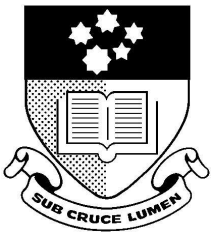
Non-Binary Spread-Spectrum Multiple-Access Communications

Derek Paul Rogers

BSc(Ma.&Comp.Sc.) BE(Hons)

Thesis submitted for the degree of
Doctor of Philosophy
in
The University of Adelaide,



Faculty of Engineering,
Department of Electrical and Electronic Engineering.

March 1995

Contents

Abstract

Non-binary code, direct-sequence spread-spectrum communication is investigated in this thesis for the asynchronous multiple-access channel. Direct-sequence spread-spectrum systems employing non-binary codes is a field in which very little prior research has been conducted. The emphasis of the research in this thesis is on a fundamental component of the system, the spreading codes. The research considers their important properties, the influences of those properties on the system performance as measured by the probability of bit error (PBE), including methods for determining the PBE, and the generation of the codes. Detailed literature reviews are provided on prior research on these issues and others of relevance to non-binary spread-spectrum.

Whilst code properties have been considered in previous literature (usually in relation to binary spreading codes), there is often a disparity between the properties that code designers emphasize and the properties that the system analysis highlights. Drawing conclusions on the relative importance of different code families or code properties, by conducting tests on subsets of actual codes, is shown to be potentially subjective because of the variation that factors such as code phase can cause. This thesis therefore develops a technique to allow different code properties to be investigated in a less subjective manner. It confirms expected results and explains others given in the literature for which an explanation has not previously been provided. The conclusions drawn by applying the technique also lead to a refined philosophy of code design, and the recognition of an important tradeoff that can allow a potentially greater number of codes.

A novel method of non-binary code generation is then developed based upon this refined philosophy. The technique is completely different to any prior method employed in spread-spectrum communication. The development of this technique, comparisons with the conventional approach, and an examination of different properties of the codes provides a good insight into code generation and is perhaps the most important contribution of this thesis. For completeness, subsets of codes produced by the novel method are compared with subsets produced by other methods, resulting in some important methods of selecting subsets of the new codes. The new approach also provides substantial future research possibilities.

Declaration

This work contains no material which has been accepted for the award of any other degree or diploma in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text.

I give consent to this copy of my thesis, when deposited in the University Library, being available for loan and photocopying.

SIGNED: ..... DATE: .....

Acknowledgements

I gratefully acknowledge the assistance and support of my supervisor, Associate Professor B.R. Davis.

My thanks to: Fred Bullock from the Telecom Research Laboratories, Melbourne, Australia; Kari Kärkkäinen from the Telecommunication Laboratory at the University of Oulu, Finland; and my colleagues at the Mobile Communications Research Centre, University of South Australia, for the provision of papers and many helpful discussions.

Thanks also to Fatih Özlütürk, from the Department of Electrical and Computer Engineering, University of Massachusetts, USA, for the provision of papers which he coauthored with Alex W. Lam; Czesław Kościelny of the Institute of Engineering Cybernetics, Wrocław Technical University, Poland, for providing copies of papers by himself and Władysław Mochnacki; and the engineering subject librarians at John Hopkins and Princeton universities, for the provision of some conference papers.

This work was supported by an Australian Postgraduate Research Priority Award from the Australian Research Council, and a Supplementary Scholarship from the Mobile Communications Research Centre of the Signal Processing Research Institute, The Levels, Pooraka, South Australia.

My thanks also to my office colleagues Sanjay, Jonathan, John and Andrew. Finally and most importantly this thesis is dedicated to the memory of my mum, Carolyn Anne (1943–1992) and my dad, David James Rogers (1937–1994). They gave all they could to help fulfil this dream, but sadly never lived to see it completed.

List of Publications

Journal Publication

1. ROGERS, D.P.,
   The Dual Problem of pseudorandom code generation for quadriphase spread-spectrum multiple-access,
   in **Australian Telecommunication Research Journal**, Vol. 27, No. 1, May 1993, pp.19–33.

Conference Publications

1. ROGERS, D.P.,
   Higher-level code-division multiple-access (HCDMA) systems,
   in **Mobile and Personal Communication Systems, First International Workshop**, Adelaide Australia, 12–13 November, 1992, pp.149–161.

2. ROGERS, D.P. and DAVIS, B.R.,
   Correlation features that influence the performance of a quaternary CDMA system,
   in **IEEE Second International Conference on Universal Wireless Access**, Melbourne Australia, 18–19 April, 1994, pp.53–57.

3. ROGERS, D.P. and DAVIS, B.R.,
   Code Properties: Influences on the performance of a quaternary CDMA system,
   in **IEEE Third International Symposium on Spread Spectrum Techniques and Applications, (ISSSTA'94)**, Oulu Finland, 4–6 July, 1994, pp.494–499.

List of Acronyms

AIP	Average Interference Parameter
AMPS	Advanced Mobile Phone System
AO	Auto Optimal
AWGN	Additive White Gaussian Noise
BPSK	Binary Phase Shift Keyed
CDF	Cumulative Density Function
CDMA	Code Division Multiple Access
CT	Continuous Time
DP	Dual Problem
DPSK	Differential Phase Shift-Keying
DS	Direct Sequence
DT	Discrete Time
ETSI	European Telecommunications Standards Institute
FDMA	Frequency Division Multiple Access
FH	Frequency Hopped
FPLMTS	Future Public Land Mobile Telecommunications System
FSK	Frequency Shift-Keying
FZC	Frank Zadoff Chu
GF	Galois Field
GPS	Global Positioning Satellite
GQR	Gauss Quadrature Rules
GSM	Global System for Mobiles
ISI	Intersymbol Interference
ITU	International Telecommunications Union
LFSR	Linear Feedback Shift Register
LSE	Least Sidelobe Energy
m-sequence	Maximal-length shift register sequence
MAI	Multiple Access Interference
MLS	Maximal-length sequence
MSC	Mean-Square Crosscorrelation (Aperiodic)
MSE	Maximum Sidelobe Energy
MSK	Minimum Shift Keying
OQPSK	Offset Quaternary Phase Shift Keying
PBE	Probability of Bit Error
PN	Pseudonoise/Pseudorandom
PSK	Phase Shift-Keying
Q-CDMA	Quaternary-level code CDMA
QPSK	Quaternary Phase Shift Keying
r.o.u.	Roots of Unity
R.F.	Radio Frequency
SNR	Signal to Noise Ratio
SS	Spread Spectrum
SSMA	Spread Spectrum Multiple Access
TCM	Trellis Coded Modulation
TDMA	Time Division Multiple Access
TIA	Telecommunications Industry Association
UMTS	Universal Mobile Telecommunications System

List of Symbols

ϕ	Discrete-time Even periodic correlation
$\widehat{\phi}$	Discrete-time Odd periodic correlation
$\overline{\phi}$	Discrete-time Even or Odd periodic correlation
ϕ_{CT}	Continuous-time Even periodic correlation
$\widehat{\phi}_{CT}$	Continuous-time Odd periodic correlation
$\overline{\phi}_{CT}$	Continuous-time Even or Odd periodic correlation
C	Discrete-time Aperiodic correlation
$\mathcal{C}$	Capacity
B_c	Spread (transmitted) bandwidth (Hz)
B_d	Data (narrowband) bandwidth (Hz)
t	Time
$\Psi(t)$	Code-chip pulse waveform
$p(t)$	Data-chip pulse waveform
$s(t)$	Transmitted signal
$r(t)$	Received signal
$n(t)$	Additive White Gaussian Noise
$d_u(t)$	Binary data waveform of u^{th} user
d_m	Binary data sequence of u^{th} user
$c_u(t)$	Complex spreading code waveform of u^{th} user
c_n	Complex code sequence of u^{th} user
τ	Propagation/transmission delay
ξ	Initial carrier phase
θ	Received carrier phase $\xi - \omega_o\tau$
$\varphi(\bullet)$	Euler totient function
ω_o	Carrier frequency
$I_{u,1}$	Multiple-access interference between the u^{th} received signal and the despreading sequence
T	Data bit time (seconds)
T_c	Code chip time (seconds)
N	Code period (symbols)
P_e	Average probability of bit-error
E_b/N_o	Bit-energy to noise ratio
$Q(\bullet)$	Complementary cumulative unit Gaussian distribution
$f_x(x)$	Probability density function of the random variable x
$F_x(x)$	Cumulative density function of the random variable x
j	$\sqrt{-1}$
m	Code symbol memory order
q	Code alphabet cardinality
U	Number of transmitters, users or codes
D	Delay element (operator)
$\mathcal{Z}_q$	Modulo-q arithmetic and numbers
$\mathcal{C}_4$	Complex arithmetic on $\{\pm j, \pm 1\}$
$L = \lambda(c)$	Linear complexity of sequence c
$\oplus$	DP addition
$\otimes$	DP multiplication
$+$	Real/GF(q) addition
$*$	Real/GF(q) multiplication
$\mathcal{E}(\bullet)$	Expectation/average

Chapter 1

Introduction

Mobile or personal communications is an area of research receiving increasing attention, primarily due to the public's seemingly insatiable[1] demand for the technology. In the provision of this technology, the first issue that must be decided upon is the multiple-access strategy. Three basic multiple-access strategies exist with digital communications:

- Time-Division Multiple-Access (TDMA)
- Frequency-Division Multiple-Access (FDMA)
- Spread-Spectrum Multiple-Access (SSMA) or Code-Division Multiple-Access (CDMA).

In a TDMA system each user is allocated some discrete time slots when they can transmit information. The information may be transmitted at any available frequency. FDMA in contrast divides the frequency spectrum into discrete bands, so a user can transmit information whenever they desire, but the information must be transmitted in a given frequency band. Spread-spectrum multiple-access however, allows all users to employ the entire spectrum at all times, with each signal being distinguished by a unique code. While there are differences between the terms spread-spectrum multiple-access and code-division multiple-access, because this thesis is concerned with a system where a high-rate code is used to spread the bandwidth, the terms can and will be used interchangeably.

A spread-spectrum (SS) signal is one in which the bandwidth of the transmitted signal has been expanded beyond the minimum necessary for the transmission of the

[1] Figure 8.2 of [13] shows that the expected number of mobile communication subscribers in Western Europe in the year 1995 is 7.44 million, in the year 2000, 17.88 million subscribers, and in the year 2010, 30.85 million subscribers.

information. The spreading process must also be independent of the information, so wideband Frequency Modulation (FM) systems are not classified as spread-spectrum.

The reason for spreading the spectrum can be seen from Shannon's theorem [177] for the band-limited additive white Gaussian noise (AWGN) channel:

$$C = \int_0^W \log_2 \left(1 + \frac{P(f)}{N(f)}\right) .df \tag{1.1}$$

where W is the available bandwidth, $P(f)$ the optimally chosen signal power density and $N(f)$ the noise power density. The capacity $\mathcal{C}$ of the channel to transmit error free information is enhanced as the bandwidth is increased (under a constant total signal power constraint), even though the signal to noise ratio (SNR) is reduced by the increased bandwidth. Scholtz commented in his paper on the evolution of spread-spectrum communications [174], that Shannon's theorem and his random signalling arguments used to prove the noisy channel coding theorem, may have further motivated the study of noise-like waveforms and spread-spectrum communications. The first direct-sequence spread-spectrum systems were developed soon after Shannon's publication in 1948.

