1

**PM-1 3½"x4" PHOTOGRAPHIC MICROCOPY TARGET
NBS 1010a ANSI/ISO #2 EQUIVALENT**

PRECISIONSM RESOLUTION TARGETS

PIONEER IN METHYLENE BLUE TESTING SINCE 1974

1388 COUNTY ROAD 8, BURNINGWELL, WY 82407 USA
TEL: 612 426 7867 FAX: 612 426 7867 TOLL: 800 826 6666

National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file - Votre référence

Our file - Notre référence

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

**COMPOSITE SEQUENCES FOR RAPID ACQUISITION
OF DIRECT-SEQUENCE SPREAD SPECTRUM SIGNALS**

by

Sean Faulkner, B.Sc.Hons., B.Eng., M.Eng.

**A thesis submitted to the
Faculty of Graduate Studies and Research
in partial fulfillment of
the requirements for the degree of**

Doctor of Philosophy

**Department of Electronics
Carleton University
Ottawa, Ontario**

September 1992

© Sean Faulkner, 1992

National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your title / Votre référence

Your title / Votre référence

The author has granted an irrevocable non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of his/her thesis by any means and in any form or format, making this thesis available to interested persons.

L'auteur a accordé une licence irrévocable et non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de sa thèse de quelque manière et sous quelque forme que ce soit pour mettre des exemplaires de cette thèse à la disposition des personnes intéressées.

The author retains ownership of the copyright in his/her thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without his/her permission.

L'auteur conserve la propriété du droit d'auteur qui protège sa thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

ISBN 0-315-79889-0

Canada

The undersigned hereby recommend to
the Faculty of Graduate Studies and Research
acceptance of the thesis,

COMPOSITE SEQUENCES FOR RAPID ACQUISITION OF
DIRECT-SEQUENCE SPREAD SPECTRUM SIGNALS

submitted by

SEAN ANTHONY FAULKNER, B.SC., B.ENG., M.ENG.

in partial fulfilment of the requirements
for the degree of Doctor of Philosophy.

Chair, Department of Electronics

Thesis Supervisor

Carleton University

September 23, 1992

Abstract

The composite sequences, a class of spreading sequences for direct-sequence spread spectrum (DS-SS) communications, are investigated for the case of components which are binary maximal-length sequences. The relevant properties of the composite sequences are derived and in particular, the acquisition time performance is determined for a noisy environment. It is demonstrated in this thesis that the composite sequences are a large, balanced class of spreading sequences with high linear span, reasonable autocorrelation performance, an essentially featureless power spectrum, improved security and rapid acquisition capability.

A novel subclass of composite sequences, termed the sliding composite sequences, is also presented here. As with the composite sequences, the properties and performance of sliding composite sequences are investigated and derived. It is demonstrated that the sliding composite sequences are a large, nearly balanced class of spreading sequences with high linear span, an essentially featureless power spectrum and improved security. Most importantly, through exploitation of the inherent rapid acquisition structure of the sliding composite sequence construction, a novel acquisition algorithm is developed which gives orders of magnitude reduction in acquisition time for DS-SS communications.

In addition, a novel algorithm for the generation of primitive polynomials is presented in this thesis and the aperiodic autocorrelation magnitude of m-sequences is bounded empirically.

Acknowledgments

The author extends his most sincere appreciation for the long-term guidance and friendship of his thesis supervisor, Professor Jim Wight.

To the Department of National Defence, I extend my thanks for allowing me to proceed into the PhD program under the Postgraduate Training on Scholarship program.

I would like to thank Dr. Frank Palmer, Dr. Ray Carbonneau and the staff of the Electronic Warfare Division at the Defence Research Establishment Ottawa for use of their resources, both material and intellectual. I could not adequately praise the support of the many individuals involved in this process — suffice it to say to all, I am extremely grateful! To some particular individuals at DREO, I must give specific thanks:

to Frank Palmer for opening up the opportunities

to Ray Carbonneau for keeping them open

to Rob Fry for solving all of my technical problems and carrying the extra food

to Lorne Gutz for fixing the hardware and software and teaching me about the good life — Nahanni '94 !

to Nicole Brousseau for many things

to Doug Hill for letting me in on all the secrets and teaching me how to deal with people

to Andrew Mudry for teaching me late night philosophy and the work ethic

I am very grateful to my parents who have supported all of my academic endeavours through endless years of work avoidance.

To my wife, who's stayed with me even though I have technically abandoned her for months. Thanks to you, Anne-Marie, and to Andrew and Katie who have grown up so much since I last saw them.

I would like to thank the following institutions for their financial support: NSERC for support under a Postgraduate Scholarship, the Ontario government for support under an Ontario Graduate Scholarship and DREO for support under contract W7714-9-9213.

Table of Contents

Acknowledgments	ii
Abstract	iii
List of Tables	vii
List of Figures	viii
List of Acronyms	x
List of Symbols	xi
1 Introduction	1
1.1 Motivation	1
1.2 Thesis Organization	3
1.3 Thesis Contributions	3
2 Background	5
2.1 Spread Spectrum Communications	5
2.1.1 Direct-Sequence Spread Spectrum	6
2.2 DS-SS Acquisition	10
2.2.1 Single Dwell Serial Search Acquisition	14
2.2.2 Double Dwell Serial Search Acquisition	17
2.3 Theory of Sequences	22
2.3.1 Galois Field Theory	22
2.3.2 Linear Recursions and Code Generators	26
2.3.3 Decimation	36
2.3.4 Correlation	37
2.4 Spreading Sequences for DS-SS Communications	41
2.5 Rapid Acquisition Sequences	50
2.5.1 Combination Sequences	51
2.5.2 Composite Sequences	54

3	Composite Sequences	63
3.1	Introduction	63
3.2	Primitive Polynomial Generation	64
3.2.1	The Algorithm	65
3.3	Generation of Composite Sequences	69
3.4	Properties of Composite Sequences	73
3.4.1	Enumeration	73
3.4.2	Linear Span	74
3.4.3	Correlation Functions	77
3.4.3.1	Periodic Autocorrelation Function	79
3.4.3.2	Aperiodic Autocorrelation of M-Sequences	84
3.4.4	Power Spectrum	93
3.5	Security of Composite Sequences	95
3.6	Acquisition Time Performance	104
3.7	Summary and Conclusions	115
4	A New Subclass of Composite Sequences	118
4.1	Introduction	118
4.2	Generation of Sliding Composite Sequences	119
4.3	Properties of Sliding Composite Sequences	121
4.3.1	Enumeration and Linear Span	122
4.3.2	Power Spectrum	124
4.4	Security of Sliding Composite Sequences	127
4.5	Acquisition of Sliding Composite Sequences	129
4.6	Summary and Conclusions	134
5	Conclusions and Recommendations	136
5.1	Summary	136
5.2	Future Work	138
Appendix A	Calculation of the Power Spectrum of M-Sequences	140

Appendix B	Calculation of the Power Spectrum of Composite Sequences . .	143
Bibliography		147

List of Tables

Table 2.1	The elements of $GF(2^3)$ generated by $f(x) = x^3 + x^2 + 1$	24
Table 2.2	Shift register states and output for the sequence using $f(x) = x^3 + x^2 + 1$.	30
Table 2.3	Example application of the Berlekamp-Massey algorithm	35
Table 3.1	Application of the BMA to $\{b_{3n}\}$	67
Table 3.2	Application of the BMA to $\{b_{5n}\}$	68
Table 3.3	Enumeration of composite sequences over $GF(2)$	75
Table 3.4	Linear span of composite sequences over $GF(2)$	78
Table 3.5	Bounds on the maximum aperiodic autocorrelation magnitude for m-sequences	86
Table 3.6	C_{max} Statistics for the m-sequences of linear span 3	88
Table 3.7	C_{max} Statistics for the m-sequences of linear span 4	88
Table 3.8	C_{max} Statistics for the m-sequences of linear span 5	88
Table 3.9	C_{max} Statistics for the m-sequences of linear span 6	88
Table 3.10	C_{max} Statistics for the m-sequences of linear span 7	89
Table 3.11	C_{max} Statistics for the m-sequences of linear span 8	89
Table 3.12	C_{max} Statistics for the m-sequences of linear span 9	89
Table 3.13	C_{max} Statistics for the m-sequences of linear span 10	90
Table 3.14	C_{max} Statistics for the m-sequences of linear span 11	91
Table 3.15	C_{max} Statistics for the m-sequences of linear span 12	92

List of Figures

Figure 2.1	A DS-BPSK transmitter	7
Figure 2.2	A DS-BPSK receiver	9
Figure 2.3	Block diagram of a single dwell PN acquisition system	12
Figure 2.4	Block diagram of a double dwell acquisition system	18
Figure 2.5	Acquisition performance improvement factor for double dwell system over single dwell system; SNR = - 10 dB	21
Figure 2.6	An m-stage linear feedback shift register	27
Figure 2.7	Galois linear feedback shift register generator	29
Figure 2.8	Galois sequence generator for $f(x) = x^3 + x^2 + 1$	30
Figure 2.9	Power spectrum of an m-sequence	44
Figure 2.10	Formation of the autocorrelation function of a combination sequence .	53
Figure 2.11	Baseband rapid acquisition receiver for a composite sequence	59
Figure 2.12	Theoretically achievable acquisition time reduction for the composite sequences	61
Figure 3.1	Composite sequence generator circuit	71
Figure 3.2	The product of the autocorrelation functions of the component sequences	81
Figure 3.3	Example periodic autocorrelation function of a composite sequence . .	83
Figure 3.4	Power spectrum of the fast component sequence $b(x) = x^3 + x + 1$; $f_c = 700$ kHz	96
Figure 3.5	Power spectrum of the slow component sequence $a(x) = x^3 + x + 1$; $f_c/N_b = 100$ kHz	97
Figure 3.6	Power spectrum of a composite sequence $a(x) = b(x) = x^3 + x + 1$; $f_c = 700$ kHz	98
Figure 3.7	Power spectrum of a composite sequence $a(x) = b(x) = x^8 + x^4 + x^3 + x^2 + 1$; $f_c = 5.1$ MHz	99
Figure 3.8	Ratio of decoding times for composite sequences vs m-sequences . .	101

Figure 3.9	Ratio of search time for composite sequences vs m-sequences for brute force correlation	103
Figure 3.10	Baseband acquisition system for composite sequences	106
Figure 3.11	Acquisition performance improvement factor for composite sequences over single dwell acquisition technique; SNR = -10 dB, $N_a = 15$, $N_b = 31$	109
Figure 3.12	Acquisition performance improvement factor for composite sequences over single dwell acquisition technique; SNR = 0 dB, $N_a = 15$, $N_b = 31$	110
Figure 3.13	Acquisition performance improvement factor for composite sequences over single dwell acquisition technique; SNR = 0 dB, $N_a = 15$, $N_b = 127$	112
Figure 3.14	Acquisition performance improvement factor for composite sequences over single dwell acquisition technique; SNR = 0 dB, $N_a = 63$, $N_b = 31$	113
Figure 3.15	Acquisition performance improvement factor for composite sequences over single dwell acquisition technique; SNR = 0 dB, $N_a = 31$, $N_b = 15$	114
Figure 4.1	Sliding composite sequence combination process	120
Figure 4.2	Power spectrum of a sliding composite sequence $a(x) = b(x) = x^3 + x + 1$; $f_c = 600$ kHz	126
Figure 4.3	Power spectrum of a sliding composite sequence $a(x) = b(x) = x^8 + x^4 + x^3 + x^2 + 1$; $f_c = 5.08$ MHz	128
Figure 4.4	Acquisition system for sliding composite sequences	131
Figure A.1	The autocorrelation function of m-sequences	141

List of Acronyms

AO	Auto-Optimal
BCH	Bose-Chaudhuri-Hocquenghem
BMA	Berlekamp-Massey Algorithm
BPF	Bandpass Filter
BPSK	Binary Phase Shift Keying
CDMA	Code Division Multiple Access
DS	Direct-Sequence
FH	Frequency-Hopped
gcd	Greatest Common Divisor
GF	Galois Field
GMW	Gordon-Mills-Welch
GPS	Global Positioning System
IF	Intermediate Frequency
lcm	Least Common Multiple
LFSR	Linear Feedback Shift Register
LPD	Low Probability of Detection
LPE	Low Probability of Exploitation
LPI	Low Probability of Interception
LSE	Least Sidelobe Energy
MSK	Minimum-Shift-Keying
PCN	Personal Communications Network
PN	Pseudonoise
QPSK	Quadrature Phase Shift Keying
RARASE	Recurion-Aided Rapid Acquisition by Sequential Estimation
RASE	Rapid Acquisition by Sequential Estimation
RS	Reed-Solomon
SAW	Surface Acoustic Wave
SNR	Signal-to-Noise Ratio
SPR	Sidelobe-to-Peak Ratio
SS	Spread Spectrum
TDRSS	Tracking and Data Relay Satellite System
VLSI	Very Large Scale Integration

List of Symbols

A	slow component sequence
a_n	elements of sequence A
$a(x)$	slow component sequence characteristic polynomial
B	fast component sequence
$B(x)$	intermediate polynomial in Berlekamp-Massey algorithm
B_a	balance of component sequence A
B_b	balance of component sequence B
B_c	balance of composite sequence C
$\bar{B}_c$	mean value of balance of sliding composite sequence C
B_{IF}	noise bandwidth of the bandpass filter
B_{IF2}	noise bandwidth of the bandpass filter for the slow sequence acquisition
b_n	elements of sequence B
$\tilde{b}_n$	± 1 -valued sequence associated with b_n
$b(x)$	fast component sequence characteristic polynomial
C	composite sequence
$C_A(\tau_a)$	aperiodic autocorrelation function of slow component sequence
$C_B(\tau_b)$	aperiodic autocorrelation function of fast component sequence
$C_C(\tau)$	aperiodic autocorrelation function of composite sequence
$C_{C_1, C_2}(\tau)$	aperiodic cross-correlation function of composite sequences
$C_i(\tau)$	aperiodic autocorrelation function
$C_{i,j}(\tau)$	aperiodic cross-correlation function
C_{max}	maximum aperiodic autocorrelation magnitude
C_r	cyclotomic coset with leader r
$c_i(t)$	sequence time waveform
c_n	elements of the sequence C
$c_n^{(i)}$	spreading sequence of i^{th} user
$c(x)$	characteristic polynomial of the composite sequence C
D	three-component composite sequence
d	intermediate value in the Berlekamp-Massey algorithm
d_i	coefficient of the characteristic polynomial of fast component sequence
$d_i(t)$	data signal
$d_n^{(i)}$	data sequence of i^{th} user
E	third component of a three-component composite sequence
e_i	coefficient of the characteristic polynomial of slow component sequence
$f(x)$	characteristic polynomial
$f^*(x)$	reciprocal characteristic polynomial
f_c	chip rate

f_d	data rate
f_i	binary coefficients of $f(x)$
f_o	carrier frequency
$f_\alpha(x)$	characteristic polynomial with primitive root α
G	abelian group
$GF(2)$	finite field of two elements
$GF(q)$	finite field of q elements
$g'(x)$	generating polynomial of a sequence
H	subgroup of G
K	false alarm penalty factor
K_2	false alarm penalty factor for second dwell
k_i	exponent of each prime factor in decomposition of N
L	linear span of composite sequences
L_{Bent}	linear span of Bent sequences
L_{GMW}	linear span of GMW sequences
L_{No}	linear span of No sequences
M	intermediate value in Berlekamp-Massey algorithm
m	degree of characteristic polynomial
m_a	degree of characteristic polynomial of slow component sequence
m_b	degree of characteristic polynomial of fast component sequence
$m_i(t)$	phase-modulated data signal
$m_\alpha(x)$	minimal polynomial of α
N	period of spreading sequence
N_a	period of slow component sequence
N_b	period of fast component sequence
N_c	period of composite sequence
$N_c(m_a)$	number of sliding composite sequences
$N_c(m_a, m_b)$	number of composite sequences
N_d	period of three-component composite sequence
N_e	period of third-component of three-component composite sequence
N_{GMW}	number of GMW sequences
$N_I(m)$	number of irreducible polynomials of degree m
N_{No}	number of No sequences
$N_P(m)$	number of primitive polynomials of degree m
N_1	period of first component of combination sequence
N_2	period of second component of combination sequence
P_d	probability of detection
P_{d1}	probability of detection of first dwell
P_{d2}	probability of detection of second dwell
P_{fa}	probability of false alarm
P_{fa1}	probability of false alarm of first dwell

P_{fa2}	probability of false alarm of second dwell
$p_c(t)$	chip pulse signal
$p_d(t)$	data pulse signal
p_i	prime factors in decomposition of N
q	number of search cells in acquisition system
q	decimation number
q_1	size of search space for fast sequence acquisition
q_2	size of search space for slow sequence acquisition
$R_{1,j}(\Delta)$	continuous cross-correlation function
r	decimation number
$S_a(f)$	power spectrum of slow component sequence A
$S_b(f)$	power spectrum of fast component sequence B
$S_c(f)$	power spectrum of composite sequence C
$s(i)$	sidelobe energy
$s_A(\beta)$	state of the sequence generator for sequence A
$s_B(\alpha)$	state of the sequence generator for sequence B
$s_i(t)$	transmitted spread spectrum signal
T	integration time in continuous cross-correlation
$T(x)$	intermediate polynomial in Berlekamp-Massey algorithm
T_{acq}	acquisition time
$\bar{T}_{acq}$	mean acquisition time
$T_{acq}(\text{comp seq})$	acquisition time of composite sequences
$T_{acq}(\text{conv})$	conventional acquisition time
$T_{acq}(\text{double dwell})$	acquisition time of double dwell acquisition system
$T_{acq}(\text{opt})$	optimal achievable acquisition time
$T_{acq}(\text{single dwell})$	acquisition time of single dwell acquisition system
$T_{acq}(\text{scs})$	acquisition time of sliding composite sequences
$T_{acq}(\text{max})$	maximum total acquisition time
T_c	sequence chip duration
T_d	data bit duration
$\text{Tr}(x)$	trace polynomial
$V(N)$	total number of cyclotomic cosets
α	root of a primitive polynomial
β	root of a primitive polynomial
γ	element of $\text{GF}(2^m)$
$\delta(f)$	delta function
η_1	first acquisition integration threshold
η_2	second acquisition integration threshold
$\theta_A(\tau_a)$	autocorrelation function of slow component sequence
$\theta_B(\tau_b)$	autocorrelation function of fast component sequence
$\theta_C(\tau)$	autocorrelation function of composite sequence
$\hat{\theta}_C(\tau)$	odd autocorrelation function of composite sequences

$\theta_{C_1, C_2}(\tau)$	cross-correlation function of composite sequences
$\hat{\theta}_{C_1, C_2}(\tau)$	odd cross-correlation function of composite sequences
$\theta_i(\tau)$	periodic autocorrelation function
$\hat{\theta}_i(\tau)$	odd autocorrelation function
$\theta_{i,j}(\tau)$	periodic cross-correlation function
$\hat{\theta}_{i,j}(\tau)$	odd cross-correlation function
λ	correlation pulse shape constant
σ_{acq}^2	variance of acquisition time
$\sigma_{B_c}^2$	variance of balance of the sliding composite sequence C
$\phi(N)$	Euler totient function
Δ	phase shift variable in continuous cross-correlation function
τ	phase shift of sequence
τ_a	phase shift of slow component sequence A
τ_b	phase shift of fast component sequence B
τ_d	integration dwell time
τ_{d1}	first integration dwell time
τ_{d2}	second integration dwell time
τ_p	propagation delay
$\hat{\tau}_p$	estimate of the propagation delay
$\mu(i)$	Möbius function

Chapter 1

Introduction

1.1 Motivation

Modern digital military communications systems are required to be fast, reliable and secure. In many cases, these systems must operate in hostile environments where communications security is desirable and rapid signal acquisition is essential. The signals may be subjected to interference such as jamming or multipath, which must be rejected or at least diminished. As well, there may be a large number of signals sharing the same bandwidth and data integrity must be assured.

Direct-sequence spread spectrum (DS-SS) techniques are ideally suited to meet these criteria, in particular the interference rejection and multiple-accessing requirements. However, one of the biggest difficulties for DS-SS systems is rapid spreading sequence synchronization between the transmitter and the receiver. This is due to the opposing constraints of short sequence length for synchronization and long sequence length for security. To complicate matters further, the longer it takes to perform synchronization, the more likely a jammer can interfere with the process. In high-resolution ranging applications, the short sequence length for synchronization is countered by the long sequence length required to ensure there is no range ambiguity. The DS-SS signal can only be despread and the data demodulated when synchronization has been achieved. Any delay in the time to synchronize is a delay in communications and this must be minimized to limit the inconvenience to the users.

There has been considerable research conducted in the area of synchronization schemes for DS-SS employing binary phase-shift-keying (BPSK). Most of this research has been directed towards accelerating the process of acquisition. The majority of these approaches have been based on developing different hardware architectures to solve the

problem; these have been incremental improvements to an essentially "brute force" serial search technique.

In the past, a number of algorithmic approaches to the synchronization problem have been developed based on modifying the spreading sequence structure to achieve rapid acquisition capability. These techniques are split into the families of combination sequences [1, 2] and composite sequences [3, 4]; they involve breaking the spreading sequence into sub-components and synchronizing individually on each component. For combination sequences, the components consist of m-sequences of relatively prime periods. In the case of composite sequences, the components are sequences which have different clock rates, whereby the elements of a slow sequence are equal in duration to the length of one period of the fast sequence. Previous research has demonstrated the utility of these techniques for rapid acquisition [1, 2, 3, 5].

The combination sequences have been well studied with respect to correlation properties, interference rejection, multiple-accessing and linear span [6]. Unfortunately, these sequences provide little security such that an unintended listener can determine the spreading sequence with very little effort. Composite sequences were originally presented in Beale [4] and Stark [7] as an alternative approach to combination sequences. It is demonstrated in this thesis that the composite sequences achieve all of the desirable features of combination sequences and provide improved security against eavesdroppers. The composite sequences have previously been examined empirically, but for the most part, the synthesis, structure and performance of the composite sequences is not well understood and thus warrants further investigation.

In this thesis, the composite sequences are applied to the problem of acquisition for DS-SS communications and new insight is obtained through analysis of the synthesis, generation, structure and performance of the composite sequences. As well, a primitive polynomial generation algorithm will be presented which permits rapid determination of the components of the composite sequences to be synthesized.

A novel sub-class of the composite sequences is also presented in this thesis, termed the sliding composite sequences. The properties of these sequences are derived and it

will be seen that the sliding composite sequences provide improved acquisition time performance over the composite sequences. Ultimately, the thesis will demonstrate that this novel family of sequences is advantageous in terms of security, enumeration, power spectrum considerations and acquisition time at a small expense in sequence balance.

1.2 Thesis Organization

Chapter 2 describes the background theory of spreading sequences for direct-sequence spread spectrum communications and in particular, the problem of acquisition of DS-SS communications signals. Chapter 3 presents the results of research into the properties and performance of the composite sequences as well as a new algorithm for the generation of primitive polynomials. In Chapter 4, the sliding composite sequences are presented and analysis into their properties is carried out, including their synthesis, generation, enumeration, security, power spectrum and acquisition time performance. The thesis is concluded and future work is recommended in Chapter 5.

1.3 Thesis Contributions

The major contribution of this thesis is that a sequence design is proposed and analyzed which allows one to carry out rapid acquisition of direct-sequence spread spectrum signals. This novel sub-class of the composite sequences, termed the sliding composite sequences, is analyzed in terms of sequence properties including the generation, enumeration, linear span and power spectrum. The security of these sequences is examined through presentation of the techniques which an unintended listener would be required to carry out in order to exploit these sequences. The acquisition performance of sliding composite sequences is evaluated and a novel acquisition algorithm is presented which exploits the inherent rapid acquisition structure of these sequences.

Previous work is presented which led to the development of the class of composite sequences [3, 4]. A comprehensive and novel analysis of the composite sequences is carried out in this thesis leading to the derivation of the properties of composite

sequences including the generation, enumeration, linear span, correlation functions and power spectrum. The periodic autocorrelation function is derived and the aperiodic autocorrelation of m-sequences is analyzed to develop bounds on the out-of-phase periodic autocorrelation magnitude of composite sequences. The security of composite sequences and their acquisition performance are also analyzed.

It will be shown in this thesis that the composite sequences are a balanced, high linear span, large class of spreading sequences with low out-of-phase autocorrelation magnitude and a featureless power spectrum which permit rapid acquisition to be carried out. It will be further shown in this thesis that the sliding composite sequences are a secure, nearly balanced class of rapid acquisition spreading sequences with a high linear span, large enumeration and a featureless power spectrum.

Chapter 2

Background

2.1 Spread Spectrum Communications

Spread spectrum communication and navigation systems have been operating successfully in the military and commercial realms for many years. Systems such as the Space Shuttle [8], the Global Positioning System (GPS) [9], the Tracking and Data Relay Satellite System (TDRSS) [8], Starfix [10] and OmniTRACS [11] all utilize spread spectrum signalling to achieve reliable and robust information transmission. In the last decade, increasing interest in easing spectral congestion has led to significant advances in the commercial application of spread spectrum techniques and many exciting developments are now on the verge of reaching the marketplace including personal communications networks (PCN) and mobile cellular communication [12, 13].

Spread spectrum is defined as modulation techniques employed to widen the RF bandwidth of a signal such that the transmitted bandwidth is much wider than would be necessary for information transmission alone. The distinguishing features of spread spectrum signals are that the signal bandwidth is much larger than the information bandwidth and the spectral characteristics of the signal are determined by both the spreading waveform and the information waveform.

The technique for bandwidth spreading determines the type of spread spectrum signal. The most common types of spread spectrum signals are direct-sequence (DS) and frequency-hopped (FH) spread spectrum. Hybrid direct-sequence/frequency-hopped (DS/FH) spread spectrum is also employed. In this thesis, the focus will be on direct-sequence spread spectrum communications. Extensive treatments of all forms of spread spectrum modulation can be found in Ziemer and Peterson [8], Simon *et al* [14], Dixon [15] and Torrieri [16].

2.1.1 Direct-Sequence Spread Spectrum

Direct-sequence spread spectrum signals are typically obtained by phase-shift-keying a carrier frequency at a high rate. The modulation can be either binary phase-shift-keying (BPSK), quadrature phase-shift-keying (QPSK), m-ary PSK or other types, such as minimum-shift-keying (MSK). The modulation type of interest in this thesis is binary phase-shift-keyed DS-SS (denoted DS-BPSK). Much of the work in this thesis can be extended to application to DS-QPSK modulation.

A simplified block diagram of a DS-BPSK transmitter can be seen in Fig. 2.1. The binary data source transmits a signal with a period T_d and rate $f_d = 1/T_d$ defined as

$$d_i(t) = \sum_{n=-\infty}^{\infty} d_n^{(i)} p_d(t - nT_d) \quad (2.1)$$

where $p_d(t)$ is a rectangular pulse of duration T_d and $d_n^{(i)}$ is a binary data sequence corresponding to the i^{th} user. Similarly, the sequence generator produces a spreading sequence waveform of frequency $f_c = 1/T_c$ defined as

$$c_i(t) = \sum_{n=-\infty}^{\infty} c_n^{(i)} p_c(t - nT_c) \quad (2.2)$$

where $p_c(t)$ is a rectangular pulse of duration T_c and $c_n^{(i)}$ is a binary spreading sequence corresponding to the i^{th} user. The data phase-modulates a carrier of frequency f_0 and the resulting signal,

$$m_i(t) = d_i(t) \cos(2\pi f_0 t) \quad (2.3)$$

is BPSK spread by multiplying $m_i(t)$ by the spreading waveform $c_i(t)$. The resulting signal $s_i(t)$, given by

$$s_i(t) = c_i(t) d_i(t) \cos(2\pi f_0 t) \quad (2.4)$$

has a peak-to-null bandwidth of f_c . The transmitted signal is assumed to propagate via a distortionless path having delay τ_p and is received together with some interference and/or channel noise.

Figure 2.1: A DS-BPSK transmitter [8]

Demodulation is accomplished by mixing the received signal with the spreading sequence which has been delayed by an estimate of the transmission delay $\hat{\tau}_p$, as shown in Fig. 2.2. This remodulation or correlation of the received signal with the delayed spreading waveform is called despreading and is one of the most important functions in any spread spectrum system. Determination of the delay estimate, $\hat{\tau}_p$, is achieved through the use of synchronization circuitry which will be described later. The despread signal is then phase demodulated to regain the data waveform.

Direct-sequence spread spectrum signals have several advantages over conventional modulation techniques. By utilizing high rate spreading sequences with chip rates on the order of 100 to 1000 times the data rate, DS-SS signal spectra can be obtained which have a very low probability of detection and interception. As a result, and through the use of high complexity spreading sequences, exploitation of the DS-SS signal can be minimized.

One of the initial requirements which led to the development of DS-SS systems was to obtain communication systems which are resistant to jamming; some of the jamming techniques which the signal must mitigate include broadband jamming, partial-band jamming, tone, pulse or repeat-back jamming. The other major advantage is the rejection of interference which typically takes the form of multipath, channel noise, narrowband communicators or other DS-SS users in the same band. Multiple users can share the same bandwidth by utilizing spreading sequences which, if chosen correctly, exhibit low cross-correlations between each other; this is termed the code-division multiple-accessing (CDMA) capability of DS-SS.

Additional advantages of DS-SS systems are that they permit high-resolution ranging and accurate universal timing. This is achieved by utilizing high rate spreading sequences with a correspondingly short chip duration. Then, using the fact that the autocorrelation function of applicable spreading sequences is impulse-like, the propagation delay of the received signal can be identified with a resolution of one sequence chip. Note that the term chip describes a spreading sequence element, whereas the term bit is reserved for the elements of data sequences.

Figure 2.2: A DS-BPSK receiver [8]

The disadvantages of DS-SS systems include increased system complexity and difficulties in achieving synchronization between the spreading sequences of the transmitter and the receiver. The system complexity of DS-SS systems is continuously decreasing as advances in VLSI technology are applied to the design of these systems.

An area of continuing research is in DS-SS systems which synchronize rapidly and accurately. DS-SS signals can only be despread and the data demodulated if the transmitter and receiver obtain and maintain synchronization between their spreading sequences. Typically, the problem with synchronization is that the spreading sequence is very long and most techniques require a large portion of the sequence before synchronization can be achieved. Much time and effort has been devoted to developing acquisition schemes which allow this process to occur with minimal time delay and signal degradation.

2.2 DS-SS Acquisition

The most important phase of DS-SS communications is the synchronization of the transmitter and receiver spreading sequences [17, 18, 19]. Typically, the process of synchronization is performed in two steps, sequence acquisition, then tracking using one of the available tracking loops [14]. Acquisition is the process of successive decisions whereby the goal is to bring the two spreading sequences into coarse time alignment within one chip interval. Tracking is the subsequent continuous fine alignment of the two sequences to within a small percentage of one chip interval, typically maintained by means of a closed loop operation such as with a phase-locked loop.

