case, the CCFs are zero for all other time shifts, including the ones around zero time shift position. It should be noted that the methods presented here can also apply to generalized Frank sequences (Suehiro & Hatori, 1988) and generalized Chu sequences (Popović, 1992).

Based on Frank and Chu sequences, two classes of real-valued sequences and a class of combined Frank/Chu sequences have been obtained. It is shown that the two classes of real-valued sequences have useful symmetrical properties. By defining periodic complementarity, it is proved that the proposed sequences form two classes of periodic complementary sequences and that every complementary pair has an uncorrelated mate. From the calculated ACF/CCF results, it is demonstrated that they also have good periodic and nonperiodic ACF/CCFs. It is conjectured that the maximum out-of-phase ACF and maximum CCF are asymptotically bounded by $O(\sqrt{L})$.

Chapter 8

Hybrid CCMA/SSMA Coding Scheme

8.1 Introduction

Gallager argues that there is a need for a more combined approach to multiple-access communication, focused on coding and decoding techniques. In particular, he points out that what is needed is a coding technology that is applicable for a large set of transmitters of which a small, but variable, subset is active simultaneously (Mathys, 1990; Gallager, 1985).

Mathys has proposed a coding scheme which aims to fill the gaps between the information theory and collision resolution approaches (Mathys, 1990). His idea comes mainly from the following observation: in many multiuser communication situations, interference from other users can be tolerated up to a certain level by using collaborative coding multiple-access; if too many users are active at the same time, however, collisions will occur and one has to start retransmitting messages according to some collision resolution scheme. In this sense, he regards his code construction as a building block of a hybrid multiple-access communication system which employs both collaborative coding and collision resolution. Similar attempts that point in the same direction are described in (Massey & Mathys, 1985; Bar-David *et al.*, 1987).

This chapter will focus on multiaccess information theory and spread spectrum techniques. The general idea behind such multiple access communication schemes is that one can find sets of signals which can be mixed together to form a composite signal, with the individual signals in the set being recoverable from the composite signal at the receiver. Normally, the mixing is assumed to be the result of linear addition of the signals and the recovery is assumed to be

accomplished by linear filtering. For the CCMA system, the isolation between users is based on the code structure. On the other hand, in the SSMA system, the isolation between users is based on the good ACF/CCF properties of the sequences used.

Both the CCMA technique and the SSMA technique permit efficient simultaneous transmission by several users sharing a common channel, without subdivision in time or frequency. In an SSMA system, all transmitters share the same overall transmission bandwidth, with isolation being achieved by an appropriate choice of sequences for the terminals. The advantage of SSMA is that it appears to offer promise of reliable operation over dispersive radio paths and can provide resistance against high levels of interference and jamming. In addition, unlike most of the CCMA schemes, SSMA systems do not require all the users to be active simultaneously. However, the number of sequences available with a given sequence family is limited; the partial correlations of the bearer sequences used in SSMA are not ideal and are a source of system "self-noise" which eventually causes a limit on the number of simultaneous users.

The CCMA technique appears to be more attractive in practice because of its higher combined information rate and larger number of permitted users. However, there are difficulties in symbol and block synchronization among all the users in the system. In fact, most of the previous studies are based on the assumption of a noiseless synchronized adder channel with all the users in the system being always simultaneously active. In addition, when the number of users and the length of the codes increase, in general, it will be extremely difficult to decode (decompose) the sum codeword into its component codewords.

In this chapter, a new hybrid CCMA/SSMA coding scheme is proposed (Fan & Darnell, 1994b). It is expected that this hybrid scheme will provide a more powerful multiple-access capability and a better performance by exploiting the individual merits and reducing the individual disadvantages of CCMA and SSMA. The emphasis of the coding scheme is on finding a simple and efficient multiaccess procedure applicable to a large set of transmitters, of which a variable subset is active simultaneously. Further, the complexity of the implementation should be very low.

8.2 Hybrid CCMA/SSMA System Model

The system model of the hybrid CCMA/SSMA scheme is shown in Fig. 8.1. This can be considered as a concatenated multiple access communication scheme. Suppose each sub-CCMA system has N users, the SSMA system has K spreading sequences and each sequence is modulated by a sum codeword from a sub-

CCMA adder channel output; then the system can accommodate NK users. If the Q -ary CCMA ring codes proposed in Chapter 3 are employed, then any number of $T \leq NK$ users can be active at any time. If each CCMA has N users, where at most T users are active at any time, then the hybrid system will have NK users, with at most TK users active at any time. Further, because each sub-CCMA is separated by SSMA spreading codes, then each sub-CCMA can employ the same CCMA codes, which are distinguishable at the receiver due to the low CCFs between spreading codes.

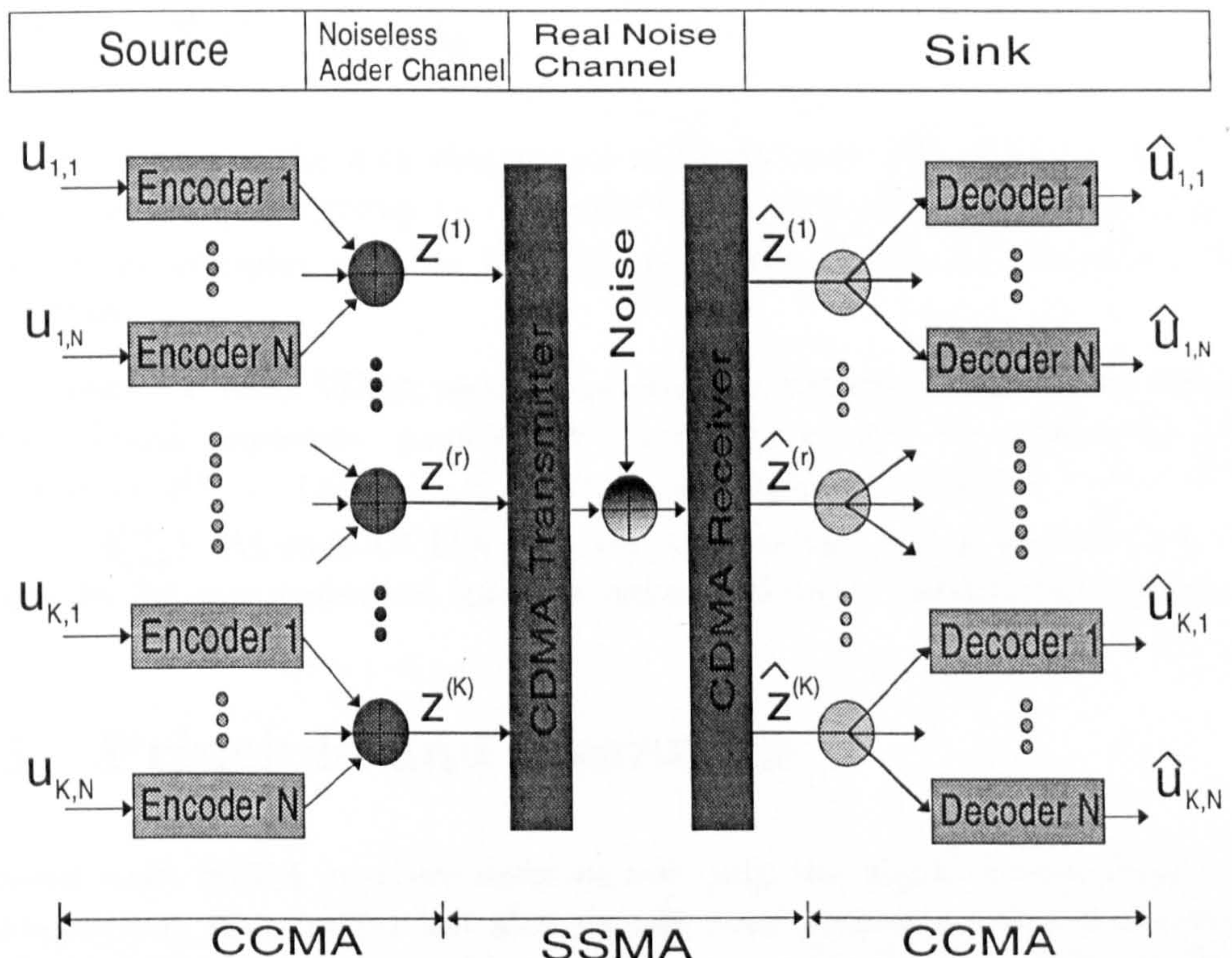


Figure 8.1: Hybrid CCMA/SSMA System Model

It will be demonstrated that the hybrid system provides a very flexible and powerful multiple accessing method.

Now let us consider a scheme using modulatable Frank or Chu sequences as spreading code sequences and the Q -ary ring codes presented in Chapter 3, or any other known codes, as CCMA codes.

As indicated previously in Chapter 7, the generalized Frank and Chu sequences can be considered as modulated sequences obtained by modulating one of the corresponding original Frank or Chu sequences with complex numbers (information data) of absolute value 1. Let q be a prime number; then there are

$(q - 1)$ original Frank or Chu sequences of length $L = q^2$. Each of the original sequences is now assigned to $(q - 1)$ groups of users. Each group of CCMA users shares an SSMA transmitter. Each transmitter modulates the assigned original sequence with the sum codeword which is the output of the CCMA adder channel. However, before modulation, the sum codeword $z^{(r)}$ must be transformed into a complex number of absolute value 1. Suppose the element $z_k^{(r)}$ of the sum codeword is a Q -ary number, we can use the following mapping:

$$b_k^{(r)} = e^{\frac{i2\pi}{Q}z_k^{(r)}}, \quad z_k^{(r)} \in Z_Q \quad (8.1)$$

where $z_k^{(r)}$ denotes the k -th element of the sum code $z^{(r)}$ in the r -th CCMA channel output (user-group r). Because the information z_i is carried by the phase of the complex number $b_k^{(r)}$, this mapping can be considered as *phase modulation*.

At the receiver, each SSMA receiver possesses a filter matched to the assigned original Frank sequence. Another device is also needed to recover the phase information $z^{(r)} = (z_0^{(r)}, \dots, z_{q-1}^{(r)})$ from the sampled complex vector $b^{(r)} = (b_0^{(r)}, \dots, b_{q-1}^{(r)})$. At each CCMA receiver, the corresponding algorithm is used to decode the sum codeword into the individual users' information signals.

8.3 Principle and Examples

Because each SSMA receiver receives not only the signal transmitted by its corresponding transmitter but also signals transmitted by other transmitters, co-channel interference must be taken into account. In asynchronous SSMA, noncorresponding signals are added to the corresponding signal asynchronously.

Firstly let us consider the following modulatable Frank sequences with prime q ,

$$s_n^{(r)} = b_k^{(r)} f_{jq+k}^{(r)} = b_k^{(r)} e^{\frac{i2\pi}{q}rkj}, \quad 0 \leq k, j < q; \quad (r, q) = 1 \quad (8.2)$$

where $|b_k^{(r)}| = 1$, $0 \leq k < q$, carries the information to be communicated.

Let $s^{(r)}$ be the corresponding modulated sequence and $s^{(s)}$ be a noncorresponding modulated sequence. For any integer $n = jq + k$ and $\tau = uq + v$, $1 \leq j, k \leq q - 1$, the integer $n + \tau$ can be represented as $n + \tau = (j + u + \epsilon)q + (k + v - \epsilon q)$, where $\epsilon = 0$, if $k + v \leq q - 1$, and $\epsilon = 1$, if $k + v \geq q - 1$. If the noncorresponding modulated sequence $s^{(s)}$ is input to the filter matched to the original

Frank sequence $f^{(r)}$, then the discrete output of the matched filter is given by (note: for original Frank sequence, $b_k^{(r)} = 1$)

$$\begin{aligned}
 R_{r,s}(uq + v) &= \sum_{n=0}^{q^2-1} s_{jq+k}^{(s)} f_{(jq+k)+(uq+v)}^{(r)*} \\
 &= \sum_{k=0}^{q-1} \sum_{j=0}^{q-1} b_k^{(s)} s_{jq+k}^{(s)} f_{(j+u+\epsilon)q+(k+v-\epsilon q)}^{(r)*} \\
 &= \sum_{k=0}^{q-1} b_k^{(s)} \alpha^{-r(u+\epsilon)(k+v-\epsilon q)} \sum_{j=0}^{q-1} \alpha^{kj(s-r)-jr(v-\epsilon q)} \quad (8.3) \\
 &= \sum_{k=0}^{q-1} b_k^{(s)} \alpha^{-r(u+\epsilon)(k+v)} \sum_{j=0}^{q-1} \alpha^{j(k(s-r)-rv)}
 \end{aligned}$$

The inner sum in Eqn 8.3 is equal to 0, if $k(s-r) - rv \neq 0$, and is equal to $q = \sqrt{L}$, if $k(s-r) - rv = 0$. Since q is a prime, $s-r \neq 0 \pmod{q}$, thus the equation $k(s-r) - rv = 0$ has a unique solution $k_0 = \frac{rv}{s-r}$. Hence

$$R_{r,s}(\tau) = q b_{k_0+v}^{(s)} \alpha^{-r(u+\epsilon)(k_0+v)} \quad (8.4)$$

If the corresponding modulated sequence $s^{(r)}$ is input to the filter matched to $f^{(r)}$, then from Eqn 8.3,

$$\begin{aligned}
 R_{r,r}(uq + v) &= \sum_{k=0}^{q-1} b_k^{(r)} \alpha^{-r(u+\epsilon)(k+v)} \sum_{j=0}^{q-1} \alpha^{-jrv} \\
 &= \begin{cases} q \sum_{k=0}^{q-1} b_k^{(r)} \alpha^{-ruk}, & v = 0 \\ 0, & v \neq 0 \end{cases} \quad (8.5)
 \end{aligned}$$

Now it is assumed that all the transmitters are synchronous, i.e. $\tau = uq + v = 0$. With this assumption,

$$R_{r,s}(0) = q b_0^{(s)}, \quad R_{r,r}(0) = q \sum_{k=0}^{q-1} b_k^{(r)} \quad (8.6)$$

In this synchronous SSMA, assume that the received signal is the noncorresponding modulated sequence $s^{(s)}$; if we sample the product sequence $s^{(s)} \cdot f^{(r)*}$

at $k, q+k, 2q+k, \dots, (q-1)q+k$ positions, then by summing these samples together we obtain the decoded output:

$$\begin{aligned}\hat{b}_k^{(r)} &= \sum_{j=0}^{q-1} s_{jq+k}^{(s)} f_{jq+k}^{(r)*} = \sum_{j=0}^{q-1} b_k^{(s)} \alpha^{sjk} \alpha^{-rjk} \\ &= b_k^{(s)} \sum_{j=0}^{q-1} \alpha^{jk(s-r)} = \begin{cases} qb_0^{(s)}, & k=0 \\ 0, & k \neq 0 \end{cases},\end{aligned}\quad (8.7)$$

where $qb_0^{(s)}$ represents the co-channel interference due to the existence of the noncorresponding received sequence $s^{(s)}$. Thus, all co-channel interference from any other users gathers into the first element in the output sequence. In order to correctly recover the desired information, the first element of $b^{(r)}$ should not carry information.