Two fundamental types of spread-spectrum systems are commonly employed: Direct-Sequence (DS) and Frequency-Hopped (FH). In frequency-hopped spread-spectrum the frequency of the carrier onto which the information is impressed is determined by the code. In a direct-sequence or phase-coded system the information sequence is multiplied by the code. The code therefore selects the phase of the carrier.

There are advantages with both types of systems. Theoretically a direct-sequence system can be shown to perform about 2.5dB to 3dB better than a frequency-hopped system, for a given system bandwidth. However, this is mainly as a result of the use non-coherent detection in a FH system. In practice, the difference can also be illusory because a FH system can employ a greater bandwidth than a DS system. Hybrid schemes which combine direct-sequence and frequency-hopping often prove to be the best and many systems employ such techniques. Hybrid systems are also possible with other multiple-access methods and indeed several researchers (for example [2, 12]) are looking at ways of implementing CDMA within the GSM (Global System for Mobiles) TDMA standard. The research in this thesis is restricted to a direct-sequence system, but the ideas could be equally well applied to a hybrid scheme.

Historically (see for example [181]), analogue mobile (or personal) communication systems and some second generation digital systems (e.g. GSM, Digital AMPS) have employed TDMA and/or FDMA. Spread-spectrum techniques however, were initially developed for military applications so as to counter enemy jamming, [179]. This meant that the majority of research into spread-spectrum systems was classified information and it was not until circa 1970 that spread-spectrum systems were discussed in the open literature in any significant detail.

Having been developed for the harsh military radio communications environment, spread-spectrum techniques are recognised (for example [29, 27, 104, 145, 76, 190]) as being able to provide many advantages if applied to mobile (or personal) communications networks. These advantages are either unavailable to TDMA or FDMA systems, or can only be obtained with a greatly increased system complexity. Many of these advantages, as the discussions below show, occur as a direct result of employing PN codes to spread the spectrum.

The advantages of CDMA include:

1. *Automatic addressing.*

2. *Asynchronous multiple-access.*

The codes provide a means of addressing to indicate which receiver the transmitted information is intended for. In a TDMA system synchronisation or tracking problems can occur and this leads to misalignment between the transmitter and receiver time slots. To avoid the loss of the message when this occurs, additional information must be transmitted to indicate to which receiver the message was directed. Thus CDMA systems also allow for asynchronous access, which is important as not only can users transmit whenever they want, but it allows for some flexibility in relation to the different propagation delays along different paths through the channel. Asynchronous multiple access also allows for a reduction in network management overheads and is better for bursty traffic.

3. *Increased security or privacy.*

4. *Ability to overlay existing narrowband systems.*

5. *Lower transmit powers are required for traffic loads less then capacity.*

The codes also provide data security so that additional data encryption may not be necessary. This, and the lower probability of intercept of the signal because of its lower power spectral density make the system more secure than conventional narrowband TDMA or FDMA systems. If the bandwidth expansion factor of a spread-spectrum system, given by the ratio of the transmitted (spread) bandwidth B_c to the unspread data bandwidth B_d, is $B_c/B_d \approx N$ where N is the code period, then the power spectral density of the SS signal is reduced by N in comparison to an equivalent narrowband (data) signal. The low power spectral density of spread-spectrum signals also implies that they cause little interference to existing narrowband systems. This results in less electromagnetic compatibility problems and means that spread-spectrum systems can be overlayed over existing narrowband systems (see for example [123, 124]). The last point is important because if, for example, CDMA is introduced as the third generation system, then the transition between systems is far simpler. Spread-spectrum systems have also been shown (see for example [3, 4]), to require lower transmit powers which not only further reduces electromagnetic compatibility problems, but also leads to increased battery life in portable equipment, a feature attractive to mobile phone users.

6. *Graceful degradation.*

The quality of service in a CDMA system is determined by the interference resulting from the non-orthogonality of different users' codes. The interference is dependent upon the number of active users. If the number of active users decreases then the performance will improve, which is again an advantage if the traffic is bursty rather than constant. If the number of active users increases, then all experience worse performance and the system degrades gracefully, unlike TDMA or FDMA where the effective number of users must remain constant.

7. *Resistance to multipath propagation or fading.*

Direct-sequence systems mitigate the effects of multipath propagation, and frequency-hopped systems can alleviate fading by avoiding those frequencies. Multipath propagation and fading are two common problems encountered on mobile communications channels. The use of a RAKE receiver also allows direct-sequence SSMA systems to

combine all of the interfering multipath signals constructively. A TDMA system cannot overcome multipath propagation and requires equalizers to mitigate the effects of frequency fading.

8. *No frequency management is required.*

9. *Soft handoff can be used between cells in a cellular network.*

10. *Increases in capacity can be obtained by exploiting the voice activity factor and using antenna sectorisation.*

CDMA systems do not require the frequency planning of existing cellular FDMA systems either, because each cell and user is allocated the entire frequency band. Thus frequency reuse, although not theoretically required, is substantially reduced in a practical cellular CDMA system. This not only leads to an increase in capacity, but it allows soft handoff to be employed in the system. Soft handoff (which is discussed in [190, 192]) reduces the possibility of call dropping, which often occurs in the transition from one cell to the next. Soft handoff also significantly increases the coverage radius of each cell. An increase in cell size leads to a reduction in the number of base stations required which has both social (or environmental) and economic advantages.

The final advantage listed above, increased capacity for SSMA systems, is a contentious issue in the literature. Capacity improvements can be obtained in spread-spectrum systems by exploiting the voice activity factor (see [43] for a discussion on this), or through the sectorisation of antennas. This capacity improvement (over conventional analog cellular systems) has been shown by the field trials discussed later in this section. The paper by Newson and Heath [131, p.683] makes the point however, that capacity-enhancing features may also be applied in FDMA and TDMA systems and comparisons should therefore involve more advanced versions of these multiple-access techniques. This is certainly true, but as Pickholtz remarked in [145], to exploit voice activity in a TDMA or FDMA system requires centralised control and the implementation of demand assignment strategies, whereas CDMA systems do not require such centralised control.

In summary therefore, SSMA systems have many advantages: technical, social, and economic, over other multiple access schemes in a mobile or personal communications

environment. No system is without its disadvantages however, and several important ones were originally perceived with a DS-SSMA system. These are now discussed.

The originally perceived disadvantages with DS-SSMA were:

1. *The Near-Far effect.*

In a mobile communication channel, signal attenuation is approximately an inverse function of distance raised to some exponent, which is typically between three and four. Thus if the desired signal transmitter is farther away from the receiver than the interfering transmitter and they transmit with the same power, then the desired signal will be overwhelmed by that of the interferer. This problem is termed the Near-Far effect. A significant amount of research (on power control algorithms for example), has been devoted to this problem and it is no longer perceived as a significant shortcoming. Kavehrad and Ramamurthi discuss the use of pilot tones as a technique for overcoming the Near-Far effect in [81]. An alternative is to employ a hybrid direct-sequence/slow frequency-hopping system. The Near-Far effect is then reduced because the probability that two or more users have the same frequency has been reduced. Verdú also makes the point in [189], that "*... the near-far problem is not a flaw of CDMA, as widely believed, but of the inability of the conventional receiver to exploit the multiaccess interference*". Research into multiuser systems attempts to overcome this problem by designing a receiver to reduce or cancel the multiple access interference (MAI).

2. *The necessity to give each user a unique code.*

The necessity to give each user a unique code was also initially considered a problem, as many binary code generation techniques produce an insufficient number of codes. Research has been conducted on code reassignment algorithms (e.g. [83, 73, 71, 47]), as one solution to this problem however, the currently favoured solution is to employ *long* codes. *Long* codes are discussed later in this section in relation to the Qualcomm [160] system because this is the solution employed in several operational CDMA systems. Another solution to overcome an insufficient number of codes is to employ non-binary codes, and this is the solution investigated in this thesis.

3. *Increased complexity.*

In regard to the final perceived disadvantage, advances in the past decade in VLSI (Very Large Scale Integration), ASIC (Application Specific Integrated Circuits), and signal processing technology (see for example [190, 140]), have made it possible to implement (cost effectively) spread-spectrum systems for consumer products. The paper [115] by Magill et. al., from which the following quote is taken, provides an overview of a variety of commercial applications of spread-spectrum systems including the Low Earth Orbit (LEO) satellite proposals.

> "*The proliferation of SS products for commercial applications began with*
>
> - *the emergence of the GPS* [Global Positioning Satellite] *system*
> - *the successful demonstration of SS for cellular telephones*
> - *the allocation of the Instrumentation* [Industrial], *Scientific, and Medical (ISM) bands in the USA by the FCC* [Federal Communications Commission].
>
> *In 1989, the FCC mandated special use of the ISM bands so that an SS system is permitted to operate without license so long as the system does not interfere with an existing system in these frequency bands.*
>
> ...
>
> *A direct sequence CDMA spread-spectrum signal was chosen for GPS because it provided a means of incorporating accurate ranging, data transmission, multipath mitigation, multiple access, interference rejection, and access security in a convenient manner.*
>
> *The Qualcomm OmniTRACS system*[2] *... return link signal ... employs a combination of direct sequence CDMA and frequency hopping in order to ensure that users will not interfere with adjacent satellite systems.* " ···[115]

It was not until 1991 that the first serious commercial proposal (including power control techniques), for the use of CDMA for personal communications services (PCS) was made. On December 5, 1991 Qualcomm [160] presented the results of field trials conducted late in 1989 for a CDMA system to the Cellular Telecommunications Industry

[2] An extension of the GPS system that includes two-way data messaging as well as position reporting.

Association (CTIA). The success of these trials led to the formation of a new subcommittee TR45.5 of the Telecommunications Industry Association (TIA) in early 1992 to develop standards for digital cellular spread-spectrum. Further independent trials continued to be conducted in other locations throughout the world [191, 139, 36, 86], including some in Australia by the Telstra Research Laboratories in 1993, [121, 122]. The success of these trials led to the adoption [32] of the CDMA standard by the TIA in July 1993 as an interim standard (IS-95) for second generation systems in the United States of America. Additional CDMA standards (e.g. IS-99 for data) are currently under development for consideration by the TIA and the Joint Technical Committee for standardisation for the third generation system, [26]. Qualcomm trials were also conducted in South Korea and this led to the adoption in April 1994 of CDMA as the choice for digital wireless telephony in South Korea. CDMA cellular systems are also expected to be deployed for public use in Seattle, Los Angeles, New England, New York, and Little Rock in the USA in 1995.

Independently of Qualcomm, the CODIT (Code Division Testbed) project within the European RACE II programme (see for example [10, 7, 15, 120]) is investigating CDMA as an access method for the third generation system UMTS (Universal Mobile Telecommunication System) or FPLMTS (Future Public Land Mobile Telecommunication System). These are being standardised by ETSI (European Telecommunications Standards Institute) and the ITU-R (International Telecommunications Union - Radio), Task Group 8/1.

Thus CDMA and spread-spectrum systems are moving away from the initial research phase and into the commercial phase, and many electronics companies (particularly in Taiwan and Korea) have started developing CDMA products and finding new applications for CDMA. This will of course generate more research issues.