In some of the literature, the process of acquisition is further subdivided into two phases: the coarse acquisition process described above and fine acquisition. Fine acquisition is defined as the transition process from coarse acquisition to tracking; this is typically defined in terms of a search/lock strategy [14] and yields a verification of the validity of a positive acquisition before turning control over to the tracking loop. In this thesis, the term acquisition will be used to describe the coarse acquisition process. The emphasis in this thesis is on the application of composite sequence techniques to improve the speed of the acquisition process. The reader is referred to Simon *et al* [14],

Hopkins [20] and Holmes and Chen [21] for details on fine acquisition and Polydoros and Weber [22], Simon [23], Hopkins [24], LaFlame [25] and Yost and Boyd [26] for information on tracking.

There are two classes of techniques available for the acquisition of DS-SS signals: hardware based approaches and rapid acquisition sequence techniques. The hardware schemes are based on testing all possible spreading sequence phases relative to the received signal until some correlation threshold is exceeded. A good historical survey of these techniques can be found in Simon *et al* [14] although some of the more interesting schemes will be detailed here. Polydoros [27] also carried out a comprehensive survey of acquisition techniques and defined a classification of the various schemes based on their structure.

The simplest and most fundamental scheme is the single dwell, uniform stepping, serial search technique [21], illustrated in Fig. 2.3. In this scheme, a single integration is performed at each of the N possible spreading sequence phase alignments for a fixed period of time in a serial fashion until the correct relative phase alignment has been detected. The correlation time required at each test phase is a function of the received signal-to-noise ratio (SNR) and the decision threshold, with the time required increasing as the SNR decreases. Using a simplified model of the acquisition process, it can be seen that, on average, $\frac{1}{2}N$ integrations are required to acquire, where N is the period of the spreading sequence. Each of these $\frac{1}{2}N$ integrations are of duration τ_d , where τ_d is a function of the received SNR. Thus, the average acquisition time is $\bar{T}_{acq} = \frac{1}{2}N\tau_d$. This scheme is most attractive for low SNR environments but can yield very long acquisition times for large values of N . This technique will be discussed in detail in Section 2.2.1. For higher SNR environments, techniques such as sequential estimation [28] give improved acquisition time performance; these techniques will be described later in this section. In Sage [29], the serial search was performed by linearly varying the time difference between the incoming signal and the waveform generated at the receiver with an on-going decision process determining when acquisition was achieved. This classical technique is referred to as the sliding correlator acquisition system.

Figure 2.3: Block diagram of a single dwell PN acquisition system [14]

The single dwell, serial search technique was later generalized by Rappaport and Schilling [30] who examined a double dwell system and by DiCarlo [31] who developed a multiple dwell system. In the multiple dwell, serial search technique, the integration time is varied by increasing it towards some maximum value in discrete steps, with a threshold decision being made after each step. The maximum integration time is a function of the desired probabilities of detection and false alarm. An incorrect sequence alignment is dismissed as soon as a false decision is encountered. This reduces the acquisition time considerably by rapidly eliminating incorrect alignments instead of performing full integrations at all of the incorrect sequence phases. Davidovici [32] refined this further by developing a double dwell, serial search system where the correlation threshold is set based on the partial period cross-correlation bounds of spreading sequences. The double dwell system will be described in detail in Section 2.2.2.

In an effort to reduce the acquisition time further, several authors have attempted to parallelize the process by performing simultaneous correlation threshold tests at several sequence phases. Some of the different technologies employed to parallelize the process include analog matched filters [33], digital matched filters [34, 35], surface acoustic wave (SAW) tapped delay lines [36], parallel SAW convolvers [37] and acousto-optic time-integrating correlators [38].

In Cheng [39], analysis was carried out on the performance of a parallel acquisition scheme in the presence of data modulation. The performance of this scheme in the presence of doppler shift only and a combination of doppler shift and data modulation was extended in Cheng, Hurd and Statman [40], where the doppler shift manifested itself in the form of both carrier-frequency offset and chip-frequency offset. The analysis of the effect of data modulation and/or narrowband interference on sequence acquisition was performed in Siess and Weber [41], and Milstein [42] has analyzed the effect of interference rejection filters on acquisition performance. Another interesting approach was proposed in Dlugos and Scholtz [43], where the performance of a parallel acquisition scheme using an antenna array was carried out with a maximum-likelihood procedure to detect sequence alignment.

Some of the classical acquisition techniques include the Rapid Acquisition by Sequential Estimation (RASE) system described in Ward [28] and the Recursion-Aided RASE (RARASE) system detailed in Ward and Yiu [44]. Another related technique is categorized as an error-correcting sequential estimation method and is detailed in Kilgus [45]. These sequential estimation techniques are based on estimating the phase of the incoming signal to set the initial position of the sequence generator in the receiver. Tracking is then attempted while continuing the correlation tests between the incoming signal and the spreading sequence of the receiver. These cross-correlation tests soon determine whether the estimate of the sequence phase is correct and if not, a new estimate is made and the process is repeated. The sequential estimation techniques are much faster than the single and multiple dwell schemes for high SNR's and for systems employing long spreading sequences. The problem with the sequential estimation techniques is their susceptibility to noise and interference since the estimation is performed on an individual chip basis and makes no use of the processing gain of DS-SS signals.

The problem with all of the above approaches is that they are hampered by the requirement to test all possible relative spreading sequence phase alignments between the received signal and the reference sequence. None of the above techniques attempt to address this inherently slow approach to the acquisition problem. As will be discussed, some of the newer approaches have attempted to address the problem by developing spreading sequence structures which permit significant reductions in the computational effort required to acquire. Thus, whereas the conventional acquisition techniques have acquisition times proportional to N^2 , the rapid acquisition sequence techniques achieve acquisition times proportional to the sequence period N . Before describing these rapid acquisition sequence techniques in detail, background material on the theory governing spreading sequences and a survey of spreading sequence techniques will be presented in the sections which follow.

2.2.1 Single Dwell Serial Search Acquisition

The block diagram and a basic description of the single dwell, uniform stepping, serial search acquisition system was previously given in Section 2.2. As well, it was

stated that the average acquisition time is $\bar{T}_{\text{acq}} = \frac{1}{2}N\tau_d$, where N is the sequence period and τ_d is the integration time at each phase of the spreading sequence. This is the most simplistic view of acquisition, which is in fact a far more complex problem. The factors affecting single dwell, serial search acquisition will now be described and the acquisition performance will be given. A detailed discussion and derivation can be found in Holmes [46] and Holmes and Chen [21].

The average acquisition time given above assumes that the N chips are searched in one chip steps, the dwell time is τ_d seconds, the detection probability P_d is one, and the false alarm probability P_{fa} is zero. The practical considerations of a non-zero probability of false alarm and a non-unity probability of detection will now be included in the analysis of acquisition performance [21, 46].

Assume there are q cells to be searched. It was assumed before that $q = N$, the period of the sequence to be searched; however, q is typically some multiple of N so that if the update size is one-half chip, then $q = 2N$. Also, assume that if the output of the integrate and dump circuit exceeds the preset threshold, the system goes into a verification mode which will be characterized by an extended dwell time $K\tau_d$, where $K \gg 1$. This time interval of $K\tau_d$ seconds is thus considered to be the penalty time associated with obtaining a false alarm. Hence, at each test position (excluding the single correct sequence phase position) one of two events can take place: either a false alarm occurs whereby acquisition is indicated when the sequences are actually misaligned, with probability P_{fa} and a penalty time of $K\tau_d$, or no false alarm occurs with probability $(1 - P_{fa})$ and single dwell time τ_d . Also, at the correct sequence phase position, either a correct detection occurs with probability P_d , or no detection occurs, with probability $(1 - P_d)$.

Now, the time to acquire, T_{acq} is a random variable which depends on the initial sequence phase position of the reference sequence generator in the receiver relative to that of the incoming signal. Ideally, the time to acquire is expressed in terms of its probability distribution function, but in practice, the mean acquisition time $\bar{T}_{\text{acq}}$ and the acquisition time variance σ_{acq}^2 are used to give a reasonable approximation of acquisition

time performance [46]. It will be assumed that there is no sequence doppler present and that the probability of detection is time invariant, i.e., that only one search cell corresponds to the correct sequence phase alignment. Thus, it can be shown that the mean time to acquire is given as [46]

$$\bar{T}_{\text{acq}} = \frac{2 + (2 - P_d)(q - 1)(1 + K P_{fa})}{2P_d} \tau_d \quad (2.5)$$

For the usual situation where $q \gg 1$, the mean acquisition time can be approximated by

$$\bar{T}_{\text{acq}} = \frac{(2 - P_d)(1 + K P_{fa})}{2P_d} (q\tau_d) \quad (2.6)$$

Similarly, it can be shown that for the practical case where $q \gg 1$ and $K \ll q$, the variance of the acquisition time is [46]

$$\sigma_{\text{acq}}^2 = \tau_d^2 (1 + K P_{fa})^2 q^2 \left(\frac{1}{12} + \frac{1}{P_d^2} - \frac{1}{P_d} \right) \quad (2.7)$$

The probability of detection P_d for a fixed integration period following a square law detector whose input is signal plus band-limited Gaussian noise is usually approximated as [46]

$$P_d = \text{erfc} \left(\frac{\text{erfc}^{-1}(P_{fa}) - \sqrt{B_{IF}\tau_d} \text{SNR}}{\sqrt{1 + 2\text{SNR}}} \right) \quad (2.8)$$

where P_{fa} is the probability of false alarm, B_{IF} is the noise bandwidth of the bandpass filter (BPF), τ_d is the integration dwell time, and SNR is the signal-to-noise ratio at the output of the square-law detector. The complementary error function is defined as [47]

$$\text{erfc}(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-y^2/2} dy \quad (2.9)$$

The procedure used to determine acquisition time performance is as follows: For a given P_{fa} , P_d and SNR, use (2.8) to determine $B_{IF}\tau_d$. From a specified BPF bandwidth B_{IF} , the dwell time τ_d is then found. Then, substitute P_d , P_{fa} and τ_d into (2.6) and (2.7), with specified values of q and K , to obtain $\bar{T}_{\text{acq}}$ and σ_{acq}^2 , respectively.

In Simon *et al* [14], several modifications to these results were made to take into account the effects of sequence timing misalignment, data modulation distortion, noise spectral density reduction due to the despreading operation, the probability of hand-over from acquisition mode to tracking mode (of interest for low SNR environments [46]), and signal dynamics such as sequence doppler and its derivative. While these factors are not discounted, they are considered to be secondary effects; in the interest of clarity, these effects will not be taken into account in considering the acquisition time performance of DS-SS systems and in particular, in comparing the performances of the acquisition schemes which will be presented later in this thesis.

2.2.2 Double Dwell Serial Search Acquisition

The single dwell, serial search acquisition technique is easily generalized to a double dwell system with the resulting system model shown in Fig. 2.4. In this scheme, two integration periods are employed with subsequent threshold comparisons for each test phase. The first integration dwell time τ_{d1} is small and the second dwell time τ_{d2} is longer. In this way, the acquisition time is reduced since incorrect sequence phase alignments will be dismissed earlier by the short dwell integration than would be dismissed in the single dwell acquisition system. If the first threshold η_1 is exceeded, then without changing the sequence phase, the longer dwell time procedure is carried out, providing a higher probability of detection and a lower probability of false alarm. In the case where either threshold test fails, the local sequence generator is delayed by some amount, typically one-half chip, and the tests are re-initiated. The process continues until both thresholds are exceeded, at which time the tracking loop is activated. Since the majority of cells examined correspond to incorrect phase alignments, then the quick dismissal of these cells by the short dwell integration will produce a considerable reduction in acquisition time. The acquisition time performance of the double dwell acquisition system will now be described.

The acquisition time performance is derived in detail in Simon *et al* [14] and Holmes and Chen [21] using flow graph analysis techniques to obtain moment generating functions [48]. For the double dwell acquisition system, it can be shown that for $q \gg 1$, the mean

Figure 2.4: Block diagram of a double dwell acquisition system

acquisition time is [21]

$$\bar{T}_{\text{acq}} = \frac{2 - P_d}{2P_d} \{ \tau_{d1} + P_{fa1}(\tau_{d2} - \tau_{d1})(1 + K_2 P_{fa2}) \} q \quad (2.10)$$

and the variance of the acquisition time is [21]

$$\sigma_{\text{acq}}^2 = q^2 [\tau_{d1} + P_{fa1}(\tau_{d2} - \tau_{d1})(1 + K_2 P_{fa2})]^2 \left(\frac{1}{12} + \frac{1}{P_d^2} - \frac{1}{P_d} \right) \quad (2.11)$$

where P_{fa1} is the probability of false alarm associated with the first dwell, P_{fa2} is the probability of false alarm associated with the second dwell, K_2 is the penalty factor associated with a false alarm on the second dwell and $P_d = P_{d1} P_{d2}$ is the system detection probability, determined as the product of the detection probabilities of dwells one and two. Note that if $\tau_{d1} = 0$ and $P_{fa1} = 1$, then (2.10) and (2.11) agree with the results of (2.6) and (2.7) for the single dwell case.

The performance of the double dwell system will now be compared to that of the single dwell system in order to assess the impact of the various parameters on the improvement which can be obtained with the double dwell system. Again, the arguments for the choices selected are given in Simon *et al* [14]. The decision thresholds η_1 and η_2 are chosen such that $P_{d1} = P_{d2}$ permitting a simple upper bound on performance. Then, in order to guarantee that the system detection probability for the double dwell system is equal to or greater than that of the single dwell system, the detection probabilities are chosen as

$$P_{d1} = P_{d2} = \frac{1 + P_d}{2} \quad (2.12)$$

where P_d is the detection probability of the single dwell system. Similarly, if P_{fa} denotes the false alarm probability of the single dwell system, then setting

$$P_{fa2} = P_{fa} \quad (2.13)$$

will ensure that the double dwell system achieves an equal or lower false alarm probability than the single dwell system.

So, the mean acquisition time for the double dwell system can be compared to that of the single dwell system using the ratio

$$\frac{\bar{T}_{\text{acq}}(\text{single dwell})}{\bar{T}_{\text{acq}}(\text{double dwell})} = \frac{(1 + K P_{fa})\tau_d}{\tau_{d1} + P_{fa1}(\tau_{d2} - \tau_{d1})(1 + K_2 P_{fa2})} \quad (2.14)$$

It is assumed that the double dwell and the single dwell systems have the same false alarm penalty time, i.e., $K\tau_d = K_2(\tau_{d2} - \tau_{d1})$; then the ratio can be simplified to

$$\frac{\bar{T}_{\text{acq}}(\text{single dwell})}{\bar{T}_{\text{acq}}(\text{double dwell})} \simeq \frac{\tau_d}{\tau_{d1} + P_{fa1}(\tau_{d2} - \tau_{d1})} \quad (2.15)$$

The computational procedure is then as follows: For a given P_d , P_{fa} , and SNR, compute $B_{IF}\tau_d$ for the single dwell system using (2.8); i.e., solve for

$$B_{IF}\tau_d = f(P_d, P_{fa}, \text{SNR}) \quad (2.16)$$

where $f(\cdot)$ represents the solution of (2.8) for $B_{IF}\tau_d$. Similarly, for the double dwell system, use $P_{d2} = (1 + P_d)/2$, $P_{fa2} = P_{fa}$ and SNR in (2.8) to determine $B_{IF}\tau_{d2}$, i.e., solve

$$B_{IF}\tau_{d2} = f\left(\frac{1 + P_d}{2}, P_{fa}, \text{SNR}\right) \quad (2.17)$$

Similarly, solve

$$B_{IF}\tau_{d1} = f\left(\frac{1 + P_d}{2}, P_{fa1}, \text{SNR}\right) \quad (2.18)$$

by varying the parameter P_{fa1} such that $\tau_{d1} + P_{fa1}(\tau_{d2} - \tau_{d1})$ is minimized. The resulting values of $B_{IF}\tau_d$, $B_{IF}\tau_{d1}$, $B_{IF}\tau_{d2}$ and P_{fa1} are substituted into (2.15) to give the improvement of the double dwell over the single dwell system.

This improvement factor is plotted against P_{fa} with P_d as a parameter in Figure 2.5 for SNR = -10 dB. The curves correspond to P_d values of .1, .5 and .9, from highest to lowest. It is clear that for a fixed SNR, the performance improvement increases for larger values of P_d and lower false alarm probabilities. However, while P_d impacts T_{acq} of the double dwell acquisition technique, it has little impact on the improvement factor.

Figure 2.5: Acquisition performance improvement factor for double dwell system over single dwell system; SNR = - 10 dB

2.3 Theory of Sequences

This thesis will primarily involve analysis of the properties of specific classes of spreading sequences which could be used in DS-SS systems. Although the interaction between the spread spectrum concerns and sequence issues is important, the primary focus will be on the structure and theory of sequences: spread spectrum is simply one area where these sequences find application. For example, much of this work can also be applied to cryptography as noted in Beker and Piper [49] and Konheim [50].

2.3.1 Galois Field Theory

A field with a finite number q of elements is called a *finite field*, or *Galois field*, and is denoted by $GF(q)$, where q is a prime. A field $GF(q^m)$ having q^m elements is called an *extension field* of the field $GF(q)$. The order of a field is defined as the number of elements in the field. The Galois fields of interest for binary sequences are $GF(2)$ and its extension fields $GF(2^m)$, for positive integers m . The reader is referred to Lidl and Neiderreiter [51] and Berlekamp [52] for extensive treatments of finite fields and their properties.

Consider polynomials in x whose coefficients are elements of $GF(2)$. A polynomial of degree m over $GF(2)$ has the form

$$f(x) = f_0x^m + f_1x^{m-1} + f_2x^{m-2} + \cdots + f_{m-1}x + f_m \quad (2.19)$$

where the coefficients f_i are elements of $GF(2)$, i.e., $f_i \in \{0, 1\}$. The reciprocal polynomial of $f(x)$ is defined as

$$f^*(x) = x^m f\left(\frac{1}{x}\right) \quad (2.20)$$

Note that the arithmetic operations are defined for these polynomials in exactly the same manner as polynomials with integer coefficients except that the coefficients are operated upon modulo-two.

A polynomial $f(x)$ over $GF(2)$ of degree m is said to be *irreducible* if $f(x)$ is not divisible by any non-trivial polynomial over $GF(2)$ of degree less than m . It has been

shown that any irreducible polynomial over $GF(2)$ of degree m divides $x^{2^m-1} + 1$ [53]. An irreducible polynomial $f(x)$ of degree m is said to be *primitive* if the smallest positive integer N for which $f(x)$ divides $x^N + 1$ is $N = 2^m - 1$. Note that: if $f(x)$ is primitive, then the reciprocal polynomial $f^*(x)$ is also primitive.

The number $N_I(m)$ of irreducible polynomials over $GF(2)$ of degree m is given by

$$N_I(m) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) 2^d \quad (2.21)$$

which asymptotically approaches $2^m/m$. The sum is over all integral divisors d of m and $\mu(\cdot)$ is the Möbius function

$$\mu(i) = \begin{cases} 1, & i = 1 \\ (-1)^j, & i = \text{product of } j \text{ distinct primes} \\ 0, & i \text{ divisible by a perfect square} \end{cases} \quad (2.22)$$

The members of the set $\{0, 1, \alpha, \alpha^2, \dots, \alpha^{2^m-2}\}$ constitute the 2^m elements of a Galois field $GF(2^m)$ where α is a root of a primitive polynomial of degree m over $GF(2)$. The exponent i of α^i is calculated modulo $(2^m - 1)$ since $\alpha^{2^m-1} = 1$. These elements can be represented as *pseudopolynomials* of degree less than m whereby the polynomial representation of α^i is given by

$$\alpha^i \bmod f(\alpha) \quad (2.23)$$

where $f(x)$ is the primitive polynomial from which the Galois field was generated. The elements of $GF(2^3)$ generated by the primitive polynomial $f(x) = x^3 + x^2 + 1$ are given in Table 2.1. It will be seen later that this polynomial representation has a direct correspondence to the state of a sequence generator.

Definition 2.1 For any $\alpha \in GF(2^m)$, let $m_\alpha(x)$ be the polynomial of smallest degree over $GF(2)$ having α as a root such that $m_\alpha(x) = 0$. This polynomial $m_\alpha(x)$ is called the minimal polynomial of α and it is irreducible.

There are $\phi(N)$ integers from 1 to N which are relatively prime to N , with $\phi(N)$ the Euler totient function defined as

$$\phi(N) = \begin{cases} 1 & N = 1 \\ N - 1 & N \text{ prime} \\ \prod_{i=1}^j p_i^{k_i-1} (p_i - 1) & \text{otherwise} \end{cases} \quad (2.24)$$

Table 2.1 The elements of $\text{GF}(2^3)$ generated by $f(x) = x^3 + x^2 + 1$

power representation	polynomial representation
0	0
1	1
α	α
α^2	α^2
α^3	$1 + \alpha^2$
α^4	$1 + \alpha + \alpha^2$
α^5	$1 + \alpha$
α^6	$\alpha + \alpha^2$

where N is a product of J distinct primes p_i , or

$$N = \prod_{i=1}^J p_i^{k_i} \quad (2.25)$$

These $\phi(N)$ integers form an abelian group G under multiplication modulo- N , where $N = 2^m - 1$ for our purposes. The set of numbers $H = \{1, 2, 4, \dots, 2^{m-1}\}$ forms a subgroup of G with m elements for $N = 2^m - 1$. This subgroup, when multiplied by any other element of the group, yields a coset.

Proper cyclotomic cosets, C_r , can be obtained by multiplying elements of H by an element r of G such that r is relatively prime to N . For example, with $N = 31$, the proper cyclotomic cosets are

$$\begin{aligned} C_1 &= \{1, 2, 4, 8, 16\} \\ C_3 &= \{3, 6, 12, 24, 17\} \\ C_5 &= \{5, 10, 20, 9, 18\} \\ C_7 &= \{7, 14, 28, 25, 19\} \\ C_{11} &= \{11, 22, 13, 26, 21\} \\ C_{15} &= \{15, 30, 29, 27, 23\} \end{aligned} \quad (2.26)$$

The number of proper cyclotomic cosets is exactly $\phi(2^m - 1)/m$ and the size or order of each proper coset is m . The number of primitive polynomials $N_P(m)$ is equal to the number of proper cyclotomic cosets and can be expressed as

$$N_P(m) = \frac{\phi(2^m - 1)}{m} \quad (2.27)$$

A cyclotomic coset $C_r = rH$ is called *improper* if r is not relatively prime to N . In other words, if

$$\gcd(r, N) \neq 1 \text{ for } 1 \leq r \leq N \quad (2.28)$$

For the example with $N=31$, $C_0 = \{0\}$ would be the only improper cyclotomic coset. Proper and improper cyclotomic cosets constitute the set of cyclotomic cosets modulo

$(2^m - 1)$. There are [54]

$$Y(N) = -1 + \frac{1}{m} \sum_{d/r_1} \phi(d) 2^{m/d} \quad (2.29)$$

cyclotomic cosets in all. Group elements p and q belong to the same cyclotomic coset if and only if there exists some integer j , $0 \leq j \leq m - 1$, such that

$$p = 2^j q \bmod (2^m - 1) \quad (2.30)$$

The smallest element r of a cyclotomic coset C_r is called the *cyclotomic coset leader*.

Let C_i and C_j be cyclotomic cosets containing the integers p and q respectively. Then C_i is called the *inverse cyclotomic coset* of C_j if there exists some integer k , $0 \leq k \leq m - 1$, such that

$$pq = 2^k \bmod (2^m - 1) \quad (2.31)$$

2.3.2 Linear Recursions and Code Generators

A linear recursive sequence $\{b_n\}$ is a binary sequence which satisfies a recursion relation of the form

$$b_n = \sum_{i=1}^m f_i b_{n-i} \text{ for all } n \quad (2.32)$$

so that each element of the sequence can be calculated from the m immediately preceding elements. Assuming that $f_m \neq 0$, m is called the *degree* of the linear recursion. The operation of addition is performed modulo-two and the coefficients f_i and the sequence elements b_n are contained in the Galois field $GF(2)$ consisting of the two elements $\{0, 1\}$.

Such a sequence $\{b_n\}$ can be generated by a circuit consisting of an m -stage shift register and a modulo-two adder as shown in Fig. 2.6. The constants $f_1, f_2, \dots, f_m$ are the feedback coefficients of the generator. When the generator is properly loaded with the first m elements of the sequence $\{b_n\}$, then the infinite periodic sequence $\{b_n\}$ will be produced.

Figure 2.6: An m -stage linear feedback shift register

There is an isomorphism between linear recursive sequences and polynomials [55, 56] such that the characteristic polynomial of the sequence $\{b_n\}$ satisfying (2.32) has the form

$$f(x) = x^m + f_1 x^{m-1} + f_2 x^{m-2} + \cdots + f_{m-1} x + 1 \quad (2.33)$$

For the case of maximal-length sequences, this characteristic polynomial is a primitive polynomial. The generating structure in Fig. 2.6 is known as the Fibonacci architecture. An alternate structure which is also described by the same characteristic polynomial $f(x)$ is the Galois architecture shown in Fig. 2.7. The Galois form is useful in that the state of the generator can be determined using Galois field calculations.

For example, if the characteristic polynomial of the sequence is $f(x) = x^3 + x^2 + 1$, then the state of the Galois shift register generator can be calculated using the example from Table 2.1. Thus, the sequence and the states of the sequence generator will be as shown in Table 2.2 with the corresponding sequence generator given in Fig. 2.8. As a result, it is seen that the sequence corresponding to $f(x) = x^3 + x^2 + 1$ is $\{b_n\} = \{0011101\}$. The correspondence between the state of the shift register generator and the pseudopolynomial representation of the elements of a Galois field can be observed by comparing Tables 2.1 and 2.2.

In order to describe the sequence $\{b_n\}$ mathematically, one may associate with it the generating polynomial

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots \quad (2.34)$$

which is the z-transform of the sequence $\{b_n\}$. Assuming the shift register has initial state

$$b_{-1}, b_{-2}, \dots, b_{-m} \quad (2.35)$$

Figure 2.7: Galois linear feedback shift register generator

Table 2.2 Shift register states and output for the sequence using $f(x) = x^3 + x^2 + 1$

Cycle	Shift Register State	Output
0	1 0 0	0
1	0 1 0	0
2	0 0 1	1
3	1 0 1	1
4	1 1 1	1
5	1 1 0	0
6	0 1 1	1

Figure 2.8: Galois sequence generator for $f(x) = x^3 + x^2 + 1$

then, using (2.32) it can be shown that [54]

$$\begin{aligned}
 g(x) &= \frac{\sum_{j=1}^m f_j x^j (b_{-j} x^{-j} + \dots + b_{-1} x^{-1})}{1 - \sum_{i=1}^m f_i x^i} \\
 &= \frac{\sum_{j=1}^m f_j x^j \left(\sum_{i=1}^j b_{-i} x^{-i} \right)}{x^m f\left(\frac{1}{x}\right)}
 \end{aligned} \tag{2.36}$$

This expresses the generating polynomial $g(x)$ completely in terms of the initial conditions from (2.35) and the characteristic polynomial $f(x)$ from (2.33).

For the case of m-sequences, a more algebraic representation can be obtained based on the trace function. The general trace polynomial $\text{Tr}_{2^k}^{2^m}(x)$ from $\text{GF}(2^m)$ to $\text{GF}(2^k)$ where k divides m is defined as

$$\text{Tr}_{2^k}^{2^m}(x) = \sum_{i=0}^{\frac{m}{k}-1} x^{2^{ik}} \tag{2.37}$$

and has several useful properties delineated in Simon et al [14]. An m-sequence $\{b_n\}$ generated by (2.32) can be represented using trace notation as

$$\{b_n\} = \left\{ \text{Tr}_{2^k}^{2^m}(\gamma \alpha^n) \right\} \tag{2.38}$$

where α is the root of $f(x)$ of (2.33) and γ is some element of $\text{GF}(2^m)$. This representation is linked to the superposition of cosets method of Golomb [54] since all of the elements of a cyclotomic coset have the same trace value.

The period N of the sequence $\{b_n\}$ is the smallest positive integer N such that $b_{n+N} = b_n$ for all n . In terms of the characteristic polynomial $f(x)$, the period N is the smallest positive integer N such that $f(x)$ divides $(x^N + 1)$. When $N = 2^m - 1$, the polynomial $f(x)$ is primitive and $\{b_n\}$ is a maximal-length sequence of linear span m . The linear span, or linear complexity of a sequence $\{b_n\}$ is defined as the degree of the shortest linear recursion satisfied by the sequence. For security, a pseudorandom sequence should have a large linear span in order to minimize the predictability of the sequence [57]. If a sequence has linear span m , then its linear recursion can be determined

from any $2m$ successive elements of the sequence using techniques which will now be demonstrated.

The linear recursion and hence, the characteristic polynomial of a sequence can be determined by solving a set of linear equations. Assuming that the linear span of the sequence is m and that $2m$ consecutive sequence elements are available, then the fact that the m -sequence satisfies the linear recursion of (2.32) can be used to determine the characteristic polynomial. The decoding techniques involve the solution of $m - 1$ equations in $m - 1$ unknowns to determine the characteristic polynomial (2.33) with $f_m = 1$. There are many techniques available to solve simultaneous linear equations including substitution, Gaussian elimination and Cramer's rule [58].

For example, suppose a binary sequence is known to satisfy a linear recursion of degree 5 (i.e., $f_5 = 1$) and furthermore, a portion of the sequence is

$$\dots 101101010001\dots \quad (2.39)$$

where the first bit is on the left and subsequent bits are on the right. Applying (2.32) to overlapping segments of the sequence yields the following set of simultaneous linear equations:

$$\begin{aligned} 1 &= f_2 + f_3 + f_5 \\ 0 &= f_1 + f_3 + f_4 \\ 1 &= f_2 + f_4 + f_5 \\ 0 &= f_1 + f_3 + f_5 \end{aligned} \quad (2.40)$$

Using the fact that $f_5 = 1$ and solving we obtain:

$$\begin{aligned} f_1 &= 0 \\ f_2 &= 1 \\ f_3 &= 1 \\ f_4 &= 1 \end{aligned} \quad (2.41)$$

Hence, the resulting linear recursion is

$$b_n = b_{n-2} + b_{n-3} + b_{n-4} + b_{n-5} \quad (2.42)$$

which implies that the characteristic polynomial of the sequence is

$$f(x) = x^5 + x^3 + x^2 + x + 1 \quad (2.43)$$

This technique is computationally intensive for large values of m and does not take into account the inherent structure of the linear recursions being solved for.

The system of linear equations is a Toeplitz system of equations [59]; in other words, if the system of equations is considered in terms of matrices, each row of the matrix is a shifted version of the row above. Given that the system of equations is Toeplitz, an efficient technique exists which allows solution of these equations, called the Berlekamp-Massey algorithm (BMA).