If the received signal is a corresponding modulated sequence $s^{(r)}$, we have the desired information (excluding $b_0^{(r)}$, which is contaminated by $b_0^{(s)}$):

$$\hat{b}_k^{(r)} = b_k^{(r)} \sum_{j=0}^{q-1} \alpha^{jk(r-r)} = qb_k^{(r)} \quad (8.8)$$

Therefore, for Frank sequences of length $L = q^2$, if each transmitter uses $q-1$ elements of $b^{(r)}$, except for the first element $b_0^{(r)}$, to carry information, the information can be conveyed without co-channel interference.

Similarly, for any modulatable Chu sequence $s^{(r)}$ of length $L = q^2$, where q is a prime, we have

$$s_n^{(r)} = b_n^r \text{ mod } q c_n^{(r)} = b_n^r \text{ mod } q e^{\frac{i\pi}{L} r(n+1)n}, \quad 0 \leq n < L; \quad (r, L) = 1. \quad (8.9)$$

where $|b_k^{(r)}| = 1$, $0 \leq k < m$, carries information; let $n = jq + k$, then

$$\begin{aligned}\hat{b}_k^{(r)} &= \sum_{j=0}^{q-1} s_n^{(s)} c_n^{(r)*} = \sum_{j=0}^{q-1} b_k^{(s)} \alpha^{\frac{s(n+1)n}{2q}} \alpha^{-\frac{r(n+1)n}{2q}} \\ &= b_k^{(s)} \alpha^{\frac{s-r}{2q}(k^2+k)} \sum_{j=0}^{q-1} \alpha^{j(s-r)(k+\frac{q+1}{2})} \\ &= \begin{cases} qb_{k_0}^{(s)} \alpha^{\frac{s-r}{2q}(k_0^2+k_0)}, & k = k_0 = \frac{q-1}{2} \\ 0, & k \neq k_0 = \frac{q-1}{2} \end{cases}\end{aligned}\quad (8.10)$$

$$\hat{b}_k^{(r)} = b_k^{(r)} \alpha^{\frac{r-r}{2q}(k^2+k)} \sum_{j=0}^{q-1} \alpha^{j(r-r)(k+\frac{q+1}{2})} = q b_k^{(r)} \quad (8.11)$$

It is clear that if each transmitter uses $q - 1$ elements of $b^{(r)}$, except for the element $b_{\frac{q-1}{2}}^{(r)}$, to carry information, the information can be carried without co-channel interference.

In this hybrid CCMA/SSMA scheme, in order to match the CCMA code and the SSMA spreading code, the block length of the CCMA codes should be equal to the number of information symbols carried by the modulatable code sequences.

Example 1: Given a 2-user binary adder channel CCMA system: user 1 has two codewords $C_1 = \{00, 11\}$ and user 2 has 3 codewords $C_2 = \{00, 10, 01\}$; the code lengths are all $n = 2$ and the overall rate sum achieved is $R_{sum} = 0.5 + 0.792 = 1.293$. Now let $q = 3$, $b_k^{(r)} = e^{\frac{j2\pi}{3} z_k^{(r)}}$, where $z_k^{(r)}$ means the k -th element of sum code $z^{(r)}$ in the r -th CCMA channel output, $r = 1, 2$. There are two original Frank sequences available and each is assigned to a CCMA user group. In other words, each of the original Frank sequences is modulated by a 2-user CCMA adder channel output.

It is assumed that the channel output of CCMA-1 is $z^{(1)} = (1, 2)$ and the channel output of CCMA-2 is $z^{(2)} = (0, 1)$. Let the unwanted first information element be $b_0^{(r)} = 1$, $r = 1, 2$; the modulated sequences are therefore given by

$$s^{(1)} = (1, e^{\frac{j2\pi}{3}}, e^{\frac{j2\pi}{3}2}; 1, e^{\frac{j2\pi}{3}} e^{\frac{j2\pi}{3}}, e^{\frac{j2\pi}{3}2} e^{\frac{j2\pi}{3}2}; 1, e^{\frac{j2\pi}{3}} e^{\frac{j2\pi}{3}2}, e^{\frac{j2\pi}{3}2} e^{\frac{j2\pi}{3}}) \quad (8.12)$$

$$s^{(2)} = (1, 1, e^{\frac{j2\pi}{3}}; 1, e^{\frac{j2\pi}{3}2}, e^{\frac{j2\pi}{3}} e^{\frac{j2\pi}{3}}; 1, e^{\frac{j2\pi}{3}}, e^{\frac{j2\pi}{3}} e^{\frac{j2\pi}{3}2}) \quad (8.13)$$

At each SSMA receiver, the received sequence is $s^{(1)} + s^{(2)}$. For receiver 1, the demodulated signal is $\hat{b}^{(1)} = (6, 3e^{\frac{j2\pi}{3}}, 3e^{\frac{j2\pi}{3}2})$, where

$$\hat{b}_k^{(1)} = \begin{cases} 3b_0^{(2)} + 3b_0^{(1)}, & k = 0 \\ 3b_k^{(1)}, & k \neq 0 \end{cases} \quad (8.14)$$

For receiver 2, the demodulated signal is $\hat{b}^{(2)} = (6, 3, 3e^{\frac{2\pi}{3}})$, where

$$\hat{b}_k^{(2)} = \begin{cases} 3b_0^{(1)} + 3b_0^{(2)}, & k = 0 \\ 3b_k^{(2)}, & k \neq 0 \end{cases} \quad (8.15)$$

Now the phase information of the last two elements of $\hat{b}^{(1)}$ and $\hat{b}^{(2)}$ is passed to each of the CCMA decoders. From the following look-up decoding Table 8.1, it can be seen that each of the 6 possible composite codewords, resulting from symbol-wise addition in the channel, is distinct and can therefore be unambiguously decoded into its constituent codewords. Thus the received composite codeword $\hat{z}^{(1)} = (1, 2)$ (or $\hat{z}^{(2)} = (0, 1)$) can be simply decoded into its constituent codewords: 11, 01 (or 00, 01).

Table 8.1: Look-up Decoding Table for the 2-user CCMA system

$C_1 + C_2$		User 1: C_1	
		00	11
User 2:	00	00	11
	10	10	21
C_2	01	01	12

Example 2: Given an 8-user Q-ary adder channel CCMA system with code length 12: assign each user a cyclic code with generator $h_i(x) = (x^{12}-1)/g_i^{k_i}(x)$, where $g_i^{k_i}(x)$ is an irreducible factor of $x^{12} - 1$ over Z_5 , i.e.

$$x^{12} - 1 = \frac{(x+1)(x+2)(x+3)(x+4)(x^2+x+1)}{(x^2+2x+4)(x^2+3x+4)(x^2+4x+1)}, \text{ over } Z_5 \quad (8.16)$$

If we use modulatable Chu sequences of length $L = 13^2$, then each original Chu sequence can carry $q - 1 = 12$ information symbols which match the elements of the composite codeword of CCMA channel output. In a manner similar to Example 1, we can build a hybrid CCMA/SSMA system with $8 \times (13 - 1) = 96$ users; any number of users less than or equal to 96 can be active simultaneously at any time! The encoding and decoding algorithms of both CCMA and SSMA are simple, as described above and in Chapter 3.

8.4 Concluding Remarks

In this chapter, a novel hybrid CCMA/SSMA coding scheme is proposed. For traditional SSMA, it is quite difficult to synthesize a large family of sequences with optimal correlation properties. For example, both Frank and Chu sequences and their generalizations have ideal ACFs and optimal CCFs; however for any given prime q , there are only $q - 1$ sequences of length $L = q^2$ that can

be obtained. Although there are some known large families of sequences (e.g. Gold Sequences etc.), because of their relatively high CCF values, the number of active users is not very large due to the fact that excessive co-channel interference cannot be tolerated in practical systems. The CCMA technique has the advantages of higher combined information rate and a larger number of permitted users, but its decoding complexity is prohibitively high for large number of users and most of the existing CCMA schemes are based on the assumptions of a noiseless synchronized channel and all users in the system always being simultaneously active. The new hybrid coding scheme provides a powerful multiple-access capability and a simple, efficient decoding method. In this coding scheme, only a small number of CCMA codes and spreading code sequences are needed to construct a large multiple-access system with many users. If the topology of the multi-access communications network is appropriate, then this hybrid CCMA/SSMA scheme becomes an attractive option.

Chapter 9

Conclusions and Recommendations for Further Work

The major research reported in this thesis has been carried out in order to investigate various multiple-access coding schemes to improve the efficiency of CCMA and SSMA communication system designs. These investigations involved the following main areas: multiple access channels, multiple access techniques, error-correcting codes, superimposed codes, cyclic multiaccess ring codes, orthogonal complementary sequences, real and complex sequences with optimal or near optimal correlations and hybrid CCMA/SSMA multiple-access coding.

This chapter summarises the work undertaken during the period of the research. Overall conclusions and a review of the original results obtained are given. Extensions and suggestions which the author feels to be worthy of further study are also described.

9.1 Conclusions

This research programme can be divided into three parts. The first part is concerned with CCMA coding (Chapters 2 and 3); the second part investigates the SSMA coding (Chapters 4,5,6 and 7); the third part studies the hybrid CCMA/SSMA coding (Chapter 8). Most of the results obtained in this thesis have been published in academic journals, edited books or conference proceedings. Appendix A is a list of papers which have either been published or submitted for publication, where the majority of the material in the first

part (Publications - After 1992) are the direct results of the work carried out by the author during the course of this research programme.

The first part of this research is contained in two chapters. Chapter 2 investigated the CCMA coding technique for the multiaccess binary adder channel and Chapter 3 considered CCMA coding for the multiaccess Q -ary adder channel. In both cases, a static assignment strategy has been used, i.e. each of the N users is given its own code and any T of the N distinct users can co-exist with each other for transmission over a given channel.

For the CCMA system with a multiaccess binary adder channel, a class of superimposed codes has been analysed. The superposition mechanism used is normal addition. By studying the relationship between the constant weight codes and disjunctive codes, some important results related to the decomposition of the disjunctive codes in the noiseless and noisy cases have been derived. It has been proved that if the number of active users $|A| \leq T \ll N$, we can decompose the composite received word into its component codewords in noiseless N-BAC. In the noisy case, the number of active users and the codewords can also be correctly recovered provided that the weight of the error pattern satisfies $Wt(e) = \sum_{j=1}^n |e_j| < \min \{w - \lambda|A|, \frac{w}{2}\}$. Several efficient decoding algorithms for both the noiseless and the noisy channel are developed. In this chapter, each user is given only one codeword; the code guarantees unique identification of all active users as long as the number of active users does not exceed T . However if each user has available a set of codewords, information can also be transmitted.

For the CCMA system with a multiaccess Q -ary adder channel, a class of cyclic uniquely decodable codes with symbols from an arbitrary finite integer ring has been proposed. The codes discussed can be used in the CCMA system with N users; any number of $T \leq N$ (not $T \ll N$) users can be simultaneously active at any time, and the channel output symbol value is the arithmetic sum of the Q -ary input symbol values, in the absence of noise. The code construction is based on the factorization of $x^n - 1$ over the unit ring of an appropriate extension of a finite integer ring. It has been shown that the class of codes can be identified uniquely. The maximum achievable sum rate is 1 when all users are active simultaneously. A remarkable advantage of this coding scheme is that it can be decoded by a very low complexity decoding algorithm. The decoder can easily identify all T active users (T is unknown in advance to the decoder), and correctly recover their respective messages.

The second part of the research is included in the subsequent 4 chapters. Chapter 4 deals with the design of orthogonal complementary codes for use in synchronous SSMA systems. Chapters 5,6 and 7 describe research into the code sequences used in asynchronous SSMA system. There are three basic require-

ments that all SSMA code sequences should meet: (1) a large family size of sequences due to the need to support a large number of simultaneous users; (2) small out-of-phase ACFs to allow unambiguous message synchronization; (3) small CCFs in order to minimize co-channel interference due to competing, simultaneous traffic components across the channel. The work of this part has contributed to various aspects of coding in the binary, real non-binary and complex domains.

For the synchronous SSMA system, a new approach employing orthogonal complementary sets has been presented in Chapter 4. In this chapter, the earlier concept of uncorrelated sets of complementary sequences has been extended to orthogonal sets of complementary sequences. It has been shown that the number of sets in an OCSS is much larger than the number of UCSS with the same parameters P and M . By clarifying the concepts of complementarity, uncorrelatedness and orthogonality, recursive formulas for constructing orthogonal complementary sets have been proposed; methods for synthesizing new orthogonal complementary sets from known ones with same dimensions have been discussed. Conjectures relating to maximally orthogonal complementary sets were also given. Lastly an application of orthogonal complementary sets to synchronous SSMA systems was described.