The system developed by Qualcomm and indeed most research into SSMA or CDMA has been concerned with $\{\pm 1\}$ binary spreading codes, with only a small but increasing amount of research considering non-binary systems. A non-binary system refers to one where the spreading code elements are non-binary (or complex numbers). To digress slightly, the data sequence is always regarded as being binary in this thesis. However, an examination of binary code generation techniques shows that many techniques provide

an insufficient number of codes at moderate bandwidth expansion factors. When applied in the personal or mobile environment, the insufficient number of suitable codes can be an important problem. Several solutions to this problem exist, as has been previously remarked in the discussion on the perceived disadvantages of CDMA. One solution is to employ a higher bandwidth expansion factor B_c/B_d. This means that for a constant data-bit time (T), the code-chip time (T_c) must be decreased as $B_c/B_d \approx T/T_c$. The code-chip time is of course limited by the switching and processing times in the receiver and transmitter circuitry, and as the transmitted signal bandwidth is approximately $1/(T_c)$, the value of T_c may be constrained by statuary regulations.

A second solution to overcome an insufficient number of codes is that employed in the Qualcomm system [160] and in some aspects of the CODIT project [7]. The solution is to employ *long* spreading sequences instead of *short* spreading sequences. *Short* codes is a term that refers to the situation in which the code length equals the data bit length. *Short* codes are often used in the uplink (mobile to base) for the multiple access channel because they can provide more rapid acquisition and are better for burst traffic. Analogously *long* codes is a term used to describe the situation where one unique very long pseudorandom sequence is employed for all users. The length of the code is much greater than the data bit length and the code spans more than one data bit, hence a different code chip pattern is associated with each data symbol. Different users are allocated different phases of the very long code. *Long* codes therefore avoid the necessity of code planning or reassignment and they allow multiple bit-rates to be easily implemented (see for example [11]). However, the disadvantage with *long* codes is in analysing the system as one then has to be concerned with the partial periodic crosscorrelations of codes, and this complicates the analysis. Relevant literature that considers the partial periodic crosscorrelation of codes includes [179, Vol. I, pp.294–295] and [151, 172, 66]. This problem is similar to that encountered in the acquisition of sequences except that it is the partial periodic autocorrelation in that case. In this thesis only *short* codes are investigated. Further information on *long* codes can be found in the following papers, [186, 79]. The second referenced paper, by Kärkkäinen et. al., found that *short* code systems perform slightly better than *long* code systems.

A third solution to the problem of an insufficient number of available codes is to consider a higher-cardinality code alphabet, i.e. non-binary codes. This solution overcomes the practical problems of the first solution mentioned and if *short* spreading sequences are employed, the analytical problems of the second approach above. Using non-binary codes also provides an additional advantage, because sets of codes can be found whose crosscorrelations are less than those for sets of binary sequences. This result, which the author's intuition suggested was true, is proven in section 1.3. An important point to note is that although this thesis concentrates on *short* codes, non-binary codes may also be applied to *long* period code systems. Aspects of this thesis may then be applicable to that application.

This thesis therefore investigates non-binary codes for spread-spectrum communications. In the next section an outline of the thesis is given and this discusses the research issues as well as the manner in which they are investigated.

1.1 Outline Of The Thesis

This thesis investigates non-binary spread-spectrum multiple-access communications. The research considers code generation techniques, system performance (as measured by the probability of bit error), how performance is influenced by the different properties of the codes, and how those properties relate to the code generation technique. The research refines the code design philosophy and investigates this by developing a novel code generation technique.

Section 1.2 reviews the basic theory of spread-spectrum communications. While the reader may be familiar with the basic theory, since it is frequently provided in the literature, the purpose of section 1.2 is to define the relevant symbols and common equations employed throughout this thesis. More importantly, section 1.2 also defines the specific system under consideration. This is because the review of prior literature on non-binary systems, given in section 1.3.1, shows that different authors may use different terminology to describe the same system, or the same terminology to describe different systems. Section 1.2 therefore clearly defines the non-binary system investigated in this thesis.

The motivation for researching non-binary spread-spectrum systems has been dis-

cussed previously. Section 1.3 continues the discussion and explains, in further detail, the advantages of using non-binary codes. Importantly, section 1.3 proves that non-binary codes can be found whose peak crosscorrelation value is less than that of the so-called *best* binary codes.

The crosscorrelation between codes is only one of many properties which are considered in the literature. Section 1.4 therefore reviews and explains properties commonly referred to in the literature on code generation. What that section highlights is that although the randomness properties of the codes are well defined, the correlation properties are not, yet the theory in section 1.2 shows that the crosscorrelations between codes determine the performance in a multiple-access environment. Section 1.4 therefore suggests the first research issue: an investigation to determine the important code properties and their relative importance for the multiple-access channel. This issue is of course important when comparing or designing spreading codes; the system or code designer must possess a good understanding of code properties. The early chapters in this thesis therefore investigate code properties, and the later chapters code generation.

To digress slightly, the literature review of methods for approximating or bounding the PBE, given in section 2.1, strengthens the need to resolve this issue, as do the recent results of others (e.g. Chen and Oksman [24]), which are discussed in chapters 2 and 3. Consideration of the literature review of non-binary code generation techniques, given in section 4.2, also highlights that many code designers do not emphasize the properties system designers do. Clearly therefore there is a need to resolve the research issue above, because of the disparity in the literature.

Section 1.4 reviews the desirable properties of PN codes historically given in the literature on spreading codes. Analogously, section 2.1 shows the properties system designers emphasize by reviewing methods for approximating and bounding the bit error probability. These techniques also propose several merit factors. Primarily, merit factors are used to optimise the performance of a given set of codes by selecting the appropriate code phase (or code starting point). The variation in the PBE, due to the phase of the code, can be significant as section 2.2.2 shows. More importantly, the results of section 2.2.2 serve another purpose, they show that it is not possible to resolve the research issue, on the importance of code properties, by conducting tests on sets of

actual codes without the conclusions being potentially subjective.

Thus chapter 2 serves several related purposes simultaneously. Section 2.1 reviews methods for approximating and bounding the PBE, the measure of performance used in the thesis. The review is divided into two halves, the first considers approximation techniques, the second bounds on the PBE. These two reviews are important for several reasons:

1. They highlight properties of the crosscorrelation spectra to consider when resolving the research issue.

2. They discuss in detail the method used in this thesis to bound the PBE for sets of deterministic sequences.

3. They assist in chapter 3 in developing a novel approach which does resolve the research issue.

The first point above leads to a discussion on merit factors in section 2.2.1. Merit factors emphasize properties system designers consider important; they are used in selecting subsets of codes and optimising the performance of a given set of codes. Sections 2.2.1 and 2.2.2 therefore explain and investigate the use of merit factors so as to determine which factor provides the optimal code phase selection. The literature is not clear on this issue, but it needs to be resolved if different code properties or families are to be compared by testing actual sets of sequences. These sections do identify the most appropriate criteria for selecting the code phase, and consequently they highlight important code properties (expressed by the merit factors). This is because each criteria (for selecting the code phase) emphasizes different merit factors or code properties. The most appropriate criteria for selecting the code phase is also used in chapter 5 to compare different code families. More importantly however, section 2.2.2 and the summary in section 2.3 show that comparing code families or code properties (resolving the research issue) by conducting tests on actual sets of sequences can provide subjective conclusions unless care is taken. This knowledge is applied in chapter 5 where different families of codes are compared.

Chapter 3 therefore develops a new method specifically to examine the influence of different crosscorrelation properties on performance in a less subjective manner. This

technique and an examination of other code properties leads to a refinement of the conventional code design philosophy. This refinement is consistent with, but an extension of one proposed by others such as Hui [72], Burr [19] and Kärkkäinen [80, 77, 78], whose research and conclusions are discussed in detail in section 3.4. However, their approach does not specifically address code generation, which is done in this thesis.

Using the new code design strategy, chapter 4 develops a novel method of code generation. Section 4.1 familiarises the reader with the basic terminology employed in the chapter and section 4.2 reviews the literature on existing non-binary code generation methods. It is the theory of one of these techniques which provides the basis to develop a completely different theory of code generation in section 4.3. The randomness, stability, and linear complexity (security) properties of a selection codes produced by this new approach are investigated in section 4.4. Comparisons between the system performance of subsets of the new codes and those of other techniques are made in chapter 5. Finally, chapter 6 summarises the results and conclusions of the thesis and gives recommendations for future work.

1.2 Spread-Spectrum Multiple-Access

This section reviews the basic operation of a direct-sequence spread-spectrum system. The operation of this system is well known, so this section serves mainly to define many of the symbols and terms that are employed throughout the remainder of the thesis.

Figure 1.1 models an asynchronous DS/SSMA system consisting of U transmitters (or active users) at a common carrier frequency w_o; The initial carrier phase ξ_u for each transmitter is arbitrary. The transmitter for the u^{th} user comprises an information sequence $d_u(t)$, which along with the complex-valued code $c_u(t)$, is modulated onto the complex carrier $e^{j(w_o t+\xi_u)}$. Only the real part of the resultant signal is transmitted over the channel. Double lines in the figure indicate the inphase and quadrature channel signals. The real part is carried by the inphase channel, the imaginary part by the quadrature channel.

The complex code waveform $c_u(t)$ is expressed in terms of the complex code sequence

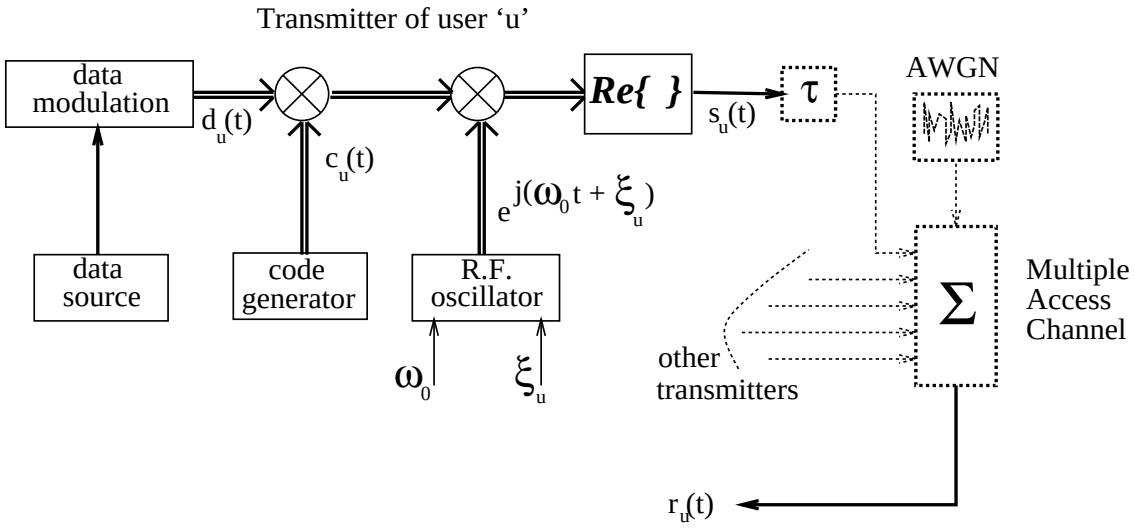


Figure 1.1: Asynchronous Multiple-Access DS/SSMA system

c_n and the code-chip pulse $\Psi(t)$ by:

$$c_u(t) = \sum_n c_n.\Psi(t - n.T_c) \tag{1.2}$$

where the sequence c_n is periodic with period N. The code-chip pulse shape $\Psi(t)$ is constrained to the time interval $[0, T_c]$ and has a total signal energy equal to one.