The BMA is often used for the decoding of Reed-Solomon (RS) and Bose, Chaudhuri and Hocquenghem (BCH) codes [52]. In Henkel [59] and Massey [60], the BMA is used to provide a general solution to the problem of synthesizing the shortest linear feedback shift register which generates a corresponding sequence of bits. In other words, the BMA solves for the minimal polynomial corresponding to a linear recursive sequence. For our purposes, the BMA will be presented in terms of our specific requirement of determining the characteristic polynomial for binary m -sequences. This algorithm requires any $2m$ consecutive bits of the m -sequence and will produce as a result the minimal polynomial corresponding to those bits. The details of the modified BMA are given below. The reader is referred to Massey [60] for the original algorithm which is generalized for the solution of non-binary sequences.

Assume that the linear span of the m -sequence is m and that $2m$ consecutive bits have been obtained $b_0, b_1, \dots, b_{2m-1}$. It is desired to determine the characteristic polynomial of the form (2.33) which corresponds to this sequence. Since (2.33) is the reciprocal of the polynomial $f(x)$ used in Massey [60], then step 7 has been added for consistency. In other words, the reciprocal must be taken of the polynomial which results from the BMA.

The steps of the algorithm are as follows:

1. Initialize $f(x) = B(x) = 1$, $n = M = 0$, $j = 1$.
2. If $n = 2m$, then go to step 7. Otherwise, compute

$$d = b_n + \sum_{i=1}^M f_i b_{n-i}$$

3. If $d = 0$, then $j = j + 1$. Go to step 6.
4. If $d = 1$ and $2M > n$, then

$$f(x) = f(x) + x^j B(x)$$

$$j = j + 1$$

Go to step 6

5. If $d = 1$ and $2M \leq n$, then

$$T(x) = f(x)$$

$$f(x) = f(x) + x^j B(x)$$

$$M = n + 1 - M$$

$$B(x) = T(x)$$

$$j = 1$$

6. Increment $n = n + 1$. Go to step 2.
7. Calculate the reciprocal of the polynomial $f(x)$. Stop.

Upon completion of step 7, the characteristic polynomial of the m-sequence which results is $f(x)$ of degree m . Table 2.3 indicates that the characteristic polynomial corresponding to the sequence of (2.39) is

$$f(x) = x^5 + x^3 + x^2 + x + 1 \quad (2.47)$$

as was found in (2.43) using the substitution method.

Table 2.3 Example application of the Berlekamp-Massey algorithm

n	M	$f(x)$	j	$B(x)$	b_n	d
0	0	1	1	1	1	1
1	1	$1 + x$	1	1	0	1
2	1	1	2	1	1	1
3	2	$1 + x^2$	1	1	1	1
4	2	$1 + x + x^2$	2	1	0	0
5	2	$1 + x + x^2$	3	1	1	0
6	2	$1 + x + x^2$	4	1	0	1
7	5	$1 + x + x^2 + x^4$	1	$1 + x + x^2$	1	1
8	5	$1 + x^3 + x^4$	2	$1 + x + x^2$	0	1
9	5	$1 + x^2$	3	$1 + x + x^2$	0	1
10	5	$1 + x^2 + x^3 + x^4 + x^5$	4	$1 + x + x^2$	-	-

2.3.3 Decimation

Let $B = \{b_n\}$ denote an arbitrary m-sequence of period N , and consider the sequence $C = \{c_n\}$ formed by taking every q^{th} bit of B (i.e., $c_n = b_{qn}$ for all positive integers n). The sequence C is said to be the *decimation* by q of B and will be denoted $\{b_{qn}\}$. Let $\gcd(a, b)$ denote the greatest common divisor of the integers a and b . If q divides N , then C has period N/q . If q and N are relatively prime, then the period of C is N . In general, the period of C is equal to $N/\gcd(q, N)$. A decimation is termed *proper* if q and N are relatively prime and *improper* otherwise.

Theorem 2.2 [14] *Let $\{b_n\}$ denote an m-sequence over $\text{GF}(2)$ with linear span m . Then:*

- (a) *A decimation $\{b_{qn}\}$ of $\{b_n\}$ is an m-sequence if and only if $\gcd(q, 2^m - 1) = 1$.*
- (b) *Two sequences $\{b_{qn}\}$ and $\{b_{rn}\}$ produced by decimations, with $\gcd(q, 2^m - 1) = 1$ and $\gcd(r, 2^m - 1) = 1$, are cyclically distinct if and only if*

$$q \not\equiv 2^k r \pmod{2^m - 1} \quad (2.48)$$

for all integers k .

- (c) *All m-sequences of period $2^m - 1$ can be constructed by decimations of $\{b_n\}$.*

An m-sequence $\{b_n\}$ is said to be in *natural orientation* if $b_n = b_{2n}$ for all n , where the indices are reduced modulo $(2^m - 1)$. If C is generated by a proper decimation of B and B is an m-sequence, then C is also an m-sequence (although B and C may be the same). If B is in natural orientation and is properly decimated, then C is also in natural orientation. If $f_\alpha(x)$ is the characteristic polynomial of B and $C = \{b_{qn}\}$, then $f_{\alpha^q}(x)$ is the characteristic polynomial of C , where $f_{\alpha^q}(x)$ can be determined as discussed in App. 5A.8 of [14]. The notation $f_\alpha(x)$ denotes the polynomial $f(x)$ with primitive root α ; in this thesis, the notation $f(x)$ will be used with the α subscript implied.

If $C = \{b_{qn}\}$ and $B = \{c_{rn}\}$, then q and r are termed *inverse decimations*. In other words, decimating sequence B by q and then by r will give sequence B . The integers q and r are inverse decimations if there exists some integer j , $0 \leq j \leq m - 1$, such that

$$qr = 2^j \pmod{2^m - 1} \quad (2.49)$$

Reciprocal decimation [61] is defined as the decimation which gives the m-sequence that is the reverse of the original m-sequence, or the reciprocal m-sequence. In order for q and r to be reciprocal decimations, it is necessary that for some positive integers x and y ,

$$q \cdot 2^x + r \cdot 2^y = 0 \pmod{2^m - 1} \quad (2.50)$$

An alternate description is that for some proper decimation q in $\text{GF}(2^m)$, the integer corresponding to the reciprocal decimation is the cyclotomic coset leader r of the coset which contains the positive integer

$$q \cdot (2^{m-1} - 1) \pmod{2^m - 1} \quad (2.51)$$

If q and r are a reciprocal decimation pair, then $\{b_{qn}\}$ and $\{b_{rn}\}$ are reciprocal sequences, whereby $\{b_{qn}\} = \{b_{rn}\}^*$. If $\{b_{qn}\} = \{b_{qn}\}^*$, then $\{b_{qn}\}$ is termed a *self-inverse* sequence.

Two m-sequences C and D obtained by proper decimations q and r , respectively, of the same m-sequence B in natural orientation, are identical if q and r belong to the same cyclotomic coset. In other words, if $\{c_n\} = \{b_{qn}\}$, then for all $j \geq 0$,

$$\{c_n\} = \{b_{(2^j q)_n}\} = \{b_{(2^j q \bmod N)_n}\} \quad (2.52)$$

If B is not in natural orientation, then C and D are shifted versions of each other. In this thesis, sequences which belong to the same cyclic class are considered equivalent.

The $N_P(m)$ cyclically distinct m-sequences are generated by $N_P(m)$ distinct primitive polynomials of degree m . Given one m-sequence B of linear span m , the remaining m-sequences of linear span m can be obtained from B by decimations $r_2, r_3, \dots, r_{N_P(m)}$ where the r_i constitute all of the proper cyclotomic coset leaders for $\text{GF}(2^m)$.

2.3.4 Correlation

For modern DS-SS systems employing multiple-accessing, the spreading sequences must satisfy the following two properties [62]:

- (i) each sequence in a set is easy to distinguish from a time-shifted version of itself;
- (ii) each sequence is easy to distinguish from every other sequence in the set.

The first of these properties is necessary to permit ease of synchronization and tracking at a receiver, and to enhance performance in multipath environments. The second property is required in a CDMA environment in order to distinguish the desired signals from the others.

The process of acquisition involves a correlation process using a system as illustrated in Fig. 2.3. For these correlation receivers, the function of interest is the magnitude of the cross-correlation [62]

$$R_{i,j}(\Delta) = \frac{1}{T} \int_0^T c_i(t) c_j(t + \Delta) dt \quad (2.53)$$

where $c_i(t)$ and $c_j(t)$ are different spreading sequences as defined in (2.2). This correlation is a measure of the similarity between any two signals with maximum correlation occurring if the two signals are identical and zero correlation if the signals are orthogonal. Assuming that $T = NT_c$, then the cross-correlation of (2.53) can be expressed as

$$R_{i,j}(\Delta) = \lambda \sum_{n=0}^{N-1} c_n^{(i)} c_{n+\tau}^{(j)} \quad (2.54)$$

where $\tau = \Delta/T_c$ and the constant λ is given by

$$\lambda = \frac{1}{NT_c} \int_0^{T_c} p_c^2(t) dt \quad (2.55)$$

with $p_c(t)$ the pulse waveform of the spreading code of (2.2). With $p_c(t)$ a rectangular pulse of duration T_c , the constant is $\lambda = 1/N$.

This leads to the periodic cross-correlation function between sequences $\{c_n^{(i)}\}$ and $\{c_n^{(j)}\}$ given by

$$\theta_{i,j}(\tau) = \sum_{n=0}^{N-1} c_n^{(i)} c_{n+\tau}^{(j)} \quad (2.56)$$

From (2.54), it is seen that $R_{i,j}(\Delta) = \lambda \theta_{i,j}(\tau)$ whenever $\Delta = \tau T_c$. For arbitrary values of Δ , $R_{i,j}(\Delta)$ can be determined from the periodic cross-correlation function $\theta_{i,j}(\tau)$

using [62]

$$R_{i,j}(\Delta) = \frac{1}{N} \theta_{i,j}(\tau') + \frac{(\tau' T_c - \Delta)}{N T_c} [\theta_{i,j}(\tau') - \theta_{i,j}(\tau' + 1)] \quad (2.57)$$

where τ' is the largest integer such that $\tau' T_c \leq \Delta$.

Since the periodic cross-correlation parameters for the continuous time signals $c_i(t)$ and $c_j(t)$ are completely determined by the cross-correlation function, we may now express the desirable sequence properties discussed above as follows:

- (i) for each sequence $\{c_n^{(i)}\}$ in the set, the autocorrelation magnitude $|\theta_{i,i}(\tau)|$ is small for $1 \leq \tau \leq N - 1$;
- (ii) for each pair of sequences $\{c_n^{(i)}\}$ and $\{c_n^{(j)}\}$, the cross-correlation magnitude $|\theta_{i,j}(\tau)|$ is small for all τ .

In other words, it is desirable to design sequences with small out-of-phase autocorrelation magnitude and small cross-correlation magnitude for all phases.

Sequence designs which satisfy these criteria will be discussed in Section 2.4. The remainder of this section will describe relevant correlation functions in terms of real-valued periodic sequences. Of particular interest are the classical periodic cross-correlation and autocorrelation functions which have been well-studied in the literature [14, 62, 63]. In CDMA systems where the spreading sequences are modulated with data, there are other correlation functions of interest. These functions include the aperiodic correlation functions [64, 65, 66, 67] and the odd correlation functions [64, 68]. Partial-period correlation functions are outside the scope of this work but details can be found in [14, 68, 69, 70].

The periodic cross-correlation function was defined in (2.56); the familiar periodic autocorrelation function is found by setting $i = j$ in (2.56) giving $\theta_{i,i}(\tau)$ which will be denoted $\theta_i(\tau)$. A good sequence design ensures that the autocorrelation function meets condition (i) above. An example of this is the autocorrelation function of m-sequences, which is given by

$$\theta_i(\tau) = \begin{cases} N & \tau = 0 \text{ mod } N \\ -1 & \tau \neq 0 \text{ mod } N \end{cases} \quad (2.58)$$

The Gold sequences are an example of a sequence design which ensures that the cross-correlation function $\theta_{i,j}(\tau)$ meets condition (ii) above; these will be discussed in the next section.

With data modulation present, a more relevant correlation function is the aperiodic cross-correlation function defined as [64, 66, 67]

$$C_{i,j}(\tau) = \begin{cases} \sum_{k=0}^{N-1-\tau} c_k^{(i)} c_{k+\tau}^{(j)} & 0 \leq \tau \leq N-1 \\ \sum_{k=0}^{N-1+\tau} c_{k-\tau}^{(i)} c_k^{(j)} & 1-N \leq \tau \leq 0 \\ 0 & |\tau| \geq N \end{cases} \quad (2.59)$$

The aperiodic cross-correlation function takes into account the effect of data transitions on the correlation of spreading sequences and is an important parameter in relating the probability of bit error performance of CDMA systems to the selection of the spreading sequence [65]. The aperiodic autocorrelation function for the sequence $\{c_n^{(i)}\}$ is $C_{i,i}(\tau)$ which will be denoted $C_i(\tau)$. The aperiodic autocorrelation function is important for the analysis of DS-SS signals in multipath environments [71] and when considering sequence synchronization in a receiver [72]. The periodic (even) cross-correlation function can be written in terms of the aperiodic cross-correlation function as $\theta_{i,j}(\tau) = C_{i,j}(\tau) + C_{i,j}(\tau - N)$.

The odd cross-correlation function $\hat{\theta}_{i,j}(\tau)$ is defined as [64, 68]

$$\hat{\theta}_{i,j}(\tau) = C_{i,j}(\tau) - C_{i,j}(\tau - N) \text{ for } 0 \leq \tau \leq N \quad (2.60)$$

since it has the property $\hat{\theta}_{i,j}(\tau) = -\hat{\theta}_{j,i}(N - \tau)$ whereas the periodic cross-correlation function satisfies $\theta_{i,j}(\tau) = \theta_{j,i}(N - \tau)$. Both of these relationships follow from the observation that $C_{i,j}(\tau) = C_{j,i}(-\tau)$. Both the odd cross-correlation and the periodic cross-correlation function are useful in evaluating the probability of bit error in CDMA systems and allow these calculations to be performed for signals with data modulation present [64, 66, 67]. Identities and bounds relating to the aforementioned correlation functions are detailed in Beale [4].

2.4 Spreading Sequences for DS-SS Communications

There are several classes of sequences which are useful for DS-SS communication systems. The selection of sequences for use in a given system is determined by the requirements of the specific application. As described in the previous section, the standard requirement for such a sequence is that its periodic autocorrelation magnitude be small at all non-zero shifts in order that correct sequence alignment can be easily detected [54, 63]. Where several such spread spectrum signals operate together in a CDMA environment, there is an additional design requirement of low periodic cross-correlation magnitude between all pairs of distinct sequences at all relative phase shifts τ . As well, in order to properly suppress the carrier and achieve a low probability of detection, it is required that the sequences be balanced, i.e., the number of ones in the sequence is as close as possible to the number of zeros. Finally, for purposes of security, there should be a great number of candidate sequences achieving a large linear span so that the linear recursion satisfied by the sequence is difficult for an interceptor to determine. In this section, the properties of several classes of binary sequences useful for DS-SS communications will be described. It will be seen that satisfying all requirements is not currently possible and the sequence design involves a compromise between conflicting parameters. When the additional requirement of rapid acquisition structure is imposed upon the design, it will be seen that most of the sequence designs fail to be satisfactory.

The maximal-length, linear feedback shift register sequences, or m-sequences, have been examined in detail by many authors including Golomb [54], Zierler [73], Braasch [74], Fillmore and Marx [75], and Smirnov [76]. These early results concentrated on the structural and autocorrelation properties of binary m-sequences with later results by authors such as Niho [77] and Helleseeth [78] discussing cross-correlation properties. The majority of this work has concentrated on periodic correlation functions, although some results have been obtained for the partial-period correlation functions, notably those of Wainberg and Wolf [79], Lindholm [80], Varakin and Volkov [81], Cartier [82] and Bekir [83].

As described in Section 2.3.2, m-sequences can be generated using linear feedback shift register circuits. The feedback taps of the generator correspond to the coefficients of primitive polynomials. From (2.27), the number of binary m-sequences of linear span m is $N_P(m)$. A new algorithm to find all of the primitive polynomials has been developed by the author and will be detailed in Section 3.2.1.

A brief account is now given of the properties of m-sequences. Here it is assumed the m-sequence $\{b_n\}$ of period $N = 2^m - 1$ has characteristic polynomial $f(x)$.

- I. The $2^m - 1$ distinct phase shifts of $\{b_n\}$ may be generated by the $2^m - 1$ possible initial states of the shift register generator.
- II. (Balance) The number of occurrences of one's in a period of $\{b_n\}$ exceeds the number of occurrences of zeros in a period of $\{b_n\}$, by one.
- III. (Run) Within one period of an m-sequence there will be 2^{m-i} runs of consecutive ones and $2^{m-i} - 1$ runs of consecutive zeros, where $1 \leq i \leq m$.
- IV. (Shift-and-Add) Given distinct integers i and j , $0 \leq i, j \leq N$, there exists a unique integer k , distinct from both i and j , such that $0 \leq k \leq N$ and

$$b_{n+i} + b_{n+j} = b_{n+k} \text{ for all } n. \quad (2.61)$$

The exact relationship between i , j and k in terms of trinomials is given in Roefs [70] and Bessarabova and Klykov [84]. It can be shown that i , j , k satisfy the trinomial of the form

$$x^i + x^j + x^k \quad (2.62)$$

which is divisible by $f(x)$. In other words,

$$x^k = (x^i + x^j) \bmod f(x) \quad (2.63)$$

allowing one to determine the shift which results from the shift-and-add process.

- V. (Autocorrelation) We define $\{\tilde{b}_n\}$ to be the ± 1 -valued sequence obtained from the m-sequence $\{b_n\}$ using

$$\tilde{b}_n = (-1)^{b_n} \text{ for all } n \quad (2.64)$$

Then, the periodic autocorrelation function of $\{\tilde{b}_n\}$ is given by (2.58). Thus, binary m-sequences have two-valued autocorrelation functions.

VL (Power Spectrum) The power spectrum $S_c(f)$, of an m-sequence of period N and chip rate $f_c = 1/T_c$, is given by

$$S_c(f) = \frac{1}{N^2} \delta(f) + \left(\frac{N+1}{N^2} \right) \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \text{sinc}^2\left(\frac{i}{N}\right) \delta\left(f - \frac{i}{N} f_c\right) \quad (2.65)$$

where $\delta(f)$ is the delta function. The derivation of this power spectrum involves Fourier transforming the autocorrelation function (2.58) [8]. See Appendix A for this derivation. The resulting spectrum is a line spectrum with a chip spectral line spacing of f_c/N and an envelope proportional to $\text{sinc}^2(f/f_c)$, except for the dc term, which has amplitude $1/N^2$. The power spectrum of an m-sequence is illustrated in Fig. 2.9.

The decimation properties are also important in determining the relationships between characteristic polynomials of different m-sequences; these were described previously in Section 2.3.3 and are discussed in detail in Sarwate and Pursley [62] and Duvall and Mortick [85].

For CDMA applications, the cross-correlation behaviour of sequences is crucial. Detailed discussions can be found in Golomb [54], MacWilliams and Sloane [63] and Sarwate and Pursley [62]. Consider the cross-correlation function, $\theta_{i,j}(\tau)$, of a pair of m-sequences, $\{a_n^{(i)}\}$ and $\{a_n^{(j)}\}$, each of period $N = 2^m - 1$. Since N is odd, it is easily seen that $\theta_{i,j}(\tau)$ must be an odd integer for all τ . In fact, it can be shown that for all τ , $\theta_{i,j}(\tau) + 1$ must be a multiple of 8, except when $\{a_n^{(i)}\}$ and $\{a_n^{(j)}\}$ correspond to a reciprocal pair of polynomials, in which case $\theta_{i,j}(\tau) + 1$ must be a multiple of 4 [78].

The mean-square cross-correlation magnitude for any pair of m-sequences is [86]

$$\frac{1}{N} \sum_{\tau=0}^{N-1} |\theta_{i,j}(\tau)|^2 = N + 1 - \frac{1}{N} \quad (2.66)$$

and the rms cross-correlation magnitude is the square root of this. For all N of interest, the rms cross-correlation magnitude can be approximated by $\sqrt{N}$, which is the square root

Figure 2.9: Power spectrum of an m-sequence [8]

of the autocorrelation peak value. Although (2.66) holds for any pair of m-sequences, it is important to note that the peak cross-correlation values depend on the specific m-sequences chosen. Gold and Kopitzke [87] empirically determined all of the cross-correlation magnitudes for all pairs of m-sequences of period up to 8191 chips. In Helleseeth [78], it was proven that the minimum number of distinct values in a cross-correlation function is three, and Gold [86] and Kasami [88] determined the pairs of primitive polynomials which give three-valued cross-correlation functions. The important result is that for any m which is not a multiple of 4, there exist pairs of m-sequences for which the cross-correlation magnitude takes on one of the three values in the set

$$\theta_{i,j}(\tau) \in \left\{ -1, \pm 2^{\lfloor (m+2)/2 \rfloor} - 1 \right\} \quad (2.67)$$

where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x . Any pair of m-sequences with this behaviour is known as a preferred pair of m-sequences. A survey of the known preferred pair relationships can be found in Trachtenberg [89].

The odd autocorrelation behaviour of m-sequences was studied by Massey and Uffner [68], Roefs [70], and Pursley and Roefs [67]. It was noted that since the odd autocorrelation function depends on the initial phase of the sequence, there is generally more than one initial phase position which minimizes the peak out-of-phase odd autocorrelation magnitude. Any initial phase which minimizes both the peak out-of-phase autocorrelation magnitude and the number of relative phase shifts at which it occurs is called an *auto-optimal* (AO) phase of the m-sequence. In Roefs [70], it was found that these AO phases were not unique, leading to an additional measure called the sidelobe energy. The sidelobe energy, defined as

$$s(i) = \sum_{\tau=1}^{N-1} \hat{\theta}_i^2(\tau) \quad (2.68)$$

allows determination of a unique optimal initial phase when minimized. The resulting phase is termed the auto-optimal phase with least sidelobe energy or AO/LSE phase. Roefs [70] determined the AO/LSE phase for all m-sequences of period up to 255. Subsequently, Skaug [90] extended these results to include all m-sequences of period up to 4095.

For CDMA systems, the odd cross-correlation function is also of interest. However due to the extensive computations required, searches for optimal sequences have assumed that the initial phase is fixed so that each code is an AO (or AO/LSE) phase, thereby optimizing odd autocorrelation performance. It is then a matter of searching relative phase shifts to empirically find the peak odd cross-correlation magnitudes. Such results have been obtained for m-sequences up to period 255 by Roefs [70] and Pursley and Roefs [67]. From these studies, it was found that the odd and even cross-correlation peaks cannot be simultaneously minimized, but there is a trade-off between the two parameters. Similarly, in Roefs and Pursley [91], an examination was carried out of the trade-off between auto- and cross-correlation performance by examining non-AO initial phases. This was performed for m-sequences up to period 127 and a slight reduction in cross-correlation peak magnitude was obtained.

Summarizing the work on m-sequences, it is possible to empirically determine optimal odd and even auto- and cross-correlation behaviour for a small set of users in a CDMA environment. However, the set of m-sequences of a given period which gives adequate correlation performance will typically be too small to be useful for CDMA. The linear span of the m-sequences is minimal, being m for m-sequences of period $N = 2^m - 1$. Finally, there is no inherent structure in the sequences which will permit rapid acquisition of the m-sequences.

In an effort to improve cross-correlation behaviour while minimizing the degradation in autocorrelation performance, the Gold sequences [46, 62, 86, 92] and Kasami sequences [62, 88] have been developed. Gold sequences are generated by a modulo-two combination of a preferred pair of m-sequences of period $N = 2^m - 1$ each. The resulting sequence is also of period $N = 2^m - 1$ and there are $N + 2$ sequences in the family corresponding to a given preferred pair of m-sequences, each sequence corresponding to a relative phase shift between the two generators. In other words, if $\{b_n^{(i)}\}$ is the m-sequence corresponding to the characteristic polynomial $f_i(x)$ and $\{b_n^{(j)}\}$ is the m-sequence corresponding to the characteristic polynomial $f_j(x)$, there are $N + 2$ Gold sequences with characteristic polynomial $f_i(x)f_j(x)$. The set of sequences includes

the original sequences $\{b_n^{(i)}\}$ and $\{b_n^{(j)}\}$, and the N sequences $\{b_n^{(i)}\} \oplus \{b_{n+k}^{(j)}\}$, for $0 \leq k \leq N - 1$. It can be shown [93] that the characteristic polynomial is of linear span $2m$ and so, the corresponding shift register circuit has $2m$ stages. Alternatively, the Gold sequences can be generated with two m -stage generators added modulo-two.

The construction of these sequences and the derivation of their periodic auto- and cross-correlation functions was described in Gold [92]. It was also shown that the cross-correlation function between two Gold sequences in the same family takes on the same magnitudes as the cross-correlation function between the original m -sequences $\{b_n^{(i)}\}$ and $\{b_n^{(j)}\}$. Since these sequences are a preferred pair of m -sequences, it follows that the cross-correlation only takes on the three possible magnitudes of (2.67). Similarly, it can be seen that the out-of-phase autocorrelation function of any non-trivial Gold sequence takes on the same three magnitudes. As with m -sequences, there are no analytical results which give the odd correlation values for Gold sequences, but some numerical results have been obtained by Roefs [70] who briefly investigated the odd auto- and cross-correlation behaviour of Gold sequences of period up to 127. Finally, as with m -sequences, there is no inherent structure in the Gold sequences which permits rapid acquisition.

The small set of Kasami sequences is constructed by the product of certain pairs of primitive polynomials of degree m and $m/2$, respectively [88]. The sequence $\{b_n^{(i)}\}$ corresponds to the primitive polynomial of degree m , and the degree $m/2$ polynomial must then correspond to the sequence $\{b_{n(2^{m/2}+1)}^{(i)}\}$ (the decimation of $\{b_n^{(i)}\}$ by $2^{m/2} + 1$). This gives a family of $2^{m/2}$ distinct sequences of period $2^m - 1$.

The linear span of the small set of Kasami sequences is $3m/2$, the degree of the product polynomial. The periodic cross-correlation and out-of-phase autocorrelation functions of these sequences take on the three values in the set $\{-1, -1 \pm 2^{m/2}\}$. Comparing the peak correlation magnitude of $2^{m/2} + 1$ with the correlation value of $2^{(m+2)/2} + 1$ (for m even) for the Gold sequences, it is seen that the small set of Kasami sequences has superior cross-correlation performance. However, a small set of Kasami sequences contains only $2^{m/2}$ sequences, whereas a family of Gold sequences contains $2^m + 1$ sequences, for period $N = 2^m - 1$ in each case.

There are several other classes of binary sequences with similar cross-correlation behaviour to Gold and Kasami sequences, described in Sarwate and Pursley [62]. These include the large set of Kasami sequences, Gold-like sequences and dual-BCH sequences.

All of the previously described sequences are generally classified as linear sequences. In addition to these sequence classes, there exist several non-linear sequence designs such as the Bent sequences [94, 95, 96], the m -like cipher sequences [97, 98], GMW sequences [99] and the No sequences [100]. All of these sequences achieve large linear span, but none have inherent structure which permits rapid acquisition to be carried out.

The Bent sequences have been detailed in Lempel and Cohn [94], Olsen, Scholtz and Welch [95] and Kumar and Scholtz [96]. In Rothaus [101], a description was made of the properties of Bent functions which are defined as follows. Let $f(x_1, x_2, \dots, x_m)$ be a Boolean function of the m binary variables $x_1, x_2, \dots, x_m$ and $F(x_1, x_2, \dots, x_m) = (-1)^{f(x_1, x_2, \dots, x_m)}$. Then $f(x_1, x_2, \dots, x_m)$ is called a Bent function if all the Fourier coefficients of F are ± 1 . This property was exploited in Olsen, Scholtz and Welch [95] to design sets of non-linear shift-register sequences with good correlation properties. Assuming m is a multiple of 4 and using an m -stage register, one can generate $2^{m/2}$ distinct Bent sequences of period $2^m - 1$. As with the small set of Kasami sequences, the peak correlation magnitude is $2^{m/2} + 1$, which is optimal. In Kumar and Scholtz [96], it was shown that the linear span of Bent sequences is lower bounded as

$$L_{\text{Bent}} \geq \binom{m/2}{m/4} 2^{m/4} \quad (2.69)$$

While Bent sequences are balanced, give reasonably large linear span and exhibit optimal correlation behaviour, there is no allowance for rapid acquisition and the possible sequence lengths are restricted to $2^m - 1$, for m a multiple of 4.

In Shaar and Davies [102], the prime sequences were developed. The prime sequences are generated by decimating the set of elements of $\text{GF}(N)$, for N a Mersenne prime (a prime number which can be expressed as $N = 2^m - 1$). In Quynh and Prasad [103], the prime interleaved sequences were generated by interleaving m -sequences of a given period, where the interleaving order is governed by the prime sequences. These

sequences achieve the same correlation bounds as the small set of Kasami sequences. In Quynh and Prasad [97], another set of interleaved sequences, the m -like sequences, was described. The prime interleaved and m -like sequences have optimal correlation functions and their linear span is significantly larger than the linear span of Bent sequences. An empirical analysis of these linear spans was carried out in Prasad and Quynh [98] although analytic expressions have not been determined. As before, however, there is no provision for rapid acquisition with these sequence designs. Earlier discussions of interleaved sequences can be found in Bluestein [104] and Surböck and Weinrichter [105].

The Gordon-Mills-Welch (GMW) sequences [106] were presented in Scholtz and Welch [99] as having correlation properties identical to m -sequences but possessing larger linear span. Assuming m is composite, or $m = JK$, and using the trace polynomial of (2.37), the GMW sequence can be specified as

$$b_n = \text{Tr}_2^{2^J} \left\{ \left[\text{Tr}_2^{2^m} (\alpha^n) \right]^r \right\} \quad (2.70)$$

where α is a primitive element of $\text{GF}(2^m)$, and the integer r , $1 \leq r \leq 2^J - 1$, satisfies $\text{gcd}(r, 2^J - 1) = 1$. Note that for $r = 1$, this reduces to the trace representation of an m -sequence as given in (2.38).

The autocorrelation function of GMW sequences is given by (2.58) as proven in Scholtz and Welch [99]. The cross-correlation behaviour has not been determined. The number of cyclically distinct GMW sequences which can be constructed for a fixed m and J is given by

$$N_{\text{GMW}} = \frac{\phi(2^m - 1)}{m} \cdot \frac{\phi(2^J - 1)}{J} \quad (2.71)$$

which is significantly larger than the number of m -sequences of degree m . The linear span of GMW sequences is given by [99]

$$L_{\text{GMW}} = J \left(\frac{m}{J} \right)^w \quad (2.72)$$

where w is the number of ones in the base-2 representation of r . This is clearly a significant increase over the linear span of m -sequences.