In Chapter 5, a new class of polyphase sequences with nearly minimal periodic auto- and crosscorrelation magnitudes has been presented. For any given prime length $L > 3$, there are L polyphase sequences. It is proved that the out-of-phase periodic ACFs and CCFs of the sequences are constant and equal to $\sqrt{L}$. Also, sequences of the same length are mutually orthogonal and the periodic correlation values asymptotically reach the Sarwate bound. In addition, it is shown that the nonperiodic and periodic ACFs/CCFs of the new sequences have nearly the same peak magnitude. For $L > 7$, the maximum nontrivial correlation parameter C_{max} of the new sequences is lower than that of Scholtz-Welch sequences.

In Chapter 6, maximal length sequences over Gaussian integers have been considered. The sequence symbols considered are required to be complex numbers, but their magnitudes are not all constant (note that in polyphase or PSK sequences, all symbols are on the unit circle in the complex plane). In this chapter, general properties of m-sequences over Gaussian integers have been discussed. Two sub-classes of m-sequences with quasi-perfect periodic ACFs have been obtained. The CCFs between the decimated m-sequences over Gaussian integers have also been studied. By applying a simple operation, it is shown that some m-sequences over rational and Gaussian integers can be transformed into perfect sequences with impulsive ACFs. The nonpolyphase complex sequences presented in this chapter have the potential for direct mapping to QAM-type constellations.

Chapter 7 is concerned with two classes of perfect codes, i.e. Frank codes and Chu codes. Apart from their periodic correlations, it is shown that they also have very favourable nonperiodic correlation properties. Some new results concerning the behaviour of the nonperiodic ACFs have been obtained. For Chu sequences, it is shown that the B_C^r is bounded by $\sqrt{L/4.34}$ if $r = 1$, and $0.48\sqrt{b/r}L$, if $r \geq 2$, $b/r \leq 0.37$; or $L/\pi \sin \pi b/r$, if $r \geq 2$, $b/r > 0.37$. For Frank sequences, it is shown that the B_F^1 , B_F^{q-1} , are asymptotic to q/π as q tends to infinity; when L is odd, $B_F^{\frac{L-1}{2}}$, $B_F^{\frac{L+1}{2}}$ are bounded by $2\sqrt{2}\frac{q}{\pi}$. It has been shown that Frank sequences have more symmetric structures and more favorable nonperiodic ACFs. It has also been proved that sets of combined Frank/Chu codes, which contain a larger number of codes than either of the two constituent sets, also have very good periodic correlation properties, and hence can be used in asynchronous SSMA to provide more users. Based on Frank codes and Chu codes, two interesting classes of real-valued codes with good correlation properties are defined. It is shown that these codes have periodic complementary properties. From the calculated ACF/CCF results, it has been demonstrated that they also have good periodic and nonperiodic ACF/CCFs.

The third part of the research is presented in Chapter 8. This part aims to link CCMA and SSMA. It has been focused on the coding and decoding techniques that are applicable for a large set of transmitters of which a variable subset is active simultaneously. The main advantages of SSMA are that it offers promise of reliable operation over dispersive radio paths and provides resistance against high levels of interference and jamming. However, due to the co-channel interference and the difficulty of obtaining a large number of good sequences, the achievable number of users is limited. The CCMA technique appears to be more attractive in practice because of its higher combined information rate and larger number of permitted users. However, most of the good codes have a very high decoding complexity and are based on the assumption of a noiseless synchronized adder channel with all the users in the system always simultaneously active. It is aimed that the hybrid scheme should provide a more powerful multiple-access capability and a better performance by exploiting their individual merits and reducing their individual disadvantages.

Chapter 8 proposes a novel hybrid CCMA/SSMA coding scheme. This hybrid scheme is a cascaded CCMA—SSMA scheme. The new hybrid coding scheme provides a very flexible and powerful multiple accessing capability and is compatible with a simple, efficient decoding method. Given an SSMA system with K users, a CCMA system with N users where at most T users active at any time, then the hybrid system will have $K \cdot N$ users with at most $T \cdot K$ users are active at any time. In this coding scheme, only a small number of CCMA codes and spreading code sequences are needed to construct a large multiple-access

system with many users. The hybrid CCMA/SSMA coding scheme is obviously superior to the individual CCMA system or SSMA system in terms of information rate, number of users, decoding complexity and external interference rejection capability.

9.2 Further Work

During the course of this research, some problems and conjectures which need further investigation have become apparent. The following are some recommended areas which the author feels to be worthy of further attention.

It has been shown in Chapter 2 that the size of the candidate CCMA code-word set can be reduced greatly by making use of the structure of the specific disjunctive code; however when T, N become large, the decoding complexity is still very high. Due to the regular structure of the constant weight codes, the large redundancy of the scheme ($T \ll N$) and the summation information due to the adder channel, it appears possible that more efficient decoding algorithms can be found. In the noisy case, neural network techniques might be employed in the decoding process with advantage.

In the work of Chapter 3, the construction of the multiaccess ring code is based on the factorization of $x^n - 1$ over the integer ring Z_Q , $Q = \sum_{i=1}^l p_i^{k_i}$. For the case of $(n, p_i) = 1$, $i = 1, \dots, l$, Shankar has proved that $x^n - 1$ be factored uniquely. However, if $(n, p_i) \neq 1$ then the factorization method is unknown and is not guaranteed to be unique. For example, $x^4 - 1 = (x^2 + 1)(x + 1)(x - 1) = (x + 3)^2(x^2 + 2x + 3)$ over Z_4 , where each of the factors is irreducible over Z_4 . In order to provide more choices for code design, it is desirable to find a systematic way of factorizing $x^n - 1$ over Z_Q , even if $(n, p_i) \neq 1$.

In SSMA communications, a large number of simultaneous users is normally required. Therefore, it is interesting to consider the maximum number of spreading sequences achievable. For the orthogonal complementary sets of sequences presented in Chapter 4, it has been shown that the number of orthogonal sets is much larger than the number of uncorrelated sets. The maximum number of orthogonal sets for a given length M and the number of sequences P in a set is unknown. It has been conjectured that the maximum number of orthogonal sets of CS is bounded by $N = PM$. By many exhaustive computer searches for small sequence lengths, this conjecture has been shown to be true. However it has not yet been proved analytically.

As far as the author is aware, there is no previous work on sequence design over Gaussian integers. In practice, it is of great interest to find such sequences

which are applicable to QAM types of signal formats. Chapter 6 is an attempt to fill this gap. By examining comprehensively, with the help of a computer, m-sequences over Gaussian integers, several useful results have been obtained. However, due to limited time, some of the results have not been proved analytically (for example, the weight distribution of the ACF).

For Chu sequences, two general bounds on the nonperiodic ACF have been established. Although several specific results for Frank sequences have been derived, the general behaviour of the nonperiodic ACF of Frank sequences remains an open problem.

For the real-valued sequences presented in Chapter 7, it has been shown that the sequences have very good ACFs and CCFs. Specifically, it has been conjectured that their out-of-phase ACF and periodic CCFs are asymptotic to $O(c\sqrt{L})$. It would be useful to prove this conjecture.

In the context of the hybrid CCMA/SSMA coding scheme, it appears necessary to develop a complete, operational hybrid CCMA/SSMA communication system and to compare its performance with that of individual CCMA and SSMA systems for a range of practical channel conditions.

References

- Abdul-Jabbar, S., & Laval, P. de. 1988 (Jun.). Constant weight codes for multiaccess channels without feedback. *Pages 150 – 153 of: Conf. Proc. on Area Comm., EUROCOM 88, Stockholm, Sweden.*
- Abramson, N. 1970. The ALOHA system - Another alternative for computer communications. *In: Proc. Fall Joint Computer Conf. AFIPS Conf., vol. 37.*
- Abramson, N. 1985. Development of the ALOHANET. *IEEE Trans. Inform. Theory*, IT-31(2), 119–123.
- Ahlsvede, R. 1971. Multi-way communication channels. *Pages 23–52 of: Proc. 2nd Int. Symp. Information Theory. Tsahkadsor, Armenia, USSR: Publishing House of the Hungarian Acad. Sc.(1973).*
- Alltop, W. O. 1980. Complex sequences with low periodic correlations. *IEEE Trans. Inform. Theory*, IT-26(3), 350–354.
- Andres, T. H., & Stanton, R. G. 1977. *Combinatorial Mathematics V, Lecture Notes in Mathematics*. Vol. 622. Melbourne: Berlin/New York:Springer-Verlag.
- Antweiler, M., & Bömer, L. 1990. Merit factor of Chu and Frank sequences. *IEE Electronic Letters*, 26(Dec. 6), 2068–2070.
- Bar-David, I., Plotnik, E., & Rom, R. 1987 (June 21-25). The capacity of the synchronizd random multiple-access channel is at least 1, achievable by forward collision resolution. *In: 1987 IEEE Inform. Theory Workshop, Bellagio, Italy.*
- Barker, R. H. 1953. *Communication Theory*(Jackson, W., Ed.). Butterworths, London. Chap. Group synchronising of binary digital systems, pages 273 – 287.
- Bömer, L., & Antweiler, M. 1992. Perfect N-phase sequences and arrays. *IEEE Journal on Selected Areas in Communications*, 10, 782–789.

- Berlekamp, E. R. 1968. *Algebraic Coding Theory*. New York: McGraw-Hill, Inc.
- Bertsekas, D., & Gallager, R. 1992. *Data Networks*. 2nd edn. Prentice-Hall, International, Inc.
- Best, M. R., Brouwer, A. E., MacWilliams, F. J., Odlyzko, A. M., & Sloane, N. J. 1966. Bounds for binary codes of length less than 25. *IEEE Trans. Inform. Theory*, 12(2), 92 – 96.
- Blake, I. F., & Mark, J.W. 1982. A note on complex sequences with low correlations. *IEEE Trans. on IT*, 28(5), 814–816.
- Bomer, L., & Antweiler, M. 1991 (June 24-28). New perfect threelevel and threephase sequences. *Page 280 of: IEEE Int. Symp. Inform. Theory, Budapest, Hungary.*
- Boztas, S., & Kumar, P. V. 1994. Binary sequences with Gold-like correlation but larger linear span. *IEEE Trans. on IT*, IT-40(2), 532–537.
- Boztas, S., Hammons, R., & Kumar, P. V. 1992. 4-phase sequences with near-optimum correlation properties. *IEEE Trans. on IT*, 38(3), 1101–1113.
- Braak, P.A.B.M.Coebrgh van den, & Tilborg, H.C.A.van. 1985. A family of good uniquely decodable code pairs for the two-access binary adder channel. *IEEE Trans. on Information Theory*, IT - 31(1), 3–9.
- Budisin, S. Z. 1990a. New complementary pairs of sequences. *IEE Electronic Letters*, 26(13), 881–883.
- Budisin, S. Z. 1990b. New multilevel complementary pairs of sequences. *IEE Electronic Letters*, 26, 1861–1863.
- Chang, J. A. 1967. Ternary sequence with zero correlation. *Proceedings of the IEEE*, 55(7), 1211–1213.
- Chang, S.C. 1984. Further results on coding for T-user multiple-access channels. *IEEE Trans. on IT*, IT-30(2), 411–415.
- Chang, S.C., & Weldon Jr., E.J. 1979. Coding for T-user multiple-access channels. *IEEE Trans. on IT*, IT-25(6), 684–691.
- Chang, S.C., & Wolf, J.K. 1981. On the T-user M-frequency noiseless multiple-access channel with and without intensity information. *IEEE Trans. on IT*, IT-27(1), 41–48.
- Chien, R. T., & Frazer, W. D. 1966. An application of coding theory to document retrieval. *IEEE Trans. Inform. Theory*, 12(2), 92 – 96.

- Chu, D. C. 1972. Polyphase codes with good periodic correlation properties. *IEEE Trans. on Information Theory*, IT - 18(July), 531-533.
- Chung. 1972. Generalized bent ... *IEEE Trans. on Information Theory*, IT - 18(July), 531-533.
- Cohen, A. R., Heller, J.A., & Viterbi, A.J.. 1971. A new coding technique for asynchronous multiple access communication. *IEEE Trans. Commun. Thch.*, COM - 19(October), 849-855.
- Cover, T.M. 1975. *Advances in Communication Systems*(Viterbi, A. Ed.). San Francisco: Academic Press. Chap. Some advances in Broadcast Channels.
- Csiszar, I., & Körner. 1981. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic. Chap. 3.
- da Rocha Jr., V. C. 1993a (July). Complementary cyclic codes. *Pages 37-42 of: IEE Int. Symp. on Commun. Theory & Appl.*
- da Rocha Jr., V. C. 1993b (Jan). On cyclic codes for the T-user Q-ary adder channel. *Page 80 of: IEEE Int. Symp. on Inform. Theory*. San Antonio, USA.
- da Rocha Jr., V. C., Markarian, G., & Honary, B. 1993. Trellis decoding of block codes for the 2-user binary adder channel. *Pages 1-8 of: ICC'93*.
- Darnell, M. 1989. *Cryptography and Coding*. The IMA Conference series. Clarendon press, Oxford(Beker, H.J. and Piper, F.C. Eds.). Chap. The theory and generation of sets of uncorrelated digital sequences, pages 23-65.
- Darnell, M. 1993a. Analogue pseudorandom waveforms for communications applications. *Pages 39-41 of: 4th IMA Conference on Cryptography and Coding*.
- Darnell, M. 1993b. *Perturbation Signals for System Identification*(Ed. K. R. Godfrey). Prentice-Hall. Chap. Periodic and non-periodic, binary and multi-level pseudo-random signals, pages 176-208.
- Darnell, M., & Kemp, A. H. 1989 (Dec.). Multilevel complementary sequence sets: synthesis and applications. *Pages 37 - 67 of: Proc. 2nd IMA Int. Conf. on 'Cryptography and Coding'*.
- Darnell, M., Fan, P. Z., & Jin, F. 1994. New classes of perfect sequences derived from m-sequences. *submitted to 1995 IEEE International Symposium on Information Theory, Whistler, Canada*.