The data waveform $d_u(t)$ can be expressed in terms of the data sequence d_m and the data-symbol pulse shape $p(t)$ via:

$$d_u(t) = \sum_{m=-\infty}^{\infty} d_m.p(t - mT) \tag{1.3}$$

with a rectangular pulse shape

$$p(t) = \begin{cases} 1 & 0 \leq t < T, \\ 0 & \text{otherwise} \end{cases} \tag{1.4}$$

In this thesis the data sequence is restricted to being $\{\pm 1\}$ binary and the spreading code sequence $\{\pm 1, \pm j\}$ quaternary. The data is restricted to binary as the emphasis of the research is an investigation of code properties and code generation. The discussion in the next section on prior research, also shows that binary data systems were found to perform better than non-binary data systems. The reasons for restricting the codes to a quaternary alphabet are also discussed in the next section. This system is referred to as Q-CDMA (quaternary-coded CDMA) in this thesis, and section 1.3.1 which reviews

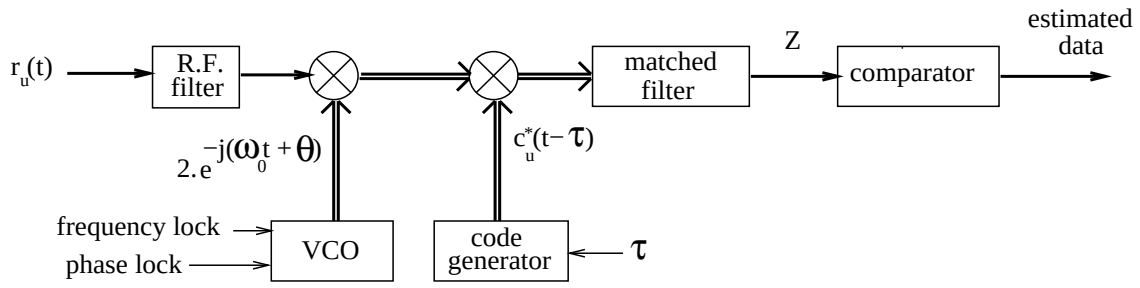


Figure 1.2: Direct-Sequence Spread-Spectrum Receiver

other non-binary systems proposed in the literature, relates the Q-CDMA system to those.

Thus the transmitted signal $s_u(t)$ for the u^{th} user can be expressed as:

$$s_u(t) = \mathcal{R}e\left\{d_u(t).c_u(t).e^{j(w_o t+\xi_u)}\right\} \tag{1.5}$$

The asynchronous multiple-access channel delays each signal by τ_u to account for the arbitrary transmission starting times and propagation delays. Background thermal noise is included by the addition of white Gaussian noise (AWGN) $n(t)$ of one-sided power spectral density N_o (W/Hz). Hence the signal $r(t)$ at the receiver in figure 1.2 (selected as corresponding to user 1), can be represented as:

$$r(t) = \sum_{u=1}^{U} \sqrt{2P_u}.s_u(t-\tau_u) + n(t) \tag{1.6}$$

where P_u denotes the received power of the u^{th} transmitter's signal. For convenience, it is assumed that all users are received with the same power P, i.e. $P_u = P$ for all u.

The frequency and phase estimates which are employed by the receiver are obtained from the synchronisation and tracking circuits of the receiver, which are not shown. In this thesis, because the emphasis is on PN codes rather than the complete system, issues of acquisition, synchronisation and tracking are avoided. The paper by Polydoros and Glisic [147] provides an extensive bibliography relevant to these issues, and the tutorial on spread spectrum systems by Pickholtz et.al. [146] provides an introductory discussion on this topic. Coherent detection is also assumed in this thesis, thus τ_1 and $\theta_1 = \omega_o\tau_1 - \xi_1$ can be set to zero without any loss of generality. Krenz et. al. [93] discuss how coherent detection may be obtained through the use of a pilot tone.

The receiver removes the carrier from the received signal, multiplies it by the de-spreading code and then integrates this over the data bit interval. The receiver is there-

fore a matched filter or correlator. Alternate receivers do exist, such as those for multiuser detection (see for example the research of S. Verdú), or those that exploit the cyclostationarity of the signal (see for example the research of W.A. Gardner), but these are not commonly employed and are therefore not considered in this thesis.

The resultant signal (Z) which is passed to the comparator to estimate the transmitted data bit can be shown to be of the form of equation 1.7. The theory summarised here follows that given in the papers of: Lam and Özlütürk [101]; Fukumasa, Kohno, and Imai [45]; and Krone and Sarwate [95]. For a complete and detailed analysis, the reader is also referred to the early work of Pursley et. al. [157, 158, 154, 155, 152], on which these and indeed most papers that discuss the theory of spread spectrum multiple access are based. Some of these papers by Pursley et. al. are briefly discussed in section 1.3.1. Thus:

$$\begin{aligned} Z &= \int_0^T r(t).[c_1(t)]^\star.dt \\ &= \sqrt{\frac{P}{2}}.T.d_0^{(1)} + \sum_{u=2}^{U} \sqrt{\frac{P}{2}}.d_0^{(u)}.\frac{I_u}{N} + \eta \end{aligned} \tag{1.7}$$

where the first component is the desired narrowband signal containing the information bit d_0 of user $u = 1$, labelled $d_0^{(1)}$; the second component is the multiple-access interference (MAI), which is the sum of the code pair interferences I_u of each user; the final component η, is a Gaussian random variable due to thermal noise, which has a zero mean and a variance of $N_o.T/4$.

Normalising the interference I_u by $\sqrt{P/2}.T_c.d_0^{(u)}$ and setting $l_u.T_c \leq \tau_u \leq (l_u + 1).T_c$ for some integer $0 \leq l_u \leq N - 1$, the normalised code pair interference $I_{u,1}$ can be expressed in terms of the continuous-time (even or odd periodic) crosscorrelation $\overline{\phi}_{CT}$ via:

$$I_{u,1} = \mathcal{R}e\{\overline{\phi}_{CT}.\mathrm{e}^{j\theta_u}\} \tag{1.8}$$

The continuous-time crosscorrelation is expressed in terms of the discrete-time (even or odd periodic) crosscorrelation ($\overline{\phi}$) as shown in equation 1.9.

$$\overline{\phi}_{CT} = \overline{\phi}(l).\widehat{\mathcal{R}}_\Psi(\tau - l.T_c) + \overline{\phi}(l+1).\mathcal{R}_\Psi(\tau - l.T_c) \tag{1.9}$$

The factors $\widehat{\mathcal{R}}_\Psi$ and $\mathcal{R}_\Psi$ are dependent upon the code-chip pulse shape and are defined

as follows:

$$\widehat{\mathcal{R}}_{\Psi}(s) = \int_{s}^{T_c} \Psi(t).\Psi(t-s).dt \tag{1.10}$$

$$\mathcal{R}_{\Psi}(s) = \int_{0}^{s} \Psi(t).\Psi(t+T_c-s).dt \tag{1.11}$$

If the code-chip pulse is rectangular, equation 1.8 can then be expressed as:

$$I_{u,1} = \mathcal{R}e\left\{[\overline{\phi}_{u,1}(l_u) + (\overline{\phi}_{u,1}(l_u+1) - \overline{\phi}_{u,1}(l_u))\delta_u]\mathrm{e}^{j\theta_u}\right\} \tag{1.12}$$

where $\delta_u = (\tau_u - l_u.T_c)/T_c$ and $\theta_u = \xi_u - \omega_o\tau_u (\mathrm{mod}\ 2\pi)$. The discrete-time crosscorrelation $(\overline{\phi})$ between the first and u^{th} users is either the discrete-time even periodic correlation (ϕ) if $d_{-1}^{(u)} = d_0^{(u)}$, or it is the odd periodic correlation $(\widehat{\phi})$ if $d_{-1}^{(u)} \neq d_0^{(u)}$. Note that d_{-1} and d_0 represent the two data bits impressed onto the received codes which span, due to asynchronism, the despreading code. Both even and odd periodic correlation can be expressed in terms of the aperiodic correlation (C):

$$C_{a,b}(l) = \begin{cases} \sum_{j=0}^{N-1-l} a_j.[b_{j+l}]^{\star} & 0 \leq l \leq N-1 \\ \sum_{j=0}^{N-1+l} a_{j-l}.[b_j]^{\star} & 1-N \leq l < 0 \\ 0 & |l| \geq N \end{cases} \tag{1.13}$$

$$\begin{aligned} \phi_{a,b}(l) &= \sum_{j=0}^{N-1} a_j.[b_{j+l}]^{\star} \\ &= C_{a,b}(l) + C_{a,b}(l-N) \end{aligned} \tag{1.14}$$

$$\widehat{\phi}_{a,b}(l) = C_{a,b}(l) - C_{a,b}(l-N) \tag{1.15}$$

Clearly the interference in the system is determined by the crosscorrelations of the codes. If $Z > 0$ and $d_0^{(1)} = -1$ (or $Z < 0$ and $d_0^{(1)} = 1$), then the comparator will give an incorrect result and a data bit error has occurred. The performance of the system is therefore measured by the probability of bit error (PBE) and is given by:

$$P_e = \frac{1}{2}\left(P\{d_0^{(1)} = 1, Z < 0\} + P\{d_0^{(1)} = -1, Z > 0\}\right) \tag{1.16}$$

For random binary data the two probabilities in this equation $P\{d_0^{(1)} = 1, Z < 0\}$ and $P\{d_0^{(1)} = -1, Z > 0\}$ are equal. Random binary data is assumed in this thesis and also in most of the analysis or simulations reported in the literature.

This section has therefore reviewed the basic theory of DS spread spectrum. Whilst the reader may well have been familiar with this theory, its purpose is to define the symbols and common equations which are employed throughout the remainder of this thesis. There is no standard agreement in the literature upon symbol notation, which a perusal of the papers on non-binary systems reviewed in the next section would show.

1.3 Non-Binary Spread-Spectrum

The majority of research into spread-spectrum communications has concentrated on systems employing binary spreading codes. The reason for this is that the code generation process is simpler. Modulo-2 arithmetic is employed and this is easily implemented electronically. Modulo-2 arithmetic is also isomorphic with the use of $\{\pm 1\}$ which simplifies both the modulation and correlation processes. It has been previously remarked however, that many binary code families contain an insufficient number of codes, particularly if they are to be considered for developing a *short* code CDMA system able to cope with the demand for personal communications services. One solution to this problem considered was to utilize longer length codes, as the number of codes in a family usually increases as the code period increases. The code period N, data-bit time T and code-chip time T_c are related by $N = T/T_c$, so for a constant data-rate increasing the code length increases the code-rate $(1/T_c)$, but $1/T_c$ is the bandwidth of the transmitted signal which is set by government and international regulations, and constrained by physical components and circuits. There is therefore a limit on T_c and consequently on N.

An alternate solution to provide a greater number of potential codes whilst maintaining the same code and data rates is to increase the size of the code alphabet. This is the solution investigated in this thesis, the consideration of non-binary codes. Non-binary codes may also be considered for use in applications involving *long* codes. This is because not only can they provide a greater number of codes, but they can also improve the performance of the system, as discussed below.