The No sequences were reported in No and Kumar [100] as providing low auto- and cross-correlation values and large linear span. Using the definition of the trace polynomial of (2.37), then a family of No sequences is a collection of $2^{m/2}$ binary sequences given by

$$\text{Tr}_2^{2^{m/2}} \left\{ \left[\text{Tr}_{2^{m/2}}^{2^m} (\alpha^{2^i}) + \gamma_i \alpha^{iT} \right]^r \right\} \quad (2.73)$$

where m must be even, $T = 2^{m/2} + 1$, α is a primitive element of $\text{GF}(2^m)$, the integer r , $1 \leq r \leq 2^{m/2} - 1$, satisfies $\gcd(r, 2^{m/2} - 1) = 1$, and the elements γ_i range over all of $\text{GF}(2^{m/2})$ taking on each value exactly once as i ranges between 1 and 2^m .

There are $2^{m/2}$ No sequences in a family and the number of families is given by

$$N_{\text{No}} = \frac{\phi(2^{m/2} - 1)}{m/2} \cdot \frac{\phi(2^m - 1)}{m} \quad (2.74)$$

where the first term corresponds to possible values of r and the second term corresponds to the number of primitive elements α of $\text{GF}(2^m)$. As with the small set of Kasami sequences, the cross-correlation function between two No sequences in the same family takes on the three values in the set $\{-1, -1 \pm 2^{m/2}\}$. The linear span is given by a complex expression [100] which is lower bounded as

$$L_{\text{No}} \geq m \cdot 2^{m-1} \quad (2.75)$$

Hence, the No sequences are excellent new sequences satisfying the requirements of low correlation magnitude, large linear span and a large set of sequences. Interestingly, within each No family is a GMW sequence and the Kasami sequences are a special case of the No sequences. Unfortunately, as with all previously described sequences, there is no inherent structure which permits rapid acquisition.

2.5 Rapid Acquisition Sequences

As described earlier, the simplest and most common acquisition technique is to serially correlate the received signal with all possible relative phases of a reference sequence until the correct phase is detected. The average acquisition time for this scheme

was shown to be $\bar{T}_{acq} = \frac{1}{2}N\tau_d$ for a sequence of period N with a fixed correlation time τ_d at each relative phase shift. For applications such as data links for remote-piloted vehicles [1] or for burst submarine communications, these long acquisition delays are unacceptable. Several techniques have been developed which attempt to address the acquisition time problem by modifying the structure of the spreading sequence.

2.5.1 Combination Sequences

One class of rapid acquisition sequences originally designed for radar ranging is the class known as optimal ranging codes [107], or combination sequences [1]. These are binary sequences where each bit is formed by a Boolean operation on two or more shorter component sequences. In general, if the periods of $\{b_n^{(i)}\}$ and $\{b_n^{(j)}\}$ are N_1 and N_2 , respectively, then the period of the combination sequence $\{b_n^{(k)}\}$ is $\text{lcm}(N_1, N_2)$, the least common multiple of N_1 and N_2 . Therefore, to maximize the length of the combination sequence, N_1 and N_2 should be relatively prime, so that $\text{gcd}(N_1, N_2) = 1$, resulting in a period of N_1N_2 .

The choice of Boolean combining law is restricted by our requirement to construct a sequence which permits rapid acquisition of the combination sequence on a component-by-component basis. In other words, we wish the received combination sequence $\{b_n^{(k)}\}$ to be correlated in turn by each component sequence such that the maximum number of correlations needed to acquire $\{b_n^{(k)}\}$ is $N_1 + N_2$. This is significantly less than the N_1N_2 correlations required for conventional sequences of length N_1N_2 . The restriction which this requirement imposes on the Boolean combining operation will now be clarified.

Suppose that modulo-two addition is chosen as the combining operation such that $\{b_n^{(k)}\} = \{b_n^{(i)}\} \oplus \{b_n^{(j)}\}$. Since we are working with ± 1 sequences, this is equivalent to multiplying the component sequences to form the combination sequence $\{a_n^{(k)}\} = \{a_n^{(i)}\} \cdot \{a_n^{(j)}\}$. Now, suppose that in the acquisition process the received sequence $\{a_n^{(k)}\}$ is correlated with a local replica of the component $\{a_n^{(i)}\}$. With the modulo-two combination law in use, the sequence of product terms $\{a_n^{(k)}\} \cdot \{a_n^{(i)}\}$ is simply the

component sequence $\{a_n^{(j)}\}$. Since $\{a_n^{(j)}\}$ is approximately balanced, then the in-phase full-period correlation magnitude will be very small and acquisition will not be successful.

Several researchers have examined the properties of combination sequences which employ the modulo-two combination operation. In Maritsas [108], it was shown that if the sequence combination operation is $\{b_n^{(k)}\} = \{b_n^{(i)}\} \oplus \{b_n^{(j)}\}$, then the corresponding characteristic polynomial is $f_k(x) = f_i(x) f_j(x)$ where $f_i(x)$ and $f_j(x)$ are the characteristic polynomials of the m-sequences $\{b_n^{(i)}\}$ and $\{b_n^{(j)}\}$ of period N_1 and N_2 , respectively. Using this construction, a balanced sequence is achieved and the autocorrelation of the sequence $\{a_n^{(k)}\} = \{a_n^{(i)}\} \cdot \{a_n^{(j)}\}$ is given by the formula

$$\theta_k(\tau) = \begin{cases} 1 & \text{if } \tau \neq k_1 T_1 \neq k_2 T_2, \quad k_1, k_2 = 0, 1, 2, \dots \\ -N_2 & \text{if } \tau = k_1 T_1 \neq k_2 T_2, \quad k_1, k_2 = 0, 1, 2, \dots \\ -N_1 & \text{if } \tau \neq k_1 T_1 = k_2 T_2, \quad k_1, k_2 = 0, 1, 2, \dots \\ N_1 N_2 & \text{if } \tau = k T_1 T_2 \quad k = 0, 1, 2, \dots \end{cases} \quad (2.76)$$

In Green [109], a simple technique for deriving the autocorrelation function of combination sequences was presented by using the fact that the autocorrelation function of the combination sequence is the product of the autocorrelation functions of the component sequences, or $\theta_k(\tau) = \theta_i(\tau) \theta_j(\tau)$. For example, with $N_1 = 7$ and $N_2 = 3$,

$$\begin{aligned} \theta_i(\tau) &= \begin{cases} 7 & \tau = 0 \pmod{7} \\ -1 & \tau \neq 0 \pmod{7} \end{cases} \\ \theta_j(\tau) &= \begin{cases} 3 & \tau = 0 \pmod{3} \\ -1 & \tau \neq 0 \pmod{3} \end{cases} \end{aligned} \quad (2.77)$$

and the autocorrelation function of $\{a_n^{(k)}\}$ is illustrated in Fig. 2.10

Titworth [107] has shown that in order to obtain optimal correlation between a combination sequence and its components, majority logic should be chosen as the combining rule, i.e., when combining n component sequences, the combination sequence bit is chosen to be a one if more than $n/2$ bits of the corresponding component sequences are ones. With n even, an arbitrary choice may be made for combination sequence bits when there are exactly $n/2$ ones in the corresponding component sequence bits. Hence, for n even, either of the Boolean functions OR or AND could be used. Titworth also showed that the component sequences should be balanced, although this will not necessarily result in a balanced combination sequence.

Figure 2.10: Formation of the autocorrelation function of a combination sequence [109]

In Milstein [1], Milstein and Ragonetti [2] and Milstein [6], an assessment was made of the suitability of combination sequences for the CDMA environment. These papers examined the cross-correlation functions of sets of combination sequences, each constructed from two component sequences, using the AND function as the combining law. The component sequences chosen were assumed to be independent random binary sequences, and the papers concentrated on the statistical behaviour of the correlation functions. It was found, for example, that the magnitude of the cross-correlation function between two independent combination sequences, each constructed from a pair of random component sequences with relatively prime periods N_1 and N_2 , has a mean value of $N_1 N_2 / 4$ and a variance of $3(N_1 + N_2 + 3) / 16$. Similarly, the magnitude of the full-period cross-correlation function between one component sequence of period N_1 and a combination sequence of period $N_1 N_2$ is seen to have zero mean and a variance of $(N_2 + 1) / 2$ [6]. For partial-period correlations using independent random binary sequences, Milstein [6] provides empirical bounds on the correlation behaviour. However, the correlation behaviour of combination sequences constructed from deterministic components, such as m-sequences, has not been analyzed. Although Milstein has demonstrated through simulations that combination sequences can support several users in a CDMA environment, there is no conclusive evidence of good CDMA performance.

Finally, if it is assumed that the components are m-sequences as in Maritsas [108], it is found that for component sequences of linear span m_1 and m_2 , where $N_1 = 2^{m_1} - 1$ and $N_2 = 2^{m_2} - 1$ are relatively prime, the linear span of the combination sequence is $m_1 + m_2$. For the combination sequence of period $N_1 N_2$ constructed here, the number of correlations required to achieve acquisition is $N_1 + N_2$. Hence, the combination sequences are good sequences in terms of correlation performance and rapid acquisition but inadequate in terms of balance, linear span and CDMA capability.

2.5.2 Composite Sequences

An alternative structure for sequences with a rapid acquisition capability has been analyzed for spread spectrum application by Stark and Sarwate [3], Beale and Tozer [5], Stark [7] and Kotov [110], and was mentioned briefly in Maskara and Das [111]. The

construction technique itself is not new: Turyn [112], Stiffler [113], Ackroyd [114] and Hollis [115] studied these sequences (referred to as tensor product sequences, Kronecker sum sequences, combination sequences and concatenated sequences, respectively) and derived their periodic autocorrelation function. As with combination sequences, the rapid acquisition of these sequences, hereafter referred to as composite sequences [5], is made possible by constructing them from two or more shorter component sequences. It is assumed in this thesis that the composite sequences are constructed through the combination of two component sequences.

As described in Stark and Sarwate [3] and Beale [4], the construction of composite sequences is as follows. Let $A = \{a_n\}$ and $B = \{b_n\}$ be periodic sequences over $GF(2)$ of periods N_a and N_b , respectively. A composite sequence $C = \{c_n\}$, is constructed from the two component sequences A and B using [3]

$$c_k = a_i + b_j \text{ where } k = iN_b + j, 0 \leq j \leq N_b - 1$$

$$0 \leq i \leq N_a - 1 \quad (2.78)$$

where the addition is carried out modulo-two. This corresponds to the modulo-two addition of each element of the component sequence A with all N_b elements (one period) of the component sequence B . In the time domain, this process is achieved by defining the chip rate of the LFSR for sequence A to be N_b times slower than the chip rate of the LFSR for sequence B , such that each element of A has the same time duration as one complete period of B . Hence, the composite sequence C has the same chip rate as B , with one period of C comprising $N_c = N_a N_b$ chips and having the same duration as one period of A . This process was termed sequence-inversion keying by Ward [116] as applied to the case of data modulating a spreading sequence, with one data element matched in duration to one period of the spreading sequence.

The correlation properties of composite sequences will now be described. Let $C_1 = \{c_n^{(1)}\}$ and $C_2 = \{c_n^{(2)}\}$ be composite sequences of the same period N_c constructed as above. The periodic cross-correlation between C_1 and C_2 using the definition of (2.56) is given by

$$\theta_{C_1, C_2}(\tau) = \sum_{n=0}^{N_a N_b - 1} c_n^{(1)} c_{n+\tau}^{(2)} \quad (2.79)$$

From Beale and Tozer [5] and Kotov [110], it can be shown that the periodic cross-correlation between C_1 and C_2 can be expressed in terms of the various correlations between the component sequences as

$$\theta_{C_1, C_2}(\tau) = \theta_{A_1, A_2}(\tau_a)C_{B_1, B_2}(\tau_b) + \theta_{A_1, A_2}(\tau_a + 1)C_{B_1, B_2}(\tau_b - N_b) \quad (2.80)$$

where $\tau = \tau_a N_b + \tau_b$, $0 \leq \tau_b \leq N_b$, $0 \leq \tau_a \leq N_a$. The periodic autocorrelation function can be obtained by setting $C_1 = C_2$, $A_1 = A_2$ and $B_1 = B_2$ in the cross-correlation function to obtain

$$\theta_C(\tau) = \theta_A(\tau_a)C_B(\tau_b) + \theta_A(\tau_a + 1)C_B(\tau_b - N_b) \quad (2.81)$$

From Stark and Sarwate [3], the odd cross-correlation and autocorrelation functions were derived as

$$\hat{\theta}_{C_1, C_2}(\tau) = \hat{\theta}_{A_1, A_2}(\tau_a)C_{B_1, B_2}(\tau_b) + \hat{\theta}_{A_1, A_2}(\tau_a + 1)C_{B_1, B_2}(\tau_b - N_b) \quad (2.82)$$

and

$$\hat{\theta}_C(\tau) = \hat{\theta}_A(\tau_a)C_B(\tau_b) + \hat{\theta}_A(\tau_a + 1)C_B(\tau_b - N_b) \quad (2.83)$$

The aperiodic correlation functions were derived in Stark and Sarwate [3] and Beale [4] as

$$C_{C_1, C_2}(\tau) = C_{A_1, A_2}(\tau_a)C_{B_1, B_2}(\tau_b) + C_{A_1, A_2}(\tau_a + 1)C_{B_1, B_2}(\tau_b - N_b) \quad (2.84)$$

and

$$C_C(\tau) = C_A(\tau_a)C_B(\tau_b) + C_A(\tau_a + 1)C_B(\tau_b - N_b) \quad (2.85)$$

Note that (2.85) was also obtained by Turyn [112], Stiffler [113] and Ackroyd [114].

In Beale [4], the results above were generalized to three-component composite sequences. Consider a composite sequence $D = \{d_n\}$ of period $N_d = N_a N_b N_c$, constructed from the three component sequences: $A = \{a_n\}$ of period N_a , $B = \{b_n\}$ of period N_b and $E = \{e_n\}$ of period N_c . As before, B is sequence-inversion keyed by A to obtain a composite sequence C of period $N_c = N_a N_b$. The resulting sequence C is then sequence-inversion keyed by E to give D . The periodic cross-correlation function

between two composite sequences $D_1 = \{d_n^{(1)}\}$ and $D_2 = \{d_n^{(2)}\}$, each constructed as above, can be expressed as

$$\theta_{D_1, D_2}(\tau) = \theta_{E_1, E_2}(\tau_e) C_{C_1, C_2}(\tau_c) + \theta_{E_1, E_2}(\tau_e + 1) C_{C_1, C_2}(\tau_c - N_c) \quad (2.86)$$

where $0 \leq \tau_e \leq N_e - 1$, $0 \leq \tau_c \leq N_c - 1$ and $\tau = \tau_e N_c + \tau_c$. Substituting in (2.84) to replace the aperiodic cross-correlation functions $C_{C_1, C_2}(\cdot)$ we obtain

$$\begin{aligned} \theta_{D_1, D_2}(\tau) = & \theta_{E_1, E_2}(\tau_e) [C_{B_1, B_2}(\tau_b) C_{A_1, A_2}(\tau_a) + C_{B_1, B_2}(\tau_b - N_b) C_{A_1, A_2}(\tau_a + 1)] \\ & + \theta_{E_1, E_2}(\tau_e + 1) [C_{B_1, B_2}(\tau_b) C_{A_1, A_2}(\tau_a - N_a) + C_{B_1, B_2}(\tau_b - N_b) C_{A_1, A_2}(\tau_a - N_a + 1)] \end{aligned} \quad (2.87)$$

where $0 \leq \tau_b \leq N_b - 1$, $0 \leq \tau_a \leq N_a - 1$, $0 \leq \tau_e \leq N_e - 1$ and $\tau = \tau_e N_a N_b + \tau_a N_b + \tau_b$. Hence, the periodic cross-correlation function between a pair of three-component composite sequences can be found through analysis of the aperiodic and periodic cross-correlation functions of the three pairs of component sequences. Equivalent results can be obtained for the other correlation functions between three-component composite sequences. Beale [4] commented that the correlation functions for multiple-component composite sequences are an extension of these results but the expressions quickly grow cumbersome.

Note that in all of the equations (2.80) to (2.85), the correlation function between two composite sequences was expressed as a function of the correlations between the component sequences. This simplifies the calculations significantly; however, in all of the previous work which has been reported, no analysis has been performed on the actual correlation behaviour of composite sequences. Thus, no information is available on precise correlation behaviour.

Beale [4] considered the balance property of composite sequences. Defining the balance B_c of sequence C to be the number of 0's in C minus the number of 1's in C , it is seen that the balance of the composite sequence C is

$$B_c = B_a \cdot B_b \quad (2.88)$$

the product of the balances of the component sequences A and B . Consequently, if the component sequences are balanced or nearly balanced, the composite sequence will be

balanced as well. This was not so with the combination sequences. In the case of m-sequence components, the composite codes will achieve a balance of $B_c = 1$. Thus, the composite sequences with m-sequence components are as balanced as the m-sequences which have $B_a = B_b = -1$.

Stark and Sarwate [3] also considered several CDMA performance measures and evaluated them for the case of composite sequences. It was found that the composite sequences have larger worst-case error probabilities than CDMA systems employing m-sequences. However, it was pointed out that for many CDMA systems, a more meaningful measure is the average bit error probability [64]. For this measure, it was found that the composite sequences perform as well as m-sequences, doing slightly better for low signal-to-noise ratios and slightly worse for higher signal-to-noise ratios.

Finally, Beale [4] proposed a rapid acquisition receiver architecture for composite sequences. Again, consider a composite sequence C of period $N_c = N_a N_b$ constructed as in (2.78). Let the chip rate of sequence B be $f_c = 1/T_c$ so that the chip rate of C is also f_c and the chip rate of component sequence A is f_c/N_b . A receiver which permits rapid acquisition of the composite sequence C is illustrated in Fig. 2.11.

The principle of operation is that the fast sequence B is first acquired, followed by acquisition of the slow sequence A , where it is assumed that the signal-to-noise ratio is sufficient to permit detection of the correlation peak of the component B . For the first correlator, integration of duration $N_b T_c$ is performed corresponding to a full period of sequence B . Since the maximum number of correlations required to achieve acquisition is N_b , then the maximum acquisition time for component sequence B is $N_b^2 T_c$ and the average acquisition time is $N_b^2 T_c / 2$.

Following this, the second correlation is performed with an integration time of $N_a N_b T_c$, corresponding to one period of sequence A (as well as the composite sequence C). Since the maximum number of correlations required to acquire sequence A will be N_a , then the maximum acquisition time for component sequence A is $N_a N_b^2 T_c$. Since

Figure 2.11: Baseband rapid acquisition receiver for a composite sequence [4]

the two correlations are performed serially, the maximum total acquisition time is

$$\begin{aligned} T_{\text{acq}}(\text{max}) &= N_b^2 T_c + N_b N_a^2 T_c \\ &= N_a N_b T_c \left(\frac{N_b}{N_a} + N_a \right) \end{aligned} \quad (2.89)$$

This is an improvement of approximately a factor of N_b over the corresponding maximum acquisition time for a conventional sequence which would be $T_{\text{acq}}(\text{conv}) = N_a^2 N_b^2 T_c$.

Beale then derived the optimal periods for the component sequences to be

$$N_b = \sqrt[3]{\frac{N_c^2}{2}} \quad (2.90)$$

and

$$N_a = \sqrt[3]{2N_c} \quad (2.91)$$

which gives the optimal achievable acquisition time of

$$T_{\text{acq}}(\text{opt}) \approx 1.89 N_c^{4/3} T_c \quad (2.92)$$

Thus, it is theoretically possible to achieve a reduction in acquisition time by a factor of

$$\frac{T_{\text{acq}}(\text{opt})}{T_{\text{acq}}(\text{conv})} = 0.529 N_c^{2/3} \quad (2.93)$$

which is plotted in Fig. 2.12. Beale acknowledges that the reduced acquisition time comes at the expense of requiring a higher signal-to-noise ratio to reliably acquire component sequence B . However, it should be noted that all of the preceding analysis on acquisition performance makes several simplifying assumptions. This leads to misconceptions on the true acquisition performance of composite sequences. A more detailed analysis of the acquisition performance of composite sequences will be given in Section 3.6 taking into account several of the more relevant factors, in particular, SNR, probability of detection P_d and the probability of false alarm P_{fa} .

Finally, it is noted in Beale [4] that an alternate architecture utilizing matched filters could be employed for rapid acquisition of composite sequences. In this scheme, cascaded matched filters are employed which are matched to each component sequence. This architecture permits longer sequences to be used than with conventional sequence

Figure 2.12: Theoretically achievable acquisition time reduction for the composite sequences

schemes which employ a single matched filter. This is possible because concatenating the sequences eases the time-bandwidth product requirement on the matched filters while resulting in a longer total sequence period.

From the preceding discussions, it appears that composite sequences provide excellent rapid acquisition capability. The actual correlation performance of the composite sequences, while it has not previously been investigated, will be discussed in Chapter 3. The linear span and enumeration of the composite sequences will be examined in Chapter 3 and the power spectrum will be derived. As well, an analytic description of the composite sequences will be presented and the security and acquisition time performance will be described.

Chapter 3

Composite Sequences

3.1 Introduction

As described in Section 2.5.2, the composite sequences have the potential to satisfy most, if not all, of the requirements for spread spectrum communications: small out-of-phase autocorrelation magnitude, small cross-correlation magnitude for certain phases, balance, large enumeration, high linear span and a featureless power spectrum.

It has been seen in the previous chapter that there are several sequence designs which meet some, but not all, of these criteria. However, none of the existing sequence designs provide a capability for rapid acquisition while adequately meeting the above requirements. It will be seen in this chapter that the composite sequences satisfy all of the criteria. For the purposes of this thesis, the research will be restricted to two-component composite sequences which employ binary m-sequences as their components.

In this chapter, the results of the analysis of composite sequences will be presented. A novel algorithm for the generation of primitive polynomials will be presented in Section 3.2 which has been found to be significantly faster than any of the existing algorithms. In Section 3.3, a new description of composite sequences is presented which defines the sequences in terms of polynomial structure. Section 3.4 describes relevant properties of composite sequences including the enumeration, linear span and the correlation functions. As well, the power spectrum of composite sequences will be derived and sample spectra will be presented. In Section 3.5, the vulnerability of composite sequences to exploitation by unintended listeners will be derived. Several techniques which could be employed by interceptors to exploit these spreading sequences will also be described. Section 3.6 will describe the acquisition time performance of composite sequences and detail an algorithm which could be employed to acquire these sequences. The results of this chapter will be summarized in Section 3.7.

3.2 Primitive Polynomial Generation

In order to generate composite sequences which consist of modulo-two summations of m-sequences, it is necessary to generate all of the possible primitive polynomials which are candidates for use as components of composite sequences. Peterson and Weldon [117] provide tables of primitive polynomials over GF(2) which unfortunately only contain a small subset of all primitive polynomials. For purposes of generalization, there are no similar comprehensive tables over fields larger than GF(2). In Gulliver [118], tables of primitive polynomials with linearly independent roots over GF(3), GF(4) and several higher fields are given. Broader tables comprehensively detailing the primitive polynomials are not available.

Thus, to complete the tables it is necessary to apply some appropriate algorithm which generates the polynomials in reasonable time. Reviews of existing techniques are provided in Gulliver [118] and Ritter [119]. Typical techniques involve exhaustive searches based on the factorizations of polynomials over finite fields [52, 120] and are very slow. The more efficient primitive-finding techniques are based on probabilistic selection of a trial polynomial $f(x)$ and the evaluation of $(x^{2^i}) \bmod f(x)$ such as in Watson [121] or Ben-Or [122]. These techniques are generally only useful for lower degree polynomials and to produce a small number of primitive polynomials.

In Luneberg [123], an algorithm for finding all irreducible polynomials over GF(q) was presented which exploits the relationship between the cyclotomic cosets and the irreducible polynomials. Unfortunately, the technique is computationally expensive due to the complex modulo- q polynomial operations required. In Gulliver [118], a sieve technique was employed to exhaustively search all possible polynomials for primitives. The technique was claimed to be reasonably fast since most reducible polynomials were eliminated with a simple test, but again, the test relied heavily on modulo- q polynomial operations with each primitive polynomial $f(x)$ of degree m requiring the formation of the test polynomials $x^{2^m-1} \bmod f(x)$, $x^{p_i} \bmod f(x)$, and $\prod (x^{2^{p_i}-1} - 1) \bmod f(x)$, for all p_i proper divisors of $2^m - 1$, and where p_i is a proper divisor of m . As with all

existing methods, Gulliver's technique is computationally expensive.

3.2.1 The Algorithm

A novel approach to the problem is presented here. The algorithm outlined below requires one reference primitive polynomial $f(x)$ of degree m and will efficiently produce all of the $N_P(m)$ primitive polynomials over $GF(2)$ of degree m .

The steps of the algorithm are as follows:

1. Initialize the program by generating and storing the $2^m - 1$ bits of the m-sequence $\{b_n\}$ corresponding to the reference primitive polynomial $f_a(x)$ of degree m .
2. Generate all of the proper decimations which will produce m-sequences. This involves finding all odd integers r_i , $1 \leq r_i \leq 2^{m-1} - 1$, which are relatively prime to $2^m - 1$ and which are cyclotomic coset leaders over $GF(2^m)$. In other words, find all integers r_i , such that for $0 \leq j \leq m - 1$, $r_i = \min \{r_i \cdot 2^j \bmod (2^m - 1)\}$.
3. Reject all of the larger members of each reciprocal decimation pair using (2.51) as the test.
4. For all proper decimations r_i , do
 - a. Generate the $2m$ bits $\{b_{nr_i}\}$ by decimating $\{b_n\}$ by r_i for $2m$ bits.
 - b. Solve for $f_{a^{r_i}}(x)$ by feeding the $2m$ bits of $\{b_{nr_i}\}$ through the Berlekamp-Massey algorithm described previously in Section 2.3.2.
5. Generate all reciprocal polynomials $f_{a^{r_i}}^*(x)$ for each polynomial $f_{a^{r_i}}(x)$ using (2.20).

The algorithm was implemented in C on a SUN 4/370 computer and the tables of primitive polynomials were compiled. This algorithm has been compared to an optimized implementation of the algorithm of Luneberg [123] and was found to be significantly faster, even though Luneberg's algorithm only finds irreducible polynomials and not primitive polynomials. Note that to find all irreducible polynomials using the above algorithm, one need only use all decimations, not just all proper decimations. As described in Section 2.3.2, the basic rationale for the improved performance is that this new algorithm takes a number of operations proportional to N^2 , where N is the

sequence period. Existing techniques take a number of operations proportional to N^3 , so the new algorithm is a significant improvement for large values of N . The determination of all primitive polynomials up to and including degree 26 (about 4 million polynomials) was completed in approximately 80 minutes. It was found that Step 3 of the algorithm improved the computational speed of the algorithm by approximately 40%.

An example will now be given using the polynomial generating algorithm to determine the primitive polynomials of degree 5 over $GF(2)$.

1. The reference polynomial using the tables of Simon et al [14] is $f_\alpha(x) = x^5 + x^2 + 1$. The m-sequence corresponding to the primitive polynomial $f_\alpha(x)$ is the 31-bit sequence $\{b_n\} = \{1001011001111100011011101010000\}$.
2. The proper decimations are 1, 3, 5, 7, 11 and 15. Comparing these with the set of cyclotomic cosets given in (2.26), it is seen that these proper decimations are the cyclotomic coset leaders over $GF(2^5)$.
3. To determine the reciprocal decimations, find all decimation pairs, q, r , such that the reciprocal decimation of q is the cyclotomic coset leader r of the proper coset containing $15q \bmod 31$. Thus, 1 and 15, 3 and 7, and 5 and 11 are the reciprocal decimation pairs. Reject the decimations 15, 7 and 11.
4. Decimate $2m = 10$ bits of $\{b_n\}$ by 1, 3 and 5, giving the m-sequence elements

$$\begin{aligned}\{b_n\} &= \{1001011001\} \\ \{b_{3n}\} &= \{1111101110\} \\ \{b_{5n}\} &= \{1110100010\}\end{aligned}\tag{3.1}$$

Of course, $f_\alpha(x) = x^5 + x^2 + 1$ is already known. It is only necessary to determine $f_{\alpha^3}(x)$ corresponding to $\{b_{3n}\}$ and $f_{\alpha^5}(x)$ corresponding to $\{b_{5n}\}$. Table 3.1 shows the results of the BMA on $\{b_{3n}\}$ and Table 3.2 shows the results of the BMA on $\{b_{5n}\}$. Taking the reciprocal of the results of Tables 3.1 and 3.2, it is found that $f_{\alpha^3}(x) = x^5 + x^4 + x^3 + x^2 + 1$ and $f_{\alpha^5}(x) = x^5 + x^4 + x^2 + x + 1$.

5. The reciprocal polynomials for each polynomial $f_{\alpha^r}(x)$ are found giving $f_\alpha^*(x) = x^5 + x^3 + 1$, $f_{\alpha^3}^* = x^5 + x^3 + x^2 + x + 1$ and $f_{\alpha^5}^* = x^5 + x^4 + x^2 + x + 1$. Thus, the

Table 3.1 Application of the BMA to $\{b_{3n}\}$

n	M	$f(x)$	j	$B(x)$	b_n	d
0	0	1	1	1	1	1
1	1	$1 + x$	1	1	1	0
2	1	$1 + x$	2	1	1	0
3	1	$1 + x$	3	1	1	0
4	1	$1 + x$	4	1	1	0
5	1	$1 + x$	5	1	0	1
6	5	$1 + x + x^5$	1	$1 + x$	1	0
7	5	$1 + x + x^5$	2	$1 + x$	1	1
8	5	$1 + x + x^2 + x^3 + x^5$	3	$1 + x + x^5$	1	0
9	5	$1 + x + x^2 + x^3 + x^5$	4	$1 + x + x^5$	0	0
10	5	$1 + x + x^2 + x^3 + x^5$	5	$1 + x + x^5$	-	-

Table 3.2 Application of the BMA to $\{b_{5n}\}$

n	M	$f(x)$	j	$B(x)$	b_n	d
0	0	1	1	1	1	1
1	1	$1 + x$	1	1	1	0
2	1	$1 + x$	2	1	1	0
3	1	$1 + x$	3	1	0	1
4	3	$1 + x + x^3$	1	$1 + x$	1	0
5	3	$1 + x + x^3$	2	$1 + x$	0	0
6	3	$1 + x + x^3$	3	$1 + x$	0	0
7	3	$1 + x + x^3$	4	$1 + x$	0	1
8	5	$1 + x + x^3 + x^4 + x^5$	1	$1 + x + x^3$	1	0
9	5	$1 + x + x^3 + x^4 + x^5$	2	$1 + x + x^3$	0	0
10	5	$1 + x + x^3 + x^4 + x^5$	3	$1 + x + x^3$	-	-

list of primitive polynomials of linear span 5 is

$$\begin{aligned}
 &x^5 + x^2 + 1 \\
 &x^5 + x^3 + 1 \\
 &x^5 + x^4 + x^3 + x^2 + 1 \\
 &x^5 + x^3 + x^2 + x + 1 \\
 &x^5 + x^4 + x^3 + x + 1 \\
 &x^5 + x^4 + x^2 + x + 1
 \end{aligned} \tag{3.2}$$

From (2.24) and (2.27), the number of primitive polynomials is $N_P(5) = \phi(31)/5 = 30/5 = 6$, which is the number of polynomials found above.