- de Visme, G. H. 1971. *Binary Sequences*. London, England: The English Universities Press.
- Deaett, M.A., & Wolf, J.K. 1978. Some very simple codes for the nonsynchronized two-user multiple-access adder channel with binary inputs. *IEEE Transactions on Information Theory*, IT-24(5), 635-636.
- Dixon, R. C. 1984. *Spread Spectrum Systems*. 2nd edn. John Wiley & Sons.
- Egri, R.G., & Horrigan, F. A. 1994. A finite group of complex integers and its application to differentially coherent detection of QAM signals. *IEEE Transactions on Information Theory*, 40(1), 216-219.
- Eliahou, S., Kervaire, M., & Saffari, B. 1990. A new restriction on the lengths of Golay complementary sequences. *Journal of Combinatorial Theory (A)*, 55, 49-59.
- Ericson, T. 1987. Concatenated codes and constant weight codes for multiple access communication. *Pages 956 - 958 of: International Conference on Communications*.
- Ericson, T., & Györfi, L. 1988. Superimposed codes in R^n . *IEEE Trans. Inform. Theory*, 34(4), 877 -880.
- Ericson, T., & Levenshtein, V. 1993 (Jan.). Superimposed codes in Hamming space. *Page 296 of: IEEE International Symposium on Information Theory, Austin TX*.
- Everett, D. 1966. Periodic digital sequences with pseudonoise properties. *G.E.C. Journal*, 33, 115-126.
- Fan, P. Z., & Darnell, M. 1994a. Aperiodic autocorrelation of Frank Sequences. *submitted to IEE Proceedings Pt. F*.
- Fan, P. Z., & Darnell, M. 1994b. Hybrid CCMA/SSMA coding scheme. *IEE Electronic Letters*, 30(25), 2105-2106.
- Fan, P. Z., & Darnell, M. 1994c. Maximal length sequences over Gaussian integers. *Electron. Lett.*, 30(16), 1286-1287.
- Fan, P. Z., & Darnell, M. 1994d (December 12-14). On Real and complex sequences with good correlation functions. *Pages 1-5 of: Third UK/Australian International Symposium on 'DSP For Communication Systems', Session 1*.
- Fan, P. Z., Darnell, M., & Honary, B. 1993a (May). New class of CDMA systems using orthogonal complementary sequences. *Pages 251-254 of: Fifth Bangor Symposium on Communications*.

- Fan, P. Z., Darnell, M., & Honary, B. 1993b (July). Orthogonal complementary pairs of sequences. *Pages 118-121 of: 2nd International Symposium on Communication Theory and applications.*
- Fan, P. Z., Darnell, M., & Honary, B. 1994a. *Codes and Cyphers* (Ed. P. G. Farrell). Oxford University Press. also presented in Fourth IMA Conference on Cryptography and Coding (Cirencester, UK, December 1993). Chap. Orthogonal complementary sets of sequences, pages 11-18.
- Fan, P. Z., Darnell, M., & Honary, B. 1994b. Crosscorrelations of Frank sequences and Chu sequences. *Electron. Lett.*, 30(6), 477-478.
- Fan, P. Z., Darnell, M., Honary, B., & da Rocha Jr., V.C. 1994c. Cyclic codes for the T-user adder channel over integer rings. *Electron. Lett.*, 30(3), 209-210.
- Fan, P. Z., Darnell, M., & Honary, B. 1994d. New class of polyphase sequences with two-valued auto- and crosscorrelation functions. *Electron. Lett.*, 30(13), 1031-1032.
- Fan, P. Z., Darnell, M., & Honary, B. 1994e (June). Polyphase sequences with good periodic and aperiodic autocorrelations. *Page 145 of: 1994'IEEE Symposium on Information Theory.*
- Fan, P. Z., Darnell, M., & Honary, B. 1995. Superimposed codes for multiaccess binary adder channel. *accepted, to appear in IEEE Transactions on Information Theory*, IT-41(1). (also presented partly in 1994'IEEE Int. Workshop on IT, Proc. pages 30-32, Moscow, July 3-8 1994).
- Farrell, P.G. 1981. Survey of channel coding for multi-user systems. *Pages 133-159 of: Skwirzynski, J.K., & aan den Riin, Ed. Alphen (eds), New Concepts in Multi-User Communication.*
- Ferguson, T.J. 1982. Generalized T-user codes for multiple-access channels. *IEEE Trans. Inform. Theory*, IT-28(5), 775-778.
- Frank, R. L. 1963. Polyphase codes with good nonperiodic correlation properties. *IEEE Trans. on Information Theory*, IT - 9(January), 43-45.
- Frank, R. L. 1973. Comments on Polyphase codes with good correlation properties. *IEEE Trans. on Information Theory*, IT - 19(March), 244.
- Frank, R. L. 1980. Polyphase complementary codes. *IEEE Trans. on Information Theory*, IT-26(6), 641-647.

- Frank, R. L., & Zadoff, S. A. 1962. Phase shift pulse codes with good periodic correlation properties. *IRE Trans. on Information Theory*, IT - 8(October), 381-382.
- Gabidulin, E. M. 1993 (January). Non-binary sequences with the perfect periodic auto-correlation and with optimal periodic cross-correlation. *Page 412 of: Proc. IEEE Int. Symp. Inform. Theory.*
- Gabidulin, E. M., Fan, P. Z., & Darnell, M. 1994. On the autocorrelation of Golomb sequences. *submitted to IEE Proceedings Pt. F.*
- Gallager, R.G. 1985. A perspective on multiaccess channels. *IEEE Trans. Inform. Theory*, IT-31(2), 124-142.
- Gamal, A.El, & Cover, T.M. 1980. Multiple user information theory. *Proc. of the IEEE*, 68(12), 1466-1483.
- Golay, M. J. E. 1961. Complementary series. *IRE Trans. on Information Theory*, IT-7(April), 82-87.
- Golomb, S. W. 1967. *Shift Register Sequences*. San Francisco, California: Holden-Day.
- Golomb, S. W., & Scholtz, R. A. 1965. Generalised Barker sequences. *IEEE Trans. on Information Theory*, IT-11(4), 533-537.
- Griffin, M. 1977. There are no Golay complementary sequences of length $2 \cdot 9^t$. *Aequationes Mathematicae*, 15, 73-77.
- Gutleber, F. S. 1982 (October). Spread spectrum multiplexed noise codes. *Pages 15.1.1-15.1.10 of: MILCOM'82 Conference Record.*
- Gyorf, L. 1981. A block code for noiseless asynchronous multiple access OR channel. *IEEE Trans. on IT*, 27(6), 788-791.
- Hardy, G.H., & Wright, E.M. 1979. *An introduction to the theory of Numbers*. 5th edn. Oxford University Press.
- Heimiller, R. C. 1961. Phase shift pulse codes with good periodic correlation properties. *IRE Trans. on IT*, IT-7, 254-257.
- Heimiller, R. C. 1962. Author's comment. *IRE Trans. on IT*, IT-8(Oct.), 382.
- Helleseth, T. 1976. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, 16, 209-232.
- Hoholdt, T., & Justesen, J. 1983. Ternary sequences with perfect periodic autocorrelation. *IEEE Trans. on IT*, 29(4), 597-600.

- Huber, K. 1994. Codes over Gaussian integers. *IEEE Transactions on Information Theory*, 40(1), 207–216.
- Ipatov, V. P. 1979. Multiphase sequences spectrums. *Izvestiya VUZ. Radioelektronika (Radioelectronics and Communications Systems)*, 22(9), 80–82.
- Kasami, T., & Lin, S. 1976. Coding for a multiple-access channel. *IEEE Trans. Inform. Theory*, IT-22(2), 129–137.
- Kasami, T., Lin, S., & Yamamura, S. 1975a (Aug.). Further results on coding for a multiple access channel. *Pages 369–391 of: Conf. Proc., Hungarian Colloq. on Inform. Theory.*
- Kasami, T., Lin, S., & Yamamura. 1975b. *Topics in Information Theory* (I. Csiszar and P. Elias, Ed.). New York: North-Holland Publishing Company. Chap. Further results on coding for a multiple-access channel, pages 369– 392.
- Kasami, T., Lin, S., Wei, V.K., & Yamamura, S. 1983. Graph theoretic approaches to the code construction for the two-user multiple-access binary adder channel. *IEEE Trans. Inform. Theory*, IT-29(1), 114–130.
- Kautz, W. H., & Singleton, R. C. 1964. Nonrandom binary superimposed codes. *IEEE Trans. Inform. Theory*, 10(4), 363 – 377.
- Khachatrian, G.H. 1982. On the construction of codes for noiseless synchronized 2-user channels. *Prob. Contr. on Inform. Theory*, 11, 319–324.
- Khachatrian, G.H. 1983. Decoding for a noiseless adder channel with two users. *Prob. Peredach. on Inform*, 19(2), 8–13.
- Khachatrian, G.H. 1988. δ -decodable code constructions for a T-user adder channel. *Prob. Peredach. on Inform*, 24(2), 94–99.
- Khachatrian, G.H. 1989 (Aug.27-Sept.1). New code constructions for binary switching two-user channel. *Pages 122–126 of: Proc. 4th Joint Swedish-Soviet Int. Workshop Inform. theory.*
- Kleinrock, L., & Tobagi, F.A. 1975. Packet switching in radio channels: Part 1: CSMA modes and their throughput-delay characteristics. *IEEE Transactions on Communication*, COM-23(Dec.), 1400–1416.
- Kretschmer Jr., F. F., & Gerlach, K. 1991. Low sidelobe radar waveforms derived from orthogonal matrices. *IEEE Trans. on AES*, AES-27(1), 92–101.

- Krone, S.M., & Sarwate, D. V. 1984. Quadriphase sequences for spread-spectrum multiple-access communication. *IEEE Trans. Inform. Theory*, IT-30(3), 520-529.
- Kruskal, J. B. 1961. Golay's complementary series. *IRE Trans. on Information Theory*, IT-7(October), 273-276.
- Kumar, P. V., & Moreno, O. 1991. Polyphase sequences with periodic correlation properties better than binary sequences. *IEEE Trans. on IT*, 37(3).
- Kumar, P.V., Scholtz, R. A., & Welch, L. R. 1985. Generalized bent functions and their properties. *J. Combinat. Theory, series A*, 40(1), 90-107.
- Laval, P. de., & Abdul-Jabbar, S. 1988 (Jun.). Decoding of superimposed codes in multiaccess communication. *Pages 154 - 157 of: Conf. Proc. on Area Comm., EUROCOM 88, Stockholm, Sweden.*
- Lüke, H. D. 92. Families of polyphase sequences with near-optimal two-valued auto- and crosscorrelation functions. *Electron. Lett.*, 1(January), 1-2.
- Lempel, A., & Cohn, M. 1982. Maximal families of bent sequences. *IEEE Trans. on IT*, 28(6), 865-868.
- Lewis, B. L., & Kretschmer, F. F. 1982. Linear frequency modulation derived polyphase pulse compression. *IEEE Trans. on AES*, AES-18(5), 637-641.
- Liao, H. 1972. A coding theorem for multiple access communications. *In: Proc. Int. Symp. Inform. Theory, Asilomar, CA.*
- Lin, S., & Wei, V.K. 1986. Nonhomogeneous trellis codes for the quasi-synchronous multiple-access binary adder channel with two users. *IEEE Trans. on IT*, IT-32(6), 787-796.
- MacWilliams, F. J., & Sloane, N. J. A. 1977. *The theory of error-correcting codes*. New York: North-Holland.
- MacWilliams, F.J., & Sloane, N.J. 1976. Pseudo-random sequences and arrays. *Proceedings of the IEEE*, 64(December), 1715-1729.
- Massey, J. L. 1986 (July 7-19). Channel models for random-access systems. *In: NATO Advanced Study Institute on 'Performance Limits in Communications Theory and Practice'.*
- Massey, J.L. 1985. Special issue on random-access communications. *IEEE Trans. on Inform. Theory*, IT-31(2), 117-310.
- Massey, J.L., & Mathys, P. 1985. The collision channel without feedback. *IEEE Trans. on Inform. Theory*, IT-31(2), 192-204.

- Mathys, P. 1990. A class of codes for T active users out of N multiple-access communication system. *IEEE Trans. on IT*, 36(6), 1206-1219.
- Meulen van der, E.C. 1971. The discrete memoryless channel with two senders and one receiver. *Pages 103-135 of: Proc. 2nd Int. Symp. Information Theory*. Tsahkadsor, Armenian, USSR: Publishing House of the Hungarian Acad. Sc.(1973).
- Meulen van der, E.C. 1977. A survey of multi-way channels in information theory: 1961-1976. *IEEE Trans on Inform. Theory*, IT-23(1), 1-37.
- Milewski, A. 1983. Periodic sequences with optimal properties for channel estimation and fast start-up equalization. *IBM J. RES. DEVELOP.*, 27(5), 426-431.
- Miller, T.E. 1990 (October). A reliable multi-user distributive HF communications system using narrowband CDMA. *Pages 31.1-31.7 of: AGARD EPP Specialists Meeting*.
- Miller, T.E., & Darnell, M. 1990 (September). In-band CDMA: sequence options. *Pages 1-5 of: Proc. IEEE Symp. on 'Spread-Spectrum Techniques and Applications'*.
- Mow, W. H., & Li, S.-Y. R. 1992. Aperiodic autocorrelation properties of perfect polyphase sequences. *Pages 1-3 of: Proc. of Singapore ICCS/ISITA '92*.
- Mow, W.H. 1994. On the bounds on odd correlation of sequences. *IEEE Trans. on IT*, 35(3), 954-955.
- Ni, J., & Honary, B. 1993. System state-independent-unique-decodable CCMA codes. *Proc. IEE, Part I, Communications, Speech and Vision*, 140(3), 185-189.
- No, J.D., & Kumar, P.V. 1989. A new family of binary pseudorandom sequences having optimal correlation properties and large linear span. *IEEE Trans.on IT*, 35(Mar.), 371-379.
- Novosad, T. 1993. A new family of quadriphase sequences for CDMA. *IEEE Trans. Inform. Theory*, IT-39(3), 1083-1085.
- Olsen, J.D., Scholtz, R.A., & Welch, L.R. 1982. Bent-function sequences. *IEEE Trans.on IT*, IT-28(November), 858-864.
- Pickholtz, R.L., Schilling, D. L., & Milstein, L. B. 1982. Theory of spread-spectrum communications-a tutorial. *IEEE Trans. on Communications*, COM-30(5), 855-884.