The intention of a direct-sequence system is to make the signals of other users appear as random (or benign) noise to the desired signal (or user). One would intuitively expect

therefore, that a spreading signal (or code) which has more than two levels would lead to improved performance, because an increased number of possible code symbols should allow smaller crosscorrelations and hence reduced interference; Reduced interference decreases the probability of bit-error and therefore improves performance. Taking this argument to extremes, one would expect the best performance if the code alphabet size is infinite (i.e. an analogue signal). The results of Özlütürk and Lam [101] comparing binary, quaternary and non-binary ($q > 4$) sequences are in agreement with this expectation. In particular, figures 6 to 9 in their paper show an improvement in performance as the size of the code alphabet is increased. Further information on other results from the research of Özlütürk and Lam on non-binary codes is provided later in this section.

There are practical reasons against using an infinite code alphabet and generally it is best to limit the alphabet to quaternary as this avoids amplitude modulation (other than inversion on the inphase and quadrature channels). Amplitude modulated signals can often suffer problems in the mobile environment due to fading. To maintain the necessary linear operation required with amplitude modulation, the high power amplifier of the transmitter needs to be 'backed off'. This then causes the amplifier to be inefficient in terms of power usage. In relation to phase modulated or roots of unity (r.o.u.) signals where the number of phases is greater than four, the greater number of phases may only be maintained with coherent detection if the medium is phase stable. Such stability may not be able to be provided in the mobile environment when longer code lengths are employed. For these reasons, whilst this thesis investigates non-binary codes of any cardinality, quaternary codes are emphasized.

The intuitive expectation of smaller (peak) crosscorrelation values for non-binary in comparison with to binary sequences has been proven to be true by Kumar and Moreno in [98], (see also [185]). Using the Sidelnikov bound[3] on the peak even periodic crosscorrelation $\phi_{\max}$, [98] shows (with modifications to the notation to be consistent with this thesis), that for binary ($q = 2$) sequences:

$$\phi^2_{\max} > (2k+1)(N-k) + k(k+1)/2 - \frac{2^k N^{2k+1}}{U(2k!)\binom{N}{k}} \tag{1.17}$$

[3]The Sidelnikov bound applies for sequences generated using finite field arithmetic. This is important to note as in chapter 4 some sequences generated do not employ finite field arithmetic. For information comparing the Sidelnikov and Welch bounds see [98, p.604] and [97].

for $0 \leq k < 2N/5$, and for non-binary ($q > 2$) sequences with any $k \geq 0$:

$$\phi^2_{\max} > \frac{k+1}{2}(2N-k) - \frac{2^k N^{2k+1}}{U(k!)^2\binom{2N}{k}} \tag{1.18}$$

In the above equations the family size U is related to the code length N via $U = N^r$, with r a real number and $k = \lfloor r \rfloor$, i.e. k is the closest integer less than or equal to r. If r is an integer and $N \gg r$, then the approximation to the Sidelnikov bound for binary codes is:

$$\phi^2_{\max} > N\left((2r+1) - \frac{1}{\prod_{m=1}^{r}(2m-1)}\right) \tag{1.19}$$

and for non-binary codes:

$$\phi^2_{\max} > N\left(r + 1 - \frac{1}{r!}\right) \tag{1.20}$$

This can be reduced for $r = 1$ to the following:

$$\phi^2_{\max} \approx \begin{cases} 2N & \text{if } q = 2 \\ N & \text{if } q > 2 \end{cases} \tag{1.21}$$

Hence the peak crosscorrelation of the best non-binary codes can be approximately 70% of the peak value for the best binary codes[4], thus improving the worst case system performance.

With regard to the *best* binary sequences, Gold codes [52] have been shown [171, p.606] to be optimal in relation to the Sidelnikov bound. That is, they have the minimum peak crosscorrelation value for their code period and family size. A set of quaternary sequences which have a smaller peak crosscorrelation than binary Gold codes are those developed by Solé [180] and independently by Boztaş, Hammons and Kumar [17, Family $\mathcal{A}$]. These codes are often referred to as '4-phase' or '4-phase optimal' codes in some literature where comparisons are being made with binary sequences. In this thesis they will be referred to as Boztaş codes to avoid any confusion. Detailed information on these codes is provided in chapter 4. The family size and code periods of both Boztaş and Gold codes are the same. Practical code generation techniques have therefore been developed that validate the intuitive expectation that non-binary codes should perform better than binary codes.

[4]In question time at the IEEE Universal Wireless Access conference in Melbourne in April 1994, Serdar Boztaş remarked to the author of this thesis that this result is also true for aperiodic and odd periodic correlation.

An important point to consider however, is that the above discussion considers only the peak value of the crosscorrelation, which applies in the worst case. For the average level of performance the discussions in chapter 2 and the analysis and conclusions of chapter 3, show that other features of the crosscorrelation spectrum should be considered as well as the peak value, e.g. the mean-square crosscorrelation. Harrison Rowe developed bounds on the mean-square even periodic crosscorrelation value in [165], but unfortunately his analysis does not seem easily extendable to provide the same comparison between binary and non-binary codes.

The expectation that non-binary codes can provide a better level of system performance than binary codes is also supported by simulation and analytical studies. In simulating a DS/SSMA system Cacopardi et. al. [21, 20] found that for codes of period $N = 127$, the use of Boztaş codes could allow up to 50% more users than binary Gold codes at a probability of bit error appropriate for speech (PBE $= 10^{-3}$). The analytical results of Lam and Özlütürk [100, 136, 101] also showed that the quaternary Boztaş codes performed better than binary Gold codes, and these results were for the performance on average. These papers by Özlütürk and Lam further show that non-binary codes with $q > 4$, such as the Frank-Zadoff-Chu (FZC) codes (discussed in chapter 4) could provide even better performance, but the improvement was not as significant as that between binary and quaternary codes.

Thus the intuitive expectation that non-binary codes can lead to improved performance has been proven for the worst case, and is supported by simulation and particularly analytical results for the on-average case. It is for this reason, as well as the greater number of codes that they can provide, that non-binary code spread-spectrum is investigated in this thesis.

To familiarise the reader with spread-spectrum systems other than the conventional binary system, the following section reviews the key papers in the literature on this. Detailed literature reviews on other topics relevant to the research are provided in later chapters. Those later reviews consider techniques for determining the probability of bit-error of a spread-spectrum system, the measure of system performance used in the thesis, and non-binary code generation. The review in the next section describes specific systems and their associated terminology. This is important because the same terminology may

often be employed in different contexts, which then requires the reader to be careful when making comparisons between systems.

1.3.1 Prior Research: Non-Binary Spread-Spectrum Systems

Early research in the open literature on spread-spectrum systems other than binary was conducted by Pursley and Garber who published several papers on this. In a 1978 paper [154] Pursley and Garber considered two types of quadriphase spread-spectrum system. Two systems were considered because they noted that although a quaternary sequence can be decomposed into two binary sequences (as shown in chapter 4), there are certain quadriphase sequences with a correlation property that cannot be represented by a pair of binary sequences with the same type of correlation property. Pursley and Garber discussed Barker codes (see chapter 4) as example of this.

The first system they considered was termed orthogonal biphase-coded carrier spread-spectrum. This system consisted of a pair of binary data signals and a pair of binary code waveforms. One data sequence and spreading code for the inphase channel, the other data sequence and other spreading code for the quadrature channel. The analysis in their paper showed that the aperiodic correlation of each binary code played an important role. This is in contrast to the second system considered which was termed quadriphase-coded carrier spread spectrum. In the second system each inphase and quadrature carrier was phase modulated ($\{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\}$ radians) by one code. Two binary data bit streams then multiplied each carrier. The analysis in the paper found that the complex correlation parameters were important in the quadriphase-coded carrier system. This first system is therefore not a non-binary coded system in the context of this thesis, whereas the second system is, but neither is it the conventional binary system, hence its review here.

It should also be noted that the literature often refers to spread-spectrum systems that use binary data and a single binary code only on the inphase channel as BPSK (Binary Phase Shift-Keyed) spread-spectrum. Both of the above quadriphase spread-spectrum systems are also referred to as QPSK (Quadriphase Shift-Keyed) spread-spectrum or occasionally quaternary spread-spectrum. However, a large proportion of the literature employing the term QPSK spread-spectrum generally refers to the biphase-coded carrier system.

Pursley, Garber and Lehnert extended QPSK spread-spectrum to consider "generalised quadriphase spread-spectrum" in a 1980 paper [155]. This was a biphase-coded carrier system, but a time offset was allowed between the inphase and quadrature channels. The system was then termed offset QPSK (OQPSK) spread-spectrum. The analysis of this system was provided in the paper and an expression for the average signal to noise ratio (SNR) derived. The average SNR was a parameter proposed by Pursley and Garber in [150] as a measure of the performance of the system. An approximation to the PBE, the performance measure used in this thesis, can be obtained by using the average SNR. This approximation is discussed in detail in chapter 2.

Pursley et. al.'s 1980 paper also modified the analysis to not only allow an offset between the inphase and quadrature channels, but to consider different code-chip pulse shapes. If the code-chip waveform $\Psi(t)$ is sinusoidal:

$$\Psi(t) = \begin{cases} \sqrt{2}.\sin\left(\frac{\pi.t}{T_c}\right), & 0 \leq t < T_c \\ 0, & \text{otherwise} \end{cases} \tag{1.22}$$

and the offset between the inphase and quadrature channels is $T_c/2$, half the code-chip duration, then the resultant signal is termed minimum shift-keyed (MSK) spread-spectrum. More information on MSK spread-spectrum including relevant literature is provided in section 3.2.3 in chapter 3.

Garber and Pursley continued the investigation into OQPSK spread-spectrum in [46]. In this later paper they provided a generalised expression for the transmitted signal, which employed $\{\pm 1, \pm j\}$ codes with the orthogonal quadriphase-coded carrier system. This system is then equivalent (see for example Krone and Sarwate [95]) to the system of this thesis discussed in section 1.2. The author of this thesis found that the references provided in section 1.2 gave a clearer description of the system. Garber and Pursley's paper also used the average interference parameter (AIP), a component of the average SNR parameter, to compare different systems. The average interference parameter is discussed in detail in section 2.2.1 of chapter 2 and is frequently referred to in later chapters of this thesis.

Comparisons between the systems discussed so far have been conducted in a few papers, and before continuing the review of different non-binary systems, three of these papers are discussed below. These papers by Laforgia et. al., Lunayach, and Torrieri (all

referenced below), provide some interesting results and important points to note.

Laforgia, Luvison and Zingarelli compared BPSK, QPSK, OQPSK and MSK spread-spectrum in [99] using the results obtained from simulations of each system. Examining the results of their paper, in particular [99, Table IV], they found that for lower bit-energy to noise (E_b/N_o) ratios MSK had a lower PBE than QPSK, which was lower than OQPSK; This was for ten users and a code period $N = 511$. As the E_b/N_o ratio increased further, a region where the codes have more influence on performance (refer section 2.1), QPSK performed better than MSK and OQPSK was significantly worse. When fifteen users were considered OQPSK still performed the worst, but the difference was not as significant as previously. These are interesting results and they illustrate an issue, that is, it is difficult to draw general conclusions on issues relevant to spread-spectrum communications, in this case on which is the best modulation method, from tests conducted on sets of actual sequences (either by analysis or simulation). This problem and a means of its solution are investigated in subsequent chapters in this thesis.