3.3 Generation of Composite Sequences

The algorithm of the previous section was utilized to generate all of the m-sequences required as components for composite sequences. The technique of combining the sequences of (2.78) is a representation of the combination process in the sequence domain. In order to better understand the behaviour of the composite sequences, it is necessary to derive an improved representation of the combination process in the polynomial domain.

Let $A = \{a_n\}$ and $B = \{b_n\}$ be periodic m-sequences over GF(2) of periods N_a and N_b , respectively. The m-sequences A and B are described by the characteristic polynomials $a(x)$ and $b(x)$ of degree m_a and m_b , respectively. Hence, A and B are m-sequences of period $N_a = 2^{m_a} - 1$ and $N_b = 2^{m_b} - 1$, respectively. As before, the composite sequence $C = \{c_n\}$ is constructed from the two component sequences A and B using (2.78). Thus, generating the composite sequences requires two LFSR circuits which are added modulo-two. In this configuration, the chip rate of the sequence generator for A is N_b times slower than the chip rate of the sequence generator of B , such that the duration of one element of the slow sequence A is equal to the duration of one period of the fast sequence B .

The composite sequence generator is illustrated in Fig. 3.1. The generator of the fast sequence B operates at chip rate f_c and satisfies the linear recursion

$$b_n = d_1 b_{n-1} + d_2 b_{n-2} + \dots + d_{m_b-1} b_{n-m_b-1} + b_{n-m_b} \quad (3.3)$$

where $n = 0, 1, 2, \dots$ and the d_i are elements of $GF(2)$ for $0 \leq i \leq m_b - 1$. Note that the periodic sequence $\{b_n\}$ satisfies the recursions

$$\{b_n\} = \{b_{n+m_b}\} \quad (3.4)$$

for all integers i and n . The corresponding characteristic polynomial for the fast component sequence is the primitive polynomial

$$b(x) = x^{m_b} + d_1 x^{m_b-1} + d_2 x^{m_b-2} + \dots + d_{m_b-1} x + 1 \quad (3.5)$$

Similarly, the generator of the slow sequence A operates at chip rate f_c/N_b and satisfies the linear recursion

$$a_n = e_1 a_{n-1} + e_2 a_{n-2} + \dots + e_{m_a-1} a_{n-m_a-1} + a_{n-m_a} \quad (3.6)$$

where $n = 0, 1, 2, \dots$ and the e_i are elements of $GF(2)$ for $0 \leq i \leq m_a - 1$. As above, the periodic sequence $\{a_n\}$ satisfies the recursions

$$\{a_n\} = \{a_{n+m_a}\} \quad (3.7)$$

for all integers i and n . The corresponding characteristic polynomial for the slow component sequence is the primitive polynomial

$$a(x) = x^{m_a} + e_1 x^{m_a-1} + e_2 x^{m_a-2} + \dots + e_{m_a-1} x + 1 \quad (3.8)$$

In the existing literature, the formation of the composite sequence is described in terms of the combination of the sequence elements of the component sequences A and B . The polynomial description of sequences formed by the product of several component sequences [100, 124] has not been carried out for the case of combining sequences

Figure 3.1: Composite sequence generator circuit

of different chip rates. In this thesis, a novel approach to the problem permits the combination of multiple sequences with different chip rates to be described in terms of polynomial structure. Now, since the component sequence generators are not operating at the same chip rate, the characteristic polynomial $c(x)$ is not simply the product of $a(x)$ and $b(x)$. The reference chip rate is defined as f_c , the chip rate of the fast sequence generator. The chip rate of A is N_b times slower than the chip rate of B , which means that the sequence elements of A must be stretched by a factor of N_b in order to describe the two component sequences with respect to the same chip rate. This is equivalent to replacing each shift register in the sequence generator for A by N_b registers, then running the sequence generator for A with a chip rate of f_c . In terms of polynomials, this means that the characteristic polynomial $a(x)$ is replaced by $a(x^{N_b})$ in order to describe the slow sequence A in terms of the fast chip rate f_c . Now that the two component sequences share the same reference chip rate, the composite sequence can be described as a product sequence with characteristic polynomial

$$c(x) = a(x^{N_b})b(x) \quad (3.9)$$

the product of the modified characteristic polynomials of the component sequences. This product polynomial is of degree $(m_b + m_a N_b)$ or $m_b + m_a(2^{m_b} - 1)$, which is significantly higher than the corresponding value for combination sequences or Gold sequences of $(m_a + m_b)$. The minimal polynomial corresponding to C can be determined using the techniques given in Lidl and Niederreiter [51, p.210]. In Section 3.4.2, it will be proven that $c(x)$ as given in (3.9) is the minimal polynomial which describes the composite sequence C . This polynomial corresponds to the N_b cyclically distinct composite sequences formed by the combination of the component sequences A and B . The unique generating polynomial for each of these N_b cyclically distinct composite sequences can be found using standard techniques such as given in Lidl and Niederreiter [51, p. 207].

3.4 Properties of Composite Sequences

3.4.1 Enumeration

The composite sequences can be enumerated using a simple counting argument. It is well known that the number of primitive polynomials of degree m over $\text{GF}(2)$ is $N_P(m)$ as given by (2.27). There are $N_P(m_a)$ and $N_P(m_b)$ primitive polynomials over $\text{GF}(2)$ of degree m_a and m_b , respectively, corresponding to the number of candidate slow and fast component sequences.

For the $N_P(m_a)$ slow component sequences, there are $N_a = 2^{m_a} - 1$ distinct cyclic shifts of each sequence, corresponding to the period of the slow sequence. Similarly, for each of the $N_P(m_b)$ fast component sequences, there are $N_b = 2^{m_b} - 1$ distinct cyclic shifts of each sequence, corresponding to the period of the fast sequence. Thus, for each of the $N_P(m_a) N_P(m_b)$ pairs of component sequences, there are $N_a N_b$ possible combinations of distinct shifts between the component sequences. While each of the N_b different shifts of the fast sequence B produces a cyclically distinct composite sequence, the different shifts of the slow sequence A do not produce unique composite sequences. In fact, the composite sequence which results from the sum of fast sequence B and a shift by l of slow sequence A is a shift by lN_a of the composite sequence C , or

$$a_{i+l} + b_j = c_{k+lN_a} \quad (3.10)$$

where i, j and k are defined as in (2.78), with the sequence index $i + l$ evaluated modulo N_a , the sequence index $k + lN_a$ evaluated modulo $(N_a N_b)$ and the addition defined over $\text{GF}(2)$. Hence, there are only N_b cyclically distinct composite sequences resulting from the different shifts of the component sequences, and the number of cyclically distinct composite sequences over $\text{GF}(2)$ which can be constructed for a fixed m_a and m_b is

$$\begin{aligned} N_c(m_a, m_b) &= N_b N_P(m_a) N_P(m_b) \\ &= (2^{m_b} - 1) \frac{\phi(2^{m_a} - 1)}{m_a} \frac{\phi(2^{m_b} - 1)}{m_b} \end{aligned} \quad (3.11)$$

Using the bound $\phi(p) < p$, the number of composite sequences for a fixed m_a and m_b is upper bounded by

$$N_c(m_a, m_b) < \frac{2^{m_a+2m_b}}{m_a m_b} \quad (3.12)$$

The number of composite sequences $N_c(m_a, m_b)$ constructed over GF(2) as a function of m_a and m_b is given in Table 3.3. The number of m-sequences $N_P(m_a)$ of linear span m_a over GF(2) is also given for comparison. Hence, for $m_a = 8$ and $m_b = 7$, there are $N_c(8, 7) = 36576$ cyclically distinct binary composite sequences of period $(2^8 - 1)(2^7 - 1) = 32385$ which can be constructed. In comparison, there are only 1800 m-sequences of similar period 32767. It is clear that the composite sequences are a large class of sequences. This provides an additional level of security against interception and exploitation of the underlying message as will be discussed later in Section 3.5.

3.4.2 Linear Span

As before, the linear span of a sequence $C = \{c_n\}$ is defined as the smallest degree for which C satisfies a linear recursion, or the degree of the minimal polynomial of C . For security, a pseudorandom sequence should have a large linear span in order to decrease the predictability of the sequence [57]. If a sequence has linear span m , then its linear recursion can be determined from any $2m$ successive elements of the sequence, using techniques such as the Berlekamp-Massey algorithm, which was described previously in Section 2.3.2.

The linear span of the composite sequence with characteristic polynomial given by (3.9) is now determined. By proving that $c(x)$ given by (3.9) is the minimal polynomial of C , it will be shown that the composite sequences achieve the maximum achievable linear span of $(m_b + m_a N_b)$. Before presenting the result on linear span, some background theory is required.

Definition 3.1 *The polynomials $f_1(x)$ and $f_2(x)$ are relatively prime if and only if $\gcd(f_1(x), f_2(x)) = 1$, i.e., if $f_1(x)$ and $f_2(x)$ have no polynomial factors in common.*

Theorem 3.2 (Lidl and Niederreiter [51,p.218]) *For each $i = 1, 2, \dots, k$, let C_i be a linear recurring sequence in GF(q) with minimal polynomial $f_i(x)$. If the polynomials*

Table 3.3 Enumeration of composite sequences over GF(2)

m_a	$N_P(m_a)$	Value of m_b					
		2	3	4	5	6	7
2	1	3	14	30	186	378	2286
3	2	6	28	60	372	756	4572
4	2	6	28	60	372	756	4572
5	6	18	84	180	1116	2268	13716
6	6	18	84	180	1116	2268	13716
7	18	54	252	540	3348	6804	41148
8	16	48	224	480	2976	6048	36576
9	48	144	672	1440	8928	18144	109728
10	60	180	840	1800	11160	22680	137160
11	176	528	2464	5280	32736	66528	402336
12	144	432	2016	4320	26784	54432	329184
13	630	1890	8820	18900	117180	238140	1440180
14	756	2268	10584	22680	140616	285768	1728216
15	1800	5400	25200	54000	334800	680400	4114800
16	2048	6144	28672	61440	380928	774144	4681728
17	7710	23130	107940	231300	1434060	2914380	17625060
18	7776	23328	108864	233280	1446336	2939328	17775936
19	27594	82782	386316	827820	5132484	10430532	63079884
20	24000	72000	336000	720000	4464000	9072000	54864000

$f_1(x), f_2(x), \dots, f_k(x)$ are pairwise relatively prime, then the minimal polynomial of the sum $C_1 + C_2 + \dots + C_k$ is equal to the product $f_1(x)f_2(x) \cdots f_k(x)$.

From Theorem 3.2, it is clear that $c(x)$ is the minimal polynomial of C if $a(x^{N_b})$ and $b(x)$ are relatively prime. Since $b(x)$ is a primitive polynomial (and hence, irreducible), it is only required to show that $b(x)$ is not a factor of $a(x^{N_b})$. It is sufficient to prove that the orders of the factors of $a(x^{N_b})$ are not equal to the order of $b(x)$, N_b . The order of the factors of $a(x^{N_b})$ are determined using the following result from Butler [125].

Theorem 3.3 (Butler [125]) *Let $f(x)$ be an irreducible polynomial over $\text{GF}(q)$ of degree m and order n . If t is a positive integer such that $\gcd(t, q) = 1$, let $t = t_1 t_2$, where the factors are defined by the properties $\gcd(t_1, n) = 1$, and each prime factor of t_2 is a divisor of n . Then, each irreducible factor of $f(x^t)$ has order of the form dnt_2 , where d is a divisor of t_1 .*

The following theorem is also required before proceeding to prove the main result of this section.

Theorem 3.4 (Lidl and Niederreiter [51,p.75]) *If $f(x)$ is an irreducible polynomial over $\text{GF}(q)$ of degree m , then $\text{ord}(f(x))$ divides $q^m - 1$.*

The main result of this section is now stated and proven.

Theorem 3.5 *Let $f(x)$ be an irreducible polynomial over $\text{GF}(q)$ of degree m and order n , and let $t = q^r - 1$ be a positive integer. Then, no irreducible factor of $f(x^t)$ is of degree r .*

Proof: Using the definitions in Theorem 3.3, let $t = t_1 t_2$, where the factors are defined by the properties, $\gcd(n, t_1) = 1$, and each prime factor of t_2 is a divisor of n . By Theorem 3.3, each irreducible factor $f_i(x)$ of $f(x^t)$ has order of the form dnt_2 , where d is a divisor of t_1 .

Using Theorem 3.4, if, for all i , $\text{ord}(f_i(x))$ does not divide t , then $f_i(x)$ is not an irreducible polynomial over $\text{GF}(q)$ of degree r . Now, if $d = t_1$, then $dnt_2 = nt$, which clearly does not divide t . For the case $d \neq t_1$, it will be assumed there exists some irreducible factor $f_i(x)$ such that $\text{ord}(f_i(x))$ divides t . So, $dnt_2 \mid t$, or $dn \mid t_1$. But, by

definition $\gcd(n, t_1) = 1$, so $d \mid t_1$, a contradiction. Thus, no irreducible factor of $f(x^t)$ has order a factor of $t = q^r - 1$. The desired result follows from Theorem 3.4. $\circ$

Hence, $a(x^{N_b})$ and $b(x)$ are relatively prime so that $c(x)$, as given in (3.9) is the minimal polynomial of the composite sequence C . This implies $c(x)$ achieves the maximum linear span for all combinations of components which are m-sequences and the linear span of these composite sequences is

$$\begin{aligned} L &= m_b + m_a N_b \\ &= m_b + m_a(q^{m_b} - 1) \end{aligned} \quad (3.13)$$

the degree of the minimal polynomial $c(x)$. Note that for the special case $m_a = m_b$, the linear span is $L = m_b q^{m_b}$. Necessary and sufficient conditions for the irreducibility of $a(x^{N_b})$ are obtained using a theorem stated by Cohen [126].

Theorem 3.6 (Cohen [126]) *Let $f(x)$ be an irreducible polynomial over $\text{GF}(q)$ of degree m and order n , and let $t \geq 2$ be an integer. Then, $f(x^t)$ is irreducible in $\text{GF}(q)$ if and only if the prime factors of t divide $q^m - 1$, $\gcd(t, (q^m - 1)/n) = 1$ and $\gcd(t, q^m + 1) \not\equiv 0 \pmod{4}$.*

As an example, for m-sequence components over $\text{GF}(2)$, $a(x^{N_b})$ is irreducible whenever m_b divides m_a . The maximum linear span can be determined trivially in this case. The linear span of composite sequences over $\text{GF}(2)$ is given in Table 3.4. Hence, for $m_a = 8$ and $m_b = 7$, the linear span of the composite sequences of period $(2^8 - 1)(2^7 - 1) = 32385$ is 1023. The m-sequences of similar period 32767 achieve a linear span of only 15. Clearly, the composite sequences achieve a large linear span which provides increased security against exploitation of the signal.

3.4.3 Correlation Functions

In this subsection, the correlation properties of composite sequences will be presented. As described earlier, it is desirable to derive the exact correlation performance of composite sequences for the case of components which are binary m-sequences. The periodic autocorrelation function of composite sequences will be derived in Section 3.4.3.1. As described in Section 2.3.4, the aperiodic autocorrelation function is important

Table 3.4 Linear span of composite sequences over GF(2)

m_a	Value of m_b						
	2	3	4	5	6	7	8
2	8	17	34	67	132	261	518
3	11	24	49	98	195	388	773
4	14	31	64	129	258	515	1028
5	17	38	79	160	321	642	1283
6	20	45	94	191	384	769	1538
7	23	52	109	222	447	896	1793
8	26	59	124	253	510	1023	2048
9	29	66	139	284	573	1150	2303
10	32	73	154	315	636	1277	2558
11	35	80	169	346	699	1404	2813
12	38	87	184	377	762	1531	3068
13	41	94	199	408	825	1658	3323
14	44	101	214	439	888	1785	3578
15	47	108	229	470	951	1912	3833
16	50	115	244	501	1014	2039	4088
17	53	122	259	532	1077	2166	4343
18	56	129	274	563	1140	2293	4598
19	59	136	289	594	1203	2420	4853
20	62	143	304	625	1266	2547	5108

when data transitions occur during the correlation process in an acquisition circuit. As will be described later in Section 3.6, the process of acquisition requires autocorrelating the received composite sequence with the fast component sequence, using an integration time of N_b times T_c , the fast sequence chip duration. This acquisition process involves correlating the fast sequence with inversions due to the slow sequence, which is analogous to autocorrelating a conventional spreading sequence with data transitions. Thus, it is necessary to examine the aperiodic autocorrelation function for the fast component sequences; these results will be presented in Section 3.4.3.2.

3.4.3.1 Periodic Autocorrelation Function

The autocorrelation function of composite sequences will be derived for the case of components which are binary m-sequences. The autocorrelation functions of the component sequences are

$$\theta_A(\tau_a) = \begin{cases} N_a & \tau_a = 0 \bmod N_a \\ -1 & \tau_a \neq 0 \bmod N_a \end{cases} \quad (3.14)$$

and

$$\theta_B(\tau_b) = \begin{cases} N_b & \tau_b = 0 \bmod N_b \\ -1 & \tau_b \neq 0 \bmod N_b \end{cases} \quad (3.15)$$

Then, the autocorrelation function $\theta_C(\tau)$ of the composite sequence C can be broken up into several interesting cases. For the case of $\tau = \tau_a N_b$, the following relationship is used [4]

$$\theta_C(\tau) = \theta_B(0) \theta_A(\tau_a) \quad (3.16)$$

for $\tau = \tau_a N_b$, $\tau_a \in \{0, 1, 2, \dots, N_a - 1\}$. Using this relationship, the following is obtained

$$\theta_C(\tau) = N_b \theta_A(\tau_a) = \begin{cases} N_a N_b & \tau_a = 0, \tau = \tau_a N_b \\ -N_b & \tau_a \neq 0, \tau = \tau_a N_b \end{cases} \quad (3.17)$$

For the case $\tau \neq \tau_a N_b$, the problem can be broken down even further. If $\tau_a = 0$, then using (2.81), it can be shown that

$$\begin{aligned} \theta_C(\tau) &= \theta_A(0) C_B(\tau_b) + \theta_A(1) C_B(\tau_b - N_b) \\ &= N_a C_B(\tau_b) - C_B(\tau_b - N_b) \end{aligned} \quad (3.18)$$

If $\tau_a = N_a - 1$, then

$$\begin{aligned}\theta_C(\tau) &= \theta_A(N_a - 1) C_B(\tau_b) + \theta_A(0) C_B(\tau_b - N_b) \\ &= N_a C_B(\tau_b - N_b) - C_B(\tau_b)\end{aligned}\quad (3.19)$$

Finally, for the other cases where $\tau \neq \tau_a N_b$, $\tau_a \neq 0$ and $\tau_a = N_a - 1$, it is found that

$$\begin{aligned}\theta_C(\tau) &= -C_B(\tau_b) - C_B(\tau_b - N_b) \\ &= -\theta_B(\tau_b) \\ &= +1\end{aligned}\quad (3.20)$$

Summarizing, the autocorrelation function of the composite sequence is given by the expression

$$\theta_C(\tau) = \begin{cases} N_a N_b & \tau = 0 \\ -N_b & \tau_a \neq 0, \tau_b = 0 \\ N_a C_B(\tau_b) - C_B(\tau_b - N_b) & \tau_a = 0, \tau_b \neq 0 \\ N_a C_B(\tau_b - N_b) - C_B(\tau_b) & \tau_a = N_a - 1, \tau_b \neq 0 \\ 1 & \text{otherwise} \end{cases} \quad (3.21)$$

where $\tau = \tau_a N_b + \tau_b$. Now, the product of $\theta_A(\tau_a)$ and $\theta_B(\tau_b)$ is shown in Fig. 3.2, for the case $N_a = 7$ and $N_b = 3$. The autocorrelation function (3.21) can be simplified whereby several cases can be summarized as the product of the autocorrelation functions of the component sequences, giving

$$\theta_C(\tau) = \begin{cases} N_a C_B(\tau_b) - C_B(\tau_b - N_b) & \tau_a = 0, \tau_b \neq 0 \\ N_a C_B(\tau_b - N_b) - C_B(\tau_b) & \tau_a = N_a - 1, \tau_b \neq 0 \\ \theta_A(\tau_a) \theta_B(\tau_b) & \text{otherwise} \end{cases} \quad (3.22)$$

The above expression can be simplified further using the well-known relationship [62]

$$\theta_B(\tau_b) = C_B(\tau_b) + C_B(\tau_b - N_b) \quad (3.23)$$

so that for the case of interest which employs binary m-sequence component sequences,

$$C_B(\tau_b) + C_B(\tau_b - N_b) = \begin{cases} N_b & \tau_b = 0 \text{ mod } N_b \\ -1 & \tau_b \neq 0 \text{ mod } N_b \end{cases} \quad (3.24)$$

Then, the expression for $\theta_C(\tau)$ when $\tau_a = 0$ and $\tau_b \neq 0$ can be manipulated as

$$\begin{aligned}N_a C_B(\tau_b) - C_B(\tau_b - N_b) &= N_a C_B(\tau_b) - [-1 - C_B(\tau_b)] \\ &= (N_a + 1) C_B(\tau_b) + 1\end{aligned}\quad (3.25)$$

Figure 3.2: The product of the autocorrelation functions of the component sequences

Figure 3.2: The product of the autocorrelation functions of the component sequences

Similarly, for the case $\tau_a = N_a - 1$, $\tau_b \neq 0$, the expression can be rewritten

$$\begin{aligned} N_a C_B(\tau_b - N_b) - C_B(\tau_b) &= N_a C_B(\tau_b - N_b) - [-1 - C_B(\tau_b - N_b)] \\ &= (N_a + 1)C_B(\tau_b - N_b) + 1 \end{aligned} \quad (3.26)$$

Hence, the simplified expression for the periodic autocorrelation function of the composite sequence C is

$$\theta_C(\tau) = \begin{cases} (N_a + 1)C_B(\tau_b) + 1 & \tau_a = 0, \tau_b \neq 0 \\ (N_a + 1)C_B(\tau_b - N_b) + 1 & \tau_a = N_a - 1, \tau_b \neq 0 \\ \theta_A(\tau_a) \theta_B(\tau_b) & \text{otherwise} \end{cases} \quad (3.27)$$

An example of the autocorrelation function of a composite sequence is given using the component sequences $A = \{1110100\}$ and $B = \{101\}$, which have periods $N_a = 7$ and $N_b = 3$, respectively. The resulting composite sequence is then $C = \{0100100101010101101\}$, of period $N_c = N_a N_b = 21$. Solving for the autocorrelation function of the composite sequence, we obtain the result illustrated in Fig. 3.3.

If the result of (3.27) is used to determine the autocorrelation function, then the correlation functions of the component sequences must first be determined. These are: the periodic autocorrelation function of A ,

$$\theta_A(\tau_a) = \begin{cases} 7 & \tau_a = 0 \pmod{7} \\ -1 & \tau_a \neq 0 \pmod{7} \end{cases} \quad (3.28)$$

the periodic autocorrelation function of B ,

$$\theta_B(\tau_b) = \begin{cases} 3 & \tau_b = 0 \pmod{3} \\ -1 & \tau_b \neq 0 \pmod{3} \end{cases} \quad (3.29)$$

and the aperiodic autocorrelation function of B ,

$$C_B(\tau_b) = \begin{cases} 3 & \tau_b = 0 \\ -2 & \tau_b = \pm 1 \\ 1 & \tau_b = \pm 2 \\ 0 & \text{otherwise} \end{cases} \quad (3.30)$$

Substituting the results of (3.28)-(3.30) into (3.27), one obtains the result

$$\theta_C(\tau) = \begin{cases} 21 & \tau = 0 \\ -15 & \tau = 1, 20 \\ 9 & \tau = 2, 19 \\ -3 & \tau = 3i, i \text{ an integer} \\ 1 & \text{otherwise} \end{cases} \quad (3.31)$$

Figure 3.3: Example periodic autocorrelation function of a composite sequence

which is as illustrated in Fig. 3.3.

It should be noted that $\theta_C(\tau)$ is symmetric about $\tau = N_a N_b / 2$, simplifying the required calculations. Note that since N_a , $\theta_A(\tau_a)$ and $\theta_B(\tau_b)$ are independent of the specific component sequences employed, then $\theta_C(\tau)$ is only a function of the aperiodic autocorrelation function of the fast sequence B , which is dependent upon the component sequence employed and the initial phase of B . Also, $\theta_C(\tau)$ is entirely independent of the specific slow component sequence A utilized, only being dependent on the period of A .

3.4.3.2 Aperiodic Autocorrelation of M-Sequences

It is important that the out-of-phase periodic autocorrelation magnitudes be low for good acquisition performance as described in Section 2.3.4. In order to characterize the sidelobe-to-peak ratio (SPR) for the periodic autocorrelation function of the composite sequences, it can be seen from (3.27) that it is necessary to describe the performance of the aperiodic autocorrelation function of the fast component sequence B . For the composite sequences, the sidelobe-to-peak ratio is given as

$$\begin{aligned} \text{SPR} &= \frac{|\max \{\theta_c(\tau) : \tau \neq 0\}|}{N_a N_b} \\ &= \frac{|1 + (N_a + 1) \max \{C_B(\tau_b) : \tau_b \neq 0\}|}{N_a N_b} \\ &\simeq \frac{\max \{|C_B(\tau_b)| : \tau_b \neq 0\}}{N_b} \end{aligned} \quad (3.32)$$

In other words, the SPR for the composite sequences can be characterized using the SPR for the aperiodic autocorrelation function of the m-sequence B . The problem is then to determine

$$C_{\max} = \max \{|C_B(\tau_b)| : \tau_b \neq 0\} \quad (3.33)$$

which is the maximum out-of-phase aperiodic autocorrelation magnitude for a given m-sequence for all relative phase shifts τ_b and all correlation start points.

Several authors have attempted to upper bound the aperiodic autocorrelation performance of m-sequences including Sarwate and Pursley [62], Sarwate [127], Sarwate [128], McEliece [129] and Pursley and Sarwate [130]. Pursley and Roefs [67], Roefs [70] and Sarwate [131] have also determined the optimal phases of m-sequences which

give minimal values of the out-of-phase aperiodic autocorrelation magnitude. McEliece [129] upper bounded C_{max} as

$$C_{max} \leq (1 + \ln N) \sqrt{1 + N} \quad (3.34)$$

where $N = 2^m - 1$ is the period of the m-sequence. The best upper bound is due to Sarwate [128]

$$C_{max} \leq 1 + \left(\frac{2}{\pi}\right) \ln \left(\frac{4N}{\pi}\right) \sqrt{1 + N} \quad (3.35)$$

In this thesis, C_{max} was determined empirically for m-sequences of linear span up to and including 12 and the data was fitted to an exponential using nonlinear regression techniques [132]. Thus, the empirical bound is

$$C_{max} \leq 1.10(1.46)^m. \quad (3.36)$$

The bounds defined by (3.34), (3.35) and (3.36) are shown in Table 3.5. Clearly, the bounds of (3.34) and (3.35) are of little value in giving an approximation of the maximum correlation magnitude. It is acknowledged that the exponential bound of (3.36) is not an absolute upper bound; however, it provides a good approximation of the maximum out-of-phase aperiodic autocorrelation magnitude which is expected for a given sequence period.

The maximum out-of-phase aperiodic autocorrelation magnitude can be reduced through several means. In Roefs [70] and Pursley and Roefs [67], the aperiodic autocorrelation function of m-sequences was evaluated to obtain the phase of the sequence which gives the lowest value of the maximum out-of-phase magnitude. This point is illustrated with an example. The m-sequence $\{b_n\} = \{1011100\}$ of period 7 which is generated by the characteristic polynomial $f(x) = x^3 + x + 1$ has an aperiodic autocorrelation function given by

$$C(\tau) = \begin{cases} 7 & \tau = 0 \\ 0 & \tau = \pm 1 \\ -1 & \tau = \pm 2 \\ -2 & \tau = \pm 3 \\ 1 & \tau = \pm 4 \\ 0 & \tau = \pm 5 \\ -1 & \tau = \pm 6 \\ 0 & \text{otherwise} \end{cases} \quad (3.37)$$

Table 3.5 Bounds on the maximum aperiodic autocorrelation magnitude for m-sequences

span m	period N	McEliece's bound	Sarwate's bound	Exponential Bound	Actual Value
4	15	15	9	5	5
5	31	25	14	7	7
6	63	41	23	11	11
7	127	66	38	16	16
8	255	105	60	23	22
9	511	164	94	33	34
10	1023	254	147	48	46
11	2047	390	228	70	68
12	4095	596	350	103	107
13	8191	906	534	-	-
14	16383	1370	811	-	-
15	32767	2063	1227	-	-

Now, the other six shifts of $\{b_n\}$, i.e., $\{b_{n+1}\}$, $\{b_{n+2}\}$, ..., $\{b_{n+6}\}$ have aperiodic autocorrelation functions given as

$$C(\tau) = \begin{cases} \begin{matrix} \{b_{n+1}\} & \{b_{n+2}\} & \{b_{n+3}\} & \{b_{n+4}\} & \{b_{n+5}\} & \{b_{n+6}\} \end{matrix} \\ \begin{matrix} 7 & 7 & 7 & 7 & 7 & 7 \\ 0 & 0 & -2 & -2 & 0 & -2 \\ -3 & -1 & -1 & -1 & 1 & 1 \\ -2 & 0 & 0 & 2 & 0 & -2 \\ 1 & -1 & -1 & -3 & -1 & 1 \\ 2 & 0 & 0 & 0 & -2 & -2 \\ -1 & -1 & 1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{matrix} & \begin{matrix} \tau = 0 \\ \tau \neq \pm 1 \\ \tau \neq \pm 2 \\ \tau \neq \pm 3 \\ \tau \neq \pm 4 \\ \tau \neq \pm 5 \\ \tau \neq \pm 6 \\ \text{otherwise} \end{matrix} \end{cases} \quad (3.38)$$

Thus, there are seven distinct aperiodic autocorrelation functions corresponding to the seven shifts of the m-sequence $\{b_n\}$, with each aperiodic autocorrelation function having unique values at each corresponding shift. Using the criterion of Roefs [70], one would select $\{b_{n+2}\} = \{1110010\}$ as the optimal shift of the m-sequence in terms of minimizing the maximum out-of-phase aperiodic autocorrelation magnitude.

This approach is useful for DS-SS systems where the spreading sequence period is matched to the data bit duration and could also be used with composite sequences to select which phase of the fast component sequence should be matched to the slow sequence chip duration. Alternatively, the system designer could decide to only employ those m-sequences which have an aperiodic autocorrelation which is always below some threshold level. The statistics of C_{max} for the m-sequences of linear span up to 12 are given in Tables 3.6 to 3.15. It is seen from the tables that a reduction of approximately 20% can be achieved by careful selection of the subset of m-sequences.