- Popović, B. M. 1992. Generalized chirp-like polyphase sequences with optimum correlation properties. *IEEE Trans. on Information Theory*, IT - 38(4), 1406–1409.
- Popović, B. M. 1994a. Efficient matched filter for the generalized chirp-like polyphase sequences. *IEEE Trans. on Aerospace and Electronic Systems*, 30(3), 769–777.
- Popović, B. M. 1994b. GCL polyphase sequences with minimum alphabets. *Electron. Lett.*, 30(2), 106–107.
- Popovic, B. M. 1991a. Comment on merit factor of Chu and Frank sequences. *IEE Electronic Letters*, 27(9), 776–777.
- Popovic, B. M. 1991b. Complementary sets of chirp-like polyphase sequences. *Electron. Lett.*, 27(3), 254–255.
- Pursley, M.B. 1977. Performance evaluation for phase-coded spread spectrum multiple-access communication-part I: system analysis. *IEEE Transactions on Communications*, COM-25(Aug.), 795–799.
- Pursley, M.B., & Roefs, H.F.A. 1977. Numerical evaluation of correlation parameters for optimal phases of binary shift-register sequences. *IEEE Transactions on Communications*, COM-25(Aug.), 1597–1604.
- Pursley, M.B., & Sarwate, D.V. 1977. Performance evaluation for phase-coded spread spectrum multiple-access communication-part II: code sequence analysis. *IEEE Transactions on Communications*, COM-25(Aug.), 800–803.
- Sarwate, D. V. 1979. Bounds on crosscorrelation and autocorrelation of sequences. *IEEE Transactions on Information Theory*, 25, 720–724.
- Sarwate, D. V., & Pursley, M. B. 1980. Crosscorrelation properties of pseudo-random and related sequences. *Proceedings of the IEEE*, 68(5), 593–620.
- Schalkwijk, J.P.M. 1982. The binary multiplying channel—a coding scheme that operates beyond Shannon’s inner bound region. *IEEE Trans.on IT*, IT-28(1), 107–110.
- Schalkwijk, J.P.M. 1983. On an extension of an achievable rate region for the binary multiplying channel. *IEEE Trans.on IT*, IT-29(3), 445–448.
- Schilling, D.L., Milstein, L. B., Pickholtz, R.L., Kullback, M., & Miller, F. 1991. Spread spectrum for commercial communications. *IEEE Communications Magazine*, 29(2), 66–79.

- Scholtz, R.A. 1982. The origins of the spread-spectrum communications. *IEEE Trans.on Communications*, COM-30(5), 822-854.
- Scholtz, R.A., & Welch, L.R. 1978. Group characters: sequences with good correlation properties. *IEEE Trans.on IT*, IT-24(5), 537-545.
- Scholtz, R.A., & Welch, L.R. 1984. GMW sequences. *IEEE Trans.on IT*, IT-30(May), 548-553. .
- Schweitzer, B. P. 1971. *Generalised Complementary Code sets*. Ph.D. thesis, University of California, Los Angeles, California, USA.
- Shankar, P. 1979. On BCH codes over arbitrary integer rings. *IEEE Trans. on IT*, 25(4).
- Shannon, C. E. 1961. Two-way communication channels. *Pages 611-644 of: Proc. 4th Berkeley Symp. Math. Statist. and Prob., Vol.1.*
- Shedd, D. A., & Sarwate, D. V. 1979. Construction of sequences with good correlation properties. *IEEE Transactions on Information Theory*, 25(1), 94-97.
- Sidel'nikov, V. M. 1971. On mutual correlation of sequences. *Soviet Math Doklady*, 12.
- Simon, M.K., Omura, J.K., Scholtz, R.A., & Levitt, B.K. 1985. *Spread-spectrum Communications*. Rockville,MD: Computer Science.
- Sivaswamy, R. 1978. Multiphase complementary codes. *IEEE Trans. on Information Theory*, IT-24(5), 546-552.
- Slepian, D., & Wolf, J.K. 1973. A coding theorem for multiple access channels with correlated sources. *Bell System Tech.J.*, 52(September), 1037-1076.
- Sommer, R.C. 1968. High efficiency multiple access communication through a signal processing repeater. *IEEE Trans. Commun. Tech.*, COM-16(April), 222-232.
- Suehiro, N., & Hatori, M. 1988. Modulatable orthogonal sequences and their application to SSMA systems. *IEEE Trans. on Information Theory*, IT - 34(Jan.), 93-100.
- Taki, Y., Miyakawa, H., Hatori, M., & Namba, S. 1969. Even-shift orthogonal sequences. *IEEE Transactions on Information Theory*, IT-15(March), 295-300.

- Taylor, J., & Omura, J.K. 1991. Spread spectrum technology: a solution to the personal communications services frequency allocation dilemma. *IEEE Communications Magazine*, 29(1), 48-54.
- Tseng, C. C., & Liu, C. L. 1972. Complementary sets of sequences. *IEEE Transactions on Information Theory*, 18(5), 644-652.
- Turyn, R. 1963. Ambiguity functions of complementary sequences. *IEEE Trans. on Information Theory*, IT-9(January), 46-47.
- Turyn, R. J. 1967. The correlation function of a sequence of roots of 1. *IEEE Trans. on Information Theory*, IT-13(July), 524-525.
- Turyn, R. J. 1974. Hadamard matrices, Baumert-Hall units, four symbol sequences, pulse compression and surface wave encodings. *Journal of Combinatorial Theory (A)*, 16, 313-333.
- Vanroose, P. 1988. Code construction for the noiseless binary switching multiple-access channel. *IEEE Trans. on Inform. Theory*, 34(5), 1100-1106.
- Vanroose, P., & van der Meulen, E. C. 1987 (May 24-30). On the construction of block codes for the two-user binary switching multiple-access channel. Pages 327-330 of: *Proc. 3rd Joint Swedish-Soviet Int. Workshop Inform. theory*.
- Viterbi, A. J. 1978. A processing satellite transponder for multiple access by low-rate mobile users. Pages 166-171 of: *4th Int. Conf. on Digital Satellite Communication*.
- Welch, L. R. 1974. Lower bounds on the maximum cross correlation of signals. *IEEE Trans. on IT*, 20.
- Weldon Jr., E.J.. 1978. Coding for a multiple-access channel. *Inform. Contr.*, 36(3).
- Welti, G. R. 1960. Quaternary codes for pulsed radar. *IRE Trans. on Information Theory*, IT-6(June), 400-408.
- Wen, Tong, & Guangguo, Bi. 1987 (November). Application of orthogonal complementary pair of sequences to CDMA-QAM communication system. Pages 826-829 of: *ICCT'87*.
- Wilson, J.H. 1988. Error-correcting codes for a T-user binary adder chsnnel. *IEEE Trans. on Inform. Theory*, 34(4), 888-890.

- Wolf, J.K. 1975. *Information Theory: New Trends and Open Problems*, CISM Courses and Lectures No.219(Longo, G., Ed.). Springer-Verlag. Chap. Constructive Codes for Multi-user Communication Channels.
- Wolf, J.K. 1981. Coding techniques for multiple access communication channels. Pages 83-103 of: Skwirzynski, J.K., & aan den Rijn, Ed.Alphen (eds), *New Concepts in Multi-User Communication*.
- Wyner, A.D. 1974. Recent results in the Shannon theory. *IEEE Trans. on Inform. Theory*, 20(1), 2-10.
- Zhang, N., & Golomb, S. W. 1993. Polyphase sequence with low autocorrelations. *IEEE Trans. on Information Theory*, IT - 39(May), 1085-1089.

Appendix A

Publications of the Author

A.1 Publications—After 1992

1. P. Z. Fan, M. Darnell. Hybrid CCMA/SSMA coding scheme. *Electron. Lett.*, 30(25):2105–2106, December 1994.
2. P. Z. Fan, M. Darnell, and B. Honary. Superimposed codes for multiaccess binary adder channel. *accepted, to appear in IEEE Transactions on Information Theory*, 41, 1995. (also presented partly in 1994'IEEE Int. Workshop on IT, Proc. pages 30-32, Moscow, July 3-8 1994).
3. P. Z. Fan, M. Darnell. Maximal length sequences over Gaussian integers. *Electron. Lett.*, 30(16):1286–1287, August 1994.
4. P. Z. Fan, M. Darnell, and B. Honary. New class of polyphase sequences with two-valued auto- and crosscorrelation functions. *Electron. Lett.*, 30(13):1031–1032, June 1994.
5. P. Z. Fan, M. Darnell, and B. Honary. Crosscorrelations of Frank sequences and Chu sequences. *Electron. Lett.*, 30(6):477–478, March 1994.
6. P. Z. Fan, M. Darnell, and B. Honary, and V. C. da Rocha Jr. Cyclic codes for the T-user adder channel over integer rings. *Electron. Lett.*, 30(3):209–210, February 1994.
7. P. Z. Fan, M. Darnell, and B. Honary. Orthogonal complementary sets of sequences. In *Codes and Cyphers* (Ed. P. G. Farrell), pages 11–18, Oxford University Press, 1994 (also presented in Fourth IMA Conference on Cryptography and Coding, Cirencester, UK, December 1993)

8. P. Z. Fan, M. Darnell. On Real and complex sequences with good correlation functions. *Third UK/Australian International Symposium on 'DSP For Communication Systems', Session 1, December 12-14, 1994, Coventry, UK, pages 1-5.*
9. M. Darnell, P. Z. Fan, and F. Jin. New classes of perfect sequences derived from m-sequences. *submitted to 1995'IEEE International Symposium on Information Theory, Whistler, Canada .*
10. P. Z. Fan, M. Darnell. Balanced quadriphase sequences with near-ideal autocorrelations. *submitted to 1995'IEEE International Symposium on Information Theory, Whistler, Canada .*
11. P. Z. Fan, M. Darnell, and B. Honary. Polyphase sequences with good periodic and aperiodic autocorrelations. *Proceedings of 1994'IEEE Symposium on Information Theory, Trondheim, Norway, June 26-1July, 1994, page 145.*
12. P. Z. Fan, M. Darnell. Aperiodic autocorrelation of Frank Sequences. *submitted to IEE Proceedings Pt. F.*
13. E. M. Gabidulin, P. Z. Fan, M. Darnell. On the autocorrelation of Golomb sequences. *submitted to IEE Proceedings, Part F..*
14. P. Z. Fan, M. Darnell, and B. Honary. New class of CDMA systems using orthogonal complementary sequences. In *Fifth Bangor Symposium on Communications*, pages 251–254, Bangor, UK, June 1993.
15. P. Z. Fan, M. Darnell, and B. Honary. Orthogonal complementary pairs of sequences. In *2nd International Symposium on Communication Theory and applications*, pages 118–121, Ambleside, Lake District, UK, July 1993.
16. P. Z. Fan, B. Honary, and M. Darnell. Quasi-synchronous CDMA systems: sequence options. *accepted by International Conference on Communications, Dubai-United Arab Emirates, January 1994.*
17. P. Z. Fan. Fast soft decision decoding of block codes. In *Fourth Bangor Symposium on Communications*, pages 311–314, Bangor, UK, May 1992.
18. P. Z. Fan, M. Darnell, Z. Chen, and F. Jin. Adaptive hybrid ARQ scheme using multidimensional parity-check codes. *Electron. Lett.*, 29(2):196–198, January 1993.
19. Z. Chen, P. Z. Fan, and F. Jin. On the constructions of multiple-burst error-correcting codes. *IEEE Transactions on Information Theory*, 38(1):197–200, January 1992.

20. Z. Chen, P. Z. Fan, and F. Jin. Disjoint difference sets, difference triangle sets and related codes. *IEEE Transactions on Information Theory*, 38(2):518–522, March 1992.

A.2 Publications–Before 1992

1. P. Z. Fan. *English for Special Science and Technology*, pages 1–244. Southwest Jiaotong University Press, China, 1989.
2. J. Y. Chen, P. Z. Fan and J. G. Liu. *Management Information System*, pages 1–323. China Railway Publishing Co., 1991.
3. P. Z. Fan. *High Speed Two-error-correcting Encoder/Decoder*. Chinese Patent, Int. C1 H03M 13/00, 1990. Issued No.41387.
4. P. Z. Fan. A survey of current situation made for local network of microcomputer. *Electronic Science and Technology*, 16(9):6–16, 1986.
5. P. Z. Fan. Practical fault diagnosis method for digital circuit. *Application Research of Computers*, 4(2):87–93, 1987.
6. P. Z. Fan. The measurement of channel bit-error probability and error distribution using microcomputer. *Journal of Electronic Measurement and Instrument*, 2(3):45–48, 1988.
7. P. Z. Fan and F. Jin. Fast soft-decision decoding for generalized orthogonal codes. *Journal of China Railway Society*, 10(3):10–18, 1988.
8. P. Z. Fan and F. Jin. New class of codes suitable for computer error control. *Electron. Lett.*, 24(3):144–146, 1988.
9. P. Z. Fan, Z. Chen, and F. Jin. Linear unequal error-protection array codes. *Electron. Lett.*, 24(6):333–334, 1988.
10. P. Z. Fan, Z. Chen, and F. Jin. One-step completely orthogonalisable UEP codes and their soft decision decoding. *Electron. Lett.*, 24(9):1095–1097, 1988.
11. Z. Chen and P. Z. Fan. On optimal self-orthogonal UEP codes. In *Proceedings of ICCS'88*, page session 31, Singapore, 1988.
12. Z. Chen, P. Z. Fan, and F. Jin. Optimal self-orthogonal unequal error protection codes and their construction. *Journal of China Institute of Communication*, 10(3):1–6, 1989.