R.S. Lunayach [113] also investigated quadriphase spread-spectrum communications with both BPSK and QPSK data modulation, biphase and quadriphase spreading and *long* and *short* codes. In this paper Lunayach refers to biphase spreading as the situation where the same code is impressed onto the inphase and quadrature carrier, and quadriphase spreading as the use of different binary codes on each carrier. These are different definitions to those of Pursley and Garber previously discussed. Torrieri [186, 187] who uses the terminology of Lunayach also described the latter system as quaternary direct-sequence.

This is another point to note when reading the literature on non-binary systems, the same terminology is employed in different contexts. To be certain of the terminology employed when comparing systems and particularly their conclusions, one must look at the form of the transmitted signal. To avoid any confusion of terminology in this thesis, the system is described as quaternary-coded CDMA (Q-CDMA). The definition of the system of this thesis (given in section 1.2) is the same as the biphase SS system with a polyphase-coded carrier of Fukumasa, Kohno and Imai [45]; that employed by Lam and Özlütürk [101]; and discussed by Krone and Sarwate [95] as the orthogonal quadriphase coded carrier system of Pursley et. al. in [46].

Torrieri's and Lunayach's investigations led to the following conclusions, using their terminology:

- Quadriphase DS systems performed better than binary under both tone and multiple access interference (MAI).
- Balanced quadriphase modulation was preferable to classical quadriphase modulation against tone (narrowband) interference. The performance was the same under multiple access interference for both systems.

The balanced quadriphase system of Torrieri, which using Pursley and Garber's notation is a system with the same binary data impressed onto each biphase-coded carrier, is the closest to the system utilised in this thesis. However for the system in this thesis each spreading code would be ternary $\{\pm 1, 0\}$ rather than binary. The first conclusion of better performance than the binary SS system should therefore hold for the system of section 1.2. This is because when that system is viewed as employing ternary codes on each carrier, the zeros in the codes can be exploited to reduce the crosscorrelation between different codes. In contrast, it is not intuitively obvious why the QPSK or MSK spread-spectrum systems should perform better than binary-code (BPSK) spread-spectrum. Neither is it clear whether or not the second conclusion of better performance under tone interference holds for the system in this thesis. Torrieri stated that the better performance under tone interference occurred because a tone cannot have a phase which can cancel both carriers simultaneously, and this can occur in the Q-CDMA system.

Returning to the discussion of different non-binary spread-spectrum systems, perhaps the most significant recent contributions have been made by Özlütürk and Lam in a series of papers. The research of Lam and Özlütürk [101] on non-binary spread-spectrum systems was mentioned previously to show that the use of non-binary codes can provide better performance than the use of binary codes. In their research Lam et. al. have proposed and investigated several different non-binary spread-spectrum systems which are discussed below. They have also developed analytical techniques to accurately bound the probability of bit-error for the systems they considered. Chapter 2 reviews in detail their method for bounding the probability of bit-error of the non-binary system used in this thesis. This method was employed in the thesis whenever the PBE of the system was required for a set of specific codes.

In early research [136], Özlütürk and Lam investigated the non-binary spread-spectrum system employed in this thesis. This research formed the basis of their later journal publication [101] referred to above and previously. These publications illustrated that sets of non-binary codes could be found whose performance was better than sets of the so-called *best* binary codes, Gold codes (which are discussed in chapter 4). The 1990 conference paper [136] also considered a non-binary system employing *long* and *short* codes. In agreement with the results of Kärkkäinen et. al. [79] for binary codes, previously mentioned, Özlütürk and Lam found similar levels of performance between *long* and *short* non-binary code systems.

Later publications by Lam and Özlütürk (and Tantaratana) proposed and investigated a variety of different non-binary systems. In their 1991 Information, Sciences and Systems conference paper [102] they considered a DS/SSMA system in which each user was provided with M non-binary sequences for transmission. Trellis Coded Modulation (TCM) was also incorporated with this system because of the improvement in performance TCM has provided in other applications (see for example the research of G. Ungerboeck). Similarities exist between the system in this paper and later multiuser or multicode CDMA research. Multiuser research is primarily concerned with binary code sequences, however [102] found better performance when non-binary sequences were employed. This is perhaps an issue for future multiuser CDMA research to consider.

Another system was employed in their 1992 Military Communications conference paper [137]. This paper extended the simple non-binary code SSMA system to allow M-PSK (M-ary phase shift-keyed) data. The results of this paper again show that a SSMA system with non-binary codes performs better than a corresponding SSMA system using M-PSK data and binary codes. In addition, figure 4 in the paper shows that the use of a binary data signal provides better performance than either 4-PSK or 8-PSK data. This is another reason why this thesis considers only binary data, the primary reason being that the emphasis is upon the non-binary codes.

Özlütürk, Tantaratana and Lam have also recently considered an additional non-binary code system [138]. This system uses non-coherent binary data modulations such as DPSK (differential phase shift-keying) and FSK (frequency shift-keying). Figure 4 in the paper [138] shows that BPSK data modulation performs better than either DPSK

or FSK data modulation. A point to note with this is that the channel model was the same as that used in section 1.2, i.e. multipath propagation and fading are not considered. If the model and analysis of their paper had considered multipath, fading or other non-linearities (which are associated with the components of a practical system, e.g. the high-power transmitter amplifier), then DPSK may well have provided improved performance over BPSK data modulation. This issue is not investigated in this thesis, but it could be considered in future research.

The review in this section has introduced the reader to the different non-binary spread-spectrum systems that are discussed in the literature. The review has also highlighted several important conclusions in regard to the different systems. The consideration of these conclusions contributed to the selection of the simple (or original) system investigated by Özlütürk and Lam [136, 101] for research in this thesis. The research in this thesis also concentrates on the non-binary codes, their generation and important properties, and the simple system considered by Özlütürk and Lam is the most appropriate for investigating these issues. Further, because the emphasis is on the codes all users are also assumed to be received at the same power level, and the channel is not degraded by multipath propagation or fading.

To introduce the investigation of code properties, the next section discusses the properties pseudorandom codes are desired to possess. This discussion is based on an examination of the literature on binary pseudorandom codes and the properties have been extended in that section to apply to non-binary codes. Examining the desired properties, and after a consideration of the review of methods for determining the PBE, in the early part of chapter 2, it should become clear that some properties require a more precise definition. Defining the desired code properties more precisely is the first research issue investigated in this thesis. This issue is proposed in the latter part of chapter 2 and resolved in chapter 3.

1.4 Pseudorandom Code Properties

The analysis in section 1.2 shows that the crosscorrelations between codes determine the performance in a multiple access environment, where the performance is measured

by the probability of bit error (PBE). In practice however, the choice of a CDMA code family for personal and mobile communication systems is dependent not only upon the code family size and crosscorrelation spectra, but on many factors. Other factors which require consideration when designing a complete communication system include: capacity, throughput, multipath outage, synchronisation and acquisition times. Although these are not investigated in this thesis, the reader is reminded of their importance. To commence the investigation of code properties, this section reviews those properties which are commonly discussed in the literature on pseudorandom or pseudonoise (PN) sequences.

Historically [145, 30, 114], the properties binary pseudorandom sequences used in direct-sequence spread-spectrum are desired to have, are consistent with those that could be expected to be obtained by tossing a fair coin $N = 2^m - 1$ times, and by comparing two sequences of N coin tosses. To digress slightly, the choice of the code period as $N = 2^m - 1$ corresponds to the period for a maximal-length sequence. Chapter 4 discusses maximal-length sequences in some detail because they are an important class of PN sequences. Thus to extend the desired properties to the non-binary code alphabet, the fair coin analogy may be replaced by that of a fair q-sided dice. The properties then are:

1. **Balance property**: Over the complete sequence, the number of occurrences of each symbol will be approximately equal.

2. (a) **Run property**: A run[5] of r contiguous identical symbols will occur about $N.q^{-r}$ times in the sequence of length N.

   (b) **Window property**: The occurrence of all r-tuples ($r \leq m$) will be approximately equal.

3. The autocorrelation, $\phi_i(\tau)$, of the sequence $\mathrm{PN}_i(t)$ with a time-shifted version of itself $\mathrm{PN}_i(t+\tau)$ is small except as $\tau \to 0$, where 'small' is defined relative to the inphase autocorrelation $\phi_i(0) \neq 0$.

4. The crosscorrelation, $\phi_{i,j}(\tau)$ for $i \neq j$, between $\mathrm{PN}_i(t)$ and $\mathrm{PN}_j(t+\tau)$ is small in comparison to the inphase autocorrelation for all τ.

[5]No runs of length $r > m$ can exist, otherwise the period of the sequence is $N = 1$.

The first three of these properties are referred to in this thesis as the randomness properties. The Window property is the most general and the Run and Balance properties are special cases of this. The Balance property is important as it ensures that the d.c. component (or mean value) of the code or code modulated signal can be neglected. The Run and Window properties are important for comparing the structure of the pseudorandom sequence with truly *random* noise or sequences.

The remaining two properties, referred to as the correlation properties, are also important when comparing the pseudonoise signal with random noise. Autocorrelation is important in regard to the correct selection (acquisition) of the despreading sequence by the receiver, the correct time alignment between the transmitted and despreading sequences (synchronisation and tracking), and the self-interference which arises in a multipath environment. The crosscorrelation determines the mutual interference between different simultaneously transmitted signals.

Two additional code properties are also required in certain situations: stability and a high linear complexity. Stability is important in the generation of non-linear codes, and the linear complexity of a code is a measure of how secure the code is; furthermore, linear complexity is a property often investigated for non-linear codes as well. In chapter 4 the novel method of code generation developed can produce non-linear codes, these properties are therefore discussed in detail in that chapter.

Ensuring that the spreading sequence has the listed pseudorandom properties is important, not only to practical and performance considerations, but also when analysing the system. Assuming that the sequences are truly random significantly reduces the amount of computation required in analytical techniques, and the review of methods for approximating the PBE in chapter 2 highlights this. The introduction to chapter 3 also discusses additional reasons why random codes are often assumed in place of deterministic codes. Thus if the deterministic codes satisfy properties consistent with random codes, then analytical techniques assuming the use of random codes should provide results comparable to those for deterministic codes, but with a substantially reduced amount of computation.

It is important to digress slightly at this point to make some comments in relation to randomness and finite length random sequences. Randomness is an ensemble property.

Thus in analysis, randomness is ascribed by giving a set of codes certain properties. To define a finite length sequence as *random* really refers to the a priori conditions by which the sequence was generated, not the a posteriori consideration of the properties of the sequence. Pseudorandom sequences are therefore defined as those sequences, irrespective of their generation, which have properties consistent with those expected of a random sequence, such as one generated by the tossing of a fair coin or dice. In this thesis, particularly chapter 5, where comparisons are made with random sequences, the reference is to codes generated by a program which simulates the tossing of a fair q-side dice. These issues on randomness will be discussed further in later chapters.

Returning to the discussion on desirable code properties, the ideal autocorrelation and crosscorrelation spectra are a delta function and the zero function respectively. However, in an asynchronous environment it is not possible to simultaneously satisfy both of these properties, there is a tradeoff between having good autocorrelation properties and having good crosscorrelation properties. This tradeoff is shown by the Welch bound which is discussed in section 3.4. The Welch bound shows that for a given family size as the peak crosscorrelation is reduced the peak out-of-phase autocorrelation value increases. Many designers of codes therefore seek to simultaneously minimise both the peak cross- and out-of-phase auto-correlation values for a given family size. This design approach is commonly employed and is often termed the min-max criteria. The resultant codes may also be described as being optimal with respect to the Welch bound.