Table 3.6 C_{max} Statistics for the m-sequences of linear span 3

C_{max}	Number of Sequences
3	2

Table 3.7 C_{max} Statistics for the m-sequences of linear span 4

C_{max}	Number of Sequences
5	2

Table 3.8 C_{max} Statistics for the m-sequences of linear span 5

C_{max}	Number of Sequences
6	2
7	4

Table 3.9 C_{max} Statistics for the m-sequences of linear span 6

C_{max}	Number of Sequences
10	4
11	2

Table 3.10 C_{maz} Statistics for the m-sequences of linear span 7

C_{maz}	Number of Sequences
13	6
14	4
15	6
16	2

Table 3.11 C_{maz} Statistics for the m-sequences of linear span 8

C_{maz}	Number of Sequences
19	4
20	4
21	6
22	2

Table 3.12 C_{maz} Statistics for the m-sequences of linear span 9

C_{maz}	Number of Sequences
25	2
26	4
27	10
28	6
29	4
30	8
31	6
32	6
33	0
34	2

Table 3.13 C_{max} Statistics for the m-sequences of linear span 10

C_{max}	Number of Sequences
36	2
37	4
38	6
39	8
40	16
41	2
42	4
43	8
44	2
45	4
46	4

Table 3.14 C_{max} Statistics for the m-sequences of linear span 11

C_{max}	Number of Sequences
51	4
52	2
53	10
54	12
55	18
56	18
57	14
58	10
59	22
60	16
61	10
62	14
63	6
64	10
65	6
66	0
67	2
68	2

Table 3.15 C_{max} Statistics for the m-sequences of linear span 12

C_{max}	Number of Sequences
72	2
75	6
76	4
77	4
78	8
79	8
80	6
81	10
82	8
83	12
84	6
85	8
86	14
87	10
88	6
89	10
90	2
91	2
93	6
95	2
96	2
97	2
99	4
107	2

3.4.4 Power Spectrum

Before examining the security of composite sequences, an analysis will be carried out of the power spectrum of composite spreading sequences. An important characteristic of any DS-SS signal which is to be employed in a low probability of detection (LPD) application is that the power spectrum be as featureless as possible [133]. Thus, it is desirable that the power spectrum of composite sequences approach the characteristic envelope of the power spectrum of m-sequences, but without the chip line features which normally characterize these signals. This ensures that unintended listeners can not exploit chip line or other spectral features in order to determine useful information about the DS-SS signal. For example, it was demonstrated in Skaug [134] that the Gold sequences have power spectra which may have large spectral peaks, in particular for the case of unbalanced Gold sequences. Low probability of exploitation (LPE) and other security considerations will be discussed in more detail in the next section.

The expression for the power spectrum $S_c(f)$ of composite sequences will now be derived. The fast component sequence B is an m-sequence with a chip rate f_c and period N_b and the slow component sequence A is an m-sequence with chip rate f_c/N_a and period N_a . The power spectrum of sequence A is denoted $S_a(f)$ and the power spectrum of sequence B is denoted $S_b(f)$; the expressions for $S_a(f)$ and $S_b(f)$ are derived in Appendix A to be:

$$S_a(f) = \frac{1}{N_a^2} \delta(f) + \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \frac{N_a + 1}{N_a^2} \text{sinc}^2\left(\frac{i}{N_a}\right) \delta\left(f - \frac{if_c}{N_a N_b}\right) \quad (3.39)$$

and

$$S_b(f) = \frac{1}{N_b^2} \delta(f) + \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \frac{N_b + 1}{N_b^2} \text{sinc}^2\left(\frac{j}{N_b}\right) \delta\left(f - \frac{j}{N_b} f_c\right) \quad (3.40)$$

It is clear that the combination process of composite sequences is analogous to that of combining data with a spreading sequence in a conventional DS-SS system. Following the discussion as in Ziemer and Peterson [8], the power spectrum of composite sequences

is given as

$$\begin{aligned} S_c(f) &= \int_{-\infty}^{\infty} S_a(f') S_b(f - f') df' \\ &= S_a(f) * S_b(f) \end{aligned} \quad (3.41)$$

the convolution of $S_a(f)$ with $S_b(f)$. Hence, as with the conventional case, each chip spectral line due to fast sequence B will be modulated by the power spectrum of the slow sequence A .

Deriving $S_c(f)$ as given in Appendix B, it can be shown that the power spectrum of the composite sequence C is

$$\begin{aligned} S_c(f) &= \frac{1}{N_a^2 N_b^2} \delta(f) + \frac{N_b + 1}{N_a^2 N_b^2} \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \text{sinc}^2\left(\frac{j}{N_b}\right) \delta\left(f - \frac{j}{N_b} f_c\right) \\ &+ \frac{N_a + 1}{\pi^2 N_b^2} \sum_{\substack{i=-\infty \\ i \neq k N_a}}^{\infty} \delta\left(f - \frac{i f_c}{N_a N_b}\right) \text{sinc}^2\left(\frac{\pi i}{N_a}\right) \times \\ &\quad \left[\frac{1}{i^2} + (N_b + 1) \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \frac{\text{sinc}^2(j/N_b)}{(i - j N_a)^2} \right] \end{aligned} \quad (3.42)$$

Hence, the first term describes the spectral line at dc of amplitude $1/N_a^2 N_b^2$ and the second term describes the spectral lines at integral multiples of f_c/N_b , the chip rate of the slow sequence. The third term describes all of the spectral lines at the integral multiples of $f_c/N_a N_b$, except at dc and at multiples of f_c/N_b , where the third term contributes zero. Hence, it is seen that the power spectrum of the composite sequences is only a function of the component sequence periods and the chip rate, and is not a function of the relative phase shifts or specific component sequences employed.

Simulations and experiments were carried out to test the theoretical expression given by (3.42) with selected empirical results given here. Fig. 3.4 shows the power spectrum of the fast component sequence of chip rate $f_c = 700$ kHz and characteristic polynomial $b(x) = x^3 + x + 1$. This spectrum has the characteristic shape of the power spectrum of an m-sequence as given by (3.39), with discrete chip spectral lines spaced every

$f_c/N_b = 100$ kHz. With data modulation present, the power spectrum becomes a continuous envelope. For the composite sequences, each of these spectral lines is modulated by the power spectrum of the slow component sequence as shown in Fig. 3.5. The slow sequence has a chip rate of 100 kHz and is generated with the characteristic polynomial $a(x) = x^3 + x + 1$.

The two sequences are combined to form the composite sequence which has the power spectrum illustrated in Fig. 3.6. It can be seen that Fig. 3.6 is the convolution of the spectra of Figs. 3.4 and 3.5, as expected by the theory. There are 49 discrete chip lines in each sidelobe and in each half of the main lobe, and the original chip lines from Fig. 3.4 are all suppressed significantly as expected. This experimental result was verified through calculation of (3.42).

The power spectrum of another composite sequence is shown in Fig. 3.7; the sequence employed has a fast component sequence which has a chip rate of 5.1 MHz and characteristic polynomial $b(x) = x^8 + x^4 + x^3 + x^2 + 1$. The slow component sequence has a chip rate of 20 kHz and a characteristic polynomial $a(x) = b(x)$. It is seen that the power spectrum has the same continuous envelope as that of an m-sequence.

The power spectrum of the composite sequences has been derived and determined empirically. It is seen that the spectra have good properties in terms of minimal exploitable spectral features. The power spectrum is symmetric and balanced and for sufficiently long composite sequences, the power spectrum of composite sequences approaches the continuous envelope of the power spectrum of a data-modulated m-sequence.

3.5 Security of Composite Sequences

In designing a DS-SS communications system, it is important to realize that unintended listeners will attempt to exploit the signal for their own purposes, thus compromising the privacy and security of the communications. A spreading sequence which requires significant effort to determine provides one more level of protection against signal exploitation. In this section, the composite sequences will be analyzed in terms of their

Figure 3.4: Power spectrum of the fast component
sequence $b(x) = x^3 + x + 1$; $f_c = 700$ kHz

Figure 3.5: Power spectrum of the slow component
 sequence $a(x) = x^3 + x + 1$; $f_c/N_b = 100$ kHz

Figure 3.6: Power spectrum of a composite sequence

$$a(x) = b(x) = x^3 + x + 1; f_c = 700 \text{ kHz}$$

Figure 3.7: Power spectrum of a composite sequence

$$a(x) = b(x) = x^8 + x^4 + x^3 + x^2 + 1; f_c = 5.1 \text{ MHz}$$

applicability as LPE system components; as well, the techniques to determine the specific sequence employed will be described along with the computational effort required.

There are two general classes of brute force attacks used when attempting to determine unknown spreading sequences; the approach chosen depends upon the SNR of the received signal. For high SNR's where the chip stream can be demodulated directly, the decoding techniques such as the Berlekamp-Massey algorithm are used to determine the characteristic polynomial from observation of $2m$ consecutive chips; the decoding techniques are described in Section 2.3.2. For low SNR's, the brute force correlation attacks are utilized; assuming the sequence period is known, then all $N_P(m)$ sequences of the known period are successively correlated with the received sequence for all N relative phase shifts. Hence, for an unknown m-sequence of period N and chip rate $f_c = 1/T_c$, the brute force correlation attack would require a time of $N_P(m) N^2 T_c$ to determine the sequence.

The composite sequences were examined for each class of attacks and are compared to the baseline results for the m-sequences. The linear span of composite sequences was determined in Section 3.4.2 to be

$$L = m_b + m_a(2^{m_b} - 1) \quad (3.43)$$

Thus, decoding techniques will require observation of $2L$ consecutive chips of the composite sequence in order to determine the characteristic polynomial. Comparing this to an m-sequence of similar period $N = 2^{m_a+m_b} - 1$, it is seen that the composite sequences will take longer to determine by a factor of

$$\frac{m_a(2^{m_b} - 1) + m_b}{m_a + m_b} \quad (3.44)$$

This function is plotted in Fig. 3.8 as a function of m_a and m_b . It is seen that increasing the period of the fast component sequence B exponentially increases the decoding improvement factor while using longer slow component sequences A has little impact on the security of composite sequences against decoding attacks.

As described in Section 3.4.1, there are $N_c(m_a, m_b)$ composite sequences over GF(2) for a fixed m_a and m_b . The brute force correlation attack will require correlating

Figure 3.8: Ratio of decoding times for composite sequences vs m-sequences

$N_c(m_a, m_b)$ sequences at $N_a N_b$ relative phase shifts for $N_a N_b$ chips. Hence, the brute force correlation attack requires a time of

$$N_c(m_a, m_b) N_a^2 N_b^2 T_c = N_a^2 N_b^3 N_P(m_a) N_P(m_b) T_c \quad (3.45)$$

to determine the composite sequence employed. In other words, the ratio of search time for the composite sequences over the search time for m-sequences using brute force correlation is

$$\begin{aligned} & \frac{N_a^2 N_b^3 N_P(m_a) N_P(m_b) T_c}{N_P(m_a + m_b) N_a^2 N_b^2 T_c} \\ &= \frac{(2^{m_b} - 1) N_P(m_a) N_P(m_b)}{N_P(m_a + m_b)} \end{aligned} \quad (3.46)$$

As in Section 3.4.1, $N_P(m)$ can be bounded since

$$\begin{aligned} N_P(m) &= \frac{\phi(2^m - 1)}{m} \\ &< \frac{2^m - 1}{m} \end{aligned} \quad (3.47)$$

Hence, the search time ratio can be upper bounded by

$$\begin{aligned} & \frac{(2^{m_b} - 1) \left(\frac{2^{m_a} - 1}{m_a} \right) \left(\frac{2^{m_b} - 1}{m_b} \right)}{\left(\frac{2^{m_a + m_b} - 1}{m_a + m_b} \right)} \\ &< (2^{m_b} - 1) \left(\frac{m_a + m_b}{m_a m_b} \right) \end{aligned} \quad (3.48)$$

This bound is plotted in Fig. 3.9 as a function of m_a and m_b . As with the decoding techniques, increasing the period of the fast component sequence B exponentially increases the search ratio for brute force correlation. However, increasing the period of the slow component sequence A is seen to degrade the security of composite sequences against a brute force correlation attack.

One potential source of vulnerability for the composite sequences is derived from the method of constructing these sequences, i.e., since the period of the fast sequence B is equal to the duration of one element of the slow sequence A . By adding the composite sequence C to a shift of C by an integral multiple of the period of B , the result is a

Figure 3.9: Ratio of search time for composite sequences vs m-sequences for brute force correlation

shifted version of sequence A . The shift of A can be determined using relationships (2.61) and (2.63). Hence, through this shift-and-add process, the sequence B is cancelled out. Component sequence A can then be attacked, using decoding or correlation.

Upon determination of component sequence A , the known sequence A is added to the received sequence C and sequence B is then determined. The approximate times required to perform the search are

$$2(m_a + m_b) T_c \quad (3.49)$$

for the decoding attack, and

$$[N_a^2 N_P(m_a) + N_b^2 N_P(m_b)] T_c \quad (3.50)$$

for the brute force correlation attack. Hence, the decoding time is the same as for an m -sequence of approximately the same period $N_a N_b$, and the search time for the correlation attack is less for the composite sequences than for the m -sequences. The obvious difficulty for the correlation attack is that the shift-and-add process significantly degrades the SNR of the signal to be correlated.

3.6 Acquisition Time Performance

The acquisition time performance of the composite sequences will now be derived and compared to that of the single dwell, serial search acquisition technique of Section 2.2.1. The acquisition algorithm whose principles of operation were described in Section 2.5.2 has been analyzed previously by Beale [4] ignoring the effects of the SNR of the received signal. The detailed analysis of the corrected acquisition algorithm for the composite sequences will be given here taking into account the effect of SNR, probability of detection P_d and probability of false alarm P_{fa} .

The acquisition time performance for the composite sequences could be analyzed using Markov state diagrams and system flow graphs as demonstrated in Polydoros [27] or Simon et al [14]; however, it has been determined that the process of acquiring the

composite sequences is similar to that of acquisition using the double dwell, serial search acquisition technique described in Section 2.2.2.

The principle of operation of the corrected acquisition scheme is embodied in the block diagram of Fig. 3.10, which differs significantly from that of Fig. 2.11 as described in Beale [4]. The fast sequence B is first acquired using a short integration dwell time τ_{d1} . Upon successful detection of the fast component sequence, the slow component sequence A is then acquired using a longer integration time τ_{d2} . For purposes of analysis, τ_{d1} and τ_{d2} will be chosen to be the optimal values, and will not necessarily be fixed to be integral multiples of the periods of the component sequences A and B , respectively.

The differences should be highlighted between this system and the conventional double dwell acquisition system of Fig. 2.4. In the double dwell acquisition system, the integrations are both carried out on a filtered and squared signal which has a bandwidth equal to the data bandwidth f_d . In the case of the composite sequence acquisition system, the fast sequence acquisition is performed using a bandwidth equal to that of the slow sequence, f_c/N_b , and the slow sequence acquisition is carried out using a bandwidth equal to the data bandwidth, f_d . Assuming a match between the period of the slow sequence A and the data bit duration $T_d = 1/f_d$, then the bandwidth used is $f_d = f_c/N_a N_b$.

The characterization of the time performance of the acquisition scheme for the composite sequences is very similar to the analysis for the double dwell acquisition scheme as carried out in Section 2.2.2. The number of cells to be searched, q , is typically assumed to be $q = 2N$, corresponding to a sequence phase update size of one-half chip over the full period N . For the composite sequences, the size of the search space for the fast sequence acquisition is q_1 , where typically $q_1 = 2N_b$, corresponding to twice the period of the fast sequence. For the slow sequence acquisition, the search space is of size q_2 , with a typical value of $q_2 = 2N_a$, corresponding to twice the period of the slow sequence. Then, as for the double dwell acquisition system, the mean acquisition time is

$$\bar{T}_{acq} = \frac{2 - P_d}{P_d} \{ \tau_{d1} q_1 + P_{fa1} q_2 (\tau_{d2} - \tau_{d1}) (1 + K_2 P_{fa2}) \} \quad (3.51)$$

where the second dwell time is found by solving

$$B_{IF2} \tau_{d2} = f(P_{d2}, P_{fa2}, \text{SNR}) \quad (3.52)$$

Figure 3.10: Baseband acquisition system for composite sequences

and where $f(\cdot)$ represents the solution of (2.8) for $B_{IF}\tau_d$. As was used in Section 2.2.2, $P_{d2} = (1 + P_d)/2$ and $P_{fa2} = P_{fa}$, the false alarm probability of the equivalent single dwell acquisition system. As well, $B_{IF2} = B_{IF}$, the pre-detection bandwidth for the equivalent single dwell acquisition system. Then, substituting we obtain

$$B_{IF}\tau_{d2} = f\left(\frac{1 + P_d}{2}, P_{fa}, \text{SNR}\right) \quad (3.53)$$

The solution of the first dwell time takes a little more effort. The problem is to vary P_{fa1} in solving for τ_{d1} in

$$B_{IF1}\tau_{d1} = f(P_{d1}, P_{fa1}, \text{SNR}_1) \quad (3.54)$$

such that the mean acquisition time given by (3.51) is minimized. Now, from Fig. 3.10, the pre-detection bandwidth for the first acquisition stage is

$$\begin{aligned} B_{IF1} &= \frac{f_c}{N_b} \\ &= N_a B_{IF} \end{aligned} \quad (3.55)$$

where N_a is the period of the slow component sequence. In effect, this is equivalent to stating that the slow sequence acts like data on the fast sequence and that the data bandwidth is the bandwidth of the slow sequence. Note that B_{IF1} cannot be set to B_{IF} or else the fast sequence will never be successfully acquired.

The other major difference between the double dwell acquisition technique and the acquisition system for composite sequences is that the SNR of the two acquisition stages is not the same in the composite sequence acquisition system. Thus,

$$\text{SNR}_1 = \frac{1}{N_a} \text{SNR} \quad (3.56)$$

using the assumption that the period of the slow sequence A is the same as the duration of one data bit. Substituting into (3.54), one obtains

$$N_a B_{IF}\tau_{d1} = f\left(\frac{1 + P_d}{2}, P_{fa1}, \frac{\text{SNR}}{N_a}\right) \quad (3.57)$$

where P_{fa1} is to be varied such that $\bar{T}_{acq}$ is minimized.

So, the mean acquisition time for the composite sequence acquisition system can be compared to that of the single dwell system using the ratio

$$\frac{\bar{T}_{\text{acq}}(\text{single dwell})}{\bar{T}_{\text{acq}}(\text{comp seq})} = \frac{(1 + K P_{fa}) q \tau_d}{\tau_{d1} q_1 + P_{fa1} q_2 (\tau_{d2} - \tau_{d1}) (1 + K_2 P_{fa2})} \quad (3.58)$$

It is assumed that the composite sequence and the single dwell acquisition systems have the same false alarm penalty time, i.e., $K \tau_d = K_2 (\tau_{d2} - \tau_{d1})$; then the improvement factor ratio can be simplified to

$$\frac{\bar{T}_{\text{acq}}(\text{single dwell})}{\bar{T}_{\text{acq}}(\text{comp seq})} = \frac{q \tau_d}{\tau_{d1} q_1 + P_{fa1} q_2 (\tau_{d2} - \tau_{d1})} \quad (3.59)$$

If the ratio is normalized with respect to bandwidth B_{IF} and the search space size q , then one obtains

$$\frac{\bar{T}_{\text{acq}}(\text{single dwell})}{\bar{T}_{\text{acq}}(\text{comp seq})} = \frac{(B_{IF} \tau_d)}{\frac{1}{N_a} (B_{IF} \tau_{d1} N_a) \left(\frac{1}{q_2} - \frac{P_{fa1}}{q_1} \right) + \frac{P_{fa1}}{q_1} (B_{IF} \tau_{d2})} \quad (3.60)$$

where $(B_{IF} \tau_d)$, $(B_{IF} \tau_{d1} N_a)$ and $(B_{IF} \tau_{d2})$ are the solutions of equations (2.16), (3.57) and (3.53), respectively.

The improvement factor of the composite sequence acquisition system over the single dwell, serial search acquisition technique is plotted against P_{fa} with P_d as a parameter, for various combinations of the parameters SNR, N_a and N_b in Figs. 3.11 to 3.15. For all of these plots, the solid line corresponds to $P_d = 0.1$, the dashed line corresponds to $P_d = 0.5$, and the dotted line corresponds to $P_d = 0.9$. Figs. 3.11 and 3.12 show the acquisition time performance improvement factor for composite sequences over the single dwell acquisition technique for $N_a = 15$ and $N_b = 31$ and for SNR's of -10 and 0 dB, respectively. These figures demonstrate that although SNR has significant effect on the acquisition time performance of composite sequences, the improvement factor is essentially unaffected by SNR. However, it is noted that the improvement factor decreases with higher P_{fa} at a faster rate for lower SNR's. For a fixed SNR, the improvement factor increases with decreasing P_d , with increasing values of P_{fa} decreasing the improvement factor.

Figure 3.11: Acquisition performance improvement factor for composite sequences over single dwell acquisition technique; SNR = -10 dB, $N_a = 15$, $N_b = 31$

Figure 3.12: Acquisition performance improvement factor for composite sequences over single dwell acquisition technique; SNR = 0 dB, $N_a = 15$, $N_b = 31$

Fig. 3.13 shows the improvement factor for $\text{SNR}=0$ dB, $N_a = 15$, and $N_b = 127$, corresponding to a long, fast sequence and a short, slow sequence. The same qualitative comments can be made as before although P_d is seen to have a more significant impact on the improvement factor. Figs. 3.14 and 3.15 are more realistic plots of the improvement factor which can be obtained with a long, slow component sequence and a short, fast component sequence. Fig. 3.14 shows the improvement factor vs. P_{fa} for $\text{SNR}=0$ dB, $N_a = 63$ and $N_b = 31$, while Fig. 3.15 has $\text{SNR}=0$ dB, $N_a = 31$ and $N_b = 15$. For a fixed SNR, the improvement factor increases marginally with increasing P_d and for increasing P_{fa} , the probability of detection is seen to have little effect. It is clear that as P_{fa} decreases, τ_{d2} approaches τ_d , and the improvement factor decreases towards approximately $q_2 = 2N_a$, or twice the period of the slow sequence.

In general, the improvement in acquiring the composite sequences is derived, for the most part, from the fact that the search space for the single dwell acquisition system is much larger than the search space for the composite sequence acquisition system. For the single dwell, the search space is of dimension $q = q_1 q_2$, whereas for the composite sequence acquisition technique, the search space dimensions are q_1 for the acquisition of the fast component sequence and q_2 for the acquisition of the slow component sequence.

Figure 3.13: Acquisition performance improvement factor for composite sequences over single dwell acquisition technique; SNR = 0 dB, $N_a = 15$, $N_b = 127$

Figure 3.14: Acquisition performance improvement factor for composite sequences over single dwell acquisition technique; SNR = 0 dB, $N_a = 63$, $N_b = 31$

Figure 3.15: Acquisition performance improvement factor for composite sequences over single dwell acquisition technique; SNR = 0 dB, $N_a = 31$, $N_b = 15$

3.7 Summary and Conclusions

The composite sequences are seen to be a class of spreading sequences which have many desirable features. The process of generating the composite sequences was described in Section 3.3, with the characteristic polynomial determined to be

$$c(x) = a(x^{N_b}) b(x) \quad (3.61)$$

where $a(x)$ is the characteristic polynomial of the slow component sequence and $b(x)$ is the characteristic polynomial of the fast component sequence. These component sequences are found using the novel algorithm of Section 3.2 which permits determination of all primitive polynomials in a significantly reduced time. It was determined in Section 3.4.1 that for a fixed m_a and m_b , there are

$$N_c(m_a, m_b) = N_b N_P(m_a) N_P(m_b) \quad (3.62)$$

unique composite sequences which can be generated. The linear span of composite sequences was derived in Section 3.4.2 to be

$$L = m_b + m_a N_b \quad (3.63)$$

which is significantly larger than the linear span of m-sequences; this was determined using the derived result of Theorem 3.5 of Section 3.4.2.

The periodic autocorrelation function of composite sequences was derived in Section 3.4.3.1 and it was determined that $\theta_C(\tau)$ is a simple function of the aperiodic autocorrelation function of the fast component sequence. The aperiodic autocorrelation function of m-sequences was bounded empirically in Section 3.4.3.2 and the result was applied to the bound on the maximum out-of-phase magnitude of the periodic autocorrelation function of composite sequences.

In Section 3.4.4, an approximate expression for the power spectrum of composite sequences was derived and it was seen that this power spectrum is essentially featureless; for sufficiently long component sequences, the power spectrum of composite sequences approaches the continuous envelope of the power spectrum of m-sequences. It has been

shown that the power spectrum of composite sequences is independent of the specific component sequences employed and is only a function of the component sequence periods and the chip rate. It has also been found that the chip rate lines due to the fast sequence at integral multiples of f_c/N_t have been suppressed, which is analogous to suppressing the chip lines due to the spreading sequence in a conventional DS-SS signal. The power spectrum results were verified empirically and found to match closely the analytic results.

In Section 3.5, the security aspects of composite sequences were described and the effectiveness of exploitation attacks against composite sequences was examined. It was found that the composite sequences increase the computational effort of an unintended listener exponentially compared to the effort required to exploit the m-sequences.

The acquisition time performance of composite sequences was analyzed in detail in Section 3.6. The analysis took into account the significant impact of noise on acquisition performance and it was found that the composite sequences provide a marginal improvement in acquisition performance for low SNR's; for higher SNR's, the composite sequences greatly enhance the speed of acquisition on the order of the improvements offered by a modified version of the double-dwell, serial search acquisition technique.

Hence, to summarize, it has been found that the composite sequences are a large class of spreading sequences for DS-SS communications which achieve:

1. balance;
2. high linear span;
3. reasonable periodic autocorrelation performance;
4. essentially featureless power spectrum;
5. improved LPE performance; and
6. rapid acquisition performance for moderate-to-high SNR's.

In the following chapter, a novel sequence design will be presented which is derived from the composite sequences. It will be seen that these sliding composite sequences offer many of the advantages of the composite sequences but also greatly enhance the acquisition performance for reasonable SNR's. The properties and performances of the

sliding composite sequences will be derived in a similar fashion to the analysis which has been completed in this chapter.

Chapter 4

A New Subclass of Composite Sequences

4.1 Introduction

In Chapter 3, analysis was carried out of the properties and performance of composite sequences; this analysis was carried out in terms of the various parameters relevant to the evaluation of spreading sequences for use in a DS-SS communication system. In this chapter, sliding composite sequences are presented, a subclass of the composite sequences analyzed in Chapter 3. This new class of sequences will be seen to satisfy many of the requirements for DS-SS communications with the specific advantage of permitting very rapid acquisition of the spreading sequences. As with the composite sequences, the research of this thesis has been restricted to two-component sliding composite sequences which employ binary m-sequences as their components.

In this chapter, the sliding composite sequences will be presented and the results of the analysis of these sequences will be described. It will be seen that much of the analysis of the properties of sliding composite sequences is similar to that which was carried out for the composite sequences, due to the inherently similar combination process. The sliding composite sequences will be introduced in Section 4.2 and the polynomial structure will also be examined. Section 4.3 derives and describes relevant properties of sliding composite sequences including the enumeration, linear span and power spectrum. The vulnerability of sliding composite sequences to exploitation will be examined in Section 4.4 and the performance of several exploitation attacks against the sliding composite sequences will be developed. Section 4.5 will detail an algorithm for acquisition of sliding composite sequences and the acquisition time performance of this technique will be described. The results of this chapter will be summarized in Section 4.6.

4.2 Generation of Sliding Composite Sequences

The sliding composite sequences are constructed as follows. Note that this development closely follows the corresponding discussion of the composite sequences in Section 3.3. Let $A = \{a_n\}$ and $B = \{b_n\}$ be periodic m -sequences over $GF(2)$ with periods $N_a = 2^{m_a} - 1$ and $N_b = 2^{m_b} - 1$, respectively. The m -sequences are described by the characteristic polynomials $a(x)$ and $b(x)$ of degrees m_a and m_b , respectively.

A sliding composite sequence $C = \{c_n\}$ is constructed from the two component sequences A and B using the combination process illustrated in Fig. 4.1. In this process, sequence C is seen to be the modulo-two sum of sequences A and B , where the duration of each element of sequence A is equal to one chip less than the period of sequence B . In other words, if the chip rate of the sequence generator for sequence B is f_c , then the chip rate of the sequence generator for sequence A is $N_b - 1$ times slower, or $f_c/(N_b - 1)$. Hence, the start of each new chip of sequence A will "slide" across the complete period of B , and the resulting sequence C will have period $N_a(N_b - 1)$. It is clear that the combination process constrains N_a to be equal to N_b and so, the period of C is $N_a(N_a - 1)$.

The sliding composite sequence generator is the same as the corresponding generator for the composite sequences illustrated in Fig. 3.1, except that the slow sequence generator operates at a chip rate of $f_c/(N_a - 1)$. The characteristic polynomial for the fast component sequence B is the primitive polynomial

$$b(x) = x^{m_b} + d_1 x^{m_b-1} + d_2 x^{m_b-2} + \cdots + d_{m_b-1} x + 1 \quad (4.1)$$

and the characteristic polynomial for the slow component sequence A is the primitive polynomial

$$a(x) = x^{m_a} + e_1 x^{m_a-1} + e_2 x^{m_a-2} + \cdots + e_{m_a-1} x + 1 \quad (4.2)$$

As before, since the component sequence generators are not operating at the same chip rate, the characteristic polynomial $c(x)$ is not simply the product of the polynomials $a(x)$ and $b(x)$. In fact, compensating for the different chip rates, it is clear that the sliding

Figure 4.1: Sliding composite sequence combination process

composite sequence C can be described as a product sequence with the characteristic polynomial

$$c(x) = a(x^{N_a-1}) b(x) \quad (4.3)$$

the product of the modified characteristic polynomials of the component sequences. This product polynomial is of degree $m_a + m_a(N_a - 1)$ or $m_a(2^{m_a} - 1)$. It will be seen in Section 4.3.1 that $c(x)$ as given above in (4.3) is the minimal polynomial of sequence C under most conditions. This polynomial corresponds to the N_a cyclically distinct sliding composite sequences formed by the combination of the component sequences A and B . The unique generating polynomial for each of these N_a cyclically distinct sliding composite sequences can be found using standard techniques as given in Lidl and Niederreiter [51, p. 207].