13. Z. Chen, P. Z. Fan, and F. Jin. On a new binary [22,13,5] code. *IEEE Transactions on Information Theory*, 36(1):228–229, January 1990.
14. Z. Chen, P. Z. Fan, and F. Jin. New results on self-orthogonal unequal error protection codes. *IEEE Transactions on Information Theory*, 36(5):1141–1144, 1990.
15. F. Jin, Z. Chen, and P. Z. Fan. Investigation on a new class of bilateral-checking codes. In *IEEE ISIT'90, session 332.3*, UK, 1990.
16. P. Z. Fan, Z. Chen, and F. Jin. A class of efficient algorithms for soft decision decoding of block codes. *ACTA ELECTRONICA SINICA*, 18(4):111–114, 1990.
17. P. Z. Fan. The design and implementation of a smart data transmission testing instrument. In *Proceedings of SCC'90*, pages 104–108, Chengdu, China, 1990.
18. Z. Chen, P. Z. Fan, and F. Jin. On optimal self-orthogonal quasi-cyclic codes. In *Proceedings of IEEE ICC'90*, page session 332.3, USA, 1990.
19. Z. Chen, P. Z. Fan, and F. Jin. New construction for classes of majority logic decodable codes with even minimum distance. *Electron. Lett.*, 27(7):549–550, 1991.
20. P. Z. Fan, J. Gao. A new approach of electrified railway remote control channel. In *Proceedings of RTC'91*, pages 1–6, China, 1991.

Appendix B

Proof of Various Lemmas, Theorems and Inequality

B.1 Proof 1

Lemma 1:

$$C_F^{(\tau)}(uq + v) = \begin{cases} q^2, & u = v = 0; \\ 0, & 1 \leq u \leq q-1, v = 0; \\ -e^{i\frac{2\pi r(u+1)}{q}}, & 0 \leq u \leq q-1, v = 1; \\ e^{i\frac{2\pi ru}{q}}, & 0 \leq u \leq q-1, v = q-1; \\ \frac{e^{i\frac{2\pi ru}{q}} - 1}{e^{-i\frac{2\pi r}{q}} - 1}, & u = 0, u = q-1, \\ & 2 \leq v \leq q-2; \\ \frac{2(1 - \cos \frac{2\pi ru(u+1)}{q})}{(e^{-i\frac{2\pi ru}{q}} - 1)(e^{-i\frac{2\pi r(u+1)}{q}} - 1)}, & 1 \leq u \leq q-2, \\ -\frac{2(1 - \cos \frac{2\pi ruv}{q})}{(e^{-i\frac{2\pi ru}{q}} - 1)(e^{-i\frac{2\pi rv}{q}} - 1)}, & 2 \leq v \leq q-2. \end{cases} \quad (\text{B.1})$$

Proof: For any integer $n = jq + k$ and $\tau = uq + v$, $1 \leq j, k \leq q-1$, the integer $n + \tau$ can be represented as

$$n + \tau = (j + u + \epsilon)q + (k + v - \epsilon q) \quad (\text{B.2})$$

where $\epsilon = 0$, if $k + v \leq q - 1$, and $\epsilon = 1$, if $k + v \geq q - 1$. Thus

$$\begin{aligned}
C_F^{(r)}(uq + v) &= \sum_{n=0}^{q^2-ug-v-1} a_{jq+k} a_{(jq+k)+(uq+v)}^* \\
&= \sum_{n=0}^{q^2-ug-v-1} a_{jq+k} a_{(j+u+\epsilon)q+(k+v-\epsilon q)}^* \\
&= \sum_{n=0}^{q^2-ug-v-1} \alpha^{-jv-k(u+\epsilon)-v(u+\epsilon)} \alpha^{(j\epsilon+u\epsilon+\epsilon^2)q} \\
&= \sum_{n=0}^{q^2-ug-v-1} \alpha^{-jv-k(u+\epsilon)-v(u+\epsilon)} \\
&= \sum_{n=0}^{q-1} + \sum_{n=q}^{2q-1} + \dots + \sum_{n=(q-u-2)q}^{(q-u-1)q-1} + \sum_{n=(q-u-1)q}^{q^2-ug-v-1} \\
&= \sum_{k=0}^{q-1} \alpha^{-k(u+\epsilon)-v(u+\epsilon)} \sum_{j=0}^{q-u-2} \alpha^{-jv} + \\
&\quad \alpha^{-(q-u-1)v} \sum_{k=0}^{q-v-1} \alpha^{-k(u+\epsilon)-v(u+\epsilon)} \\
&= \left(\sum_{k=0}^{q-v-1} \alpha^{-ku-uv} \frac{\alpha^{v(u+1)}-1}{\alpha^{-v}-1} + \right. \\
&\quad \left. \sum_{k=q-v}^{q-1} \alpha^{-k(u+1)-v(u+1)} \frac{\alpha^{v(u+1)}-1}{\alpha^{-v}-1} \right) + \\
&\quad \alpha^{(u+1)v} \sum_{k=0}^{q-v-1} \alpha^{-ku-uv} \\
&= \frac{\alpha^{v(u+1)}-1}{\alpha^{-v}-1} \left(\frac{1-\alpha^{uv}}{\alpha^{-u}-1} + \frac{\alpha^{-v(u+1)}-1}{\alpha^{-(u+1)}-1} \right) + \alpha^{v(u+1)} \frac{1-\alpha^{-uv}}{\alpha^{-u}-1} \\
&= \frac{\alpha^{uv}+\alpha^{-uv}-2}{(\alpha^{-v}-1)(\alpha^{-u}-1)} + \frac{2-\alpha^{v(u+1)}-\alpha^{-v(u+1)}}{(\alpha^{-v}-1)(\alpha^{-u}-1)}
\end{aligned} \tag{B.3}$$

By replacing α with $e^{i\frac{2\pi r}{q}}$ in above equation, we have

$$\begin{aligned}
C_F^{(r)}(uq + v) &= \frac{2(1-\cos \frac{2\pi r v(u+1)}{q})}{(e^{-i\frac{2\pi r v}{q}}-1)(e^{-i\frac{2\pi r(u+1)}{q}}-1)} - \\
&\quad \frac{2(1-\cos \frac{2\pi r uv}{q})}{(e^{-i\frac{2\pi r v}{q}}-1)(e^{-i\frac{2\pi r u}{q}}-1)}.
\end{aligned} \tag{B.4}$$

The rest of the lemma can be proved in a similar way.

B.2 Proof 2

Lemma 2:

$$C_C^{(r)}(\tau) = -\frac{\sin \frac{\pi r}{L} \tau^2}{\sin \frac{\pi r}{L} \tau}. \quad (\text{B.5})$$

Proof: Let $\alpha = e^{-i\frac{2\pi}{L}}$. Since $\alpha^{r\tau} \neq 1$, the following derivation is true,

$$\begin{aligned} C_C^{(r)}(\tau) &= \sum_{k=1}^{L-\tau} \alpha^{r \frac{k(k-1)}{2}} \alpha^{-r \frac{(k+\tau)(k+\tau-1)}{2}} = \alpha^{-r \frac{\tau(\tau-1)}{2}} \sum_{k=1}^{L-\tau} \alpha^{-r\tau k} \\ &= \alpha^{-r \frac{\tau(\tau-1)}{2}} \alpha^{-r\tau} \frac{1 - \alpha^{-r\tau(L-\tau)}}{1 - \alpha^{-r\tau}} = \alpha^{-r \frac{\tau(\tau+1)}{2}} \frac{1 - \alpha^{r\tau^2}}{1 - \alpha^{-r\tau}} \\ &= \frac{\alpha^{-r\tau^2/2} - \alpha^{r\tau^2/2}}{\alpha^{r\tau/2} - \alpha^{-r\tau/2}} = -\frac{\sin \frac{\pi r}{L} \tau^2}{\sin \frac{\pi r}{L} \tau}, \end{aligned} \quad (\text{B.6})$$

B.3 Proof 3

Lemma 3:

Chu sequences:

$$c_k^{(r)} = c_k^{(L-r)*} \quad (\text{B.7})$$

$$|C_C^{(r)}(\tau)| = |C_C^{(r)}(L-\tau)| \leq \tau, \quad 0 < \tau \leq (L+1)/2 \quad (\text{B.8})$$

$$C_C^{(r)}(\tau) = C_C^{(L-r)}(\tau) \quad (\text{B.9})$$

Frank sequences:

$$f_{k+jq}^{(r)} = f_{k+jq}^{(q-r)*} \quad (\text{B.10})$$

$$|C_F^{(r)}(\tau)| = |C_F^{(r)}(L-\tau)| \leq \tau, \quad 0 < \tau \leq (L+1)/2 \quad (\text{B.11})$$

$$|C_F^{(r)}(uq+v)| = |C_F^{(r)}(uq+(q-v))| \quad (\text{B.12})$$

$$C_F^{(r)}(\tau) = C_F^{(q-r)*}(\tau) \quad (\text{B.13})$$

Proof: The proofs of Eqns B.8 and B.11 are trivial and the proof of Eqns B.9 and B.12 can be found in (Zhang & Golomb, 1993). We now prove the rest of the Lemma.

(1) Proof of Eqn B.9: From Lemma 2, it is evident that

$$C_C^{(L-r)}(\tau) = -\frac{\sin \frac{\pi(L-r)}{L}\tau^2}{\sin \frac{\pi(L-r)}{L}\tau} = -\frac{\sin \frac{\pi r}{L}\tau^2}{\sin \frac{\pi r}{L}\tau} = C_C^{(r)}(\tau) \quad (\text{B.14})$$

(2) Proof of Eqn B.13: From Lemma 1,

$$\begin{aligned} C_F^{(r)}(uq + (q - v)) &= \frac{2(1 - \cos \frac{2\pi r v(u+1)}{q})}{(e^{i\frac{2\pi r v}{q}} - 1)(e^{-i\frac{2\pi r(u+1)}{q}} - 1)} - \\ &\quad \frac{2(1 - \cos \frac{2\pi r u v}{q})}{(e^{i\frac{2\pi r v}{q}} - 1)(e^{-i\frac{2\pi r u}{q}} - 1)} \\ &= -e^{-i\frac{2\pi r v}{q}} C_F^{(r)}(uq + v). \end{aligned} \quad (\text{B.15})$$

It is obvious that

$$|C_F^{(r)}((u+1)q - v)| = |C_F^{(r)}(uq + (q - v))| = |C_F^{(r)}(uq + v)|. \quad (\text{B.16})$$

(3) Proof of Eqn B.13: From Lemma 1,

$$\begin{aligned} C_F^{(q-r)}(uq + v) &= \frac{2(1 - \cos \frac{2\pi r v(u+1)}{q})}{(e^{i\frac{2\pi r v}{q}} - 1)(e^{i\frac{2\pi r(u+1)}{q}} - 1)} - \frac{2(1 - \cos \frac{2\pi r u v}{q})}{(e^{i\frac{2\pi r v}{q}} - 1)(e^{i\frac{2\pi r u}{q}} - 1)} \\ &= C_F^{(r)*}(uq + v). \end{aligned} \quad (\text{B.17})$$

Thus

$$|C_F^{(q-r)}(uq + v)| = |C_F^{(r)*}(uq + v)| = |C_F^{(r)}(uq + v)|. \quad (\text{B.18})$$

B.4 Proof 4

Theorem 24:

$$|C_F^{(1)}(uq + v)| \leq \sqrt{\frac{2}{1 - \cos \frac{2\pi}{q}}} \quad (\text{B.19})$$

Proof: From Lemma 1, it follows that

$$C_F^{(1)}(uq + v) = A - B = |A|e^{\arg A} - |B|e^{\arg B} \quad (\text{B.20})$$

where $A = \frac{2(1-\cos \frac{2\pi v(u+1)}{q})}{(e^{-i\frac{2\pi v}{q}}-1)(e^{-i\frac{2\pi(u+1)}{q}}-1)}$ and $B = \frac{2(1-\cos \frac{2\pi uv}{q})}{(e^{-i\frac{2\pi v}{q}}-1)(e^{-i\frac{2\pi u}{q}}-1)}$. We now compute their arguments and magnitudes.

$$\begin{aligned} \arg A &= \arg \frac{1}{e^{-i\frac{2\pi v}{q}}-1} + \arg \frac{1}{e^{-i\frac{2\pi(u+1)}{q}}-1} \\ &= -\arg(e^{-i\frac{2\pi v}{q}}-1) - \arg(e^{-i\frac{2\pi(u+1)}{q}}-1) \\ &= -(\frac{\pi}{2} - \frac{\pi v}{q}) - (\frac{\pi}{2} - \frac{\pi(u+1)}{q}). \end{aligned} \quad (\text{B.21})$$

Similarly,

$$\arg B = -(\frac{\pi}{2} - \frac{\pi v}{q}) - (\frac{\pi}{2} - \frac{\pi u}{q}). \quad (\text{B.22})$$

By using the following inequality (the proof is given in Appendix B.6),

$$\frac{1 - \cos \frac{2\pi uv}{q}}{1 - \cos \frac{2\pi v}{q}} \leq \frac{1 - \cos \frac{2\pi u}{q}}{1 - \cos \frac{2\pi}{q}} \quad (\text{B.23})$$

we have

$$\begin{aligned} |B| &= \sqrt{\frac{4(1-\cos \frac{2\pi uv}{q})^2}{4(1-\cos \frac{2\pi v}{q})(1-\cos \frac{2\pi u}{q})}} \leq \sqrt{\frac{(1-\cos \frac{2\pi u}{q})(1-\cos \frac{2\pi uv}{q})}{(1-\cos \frac{2\pi}{q})(1-\cos \frac{2\pi u}{q})}} \\ &= \sqrt{\frac{1-\cos \frac{2\pi uv}{q}}{1-\cos \frac{2\pi}{q}}} \leq \sqrt{\frac{2}{1-\cos \frac{2\pi}{q}}} \end{aligned} \quad (\text{B.24})$$

and

$$|A| \leq \sqrt{\frac{1 - \cos \frac{2\pi(u+1)v}{q}}{1 - \cos \frac{2\pi}{q}}} \leq \sqrt{\frac{2}{1 - \cos \frac{2\pi}{q}}} \quad (\text{B.25})$$

Due to the fact that

$$|A| \leq \sqrt{\frac{2}{1 - \cos \frac{2\pi}{q}}}, \quad |B| \leq \sqrt{\frac{2}{1 - \cos \frac{2\pi}{q}}}, \quad \arg A - \arg B = \frac{\pi}{q}, \quad (\text{B.26})$$

if $q \geq 3$, as can be seen from Fig.1, we have

$$|C_F^{(1)}(uq + v)| \leq \sqrt{\frac{2}{1 - \cos \frac{2\pi}{q}}} \quad (\text{B.27})$$

which concludes our proof.