Examining the desirable properties of PN codes it can be seen that those relating to randomness (balance, run and window) are well defined. In contrast, the crosscorrelation properties are not well defined; "How small is small?" Furthermore, the crosscorrelations between codes determine the interference and consequently the PBE of the system. The first research question considered in this thesis is therefore: "What features of the cross-correlation spectrum influence performance and to what extent?" This question still causes consternation in relation to binary codes, which the majority of spread-spectrum systems employ. There are effectively two schools of thought. Code designers tend to concentrate on the peak correlation values (the min-max criteria), and this gives an indication of the worst case performance, but how likely is it to occur? In contrast, system designers consider other features of the correlation spectrum. These features are best

illustrated by different merit factors. The peak value is of course a simple merit factor, but the reference here is to the mean-square crosscorrelation and sidelobe energy for example.

Thus to help resolve the first research issue and more precisely define the desired code properties, different merit factors are investigated in chapter 2. These merit factors were formulated from the analysis of the probability of bit error of the system. The early part of chapter 2 therefore reviews a selection of analytical methods for determining the PBE. Not only does this introduce why the merit factors were proposed, but it provides important background information for other aspects of the thesis and this is explained further in that chapter.

The relative importance of different code properties and merit factors must of course be investigated before code generation is. The early chapters of the thesis are therefore concerned with code properties, and these chapters provide some important conclusions in regard to code generation and the comparison of code families which are investigated in later chapters. To highlight the important original contributions of this thesis to its field they are summarised in the next section.

1.5 Contributions Of This Thesis

To complete the introduction, the original contributions of the thesis to its field are highlighted for the reader.

The author of this thesis recognised the potential importance and advantages of employing non-binary codes in a spread-spectrum system before conducting a literature review. Once a literature search had been conducted, it then became clear that others shared this view. The author has also noted increasing interest in this field during the last three years. To prove that non-binary systems can perform better than binary systems is clearly going to be difficult (as well as subjective), because many issues in relation to performance and desirable code properties have not been resolved for binary codes before the necessary extension to consider non-binary codes.

This thesis therefore contributes to the theory and understanding of spread-spectrum systems employing non-binary (specifically quaternary) codes on a more fundamental

level. The thesis develops a "meta-level" technique to evaluate the influence of different features of the crosscorrelation spectra on system performance. The technique itself is not as important as the conclusions drawn in relation to code properties by its use. These conclusions have important ramifications for code generation and it shown that the existing school of thought requires refinement.

In discussions with other researchers in this field (whose work is referenced), after the publication independently of work by this author, it is apparent that the conclusions drawn on code properties in this thesis are becoming increasingly accepted by system designers. However, the author is not aware of any publications by others which translate this knowledge on important code properties to the ideas in relation to code generation (and indeed a novel code generation technique) developed by the author of this thesis. Rather, others who share the views on important code properties tend to recommend the use of random codes in the system, as opposed to the prior view of designing codes to minimise the peak crosscorrelation value. Advocating the use of random codes does not resolve the issue of code generation however. Code design or generation is therefore the region where, in the opinion of the author, this thesis makes its most important contributions to the field.

This thesis therefore contributes several important ideas in relation to code design and the influence of code properties on system performance, for non-binary code spread-spectrum systems. No prior research by others has been conducted on this, to the best of the author's knowledge, and the results obtained are consistent with the small, but increasingly accepted results being published analogously for binary systems. The research of this thesis also provides many avenues for future investigation.

Chapter 2

System Performance: Deterministic Codes

In this thesis, the system performance is measured by the probability of bit-error (PBE). Obtaining the error probability by the complete simulation of a direct sequence system involves, in most cases of interest, long run times to obtain results. This was therefore considered inappropriate as a means of gaining an insight into how variations in different parameters affect performance. Such knowledge is required before code generation can be considered. Analytical techniques are therefore employed in this thesis to determine the PBE for the Q-CDMA system.

In the first section of this chapter, prior literature on analytical techniques for determining the PBE of spread-spectrum systems is reviewed. The review is not exhaustive, but it highlights key papers which employ different techniques. Many of these methods have been developed primarily for binary spread-spectrum communications, but the techniques can and in some cases have been extended to consider non-binary codes.

The review of different methods of deriving the PBE is important for several reasons:

1. An examination of the different methods provides an insight into code properties that should be considered in relation to code design, i.e. which properties does the system analysis highlight? This is to assist in resolving part of the first research issue: the identification of important code properties.

2. One technique is reviewed in section 2.1.2 in greater detail than the others. This method, which was developed by Özlütürk and Lam (based on the prior research

of others), is regarded as very accurate and it has been employed throughout the thesis whenever the PBE of a set of deterministic sequences has been calculated. It also forms the basis of the novel analysis in chapter 3, which before it was developed considered the different analytical approaches of the methods reviewed in section 2.1.

In regard to the first point, some authors also define merit factors (such as the average signal to noise ratio, or average interference parameter), as a consequence of their analysis. Merit factors are frequently employed in the literature for one of the following purposes:

1. To select the optimal phase of a code.

Section 2.2, which investigates code phase, shows that because the transmission is over an asynchronous channel, the phase of the codes is important. The phase of a code should not be confused with the phase of the transmitted signal; code phase is common terminology for the staring point of the sequence, it is not a phase angle.

2. To select subsets of codes from a large code family, or to compare code families.

Merit factors are employed for this second reason because their calculation requires substantially less computation than the calculation of the PBE does.

Section 2.2 therefore investigates the influence of the code phase on performance. This is because there is no consensus in the literature on which is the optimal criteria, and the different criteria emphasize different correlation features (via the merit factors). Thus investigating the different criteria and determining the optimal criteria assists in resolving the first research issue mentioned above.

Section 2.2.1 reviews the literature on the different criteria (or merit factors) and discusses them in detail. Section 2.2.2 then compares the performance of a selection of codes for each different criteria. These tests have been conducted in order to determine the optimal criteria (and hence important properties), but as the discussion in section 2.3 shows, they provide another important result.

This chapter therefore serves several separate, but related purposes, and these are important for later chapters of the thesis.

2.1 Methods For Determining The Bit Error Probability

In determining the probability of bit error (PBE) of a system two analytical techniques can be employed. An approximation to the PBE can be derived, or bounds (in some instances approximations to bounds) can be obtained. Bounds provide more information than an approximation as they provide a measure of the accuracy of the result, but they are computationally more intensive, hence the use of approximations.

The literature review is therefore divided between approximations and bounds on the PBE. Methods of approximating the PBE are reviewed in section 2.1.1 and bounding techniques are reviewed in section 2.1.2. As mentioned previously, the review has several purposes. One reason is to familiarise readers with the key papers and hence techniques for calculating the PBE of the system. Therefore whilst the review is extensive it is by no means exhaustive.

Another reason for the review is that understanding the different techniques and their limitations provides an insight into important code properties to consider. Recall that before code generation can be considered (in chapter 4), the designer needs to identify the important properties and their relative importance. Approximations generally provide more insight into the influence of code properties on performance than bounds, but there is always the question of the validity (and accuracy) of the approximation. The reader may be familiar with the use of a Gaussian approximation, a contentious issue in spread-spectrum literature, this approximation is discussed in detail in section 2.1.1.

In the review of methods to bound the PBE of a spread-spectrum system, the approach of Lam and Özlütürk (which is directly applicable to the QPSK and Q-CDMA systems), is reviewed in detail. There are two reasons for this, firstly it does not employ the Gaussian approximation and it can be used to provide arbitrarily tight bounds on the PBE without the need for calculation of the higher-order moments of the MAI. This technique has therefore been used throughout the thesis in all tests which required an accurate calculation of the PBE for a small set of deterministic sequences. Özlütürk and Lam's technique is used for example in section 2.2.2 where tests are conducted on a selection of sequences in order to determine the optimal code phase criteria. These

tests provide a significant conclusion in regard to resolving the first research issue on the relative importance of code properties. This conclusion leads to the research of chapter 3, and the second reason why Özlütürk and Lam's technique is reviewed in detail. An aspect of their method is used in the development of some novel analysis in chapter 3 to overcome the problem identified in section 2.2.2 (and discussed further in section 2.3).

The review of methods for determining the PBE therefore serves several purposes in regard to the research in this thesis, and some of these are relevant for the research in later chapters.

2.1.1 Approximations To The PBE

The most commonly employed approximation to determine the PBE in a spread-spectrum system is the Gaussian approximation. The Gaussian approximation assumes that the multiple access interference (MAI) may be regarded as Gaussian noise of appropriate mean and variance. This was proposed by Pursley in 1977 in a paper on system analysis [150]. By considering the variance of the MAI, Pursley derived an expression for binary codes for the average signal-to-noise ratio ($\overline{\mathrm{SNR}}$):

$$\overline{\mathrm{SNR}} = \left\{ (6N^3)^{-1} \sum_{\substack{u=1 \\ u \neq i}}^{U} [2\mu_{u,1}(0) + \mu_{u,1}(1)] + \frac{N_o}{2E_b} \right\}^{-\frac{1}{2}} \tag{2.1}$$

where $2\mu_{u,1}(0) + \mu_{u,1}(1)$ is the average interference parameter (AIP) (which is dependent on the crosscorrelations of the codes). The AIP is discussed, and $\mu_{u,1}(0)$ and $\mu_{u,1}(1)$ are defined, in the section on merit factors 2.2.1 as an understanding of this parameter is not required at this point. The probability of bit error (P_e) is then given by:

$$P_e = \mathcal{Q}(\overline{\mathrm{SNR}}) \tag{2.2}$$

where the Gaussian tail probability (or the $\mathcal{Q}$-function) is:

$$\mathcal{Q}(k) = \frac{1}{\sqrt{2\pi}} \int_k^\infty \mathrm{e}^{-\lambda^2/2} d\lambda \tag{2.3}$$

It has been shown (for example in [136]), that these equations are also applicable to non-binary systems (in particular the Q-CDMA system considered here), provided that the AIP is redefined as $2\mu_{u,1}(0) + \mathcal{R}\mathrm{e}\{\mu_{u,1}(1)\}$. Pursley had previously defined the AIP for complex-valued sequences in this manner in [154].

In the 1977 paper [150], Pursley also gave a further approximation of the average SNR which is applicable for *random* codes:

$$\overline{SNR} = \left\{ \frac{U-1}{3N} + \frac{N_o}{2E_b} \right\}^{-\frac{1}{2}} \tag{2.4}$$

This can be (and commonly is) used for an initial system design to indicate the tradeoffs between the code period (N), the number of users (U) and the bit-energy to noise (E_b/N_o) ratio.

The above equations apply when the code-chip pulse shape is rectangular, but these have been modified in later literature to consider different pulse shapes [159], and the multipath channel [75]. Holtzman [67] also improved the accuracy of the equation for random binary codes by using a conditional Gaussian approximation. The conditional Gaussian approximation is discussed further later in this section.

It has been mentioned above that the use of the Gaussian approximation by Pursley is a contentious issue in the literature. The usual justification for employing the Gaussian approximation is the Central Limit Theorem [141, pp.214–221], particularly when the code period is large. Yao [199], whose bounding technique is discussed in section 2.1.2, examined the accuracy of the approximation and concluded that although the Gaussian interference model is suitable for many situations, it is not accurate with small numbers of users, low-length codes and high SNR (E_b/N_o).