4.3 Properties of Sliding Composite Sequences

The sliding composite sequences are not a perfectly balanced class of sequences. For example, with the sliding composite sequences illustrated in Fig. 4.1, it is seen that of the 42 chips, 22 are 0's and 20 are 1's, giving an imbalance of $B_c = 22 - 20 = 2$. Although the sliding composite sequences will not be balanced, it can be shown with a simple argument that they are nearly balanced. During the duration of each element of slow sequence A , there are $N_a - 1$ chips of fast sequence B , implying a balance of either -2 or 0 during that element, with associated numbers of occurrences of $(N_a - 1)/2$ and $(N_a + 1)/2$, respectively. Since there are $(N_a + 1)/2$ 1's and $(N_a - 1)/2$ 0's occurring in sequence A , then the mean value of the balance of C is

$$\begin{aligned} \bar{B}_c &= \left(\frac{N_a - 1}{2}\right) \left(\frac{N_a - 1}{2N_a}\right) (-2) + \left(\frac{N_a - 1}{2}\right) \left(\frac{N_a + 1}{2N_a}\right) (+2) \\ &\quad + \left(\frac{N_a + 1}{2}\right) \left(\frac{N_a - 1}{2N_a}\right) (0) + \left(\frac{N_a + 1}{2}\right) \left(\frac{N_a + 1}{2N_a}\right) (0) \\ &= \frac{-(N_a - 1)^2 + (N_a - 1)(N_a + 1)}{2N_a} \\ &= \frac{N_a - 1}{N_a} \end{aligned} \quad (4.4)$$

which approaches 1 for large values of N_a . This is similar to the balance of m-sequences (-1) or the balance of composite sequences (+1). However, the variance of the balance of the sliding composite sequence C is

$$\begin{aligned}
 \sigma_{B_c}^2 &= \left(\frac{N_a - 1}{2} \right) \left(\frac{N_a - 1}{2(N_a - 1)} \right) (-2)^2 + \left(\frac{N_a - 1}{2} \right) \left(\frac{N_a + 1}{2(N_a - 1)} \right) (+2)^2 \\
 &\quad - \left(\frac{N_a}{N_a - 1} \right) E^2[B_c] \\
 &= 2N_a - \left(\frac{N_a}{N_a - 1} \right) \left(\frac{N_a - 1}{N_a} \right)^2 \\
 &= 2N_a - \frac{N_a - 1}{N_a}
 \end{aligned} \tag{4.5}$$

which approaches $2N_a - 1$ for large values of N_a ; the variance of the balance of m-sequences and composite sequences is 0. Hence, in general, the balance of sliding composite sequences will be slightly worse than that of the m-sequences or composite sequences.

4.3.1 Enumeration and Linear Span

As with the composite sequences, the sliding composite sequences can be enumerated using a simple counting argument. There are $N_P(m_a)$ primitive polynomials over GF(2) of degree m_a , corresponding to both the number of possible slow component sequences and the number of fast component sequences. For each of the $N_P(m_a)$ slow component sequences, there are N_a distinct cyclic shifts of the sequence, corresponding to the period of the slow sequence. Similarly for the $N_P(m_a)$ fast component sequences, there are N_a distinct cyclic shifts for each sequence, corresponding to the period of the fast sequence. Thus, for each of the $N_P^2(m_a)$ pairs of component sequences, there are N_a^2 possible combinations of distinct shifts between the component sequences. While each of the N_a different shifts of the fast sequence produces a cyclically distinct sliding composite sequence, the different shifts of the slow component sequence do not produce unique sliding composite sequences. Therefore, the number of cyclically distinct sliding

composite sequences over GF(2) which can be constructed for a fixed m_a is

$$\begin{aligned} N_c(m_a) &= N_a N_P^2(m_a) \\ &= (2^{m_a} - 1) \frac{\phi^2(2^{m_a} - 1)}{m_a^2} \end{aligned} \quad (4.6)$$

Again, using the bound $\phi(p) < p$, the enumeration of sliding composite sequences can be upper bounded by

$$N_c(m_a) < \frac{(2^{m_a} - 1)^3}{m_a^2} \quad (4.7)$$

The enumeration of sliding composite sequences is given in Table 3.3, with $N_c(m_a)$ determined by setting $m_a = m_b$ in the table. Hence, for $m_a = 7$, it is seen that there are 41148 cyclically distinct sliding composite sequences of period $(2^7 - 1)(2^7 - 2) = 16002$ compared to 756 m-sequences of similar period $2^{14} - 1$. Clearly, as with the composite sequences, the sliding composite sequences are a large class of spreading sequences. This provides an additional level of security against exploitation as will be discussed later in Section 4.4.

The linear span of the sliding composite sequences with characteristic polynomial given by (4.3) is now determined. By demonstrating that $c(x)$ as given by (4.3) is the minimal polynomial of C , it will be shown that the sliding composite sequences achieve the maximum achievable linear span of $m_a(2^{m_a} - 1)$. By following the same line of reasoning as in Section 3.4.2, it can be shown that $a(x^{N_a-1})$ and $b(x)$ are relatively prime except for the case when $a(x)$ is the reciprocal of $b(x)$. In this case, $b(x)$ is a factor of $a(x^{N_a-1})$ and $c(x) = a(x^{N_a-1})$ is the minimal polynomial corresponding to the sliding composite sequence C . Hence, $c(x)$ achieves maximum linear span for all combinations of components which are m-sequences of the same period except when $a(x) = b^*(x)$. So, of the $N_c(m_a)$ sequences of period $N_a(N_a - 1)$, there are $N_a N_P(m_a)[N_P(m_a) - 2]$ sliding composite sequences of linear span $L = m_a(2^{m_a} - 1)$ and $2N_a N_P(m_a)$ sliding composite sequences of linear span $L = m_a(2^{m_a} - 2)$. These values for the linear span are very close to the linear span of composite sequences which is $L = m_a 2^{m_a}$ for the case where $m_a = m_b$. Hence, the sliding composite sequences achieve a large linear span which provides increased security against exploitation of the signal.

4.3.2 Power Spectrum

In Section 3.4.4 and Appendix B, the approximate power spectrum of composite sequences was derived. The derivation of the power spectrum of the sliding composite sequences follows the same methodology, except that the slow component sequence A is an m -sequence with chip rate $f_c/(N_a - 1)$ instead of f_c/N_b , as was true for the composite sequences. So, as before, the power spectrum of sequence A is denoted $S_a(f)$ and the power spectrum of sequence B is denoted $S_b(f)$. Then, the power spectra for the component sequences are

$$S_a(f) = \frac{1}{N_a^2} \delta(f) + \left(\frac{N_a + 1}{N_a^2} \right) \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \text{sinc}^2\left(\frac{i}{N_a}\right) \delta\left(f - \frac{if_c}{N_a(N_a - 1)}\right) \quad (4.8)$$

and

$$S_b(f) = \frac{1}{N_b^2} \delta(f) + \left(\frac{N_b + 1}{N_b^2} \right) \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \text{sinc}^2\left(\frac{j}{N_b}\right) \delta\left(f - \frac{jf_c}{N_b}\right) \quad (4.9)$$

As with the composite sequences, the power spectrum of sliding composite sequences can be determined as

$$S_c(f) = S_a(f) * S_b(f) \quad (4.10)$$

the convolution of $S_a(f)$ with $S_b(f)$. Hence, as before, each chip line due to the fast sequence B will be modulated by the power spectrum of the slow sequence A . It is interesting to note that there is a significant difference between the power spectra of sliding composite sequences and composite sequences. For the composite sequences, the convolution was carried out where the component sequences had different periods and chip rates; here, the only difference between $S_a(f)$ and $S_b(f)$ is in the chip rates.

Deriving $S_c(f)$ in the same manner as was carried out in Appendix B for the composite sequences, it can be shown that the power spectrum of the sliding composite

sequence C is

$$\begin{aligned}
 S_c(f) = & \frac{1}{N_a^4} \delta(f) + \frac{N_a + 1}{N_a^4} \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \text{sinc}^2\left(\frac{j}{N_a}\right) \delta\left(f - \frac{j f_c}{N_a}\right) \\
 & + \frac{N_a + 1}{N_a^4} \sum_{i=-\infty}^{\infty} \delta\left(f - \frac{i f_c}{N_a(N_a - 1)}\right) \times \\
 & \left[\text{sinc}^2\left(\frac{i}{N_a}\right) + \frac{(N_a + 1)N_a^2}{\pi^2[j(1 - N_a) + i]^2} \sum_{\substack{j=-\infty \\ j \neq k N_a}}^{\infty} \text{sinc}^2\left(\frac{j}{N_a}\right) \sin^2\left(\frac{\pi(i + j)}{N_a}\right) \right]
 \end{aligned} \tag{4.11}$$

The first term describes the contribution of the two dc terms of amplitude $1/N_a^4$ and the second term represents the contribution due to the dc term of the slow component amplitude weighted by each of the chip lines of the fast component sequence. The third term describes the spectral components due to the dc term of the fast component sequence amplitude weighted by the chip lines of the slow component sequence and also, the rest of the spectral lines at the integral multiples of $f_c/N_a(N_a - 1)$. The difference between this expression and the power spectrum of the composite sequences expressed by (3.42) is that the composite sequences only had power at integral multiples of f_c/N_a due to the second term of (3.42); for the sliding composite sequences, there are many contributions at integral multiples of f_c/N_a due to both the second and third terms of (4.11). Hence, whereas the composite sequences had a power spectrum with suppressed chip lines at dc and at integral multiples of f_c/N_a , it is clear that the sliding composite sequences do not have suppressed chip lines at these locations.

Fig. 4.2 shows the power spectrum of a sliding composite sequence which is the combination of two m-sequences of period 7. The slow component sequence has a chip rate of 100 kHz and has characteristic polynomial $a(x) = x^3 + x + 1$. The fast component sequence has a chip rate of 600 kHz and has characteristic polynomial $b(x) = a(x)$. It can be seen that there are 42 discrete chip lines in each sidelobe and in each half of the main lobe, corresponding to the period of the sliding composite sequence. Also note that as predicted by (4.11), the carrier and the fast sequence chip lines are not suppressed

Figure 4.2: Power spectrum of a sliding composite sequence $a(x) = b(x) = x^3 + x + 1$; $f_c = 600$ kHz

as strongly as they were for the composite sequences. This is due to the fact that the width of the lobes of the power spectrum of the slow sequence do not correspond to the chip line spacing of the power spectrum of the fast sequence, as they did for the composite sequences.

The power spectrum of another sliding composite sequence is shown in Fig. 4.3; the fast component sequence has a chip rate of 5.08 MHz and a characteristic polynomial of $b(x) = x^8 + x^4 + x^3 + x^2 + 1$ and the slow component sequence has a chip rate of 20 kHz and a characteristic polynomial $a(x) = b(x)$. It is seen that the power spectrum approaches the continuous envelope of the power spectrum of m-sequences.

The power spectrum of the sliding composite sequences has been derived analytically and determined empirically. It is seen that as with the composite sequences, the spectrum has good properties in terms of minimal exploitable spectral features. The power spectrum is symmetric and the slight sequence imbalance does not impact the power spectrum in any way which would result in exploitable spectral peaks.

4.4 Security of Sliding Composite Sequences

In Section 3.5, the security of composite sequences was described in terms of the effort required to exploit the signal using either a brute force decoding or correlation attack. The sliding composite sequences will be analyzed in the same manner by determining the computational effort required to exploit these spreading sequences.

Since the sliding composite sequences have a linear span of $L = m_a(2^{m_a} - 1)$, the decoding attack will require observation of $2L = 2m_a(2^{m_a} - 1)$ consecutive chips in order to determine the characteristic polynomial $c(x)$. Comparing this to an m-sequence of similar period $N = 2^{2m_a} - 1$, it is seen that the sliding composite sequences will take longer to decode by a factor of

$$\frac{m_a(2^{m_a} - 1)}{2m_a} \approx 2^{m_a-1} \quad (4.12)$$

Hence, the computational effort to decode the sliding composite sequences doubles with each unit increase in m_a . This is the same as with the composite sequences for the case where $m_a = m_b$.

Figure 4.3: Power spectrum of a sliding composite sequence

$$a(x) = b(x) = x^8 + x^4 + x^3 + x^2 + 1; f_c = 5.08 \text{ MHz}$$

As described in Section 4.3.1, there are $N_c(m_a)$ sliding composite sequences over GF(2). So, the brute force correlation attack will require correlating $N_c(m_a)$ sequences at $N_a(N_a - 1)$ relative phase shifts for $N_a(N_a - 1)$ chips. Thus, the brute force correlation attack requires a time of

$$N_c(m_a) N_a^2 (N_a - 1)^2 T_c = N_P^2(m_a) N_a^3 (N_a - 1)^2 T_c \quad (4.13)$$

seconds to determine the sliding composite sequence employed. Hence, the brute force correlation search time for the sliding composite sequences is approximately the same as for the composite sequences, demonstrated by substituting $m_a = m_b$ into (3.46).

As with the composite sequences, one potential source of vulnerability for the sliding composite sequences is derived from the method of constructing these sequences. By adding the sliding composite sequence C to a shift of itself by an integral multiple of the period of the fast component sequence B , the result is a shifted version of sequence A with $1/N_a$ of the slow chip in error. This effectively cancels out sequence B , and sequence A can be attacked independently. Once component sequence A is determined, then by adding A to C , the fast component sequence B can be attacked. The approximate search time for this attack is the same as for the composite sequences, although the slow component sequence A has a portion of its chips in error. Thus, the sliding composite sequences afford the same level of security as the composite sequences, and are also a good candidate for LPE applications.

4.5 Acquisition of Sliding Composite Sequences

It has been seen in the previous sections of this chapter that the sliding composite sequences have essentially the same characteristics and performances as the composite sequences of Chapter 3. The rationale for sliding composite sequences is to improve the acquisition time performance of a DS-SS communication system. An algorithm which could be used to acquire these sequences will be described and the acquisition time performance of sliding composite sequences will be discussed.

A technique for acquiring sliding composite sequences can be developed which will use the inherent characteristics of the sequence class to enhance the acquisition time performance. One possible implementation of the acquisition system for sliding composite sequences is shown in Fig. 4.4 with the received signal assumed to be at baseband. The fast sequence B is first acquired using the conventional single dwell acquisition technique. The correlation is performed with an integration time of $N_a T_c$, the duration of one period of sequence B . The maximum number of correlations to be performed before acquisition occurs is clearly N_a , implying a maximum correlation time of $N_a^2 T_c$ seconds. The average acquisition time for the fast component sequence is then $N_a^2 T_c / 2$ seconds. Taking into account the effects of SNR, it is clear that the acquisition time for the fast component sequence is the same as the performance of the single dwell acquisition system of Section 2.2.1.

Upon successful acquisition of sequence B and assuming the slow sequence A is bit synchronized, then the offset in chips between the start of sequence B and the slow chip transitions is calculated and the slow sequence generator is then jumped into the correct state such that the slow sequence is immediately acquired. One approach to performing this calculation is through the use of look-up tables which is essentially instantaneous. Hence, the average total acquisition time for the sliding composite sequences is

$$\bar{T}_{acq}(scs) = \frac{N_a^2 T_c}{2} \quad (4.14)$$

In essence, the acquisition time of sliding composite sequences is proportional to N_a^2 , i.e.,

$$\bar{T}_{acq}(scs) \propto N_a^2 \quad (4.15)$$

whereas for the composite sequences,

$$\bar{T}_{acq}(comp\ seq) \propto N_a^3 \quad (4.16)$$

and for conventional sequences,

$$\bar{T}_{acq}(conv) \propto N_a^4 \quad (4.17)$$

Figure 4.4: Acquisition system for sliding composite sequences

It is clear that the sliding composite sequences offer a significant reduction in acquisition time compared to other techniques.

The state determination block shown in Fig. 4.4 will now be described. The combination process used to generate sliding composite sequences is illustrated in Fig. 4.1; observing this process, it is seen that the start location of the fast component sequence B "slides" across the slow sequence at a rate of one chip per slow chip. So, a mapping can be set up assigning each of these offset positions to a slow chip. In Fig. 4.1, the component sequences employed are $\{a_n\} = \{b_n\} = \{0011101\}$. So, if we designate $a_0 = 0, a_1 = 0, \dots, a_6 = 1$ and designate the elements of $\{b_n\}$ in a similar fashion, then we can assign the pairs

$$\begin{aligned} &(a_0, b_0) \\ &(a_1, b_6) \\ &(a_2, b_5) \\ &(a_3, b_4) \\ &(a_4, b_3) \\ &(a_5, b_2) \\ &(a_6, b_1) \end{aligned} \tag{4.18}$$

such that fast chip b_j corresponds to the beginning of slow chip a_i .

To acquire the slow sequence, the fast chip b_j corresponding to the beginning of a slow chip is determined. With the above mapping, the slow chip can be calculated to be

$$a_{(N_s-j) \bmod N_s} \tag{4.19}$$

So, knowing that the state of the sequence generator for B is the pseudopolynomial $s_B(\alpha)$, it can be determined that $s_B(\alpha)$ corresponds to state j using

$$\alpha^j = s_B(\alpha) \bmod b(\alpha) \tag{4.20}$$

where $b(x)$ is the characteristic polynomial of the sequence generator for B with primitive root α . Then, the state $s_A(\beta)$ of the sequence generator for A can be determined by

$$s_A(\beta) = \beta^{(N_s-j) \bmod N_s} \bmod a(\beta) \tag{4.21}$$

where $a(x)$ is the characteristic polynomial of the sequence generator for A with primitive root β . The calculation of this state is a trivial finite field operation; detailed descriptions of the circuitry required to perform this calculation can be found in Lin and Costello [53].

The sliding composite sequence of Fig. 4.1 will now be used to illustrate the acquisition process where $\{a_n\} = \{b_n\} = \{0011101\}$ and the characteristic polynomials are $a(x) = b(x) = x^3 + x^2 + 1$. The sequence generator and the shift register states are seen in Fig. 2.8 and Table 2.2, respectively. Assume that the fast sequence has been acquired. The state of the sequence generator for B is seen to be 111, which corresponds to the state pseudopolynomial

$$s_B(\alpha) = 1 + \alpha + \alpha^2 \quad (4.22)$$

Now, solving

$$\begin{aligned} \alpha^j &= s_B(\alpha) \bmod b(\alpha) \\ &= (1 + \alpha + \alpha^2) \bmod (1 + \alpha^2 + \alpha^3) \end{aligned} \quad (4.23)$$

for j , it is seen that $j = 4$. So, this is the fourth chip of the fast sequence. It is then known that the slow sequence generator is producing chip number

$$\begin{aligned} (N_a - j) \bmod N_a &= (7 - 4) \bmod 7 \\ &= 3 \end{aligned} \quad (4.24)$$

which corresponds to the state pseudopolynomial

$$\begin{aligned} s_A(\beta) &= \beta^3 \bmod (1 + \beta^2 + \beta^3) \\ &= 1 + \beta^2 \end{aligned} \quad (4.25)$$

Thus, to acquire the slow sequence, the slow sequence generator should be loaded with state 101, corresponding to state 3 of the generator.

It is seen that the sliding composite sequences are useful in applications requiring rapid acquisition of the spreading sequence. Whereas conventional spreading sequences require acquisition times on the order of the sequence period to the fourth power and the composite sequences are cubic, it is seen that the sliding composite sequences achieve acquisition in a time which is proportional to the square of the component sequence length.

4.6 Summary and Conclusions

In this chapter, a novel class of spreading sequences for DS-SS communications has been presented and investigated. It has been seen that the analysis of the properties of composite sequences performed in Chapter 3 is directly applicable to the case of the sliding composite sequences. The generation of the sliding composite sequences was described in Section 4.2 in terms of the sequence combination process and the characteristic polynomial which results. The sliding composite sequences are seen to be approximately as balanced as the m-sequences with enumeration and linear span on the same order as the composite sequences.

The power spectrum of the sliding composite sequences was derived in Section 4.3.2 and gives approximately the same results as for the composite sequences. For sufficiently long component sequences, the power spectrum of sliding composite sequences approaches the continuous envelope of the power spectrum of the m-sequences. The security of the sliding composite sequences was discussed in Section 4.4 in terms of the effort required by an unintended listener to exploit the sequences. It is seen that the sliding composite sequences take as much effort to exploit as equivalent composite sequences, which is significantly more than for the m-sequences.

The acquisition of sliding composite sequences was described in Section 4.5 and a novel acquisition algorithm was designed which utilizes the inherent structure of the sliding composite sequences. It has been shown that the acquisition of sliding composite sequences can be carried out in a time which is an order of magnitude faster than the composite sequences, a substantial improvement over existing techniques.

Hence, to summarize, the sliding composite sequences are a large class of spreading sequences which achieve:

1. balance;
2. high linear span;
3. essentially featureless power spectrum;
4. improved LPE performance; and

5. inherent very rapid acquisition performance.

The sliding composite sequences exhibit many of the features desirable for use as spreading sequences for DS-SS communications.

Chapter 5

Conclusions and Recommendations

5.1 Summary

This research proposed and analyzed a novel class of spreading sequences for DS-SS communications which permits rapid acquisition. A literature survey of the many available classes of binary spreading sequences for DS-BPSK communications was carried out for the m-sequences, Gold and Kasami sequences, Bent sequences, prime sequences, prime-interleaved sequences, m-like sequences, GMW sequences and the No sequences. The relevant properties of these sequences were described or determined including the enumeration, linear span, correlation functions and rapid acquisition capability. It was shown that for any of these classes of sequences, there is generally at least one performance deficiency, in particular rapid acquisition capability. The rapid acquisition sequences were described including the combination sequences and the existing work on the composite sequences. The combination sequences were found to have good properties in terms of correlation performance and rapid acquisition capability, but were deemed inadequate with respect to balance, enumeration, linear span and CDMA capability.

The composite sequences were analyzed in detail in Chapter 3. A novel algorithm was proposed which rapidly determines all primitive polynomials through exploitation of decimation and the Berlekamp-Massey algorithm. The polynomial characterization and generation of composite sequences was described, and the linear span and enumeration derived. The autocorrelation function of composite sequences was derived and the out-of-phase autocorrelation magnitude was bounded. An improved bound on the maximum magnitude of the out-of-phase aperiodic autocorrelation of m-sequences was determined empirically. The power spectrum of composite sequences was derived and it was shown that the spectrum has minimal exploitable features. The composite sequences were analyzed in terms of their security and were shown to be significantly more secure than

the m-sequences. The acquisition time performance of composite sequences in noise was derived and it was shown that the composite sequences can give significantly improved performance over single dwell, serial search acquisition techniques.

Hence, it was determined in this research that the composite sequences are a large class of spreading sequences for DS-SS communications which achieve:

1. balance;
2. high linear span;
3. reasonable periodic autocorrelation performance;
4. essentially featureless power spectrum;
5. improved LPE performance; and
6. rapid acquisition performance for moderate-to-high SNR's.

In Chapter 4, a novel class of spreading sequences was proposed and analyzed; the properties of these sliding composite sequences were derived in the same manner as for the composite sequences. The polynomial characterization and generation was described and the balance, enumeration and linear span were derived. The power spectrum was derived and observed empirically and the security considerations were discussed. Finally, a novel algorithm for performing acquisition with the sliding composite sequences was presented and the acquisition time performance was discussed.

In summary, it was shown in this thesis that the sliding composite sequences are a large class of spreading sequences which achieve:

1. balance;
2. high linear span;
3. essentially featureless power spectrum;
4. improved LPE performance; and
5. inherent very rapid acquisition performance.

Both the composite sequences and the sliding composite sequences exhibit many of the features desirable for use as spreading sequences for DS-SS communications with the sliding composite sequences having significantly improved rapid acquisition capability.

5.2 Future Work

This investigation into rapid acquisition spreading sequences for DS-SS communications forms the basis for a large number of areas which could be explored. The sequences examined were constructed by combining two binary maximal-length component sequences. The composite sequences and sliding composite sequences could be constructed using multiple component sequences which are not necessarily binary and not necessarily m-sequences. The combination process employed for the sliding composite sequences involved setting the duration of the slow sequence elements to be equal to one chip less than the period of the fast component sequence. Future work could examine the effect on the various properties of selecting different chip rate ratios between the fast and slow component sequences. The combination process employed also directs future investigations into employing composite sequences or sliding composite sequences with DS-QPSK modulation, whereby the component sequences are generated in quadrature. Also, it is clear that these spreading sequences are analogous to data modulation on a conventional spreading sequence; it is possible that the research presented here could be used to further investigate DS-SS communication signals with data modulation.

The acquisition performance of composite sequences was examined with several simplifying assumptions. The secondary effects which impact acquisition performance could be examined including the effect of sequence timing misalignments, the probability of hand-over from acquisition to tracking mode and signal dynamics such as doppler and its derivative. As well, the acquisition performance of composite sequences in non-Gaussian noise environments could be investigated. The periodic autocorrelation function of composite sequences was examined in detail. Further studies would be required into the aperiodic autocorrelation function of composite and sliding composite sequences, and the cross-correlation function between two composite sequences. This would lead to assessing the effectiveness of these sequences for use in a CDMA environment. Also, an improved analytic bound on the magnitude of the aperiodic autocorrelation function of m-sequences is still required.

Finally, the primitive polynomial generation algorithm of Section 3.2.1 can be extended to non-binary fields, in particular for $GF(3)$, $GF(4)$ and $GF(5)$.

Appendix A

Calculation of the Power Spectrum of M-Sequences

The derivation in this appendix is excerpted from Ziemer and Peterson [8] and Holmes [46] as a preliminary result to be used in determining the power spectrum of a composite sequence (see Appendix B). The power spectrum of m-sequences is determined using the Wiener-Khintchine theorem [135] which states that the power spectrum of the spreading waveform is the Fourier transform of the autocorrelation function $R_c(\Delta)$, given by (2.57). The discrete autocorrelation function of m-sequences of period N is given by (2.58),

$$\theta_c(\tau) = \begin{cases} N & \tau = 0 \text{ mod } N \\ -1 & \tau \neq 0 \text{ mod } N \end{cases} \quad (\text{A.1})$$

The discrete autocorrelation function is then substituted into (2.57) to determine the continuous autocorrelation function, $R_c(\Delta)$. For $0 \leq \Delta \leq T_c$, $\tau' = 0$ and (2.57) becomes

$$\begin{aligned} R_c(\tau) &= \frac{1}{N}(N) - \frac{\Delta}{NT_c}(N+1) \\ &= 1 - \frac{\Delta}{T_c} \left(1 + \frac{1}{N}\right) \end{aligned} \quad (\text{A.2})$$

For $T_c < \Delta < (N-1)T_c$,

$$\begin{aligned} R_c(\tau) &= \frac{1}{N}(-1) + \frac{(\tau'T_c - \Delta)}{NT_c}[-1 + 1] \\ &= -\frac{1}{N} \end{aligned} \quad (\text{A.3})$$

For $(N-1)T_c \leq \Delta < NT_c$, $\tau' = N-1$, and $\tau' + 1 = N \equiv 0 \pmod{N}$,

$$\begin{aligned} R_c(\Delta) &= \frac{1}{N}(-1) + \frac{(N-1)T_c - \Delta}{NT_c}(-1 - N) \\ &= \frac{\Delta - (N-1)T_c}{T_c} \left(1 + \frac{1}{N}\right) - \frac{1}{N} \end{aligned} \quad (\text{A.4})$$

This function is illustrated in Fig. A.1.

Figure A.1: The autocorrelation function of m-sequences

Now, defining the triangular pulse function [136] as

$$\Lambda_{T_c}(\Delta) = \begin{cases} 1 - \frac{|\Delta|}{T_c} & |\Delta| \leq T_c \\ 0 & \text{elsewhere} \end{cases} \quad (\text{A.5})$$

then the continuous autocorrelation function can be expressed as

$$R_c(\tau) = -\frac{1}{N} + \frac{(N+1)}{N} \Lambda_{T_c}(\Delta) * \sum_{i=-\infty}^{\infty} \delta(\Delta - iNT_c) \quad (\text{A.6})$$

where the $*$ denotes the convolution operation.

The Fourier transform of $\Lambda_{T_c}(\Delta)$ is given by [136]

$$\begin{aligned} \mathcal{F}[\Lambda_{T_c}(\Delta)] &= \int_{-\infty}^{\infty} \Lambda_{T_c}(\Delta) e^{-j\omega\Delta} d\Delta \\ &= T_c \text{sinc}^2(fT_c) \end{aligned} \quad (\text{A.7})$$

and the Fourier transform of a periodic impulse train is a periodic impulse train such that [137]

$$\mathcal{F}\left[\sum_{i=-\infty}^{\infty} \delta(\Delta - iNT_c)\right] = \frac{1}{NT_c} \sum_{j=-\infty}^{\infty} \delta\left(f - \frac{j}{NT_c}\right) \quad (\text{A.8})$$

Thus, the Fourier transform of the continuous autocorrelation function $R_c(\tau)$ is

$$\begin{aligned} S_c(f) &= -\frac{1}{N} \delta(f) + \left(\frac{N+1}{N^2}\right) \text{sinc}^2(fT_c) \sum_{i=-\infty}^{\infty} \delta\left(f - \frac{i}{NT_c}\right) \\ &= \frac{1}{N^2} \delta(f) + \left(\frac{N+1}{N^2}\right) \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \text{sinc}^2\left(\frac{i}{N}\right) \delta\left(f - \frac{i}{N}f_c\right) \end{aligned} \quad (\text{A.9})$$

which is illustrated in Fig. 2.9.

Appendix B

Calculation of the Power Spectrum of Composite Sequences

In this Appendix, the approximate power spectrum of composite sequences is derived. From Section 3.4.4, the power spectrum can be determined using the relationship [138]

$$S_c(f) = S_a(f) * S_b(f) \quad (\text{B.1})$$

i.e., the power spectrum of the composite sequence C is equal to the convolution of the power spectra of the component sequences A and B .