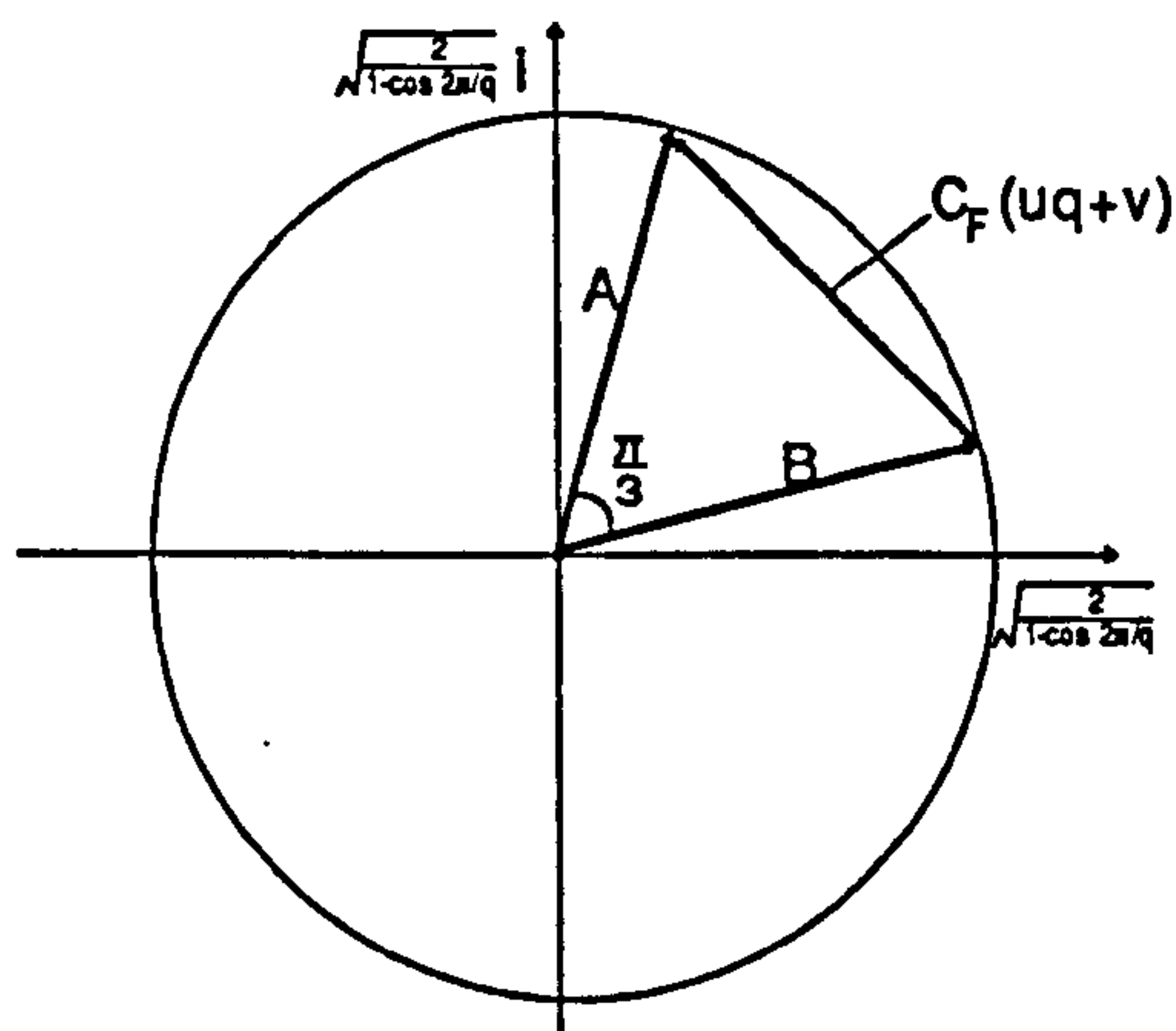


Figure B.1: Illustration of $C_F^{(r)}(uq + v) = A - B$

B.5 Proof 5

Theorem 26:

$$|C_F^{(\frac{q-1}{2})}(uq + v)| < 2\sqrt{\frac{1}{1 - \cos \frac{\pi}{q}}}. \quad (\text{B.28})$$

Proof: Based on Lemma 1,

$$C_F^{(\frac{q-1}{2})}(uq + v) = A - B = |A|e^{\arg A} - |B|e^{\arg B} \quad (\text{B.29})$$

where

$$\begin{aligned}\arg A &= \arg \frac{1}{e^{-i\frac{2\pi(q-1)v}{2q}} - 1} + \arg \frac{1}{e^{-i\frac{2\pi(q-1)(u+1)}{2q}} - 1} \\ &= -\arg(e^{-i\pi v(1-\frac{1}{q})} - 1) - \arg(e^{-i\pi(u+1)(1-\frac{1}{q})} - 1) \\ &= -(\frac{\pi}{2} - \frac{\pi v}{2}(1 - \frac{1}{q})) - (\frac{\pi}{2} - \frac{\pi(u+1)}{2}(1 - \frac{1}{q}));\end{aligned}\quad (\text{B.30})$$

$$\arg B = -(\frac{\pi}{2} - \frac{\pi v}{2}(1 - \frac{1}{q})) - (\frac{\pi}{2} - \frac{\pi(u+1)}{2}(1 - \frac{1}{q})). \quad (\text{B.31})$$

Note that $\cos \frac{\pi}{u}(1 - \frac{1}{q}) = (-1)^u \cos \frac{\pi u}{q}$; hence we have

$$|B| = \sqrt{\frac{(1 - (-1)^{uv} \cos \frac{\pi uv}{q})^2}{(1 - (-1)^v \cos \frac{\pi v}{q})(1 - (-1)^u \cos \frac{\pi u}{q})}} \quad (\text{B.32})$$

Four cases need to be considered:

1. v even, u even. By using a similar inequality, $\frac{1 - \cos \frac{\pi uv}{q}}{1 - \cos \frac{\pi v}{q}} \leq \frac{1 - \cos \frac{\pi u}{q}}{1 - \cos \frac{\pi}{q}}$, we obtain

$$\begin{aligned}|B| &\leq \sqrt{\frac{(1 - \cos \frac{\pi u}{q})(1 - \cos \frac{\pi uv}{q})}{(1 - \cos \frac{\pi}{q})(1 - \cos \frac{\pi u}{q})}} \\ &= \sqrt{\frac{1 - \cos \frac{\pi uv}{q}}{1 - \cos \frac{\pi}{q}}} \leq \sqrt{\frac{2}{1 - \cos \frac{\pi}{q}}}\end{aligned}\quad (\text{B.33})$$

2. v even, u odd. Because $\frac{1 - \cos \frac{\pi u}{q}}{1 + \cos \frac{\pi u}{q}} < 1$, $0 \leq u \leq \frac{q-1}{2}$, then

$$\begin{aligned}|B| &\leq \sqrt{\frac{(1 - \cos \frac{\pi u}{q})(1 - \cos \frac{\pi uv}{q})}{(1 - \cos \frac{\pi}{q})(1 + \cos \frac{\pi u}{q})}} \\ &< \sqrt{\frac{1 - \cos \frac{\pi uv}{q}}{1 - \cos \frac{\pi}{q}}} \leq \sqrt{\frac{2}{1 - \cos \frac{\pi}{q}}}\end{aligned}\quad (\text{B.34})$$

3. v odd, u even. Because $\frac{1 - \cos \frac{\pi v}{q}}{1 + \cos \frac{\pi v}{q}} < 1$, $0 \leq v \leq \frac{q-1}{2}$, then

$$\begin{aligned}|B| &\leq \sqrt{\frac{(1 - \cos \frac{\pi v}{q})(1 - \cos \frac{\pi uv}{q})}{(1 + \cos \frac{\pi v}{q})(1 - \cos \frac{\pi}{q})}} \\ &< \sqrt{\frac{1 - \cos \frac{\pi uv}{q}}{1 - \cos \frac{\pi}{q}}} \leq \sqrt{\frac{2}{1 - \cos \frac{\pi}{q}}}\end{aligned}\quad (\text{B.35})$$

4. v odd, u odd. Due to the fact that $1 - \cos \frac{\pi v}{q} \leq 1 + \cos \frac{\pi}{q}$, $1 - \cos \frac{\pi u}{q} \leq 1 + \cos \frac{\pi}{q}$ $0 \leq v, u \leq \frac{q-1}{2}$, the following inequality holds:

$$|B| \leq \sqrt{\frac{2^2}{(1 + \cos \frac{\pi}{q})^2}} \leq \frac{2}{1 + \cos \frac{\pi}{q}} \leq 2 \quad (\text{B.36})$$

It is now clear from above discussion that

$$|B| \leq \sqrt{\frac{2}{1 - \cos \frac{\pi}{q}}} \quad (\text{B.37})$$

$$|A| \leq \sqrt{\frac{2}{1 - \cos \frac{\pi}{q}}} \quad (\text{B.38})$$

$$\arg A - \arg B = \frac{\pi}{2} \left(1 - \frac{1}{q}\right) < \frac{\pi}{2}. \quad (\text{B.39})$$

By analogy with the proof of Theorem 24, it can be shown that

$$|C_F^{(r)}(uq + v)| < \sqrt{|A|^2 + |B|^2} \leq 2 \sqrt{\frac{1}{1 - \cos \frac{2\pi}{q}}}. \quad (\text{B.40})$$

B.6 Proof 6

Inequality Eqn B.23¹:

$$\frac{1 - \cos \frac{2\pi uv}{q}}{1 - \cos \frac{2\pi v}{q}} \leq \frac{1 - \cos \frac{2\pi u}{q}}{1 - \cos \frac{2\pi}{q}} \quad (\text{B.41})$$

Proof: Let $f(u, v) = \frac{1 - \cos \frac{2\pi uv}{q}}{1 - \cos \frac{2\pi v}{q}}$. Since $\cos \left[\frac{2\pi v}{q} \left(\frac{kq}{v} \pm u \right) \right] = \cos \frac{2\pi uv}{q}$, $k = 0, 1, \dots, v-1$, it follows that $f(u, v)$ has the following properties:

¹This proof is due to Professor W. K. Hayman (University of York) and Dr. J. Gunson (University of Birmingham).

(1). Periodicity: $f(\frac{kq}{v} + u, v) = f(u, v)$, which requires us only consider the range $0 \leq u \leq \lfloor \frac{q}{v} \rfloor$.

(2). Symmetry: $f(\frac{kq}{v} - u, v) = f(u, v)$; thus, we need only show $0 \leq u \leq \lfloor \frac{q}{2v} \rfloor$.

(3). Monotonicity in the interval $0 \leq u \leq \lfloor \frac{q}{2v} \rfloor$. This is due to the fact that $\frac{df(u,v)}{du} = \frac{2\pi v \sin \frac{2\pi uv}{q}}{q(1 - \cos \frac{2\pi v}{q})} > 0$, $0 < u < \lfloor \frac{q}{2v} \rfloor$.

Thus it suffices to prove the inequality for $0 \leq u \leq \lfloor \frac{q}{2v} \rfloor$.

Suppose that $\theta \leq \frac{\pi}{2u}$, then $\frac{\sin \theta u}{\sin \theta}$ decreases with increasing θ for $0 \leq \theta \leq \frac{\pi}{2u}$. In fact

$$\begin{aligned} \frac{d}{d\theta} \frac{\sin \theta u}{\sin \theta} &= \frac{u \sin \theta \cos \theta u - \sin \theta u \cos \theta}{\sin^2 \theta} \\ &= \frac{(u \tan \theta - \tan \theta u) \cos \theta \cos \theta u}{\sin^2 \theta} \end{aligned} \quad (\text{B.42})$$

Also

$$\frac{d}{d\theta} \frac{\tan \theta}{\theta} = \frac{\theta \sec^2 \theta - \tan \theta}{\theta^2} = \frac{\frac{1}{2} \sec^2 \theta (2\theta - \sin 2\theta)}{\theta^2} > 0 \quad (\text{B.43})$$

Thus $\frac{\tan \theta u}{\theta u} > \frac{\tan \theta}{\theta}$, $0 < \theta u < \frac{\pi}{2}$, or $(u \tan \theta - \tan \theta u) < 0$, so that $\frac{d}{d\theta} \frac{\sin \theta u}{\sin \theta} < 0$ for $0 \leq \theta \leq \frac{\pi}{2u}$.

Now because $0 \leq u \leq \frac{q}{2v}$, or $\frac{\pi v}{q} \leq \frac{\pi}{2u}$, letting $\theta = \frac{\pi v}{q}$, we have

$$\frac{\sin \frac{\pi uv}{q}}{\sin \frac{\pi v}{q}} \leq \frac{\sin \frac{\pi u}{q}}{\sin \frac{\pi}{q}} \quad (\text{B.44})$$

which is equivalent to the inequality Eqn B.23 by noting the relation $1 - \cos 2x = 2 \sin^2 x$.

B.7 Proof 7

Theorem 29:

$$B_C^{(r)}(b) = 0.48 \sqrt{\frac{b}{r}} L, \quad I_m(L) = \frac{(Lb - 1)s_0}{r}, \quad r \geq 2, \quad 0 \leq \frac{b}{r} \leq 0.37, \quad (\text{B.45})$$

where $b = f(r, k)$, $k \equiv L \pmod{r}$, $s_0 = \sqrt{\frac{z_0 r}{\pi b}}$ and $z_0 = 1.1655$.

Proof: Because $r\tau$ and L are integers, $2 \leq r \leq L-1$, $1 \leq \tau \leq L-1$, we can represent $r\tau$ as

$$r\tau = mL + s \quad -L < s < L; \quad 0 \leq m < L-1, \quad (\text{B.46})$$

where m, s are integers and are functions of τ if L and r are given. Thus, $\tau = \frac{Lm+s}{r}$ and

$$\frac{r\tau^2}{L} = \left(m + \frac{s}{L}\right) \frac{Lm+s}{r} = m\tau + \frac{sm}{r} + \frac{s^2}{Lr}. \quad (\text{B.47})$$

Because $r|(Lm+s)$, it follows that

$$\left|C_C^{(r)}(\tau)\right| = \frac{\left|\sin\left(\pi m \frac{Lm+s}{r} + \pi \frac{sm}{r} + \pi \frac{s^2}{rL}\right)\right|}{\left|\sin\left(\pi m + \pi \frac{s}{L}\right)\right|} = \frac{\left|\sin\left(\pi \frac{sm}{r} + \pi \frac{s^2}{rL}\right)\right|}{\left|\sin\left(\pi \frac{s}{L}\right)\right|} \quad (\text{B.48})$$

Furthermore, for any given integer $r \geq 2$, $(r, L) = 1$, L can be represented as $L = ar + k$, where a is an integer and $1 \leq k \leq r-1$. By using Eqn B.46, we have

$$r\tau = m(ar + k) + s = mar + mk + s. \quad (\text{B.49})$$

This means that $mk + s$ should be divisible by r , i.e. $mk + s \equiv 0 \pmod{r}$. Note that $(k, r) = 1$ because $(L, r) = 1$; there always exists an integer $b = f(r, k)$ such that $bk \equiv 1 \pmod{r}$ according to Euclid's algorithm. Therefore m can be rewritten as

$$m \equiv -bs \pmod{r} \quad (\text{B.50})$$

and thus

$$\left|C_C^{(r)}(\tau)\right| = \frac{\left|\sin\left(\pi \frac{sm}{r} + \pi \frac{s^2}{rL}\right)\right|}{\left|\sin\left(\pi \frac{s}{L}\right)\right|} = \frac{\left|\sin \frac{\pi s^2}{r} \left(b + \frac{1}{L}\right)\right|}{\left|\sin\left(\pi \frac{s}{L}\right)\right|}. \quad (\text{B.51})$$

In order to maximize Eqn B.51, let $z = \frac{\pi s^2}{r}(b + \frac{1}{L})$ and evaluate the derivative of $|C^{(r)}(\tau)|$ with respect to z , i.e.,

$$\frac{d|C_C^{(r)}(\tau)|}{dz} = \frac{d}{dz} \frac{|\sin z|}{\left| \sin \sqrt{\frac{\pi r z}{L^2(b+1/L)}} \right|} = 0. \quad (\text{B.52})$$

It is easy to check that an unrestricted maximum is reached at the point z_0 which is a root of the equation

$$\tan z = \frac{2\sqrt{\frac{\pi r z}{L^2(b+1/L)}}}{\frac{\pi r}{L^2(b+1/L)}} \tan \sqrt{\frac{\pi r z}{L^2(b+1/L)}} \quad (\text{B.53})$$

When $L \rightarrow \infty$, the right hand side of above equation will tend to $2z$, that is

$$\tan z = 2z, \quad (\text{B.54})$$

whose minimal positive root is equal to $z_0 = 1.1655$. The corresponding maximum is

$$\begin{aligned} B_C^{(r)}(b) &= \max_{\tau} \lim_{L \rightarrow \infty} |C_C^{(r)}(\tau)| \\ &= \max_z \lim_{L \rightarrow \infty} \frac{|\sin z|}{\left| \sin \sqrt{\frac{\pi r z}{L^2(b+1/L)}} \right|} \\ &= \sqrt{\frac{bL^2}{\pi r} \frac{\sin z_0}{\sqrt{z_0}}} = 0.48 \sqrt{\frac{b}{r}} L, \end{aligned} \quad (\text{B.55})$$

and

$$I_m(L) = \frac{Lm + s}{r} = \frac{(Lb - 1)s_0}{r} \quad (\text{B.56})$$

where $s_0 = \sqrt{\frac{z_0 r}{\pi b}}$. Note that $s_0 \geq 1$, we have $\frac{b}{r} \geq \frac{z_0}{\pi} = 0.37$.

B.8 Proof 8

Theorem 30:

$$B_C^{(r)} = \frac{L}{\pi} \left| \sin \left(\frac{\pi b}{r} \right) \right|, \quad I_m(L) = \frac{Lb-1}{r}, \quad r \geq 2, \quad 0.5 \geq \frac{b}{r} \geq 0.37. \quad (\text{B.57})$$

Proof: According to Eqn B.51, when $L \rightarrow \infty$ and $0 \leq \frac{b}{r} \leq 1/2$,

$$0 \leq \frac{\left| \sin \frac{\pi b s^2}{r} \right|}{\left| \sin \frac{\pi s}{L} \right|} \leq \frac{\left| \sin \frac{\pi}{2} \right|}{\left| \sin \frac{\pi s}{L} \right|} \quad (\text{B.58})$$

or

$$\frac{\pi b s^2}{r} \leq \frac{\pi}{2} \quad (\text{B.59})$$

which means $\frac{b}{r} \leq \frac{1}{2s^2}$. From $\frac{b}{r} \leq \frac{1}{2}$, we have $s = 1$. Hence

$$B_C^{(r)}(b) = \max_{\tau} \lim_{L \rightarrow \infty} \left| C_C^{(r)}(\tau) \right| = \frac{L}{\pi} \left| \sin \frac{\pi b}{r} \right|, \quad 0 \leq \frac{b}{r} \leq \frac{1}{2}, \quad (\text{B.60})$$

$$I_m(L) = \frac{Lm+s}{r} = \frac{(Lb-1)s_0}{r} = \frac{Lb-1}{r} \quad (\text{B.61})$$

Furthermore it can be shown that

$$0.48 \sqrt{\frac{b}{r}} L \geq \frac{L}{\pi} \left| \sin \frac{\pi b}{r} \right| \quad (\text{B.62})$$

where the equality holds when $\frac{b}{r} = 0.37$. Therefore

$$B_C^{(r)} = \max \left[0.48 \sqrt{\frac{b}{r}} L, \quad \frac{L}{\pi} \left| \sin \frac{\pi b}{r} \right| \right] = 0.48 \sqrt{\frac{b}{r}} L, \quad \frac{b}{r} \leq 0.37 \quad (\text{B.63})$$

When $\frac{b}{r} > 0.37$, Eqn B.45 is not true; the bound is thus given by

$$B_C^{(r)} = \frac{L}{\pi} \left| \sin \frac{\pi b}{r} \right|, \quad \frac{b}{r} > 0.37. \quad (\text{B.64})$$

which concludes the theorem.

B.9 Proof 9

Theorem 31:

$$B_C^{(1)} = \sqrt{L/4.34}, \quad I_m(L) = \sqrt{L/2.68}. \quad (\text{B.65})$$

Proof: Let $z = \frac{\pi\tau^2}{L}$ in Eqn B.5, consider the derivative of $|C_C^{(1)}(\tau)|$ with respect to z , i.e.,

$$\frac{d|C_C^{(1)}(\tau)|}{dz} = \frac{d}{dz} \frac{|\sin z|}{\left|\sin \frac{\pi}{L} \sqrt{\frac{Lz}{\pi}}\right|} = 0. \quad (\text{B.66})$$

Similarly a maximum is reached at the point which is a root of the equation,

$$\tan z = \frac{2\sqrt{\frac{\pi z}{L}}}{\frac{\pi}{L}} \tan \sqrt{\frac{\pi z}{L}} \quad (\text{B.67})$$

When $L \rightarrow \infty$, the minimal positive root is equal to $z_0 = 1.1655$ and

$$\begin{aligned} B_C^{(1)}(b) &= \max_{\tau} \lim_{L \rightarrow \infty} |C_C^{(1)}(\tau)| = \max_z \lim_{L \rightarrow \infty} \frac{|\sin z|}{\left|\sin \sqrt{\frac{\pi z}{L}}\right|} \\ &= \sqrt{\frac{L}{\pi} \frac{\sin z_0}{\sqrt{z_0}}} = \sqrt{\frac{L}{4.34}}, \end{aligned} \quad (\text{B.68})$$

$$I_m(L) = \sqrt{\frac{Lz_0}{\pi}} = \sqrt{\frac{L}{2.68}}. \quad (\text{B.69})$$

B.10 Proof 10

Theorem 32:

If L is odd and $r = \frac{L-1}{2}$, then

$$B_C^{(\frac{L-1}{2})} = \sqrt{L/2.17}, \quad I_m(L) = \sqrt{L/1.34}. \quad (\text{B.70})$$

Furthermore, the maximum out-of-phase aperiodic ACF is bounded by $\sqrt{2}$ for all odd shifts in the range $0 < \tau \leq \frac{L-1}{2}$ and even shifts in the range $\frac{L+1}{2} \leq \tau < L-1$.

Proof: When $r = \frac{L-1}{2}$, it can be shown that

$$C_C^{(\frac{L-1}{2})}(\tau) = \sqrt{\frac{1 - (-1)^\tau \cos \frac{\pi \tau^2}{L}}{1 - (-1)^\tau \cos \frac{\pi \tau}{L}}} \quad (\text{B.71})$$

When τ is even, let

$$f(\tau) = \frac{1 - \cos \frac{\pi \tau^2}{L}}{1 - \cos \frac{\pi \tau}{L}}, \quad \tau \text{ is even.} \quad (\text{B.72})$$

we now evaluate the derivative $f'(\tau)$ at $\tau = \sqrt{\frac{L}{K}}$. When $\tau = \sqrt{\frac{L}{K}}$, we have $\frac{\pi \tau}{L} = \frac{\pi}{\sqrt{KL}}$ and $\frac{\pi \tau^2}{L} = \frac{\pi}{K}$. Since K, L are positive constants and

$$\begin{aligned} \cos x &\approx 1 - \frac{x^2}{2} + \frac{x^4}{24} - \frac{x^6}{720} \\ \sin x &\approx x - \frac{x^3}{6} + \frac{x^5}{120}, \end{aligned} \quad (\text{B.73})$$

as L goes to infinity, $f'(\sqrt{\frac{L}{K}}) = 0$ implies that

$$K^4 - \frac{\pi^2}{4}K^2 + \frac{\pi^4}{72} = 0 \quad (\text{B.74})$$

The two positive roots are: $K_1 = \frac{\pi}{\sqrt{6}}$, $K_2 = \frac{\pi}{2\sqrt{3}}$. Since $f(\sqrt{\frac{L}{K_1}}) \geq f(\sqrt{\frac{L}{K_2}})$, we have

$$B_C^{(\frac{L-1}{2})} = \sqrt{f(\sqrt{\frac{L}{K_1}})} \approx \sqrt{\frac{2L(1 - \cos \sqrt{6})}{\sqrt{6}\pi}} \approx \sqrt{\frac{L}{2.17}}, \quad (\text{B.75})$$

$$I_m(L) = \sqrt{\frac{L}{K_1}} \approx \sqrt{\frac{L}{1.34}} \quad (\text{B.76})$$

If τ is odd, then

$$C_C^{(\frac{L-1}{2})}(\tau) = \sqrt{\frac{1 + \cos \frac{\pi \tau^2}{L}}{1 + \cos \frac{\pi \tau}{L}}} \leq \sqrt{\frac{2}{1 + \cos \frac{\pi \tau}{L}}} \leq \sqrt{\frac{2}{1}} = \sqrt{2} \quad (\text{B.77})$$

Therefore the maximum out-of-phase aperiodic ACF is bounded by $\sqrt{2}$ for all odd shifts in the range of $1 \leq \tau \leq \frac{L-1}{2}$.

In the range of $\frac{L+1}{2} < \tau < L-1$, the results are the same except that the parity of τ is changed.

The first half of the theorem can be proved by a simpler method. Because the length L can be represented as

$$L = 2\left(\frac{L-1}{2}\right) + 1 = 2r + 1, \quad (\text{B.78})$$

we have $k = 1$ and hence $b = 1$. Based on Eqn B.45, we have

$$B_C^{(\frac{L-1}{2})}(b) \leq 0.48 \sqrt{\frac{1}{\frac{L-1}{2}}} L = \sqrt{\frac{L}{2.17}}, \quad (\text{B.79})$$

and

$$I_m(L) = \frac{(Lb-1)s_0}{r} = \sqrt{\frac{L}{1.34}}. \quad (\text{B.80})$$