The fast component sequence B is an m-sequence with chip rate f_c and period N_b and the slow component sequence A is an m-sequence with chip rate f_c/N_b and period N_a . Thus, from the result of Appendix A, the power spectra of the component sequences are:

$$S_a(f) = \frac{1}{N_a^2} \delta(f) + \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \frac{N_a + 1}{N_a^2} \text{sinc}^2\left(\frac{i}{N_a}\right) \delta\left(f - \frac{if_c}{N_a N_b}\right) \quad (\text{B.2})$$

and

$$S_b(f) = \frac{1}{N_b^2} \delta(f) + \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \frac{N_b + 1}{N_b^2} \text{sinc}^2\left(\frac{j}{N_b}\right) \delta\left(f - \frac{j}{N_b} f_c\right) \quad (\text{B.3})$$

Hence,

$$\begin{aligned} S_c(f) &= S_a(f) * S_b(f) \\ &= \left[\frac{1}{N_a^2} \delta(f) + \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \frac{N_a + 1}{N_a^2} \text{sinc}^2\left(\frac{i}{N_a}\right) \delta\left(f - \frac{if_c}{N_a N_b}\right) \right] * \\ &\quad \left[\frac{1}{N_b^2} \delta(f) + \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \frac{N_b + 1}{N_b^2} \text{sinc}^2\left(\frac{j}{N_b}\right) \delta\left(f - \frac{j}{N_b} f_c\right) \right] \end{aligned} \quad (\text{B.4})$$

is the power spectrum of the composite sequence C . This expression can be represented as

$$\begin{aligned} S_c(f) &= [A + B] * [C + D] \\ &= [A * C] + [A * D] + [B * C] + [B * D] \end{aligned} \quad (\text{B.5})$$

Then, the equation can be evaluated by carrying out the convolution upon each individual component and recombining the results. Thus, the first component is

$$\begin{aligned} A * C &= \frac{1}{N_a^2} \delta(f) * \frac{1}{N_b^2} \delta(f) \\ &= \int_{-\infty}^{\infty} \frac{1}{N_a^2} \delta(f) \frac{1}{N_b^2} \delta(f - f') df' \\ &= \frac{1}{N_a^2 N_b^2} \delta(f) \end{aligned} \quad (\text{B.6})$$

using the sifting property of delta functions. The second component is

$$A * D = \frac{N_b + 1}{N_a^2 N_b^2} \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \text{sinc}^2\left(\frac{j}{N_b}\right) \delta\left(f - \frac{j}{N_b} f_c\right) \quad (\text{B.7})$$

Similarly, the third component is

$$B * C = \frac{N_a + 1}{N_a^2 N_b^2} \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \text{sinc}^2\left(\frac{i}{N_a}\right) \delta\left(f - \frac{i f_c}{N_a N_b}\right) \quad (\text{B.8})$$

Finally, the fourth component is

$$\begin{aligned} B * D &= \frac{(N_a + 1)(N_b + 1)}{N_a^2 N_b^2} \times \\ &\quad \left\{ \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \text{sinc}^2\left(\frac{i}{N_a}\right) \delta\left(f - \frac{i f_c}{N_a N_b}\right) * \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \text{sinc}^2\left(\frac{j}{N_b}\right) \delta\left(f - \frac{j}{N_b} f_c\right) \right\} \end{aligned} \quad (\text{B.9})$$

From the sifting property of delta functions, this convolution will be zero except when $f = i f_c / N_a N_b$ and $f = j f_c / N_b$, i.e., whenever $f = i f_c / N_a N_b$. Also, the convolution will be zero whenever $i = k N_a$, since $\text{sinc}^2(k) = 0$ for k an integer. The summations can then be combined to give

$$\begin{aligned} B * D &= \frac{(N_a + 1)(N_b + 1)}{N_a^2 N_b^2} \times \\ &\quad \sum_{\substack{i=-\infty \\ i \neq k N_a}}^{\infty} \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \text{sinc}^2\left(\frac{i - j N_a}{N_a}\right) \text{sinc}^2\left(\frac{j}{N_b}\right) \delta\left(f - \frac{i f_c}{N_a N_b}\right) \end{aligned} \quad (\text{B.10})$$

The four components (B.6), (B.7), (B.8) and (B.10) can now be combined giving

$$\begin{aligned}
 S_c(f) = & \frac{1}{N_a^2 N_b^2} \delta(f) + \frac{N_b + 1}{N_a^2 N_b^2} \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \text{sinc}^2\left(\frac{j}{N_b}\right) \delta\left(f - \frac{j}{N_b} f_c\right) \\
 & + \frac{(N_a + 1)}{N_a^2 N_b^2} \sum_{\substack{i=-\infty \\ i \neq k N_a}}^{\infty} \delta\left(f - \frac{i f_c}{N_a N_b}\right) \left[\text{sinc}^2\left(\frac{i}{N_a}\right) + \right. \\
 & \left. (N_b + 1) \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \text{sinc}^2\left(\frac{i - j N_a}{N_a}\right) \text{sinc}^2\left(\frac{j}{N_b}\right) \right]
 \end{aligned} \tag{B.11}$$

The third term of (B.11) can be simplified considerably. First of all,

$$\begin{aligned}
 & \text{sinc}^2\left(\frac{i - j N_a}{N_a}\right) \\
 &= \left(\frac{\sin \pi \left(\frac{i - j N_a}{N_a} \right)}{\pi \left(\frac{i - j N_a}{N_a} \right)} \right)^2 \\
 &= \frac{N_a^2}{\pi^2 (i - j N_a)^2} \sin^2 \pi \left(\frac{i - j N_a}{N_a} \right) \\
 &= \frac{N_a^2}{\pi^2 (i - j N_a)^2} \left\{ \sin \left(\frac{\pi i}{N_a} \right) \cos \left(\frac{\pi j N_a}{N_a} \right) - \sin \left(\frac{\pi j N_a}{N_a} \right) \cos \left(\frac{\pi i}{N_a} \right) \right\}^2
 \end{aligned} \tag{B.12}$$

Of course, $\sin \pi j = 0$ and $|\cos \pi j| = 1$ giving

$$\text{sinc}^2\left(\frac{i - j N_a}{N_a}\right) = \frac{N_a^2}{\pi^2 (i - j N_a)^2} \sin^2\left(\frac{\pi i}{N_a}\right) \tag{B.13}$$

which removes the dependence of a $\text{sinc}^2()$ function on the summation index j . Hence,

the third term of (B.11) is

$$\begin{aligned}
& \frac{N_a + 1}{N_a^2 N_b^2} \sum_{\substack{i=-\infty \\ i \neq k N_a}}^{\infty} \delta\left(f - \frac{i f_c}{N_a N_b}\right) \left[\text{sinc}^2\left(\frac{i}{N_a}\right) + \right. \\
& \quad \left. \frac{N_a^2 (N_b + 1)}{\pi^2} \sin^2\left(\frac{\pi i}{N_a}\right) \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \frac{\text{sinc}^2\left(\frac{j}{N_b}\right)}{(i - j N_a)^2} \right] \\
&= \frac{N_a + 1}{N_a^2 N_b^2} \sum_{\substack{i=-\infty \\ i \neq k N_a}}^{\infty} \delta\left(f - \frac{i f_c}{N_a N_b}\right) \left[\frac{\sin^2(\pi i / N_a)}{\pi^2 i^2 / N_a^2} + \right. \\
& \quad \left. \frac{N_a^2 (N_b + 1)}{\pi^2} \sin^2\left(\frac{\pi i}{N_a}\right) \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \frac{\text{sinc}^2\left(\frac{j}{N_b}\right)}{(i - j N_a)^2} \right] \quad (\text{B.14}) \\
&= \frac{N_a + 1}{\pi^2 N_b^2} \sum_{\substack{i=-\infty \\ i \neq k N_a}}^{\infty} \delta\left(f - \frac{i f_c}{N_a N_b}\right) \sin^2\left(\frac{\pi i}{N_a}\right) \times \\
& \quad \left[\frac{1}{i^2} + (N_b + 1) \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \frac{\text{sinc}^2\left(\frac{j}{N_b}\right)}{(i - j N_a)^2} \right]
\end{aligned}$$

Therefore, the power spectrum of the composite sequence C is

$$\begin{aligned}
S_c(f) &= \frac{1}{N_a^2 N_b^2} \delta(f) + \frac{N_b + 1}{N_a^2 N_b^2} \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \text{sinc}^2\left(\frac{j}{N_b}\right) \delta\left(f - \frac{j}{N_b} f_c\right) \\
&+ \frac{N_a + 1}{\pi^2 N_b^2} \sum_{\substack{i=-\infty \\ i \neq k N_a}}^{\infty} \delta\left(f - \frac{i f_c}{N_a N_b}\right) \sin^2\left(\frac{\pi i}{N_a}\right) \times \\
& \quad \left[\frac{1}{i^2} + (N_b + 1) \sum_{\substack{j=-\infty \\ j \neq 0}}^{\infty} \frac{\text{sinc}^2(j / N_b)}{(i - j N_a)^2} \right] \quad (\text{B.15})
\end{aligned}$$

Hence, the first term describes the spectral line at dc of amplitude $1/N_a^2 N_b^2$ and the second term describes the spectral lines at integral multiples of f_c/N_b , the chip rate of the slow sequence. The third term describes all of the spectral lines at integral multiples of $f_c/N_a N_b$, except at dc and at multiples of f_c/N_b , where the third term contributes zero.

Bibliography

- [1] L. Milstein, "The use of combination sequences in a multiple access environment," in *Proceedings: 13th Annual Allerton Conference on Circuit and System Theory*, pp. 21–27, Oct. 1975.
- [2] L. Milstein and R. Ragonetti, "Combination sequences for spread spectrum communications," *IEEE Transactions on Communications*, vol. COM-25, pp. 691–696, July 1977.
- [3] W. Stark and D. Sarwate, "Kronecker sequences for spread-spectrum communication," *IEE Proceedings Pt F*, vol. 128, pp. 104–109, Apr. 1981.
- [4] M. Beale, *Direct-Sequence Spread-Spectrum Multiple-Access Systems*. PhD thesis, University of Kent at Canterbury, Canterbury, UK, Sept. 1982.
- [5] M. Beale and T. Tozer, "A class of composite sequences for spread-spectrum communications," *Computer and Digital Techniques*, vol. 2, pp. 87–92, Apr. 1979.
- [6] L. Milstein, "Some statistical properties of combination sequences," *IEEE Transactions on Information Theory*, vol. IT-23, pp. 254–258, Mar. 1977.
- [7] W. Stark, "Kronecker sequences for spread-spectrum communications," Master's thesis, Dept. of Electrical Engineering, University of Illinois, July 1979.
- [8] R. Ziemer and R. Peterson, *Digital Communications and Spread Spectrum Systems*. New York: MacMillan Publishing Co., 1985.
- [9] R. Denaro, "NAVSTAR: the all-purpose satellite," *IEEE Spectrum*, vol. 18, pp. 35–40, May 1981.
- [10] S. Hatcher, "Starfix: Satellite navigation for maritime users," *Microwave System News*, vol. 19, pp. 35–40, July 1989.
- [11] P. Nicholson, "Ku-band communications satellite follows the nation's truckers," *Microwave Journal*, vol. 34, pp. 26–38, Mar. 1991.

- [12] D. Schilling, L. Milstein, R. Pickholtz, M. Kullback, and F. Miller, "Spread spectrum for commercial communications," *IEEE Communications Magazine*, vol. 29, pp. 66-79, Apr. 1991.
- [13] D. Schilling, R. Pickholtz, and L. Milstein, "Spread spectrum goes commercial," *IEEE Spectrum*, vol. 27, pp. 40-45, Aug. 1990.
- [14] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread Spectrum Communications*, vol. 1-3. Rockville, MD: Computer Science Press, 1985.
- [15] R. Dixon, *Spread Spectrum Systems*. New York: John Wiley & Sons, 1984.
- [16] D. Torrieri, *Principles of Secure Communication Systems*. Dedham, MA: Artech House, 1985.
- [17] A. Polydoros and C. Weber, "A unified approach to serial search spread-spectrum code acquisition - Part I: General theory," *IEEE Transactions on Communications*, vol. COM-32, pp. 542-549, May 1984.
- [18] A. Polydoros and C. Weber, "A unified approach to serial search spread-spectrum code acquisition - Part II: A matched-filter receiver," *IEEE Transactions on Communications*, vol. COM-32, pp. 550-560, May 1984.
- [19] S. Rappaport and D. Grieco, "Spread spectrum acquisition: Methods and technology," *IEEE Communications Magazine*, vol. 22, pp. 6-21, June 1984.
- [20] P. Hopkins, "A unified analysis of pseudonoise synchronization by envelope correlation," *IEEE Transactions on Communications*, vol. COM-25, pp. 770-777, Aug. 1977.
- [21] J. Holmes and C. Chen, "Acquisition time performance of PN spread spectrum systems," *IEEE Transactions on Communications*, vol. COM-25, pp. 778-784, Aug. 1977.
- [22] A. Polydoros and C. Weber, "Analysis and optimization of correlative code-tracking loops in spread spectrum systems," *IEEE Transactions on Communications*, vol. COM-33, pp. 30-43, Jan. 1985.

- [23] M. Simon, "Noncoherent pseudonoise code tracking performance of spread spectrum receivers," *IEEE Transactions on Communications*, vol. COM-25, pp. 327-345, Mar. 1977.
- [24] P. Hopkins, "Double dither loop for pseudonoise code tracking," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-13, pp. 644-650, Nov. 1977.
- [25] D. LaFlame, "A delay-lock loop implementation which is insensitive to arm gain imbalance," *IEEE Transactions on Communications*, vol. COM-27, pp. 1632-1633, Oct. 1979.
- [26] R. Yost and R. Boyd, "A modified PN code tracking loop: Its performance analysis and comparative evaluation," *IEEE Transactions on Communications*, vol. COM-30, pp. 1027-1036, May 1982.
- [27] A. Polydoros, *On the Synchronization Aspects of Direct-Sequence Spread Spectrum Systems*. PhD thesis, Department of Electrical Engineering, University of Southern California, Aug. 1982.
- [28] R. Ward, "Acquisition of pseudonoise signals by sequential estimation," *IEEE Transactions on Communications*, vol. COM-13, pp. 475-483, Dec. 1965.
- [29] G. Sage, "Serial synchronization of pseudonoise systems," *IEEE Transactions on Communication Technology*, pp. 123-127, Dec. 1964.
- [30] S. Rappaport and D. Schilling, "A two-level coarse code acquisition scheme for spread spectrum radio," *IEEE Transactions on Communications*, vol. COM-28, pp. 1734-1742, Sept. 1980.
- [31] D. C'Carlo and C. Weber, "Multiple dwell serial search: Performance and application to direct sequence code acquisition," *IEEE Transactions on Communications*, vol. COM-31, pp. 650-659, May 1983.
- [32] S. Davidovici, L. Milstein, and D. Schilling, "A new rapid acquisition technique for direct sequence spread-spectrum communications," *IEEE Transactions on Communications*, vol. COM-32, pp. 1161-1168, Nov. 1984.

- [33] Y. Su, "Rapid code acquisition algorithms employing PN matched filters," *IEEE Transactions on Communications*, vol. 36, pp. 724-733, June 1988.
- [34] A. Baier, "A low-cost digital matched filter for arbitrary constant envelope spread spectrum waveforms," *IEEE Transactions on Communications*, vol. 32, pp. 354-361, Apr. 1984.
- [35] N. Couturier, "A low-cost digital matched filter for arbitrary constant envelope spread spectrum waveforms," Master's thesis, Dept. of Electronics, Carleton University, Ottawa, Canada, 1985.
- [36] P. Baier, K. Dostert, and M. Pandit, "A novel spread-spectrum receiver synchronization scheme using a SAW-tapped delay line," *IEEE Transactions on Communications*, vol. COM-30, pp. 1037-1047, May 1982.
- [37] L. Milstein, J. Gevargiz, and P. Das, "Rapid acquisition for direct sequence spread-spectrum communications using parallel SAW convolvers," *IEEE Transactions on Communications*, vol. COM-33, pp. 593-600, July 1985.
- [38] W. Rhodes, "Acousto-optic signal processing: Convolution and correlation," *Proceedings of the IEEE*, vol. 69, pp. 65-79, Jan. 1981.
- [39] U. Cheng, "Performance of a class of parallel spread-spectrum code acquisition schemes in the presence of data modulation," *IEEE Transactions on Communications*, vol. 36, pp. 596-604, May 1988.
- [40] U. Cheng, W. Hurd, and J. Statman, "Spread spectrum code acquisition in the presence of doppler shift and data modulation," *IEEE Transactions on Communications*, vol. 38, pp. 241-250, Feb. 1990.
- [41] E. Siess and C. Weber, "Acquisition of direct sequence signals with modulation and jamming," *IEEE Journals on Selected Areas in Communications*, vol. SAC-4, pp. 254-272, Mar. 1986.
- [42] L. Milstein, "Interference suppression to aid acquisition in direct-sequence spread-spectrum communications," *IEEE Transactions on Communications*, vol. 36, pp. 1200-1207, Nov. 1988.

- [43] D. Dlugos and R. Scholtz, "Acquisition of spread spectrum signals by an adaptive array," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 37, pp. 1253–1270, Aug. 1989.
- [44] R. Ward and K. Yiu, "Acquisition of pseudonoise signals by recursion-aided sequential estimation," *IEEE Transactions on Communications*, vol. COM-25, pp. 784–794, Aug. 1977.
- [45] C. Kilgus, "Pseudonoise code acquisition using majority logic decoding," *IEEE Transactions on Communications*, vol. COM-21, pp. 772–773, June 1973.
- [46] J. Holmes, *Coherent Spread Spectrum Systems*. New York: John Wiley & Sons, 1982.
- [47] W. Alem, G. Huth, J. Holmes, and S. Udalov, "Spread spectrum acquisition and tracking performance for shuttle communication links," *IEEE Transactions on Communications*, vol. COM-26, pp. 1689–1703, Nov. 1978.
- [48] G. Hostetter, C. Savant, and R. Stefani, *Design of Feedback Control Systems*. New York: Holt, Rinehart and Winston, 1982.
- [49] H. Beker and F. Piper, *Cipher Systems*. New York: John Wiley & Sons, 1982.
- [50] A. Konheim, *Cryptography: A Primer*. New York: John Wiley & Sons, 1981.
- [51] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge, UK: Cambridge University Press, 1988.
- [52] E. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1969.
- [53] S. Lin and D. Costello, *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1983.
- [54] S. Golomb, *Shift Register Sequences*. San Francisco: Holden-Day, 1967.
- [55] M. Hall, "An isomorphism between linear recurring sequences and algebraic rings," *Transactions: American Mathematical Society*, vol. 44, pp. 196–216, Sept. 1938.
- [56] M. Ward, "The arithmetical theory of linear recurring series," *Transactions: American Mathematical Society*, vol. 35, pp. 600–628, July 1933.

- [57] E. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 732-736, Nov. 1976.
- [58] H. Anton, *Elementary Linear Algebra*. New York: John Wiley & Sons, 3rd ed., 1981.
- [59] W. Henkel, "Another description of the Berlekamp-Massey algorithm," *IEE Proceedings I*, vol. 136, pp. 197-200, June 1989.
- [60] J. Massey, "Shift register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. IT-15, pp. 122-127, Jan. 1969.
- [61] S. Faulkner, "Determination of maximal-length sequences by weight distribution analysis," Master's thesis, Carleton University, Department of Electronics, Ottawa, Ontario, Aug. 1989.
- [62] D. Sarwate and M. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proceedings of the IEEE*, vol. 68, pp. 593-619, May 1980.
- [63] F. MacWilliams and N. Sloane, "Pseudo-random sequences and arrays," *Proceedings of the IEEE*, vol. 64, pp. 1715-1729, Dec. 1976.
- [64] M. Pursley, "Performance evaluation for phase-coded spread spectrum multiple-access communications - Part I: System analysis," *IEEE Transactions on Communications*, vol. COM-25, pp. 795-799, Aug. 1977.
- [65] J. Lehnert and M. Pursley, "Error probabilities for binary direct-sequence spread-spectrum communications with random signature sequences," *IEEE Transactions on Communications*, vol. COM-35, pp. 87-98, Jan. 1987.
- [66] M. Pursley and D. Sarwate, "Evaluation of correlation parameters for periodic sequences," *IEEE Transactions on Information Theory*, vol. COM-25, pp. 508-513, July 1977.
- [67] M. Pursley and H. Roefs, "Numerical evaluation of correlation parameters for optimal phases of binary shift-register sequences," *IEEE Transactions on Communications*, vol. COM-27, pp. 1597-1604, Oct. 1979.

- [68] J. Massey and J. Uffner, Jr., "Sub-baud coding," in *Proceedings of the Thirteenth Annual Allerton Conference on Circuit and System Theory*, 1975.
- [69] D. Sarwate, M. Pursley, and T. Basar, "Partial correlation effects in direct-sequence spread-spectrum multiple-access communications systems," *IEEE Transactions on Communications*, vol. COM-32, pp. 567-573, May 1984.
- [70] H. Roefs, *Binary Sequences for SSMA Communications*. PhD thesis, University of Illinois at Urbana-Champaign, Urbana, Illinois, Aug. 1977.
- [71] D. Borth, M. Pursley, D. Sarwate, and W. Stark, "Bounds on error probability for direct-sequence spread-spectrum multiple-access communications," in *Proceedings: IEEE MIDCON Conference*, pp. 15/1.1 - 1.14, 1979.
- [72] M. Beale, "The user capacity of spread-spectrum multiple-access systems for reliable synchronisation," in *Proceedings: IEE Colloquium on Radio Systems Organization and Control, IEE Colloquium Digest No. 1980/56*, (London, UK), pp. 2/1 - 2/7, 1980.
- [73] N. Zierler, "Linear recurring sequences," *SIAM Journal of Applied Mathematics*, vol. 7, pp. 31-48, 1959.
- [74] R. Braasch, "The distribution of $(n-m)$ terms for maximal length linear pseudo-random sequences," *IEEE Transactions on Information Theory*, vol. IT-14, pp. 607-608, July 1968.
- [75] J. Fillmore and M. Marx, "Linear recursive sequences," *SIAM Review*, vol. 10, pp. 342-353, 1968.
- [76] N. Smirnov, "Applications of m -sequences in asynchronous radio systems," *Telecommunications and Radio Engineering*, vol. 24, no. 10, pp. 26-35, 1970.
- [77] Y. Niho, *Multi-Valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences*. PhD thesis, Department of Electrical Engineering, University of Southern California, Los Angeles, CA, 1972.
- [78] T. Hellesest, "Some results about the cross-correlation between two maximal linear sequences," *Discrete Mathematics*, vol. 16, pp. 209-232, 1976.

- [79] S. Wainberg and J. Wolf, "Subsequences of pseudo-random sequences," *IEEE Transactions on Communications*, vol. COM-18, pp. 606-612, Oct. 1970.
- [80] J. Lindholm, "An analysis of the pseudo-randomness properties of subsequences of long m-sequences," *IEEE Transactions on Information Theory*, vol. IT-14, pp. 569-576, July 1968.
- [81] L. Varakin and L. Volkov, "The correlation of segments of m-sequences," *Telecommunications and Radio Engineering*, vol. 28, pp. 77-81, Jan. 1973.
- [82] D. Cartier, "Partial correlation properties of pseudonoise (PN) codes in noncoherent synchronisation/detection schemes," *IEEE Transactions on Communications*, vol. 24, pp. 898-903, Aug. 1976.
- [83] N. Bekir, *Bounds on the Distribution of Partial Correlation for PN and Gold Sequences*. PhD thesis, Department of Electrical Engineering, University of Southern California, Los Angeles, CA, Jan. 1978.
- [84] A. Bessonova and M. Klykov, "The shift and add property of m-sequences," *Radiotekhnika*, pp. 59-61, June 1984.
- [85] P. Duvall and J. Mortick, "Decimation of periodic sequences," *SIAM Journal of Applied Mathematics*, vol. 21, pp. 367-372, Nov. 1971.
- [86] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation functions," *IEEE Transactions on Information Theory*, vol. IT-14, pp. 154-156, Jan. 1968.
- [87] R. Gold and E. Kopitzke, "Study of correlation properties of binary sequences," Interim Technical Report, vols. 1-4, Magnavox Research Labs, Torrance, CA, 1965.
- [88] T. Kasami, "Weight distribution formula for some classes of cyclic codes," Tech. Rep. R-285, Coordinated Science Lab, University of Illinois at Urbana-Champaign, Urbana, Illinois, 1966.
- [89] H. Trachtenberg, *On the Cross-Correlation Functions of Maximal Linear Recurring Sequences*. PhD thesis, Department of Electrical Engineering, University of Southern California, July 1970.

- [90] R. Skaug, "Numerical evaluation of the nonperiodic autocorrelation parameter for optimal phases of maximal length sequences," *IEE Proceedings Pt F*, vol. 127, pp. 230-237, June 1980.
- [91] H. Roefs and M. Pursley, "Correlation parameters of random sequences and maximal length sequences for spread-spectrum multiple access communication," *Proceedings: Canadian Communications and Power Conference*, pp. 141-143, 1976.
- [92] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Transactions on Information Theory*, vol. IT-13, pp. 619-621, Oct. 1967.
- [93] R. Rueppel and O. Staffelbach, "Products of linear recurring sequences with maximum complexity," *IEEE Transactions on Information Theory*, vol. IT-33, pp. 124-131, Jan. 1987.
- [94] A. Lempel and M. Cohn, "Maximal families of Bent sequences," *IEEE Transactions on Information Theory*, vol. IT-28, pp. 865-868, Nov. 1982.
- [95] J. Olsen, R. Scholtz, and L. Welch, "Bent-function sequences," *IEEE Transactions on Information Theory*, vol. IT-28, pp. 858-864, Nov. 1982.
- [96] P. Kumar and R. Scholtz, "Bounds on the linear span of Bent sequences," *IEEE Transactions on Information Theory*, vol. IT-29, pp. 854-862, Nov. 1983.
- [97] L. Quynh and S. Prasad, "Class of binary cipher sequences with best possible autocorrelation function," *IEE Proceedings Pt F*, vol. 132, pp. 576-580, Dec. 1985.
- [98] S. Prasad and L. Quynh, "Equivalent linear span analysis of binary sequences having an interleaved structure," *IEE Proceedings Pt F*, vol. 133, pp. 288-292, June 1986.
- [99] R. Scholtz and L. Welch, "GMW sequences," *IEEE Transactions on Information Theory*, vol. IT-30, pp. 548-553, May 1984.
- [100] J. No and P. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Transactions on Information Theory*, vol. 35, pp. 371-379, Mar. 1989.

- [101] O. Rothaus, "On 'Bent' functions," *Journal of Combinatorial Theory*, vol. 20A, pp. 300–305, 1976.
- [102] A. Shaar and P. Davies, "Prime sequences: Quasi-optimal sequences for OR channel code division multiplexing," *Electronic Letters*, vol. 19, pp. 888–890, 13 Oct 1983.
- [103] L. Quynh and S. Prasad, "New class of sequence sets with good auto- and crosscorrelation functions," *IEE Proceedings Pt F*, vol. 133, pp. 281–287, June 1986.
- [104] L. Bluestein, "Interleaving of pseudorandom sequences for synchronization," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-4, pp. 551–556, July 1968.
- [105] F. Surböck and H. Weinrichter, "Interlacing properties of shift-register sequences with generator polynomials irreducible over $GF(p)$," *IEEE Transactions on Information Theory*, vol. IT-24, pp. 386–389, May 1978.
- [106] B. Gordon, W. Mills, and L. Welch, "Some new differences sets," *Canadian Journal of Mathematics*, vol. 14, pp. 614–625, 1962.
- [107] R. Tittsworth, "Optimal ranging codes," *IEEE Transactions on Space Electronics and Telemetry*, pp. 19–30, Mar. 1964.
- [108] D. Maritsas, "On the statistical properties of a class of linear product feedback shift-register sequences," *IEEE Transactions on Computers*, pp. 961–964, Oct. 1973.
- [109] D. Green, "Product sequences with good correlation properties," *International Journal of Electronics*, vol. 67, no. 5, pp. 749–760, 1989.
- [110] Y. Kotov, "Correlation function of composite sequences constructed from two m-sequences," *Radio Engineering and Electronic Physics*, no. 9, pp. 128–130, 1974.
- [111] S. Maskera and J. Das, "Concatenated sequences for spread spectrum systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-17, pp. 342–350, May 1981.
- [112] R. Turyn, "Sequences with small correlation," in *Error Correcting Codes* (H. Mann, ed.), pp. 195–229, New York: John Wiley & Sons, 1968.

- [113] J. Stiffler, *Theory of Synchronous Communications*. Englewood Cliffs, NJ: Prentice-Hall, 1971.
- [114] M. Ackroyd, "Amplitude and phase modulation pulse trains for radar," *Radio and Electronics Engineering*, vol. 41, pp. 541-552, 1971.
- [115] E. Hollis, "Comparison of combined barker codes for coded radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-3, pp. 141-144, Jan. 1967.
- [116] R. Ward, "Digital communications on a pseudonoise tracking link using sequence inversion modulation," *IEEE Transactions on Communication Technology*, vol. COM-15, pp. 69-78, Feb. 1967.
- [117] W. Peterson and E. Weldon, Jr., *Error-Correcting Codes*. Cambridge, MA: MIT Press, 1972.
- [118] T. Gulliver, *Construction of Quasi-Cyclic Codes*. PhD thesis, University of Victoria, Victoria, B.C., 1989.
- [119] T. Ritter, "The efficient generation of cryptographic confusion sequences," *Cryptologia*, vol. XV, pp. 81-139, Apr. 1991.
- [120] D. Knuth, *The Art of Computer Programming*, vol. 2 of *Seminumerical Algorithms*. Reading, MA: Addison-Wesley, 2nd ed., 1981.
- [121] E. Watson, "Primitive polynomials (mod 2)," *Mathematics of Computation*, vol. 16, pp. 368-369, 1962.
- [122] M. Ben-Or, "Probabilistic algorithms in finite fields," in *Proceedings of the 22nd IEEE Foundations of Computer Science Symposium*, pp. 394-398, 1981.
- [123] H. Luneberg, "On Dedekind numbers," in *Combinatorial Theory*, pp. 251-257, Springer-Verlag Lecture Notes in Math, 1982.
- [124] N. Zierler and W. Mills, "Products of linear recurring sequences," *Journal of Algebra*, vol. 27, pp. 147-157, 1973.
- [125] M. Butler, "The irreducible factors of $f(x^m)$ over a finite field," *Journal London Mathematical Society*, vol. 30, pp. 480-482, 1955.

- [126] S. Cohen, "On irreducible polynomials of certain types in finite fields," *Proceedings: Cambridge Philosophical Society*, vol. 66, pp. 335–344, 1969.
- [127] D. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences," *IEEE Transactions on Information Theory*, vol. IT-25, pp. 720–724, Nov. 1979.
- [128] D. Sarwate, "An upper bound on the aperiodic autocorrelation function for a maximal-length sequence," *IEEE Transactions on Information Theory*, vol. IT-30, pp. 685–687, July 1984.
- [129] R. McEliece, "Correlation properties of sets of sequences derived from irreducible cyclic codes," *Information and Control*, vol. 45, pp. 18–25, Apr. 1980.
- [130] M. Pursley and D. Sarwate, "Performance evaluation for phase-coded spread spectrum multiple-access communication - Part II: Code sequence analysis," *IEEE Transactions on Communications*, vol. COM-25, pp. 800–803, Aug. 1977.
- [131] D. Sarwate, "Mean-square correlation of shift-register sequences," *IEE Proceedings Pt F*, vol. 131, pp. 101–106, Apr. 1984.
- [132] L. Blank, *Statistical Procedures for Engineering, Management, and Science*. McGraw-Hill, 1980.
- [133] D. Nicholson, *Spread Spectrum Signal Design: LPE and AJ Systems*. Rockville, MD: Computer Science Press, 1988.
- [134] R. Skaug and J. Hjelmstad, *Spread Spectrum in Communication*. London, UK: Peter Peregrinus, Ltd., 1985.
- [135] A. Papoulis, *Probability, Random Variables and Stochastic Processes*. New York: McGraw-Hill, 1984.
- [136] A. Poularikas and S. Seely, *Signals and Systems*. Boston, MA: PWS Publishers, 1985.
- [137] A. Oppenheim and R. Schaffer, *Discrete-Time Signal Processing*. Englewood Cliffs, N.J.: Prentice-Hall, 1989.
- [138] J. Wozencraft and I. Jacobs, *Principles of Communication Engineering*. New York: John Wiley & Sons, 1965.

END

26 05 93

FIN