In 1979, using an information theory approach, Mazo also examined [119] the validity of the Gaussian approximation. He concluded that whilst a set of codes could be found to make the approximation suitable for a particular user, the Gaussian approximation really leads to an average over all possible ways of assigning sequences in a DS SSMA system. Mazo's conclusions also show that as the peak even periodic crosscorrelation value for the code set increases, the Gaussian approximation becomes less accurate.

Pursley in his 1987 paper [153] on spread-spectrum for packet radio systems claimed that the Gaussian approximation is accurate if U/N is not too large. Pursley suggested that although one might expect the interference to be closer to Gaussian for a larger number of interferers this is only true if the interference is normalised, as required by the Central Limit Theorem, which it is not.

Pursley's comments above disagree with those of later researchers however. In 1989, Morrow and Lehnert [126] examined the Gaussian approximation in detail and their

conclusions are now well accepted. Morrow and Lehnert discussed how the Central Limit Theorem was often given as the justification for the Gaussian approximation when the code period N was large. They then showed that regardless of N, a large number of users U, was required before the standard Gaussian approximation became accurate, provided that thermal noise could be neglected (i.e. high SNR or E_b/N_o); results which are in agreement with those of Yao. They also found that the Gaussian approximation holds reasonably well when *long* spreading sequences are used, the code period $N \gg 1$, the number of users $U \gg 1$, and the PBE is not too small.

Pursley's technique, often referred to as the standard Gaussian approximation, is frequently employed throughout the literature. Clearly care must be taken with its use, and because of the regions in which it is accurate it is not used to determine the PBE for small sets of deterministic sequences in this thesis (e.g. section 2.2.2 and chapter 5). However, Pursley's technique is important for several reasons:

- Several merit factors and specifically criteria for selecting the optimal code phase have been defined and developed from the analysis. This is shown in section 2.2.1 in the review of merit factors.

- These merit factors (as section 2.2.1 shows) highlight the importance of considering not only the correlation values (related to $\mu(0)$), but also the adjacent pairs of correlation values (related to $\mu(1)$). The definitions of $\mu(0)$ and $\mu(1)$ are given in section 2.2.1.

Pursley's technique is also a suitable (and computationally convenient) approximation in regions where the PBE is small (and the performance is dominated by AWGN, rather than the code properties), a region where commercial voice-only mobile communication systems are likely to operate.

In their 1989 paper, Morrow and Lehnert developed a conditional Gaussian approximation to the PBE and claimed that this approach was more accurate than the standard approximation. In the conditional Gaussian approximation, the Gaussian approximation is applied to the probability of bit error conditioned on different variables (e.g. code delay, and the type of correlation). Sadowsky and Bahr, using large deviations theory [167], examined this approximation and found that it provided a very good estimate

if the interfering signals had equal power. When that was not the case (such as for the Near-Far situation), the technique developed in their paper was more appropriate. Their technique is a hybrid involving simulation (importance sampling) and analysis. This thesis also assumes that the interfering signals all have the same power. Removing this restriction would unnecessarily complicate the intention of the research, which is to investigate code properties and code generation.

Morrow and Lehnert's technique was developed for random binary signature sequences, but unlike equation 2.4 which does not include any factors (apart from the period N) pertaining to codes, Morrow and Lehnert's technique highlights the need to consider adjacent pairs of code symbols, or the discrete-time aperiodic autocorrelation at an offset of one code chip, i.e. $C(1)$. This parameter is estimated for random sequences in [126]. The accuracy of the conditional Gaussian approximation, particularly in the regions where the codes have the predominant influence on performance, led to it being adapted in later literature to apply to deterministic sequences. The literature on these later refinements (including the technique of Özlütürk and Lam) is discussed in the review of methods for bounding the PBE in section 2.1.2.

A suitable concluding comment on the accuracy of the Gaussian approximation is a quote from the paper by Sadowsky and Bahr: "*Of course a problem with the Gaussian approximation (conditional or unconditional) is that it is difficult to predict where it will break down.*" Careful note has been taken of this warning. However not all methods of approximating the PBE employ a Gaussian approximation, and some of these are now discussed. Many of these techniques (and those bounding the PBE) can be traced or related back to the research of Wu in [197, 196]. In the first paper [197] two methods were developed. Both techniques used the moments of the interference, because they are easier to evaluate than distributions, especially when the number of users is large. One method used a Taylor series expansion of the $\mathcal{Q}$-function and the other Gauss Quadrature Rules (GQR) to express the PBE integral as a linear combination of a finite number of values of the $\mathcal{Q}$-function. Wu's paper, which discussed the computational complexity of many prior techniques, found that the GQR approach was more efficient than a Taylor series expansion. The accuracy of each technique could also be obtained from the convergence in the terms of the series or expansion.

In the companion paper [196], the Gram-Charlier method was used to expand the unknown probability density function (PDF) of the multiple-access interference (MAI) as terms of the derivatives of a known PDF, the normal distribution. This technique had a lower computational complexity than the GQR approach, but it was inaccurate for small user numbers and high E_b/N_o ratios, regions where the codes have the dominant influence on performance.

The series expansion method of Wu was used by Pursley and Geraniotis [49] in 1982, to improve the accuracy of their approximation to the PBE. Their technique did not employ a Gaussian approximation either. In the 1982 paper, the PBE was obtained by integrating the characteristic function of the interference. This technique allowed different code-chip pulse shapes to be considered and was developed for MSK, QPSK and OQPSK as well as binary spread-spectrum. Except in special cases however, it required the numerical calculation of double integrals, which is computationally intensive, and for this reason it has not been employed in this thesis. This work has also been extended in a later paper by Geraniotis and Ghaffari [48] to consider both synchronous and asynchronous systems; random and deterministic sequences; and binary and quadriphase systems. A point to remember when considering the novel analysis of chapter 3 is that characteristic functions could have been employed, rather than the direct approach used. The author made the choice arbitrarily, both are equally acceptable and have similar limitations.

Thus in summary, Pursley's standard Gaussian approximation best highlights some important properties of codes to consider (and this will become clearer after the discussion on merit factors in section 2.2.1), but it is not suitable for the tests in this thesis which require the calculation of the PBE for small sets of deterministic sequences. This latter comment also applies to the techniques of Wu. A more accurate approximation (in the region of interest) is the one by Morrow and Lehnert, but this only applies to random sequences. However, several important techniques which bound the PBE extend this analysis to deterministic and then to non-binary sequences. These techniques are reviewed along with others in the next section, in order to identify other (additional to this section) important code properties, and to select a suitable method for accurately calculating the PBE for small sets of deterministic sequences.

2.1.2 Bounds On The PBE

Early work on determining the bit error probability in spread-spectrum systems was conducted by Yao [199]. Using a generalised moment of the multiple access interference and an isomorphism theorem from Game (or Moment Space) theory, Yao was able to relate the PBE to the generalised moment of the MAI. This theorem had been previously applied to bound the PBE in intersymbol interference problems. Yao derived expressions in [199] for the second, fourth, single exponential and multiple exponential moments, in terms of the partial crosscorrelations of the codes. The second moment is the variance of the MAI, as employed in the standard Gaussian approximation by Pursley which has been discussed in the previous section.

Yao found that the bounds for the first three moments were tight if the code length was long and the number of users small. For short codes or larger user numbers (subject to a constraint given below), the bounds were not necessarily tight. Only the use of the multiple exponential moment produced tight bounds for the PBE for most situations in which the method is valid.

Thus there are two main disadvantages with Yao's technique. Firstly, it is only suitable if the MAI is less than the signal strength. This is the constraint between the code period and number of users mentioned above. For example, Wu [197] showed that it could be applied to a maximum of 5, m-sequences of length 127, before the constraint was violated. Secondly, the complexity of Yao's technique increases rapidly as the number of codes (or users) increases.

The limitation that the total MAI must be less than the signal strength is also true of the method by Pursley, Sarwate and Stark [159], the companion paper of [49] discussed in the previous section. This approach used the convexity of the $\mathcal{Q}$-function to upper and lower bound the PBE integral (given later), by summations of terms of the $\mathcal{Q}$-function. It is therefore analogous to the Gauss Quadrature Rule approach of Wu. Although this technique was shown to be tighter than the second moment bound of Yao, its complexity also increased exponentially with the number of users. It was also remarked in this paper that this technique could be extended to consider quadriphase (or Q-CDMA) systems.

The constraint that the total MAI must be less than the signal strength, is the reason why the two methods above have not been employed in this thesis. Whilst the tests in

this thesis only consider small user numbers, Wu's example suggests that the criteria is too restrictive. Alternatives without this constraint do exist, and these are now discussed. Dou and Milstein's method [31] for binary codes for example, can be used without the restriction that the total MAI remain less than the signal strength. It also upper and lower bounds the PBE integral by summations of $\mathcal{Q}$-functions in a manner similar to the approach above.

Gauss Quadrature Rules were also applied by Laforgia, Luvison and Zingarelli [99], but their technique required evaluation of the higher order moments of the multiple access interference. A large number of moments were required for reasonable accuracy, even with small numbers of users and small code periods. The literature often regards the evaluation of the higher order moments of the MAI as a drawback of such a technique, because of the large amount of computation required in their calculation, but Laforgia et. al. presented computationally efficient algorithms to calculate these. This paper was also perhaps one of the first to present bounds on the PBE for QPSK, OQPSK and MSK, as well as binary spread-spectrum systems. The results of this paper have been discussed in section 1.3.1. This technique could have been applied in this thesis, but the discussion below leads to a discussion on the technique the author considered the most appropriate.

In 1987 in relation to random binary sequences, Lehnert and Pursley [108] developed a new approach to the bounding of the PBE. This was an important paper in the development of some later techniques, particularly the one which is employed throughout this thesis. Rather than obtain upper and lower bounds by replacing the integral involved in calculating the PBE by a summation of terms (numerical integration), the technique of this paper bounded the probability density functions (PDFs) of the code-pair interferences. Upper and lower bounds on the PBE were then obtained via the upper and lower bounds on the PDFs. An advantage of this technique was that its complexity was polynomial rather than exponential.

Lehnert and Pursley's technique was extended to consider deterministic binary sequences by Nazari and Zeimer in 1988, [130]. Instead of bounding the PDF, their approach bounded the cumulative density function (CDF) of the MAI. This technique clearly highlights the importance of considering not only correlation values, but also the

adjacent pairs of values. This is in agreement with the properties Pursley's standard Gaussian approximation emphasizes, and it is not unexpected given that the continuous-time (CT) crosscorrelation can be expressed in terms of the values and adjacent pairs of values of the discrete-time (DT) crosscorrelation. Nazari and Zeimer's paper also provides a very clear explanation on obtaining the upper and lower bounds on the PBE from the CDF of the MAI. It also rigorously proves that their approach does provide upper and lower bounds on the PBE. To digress slightly, Lehnert also extended his approach to consider deterministic sequences in 1989 in [106].

The extension of Nazari and Zeimer's analysis to non-binary CDMA systems was made independently by Hsu and Lehnert [68], and Özlütürk and Lam [136], in conference papers in 1990. Özlütürk and Lam initially considered the non-binary spread-spectrum system of this thesis and then in later research applied this to M-ary data modulation, and non-coherent and trellis coded modulation systems [102, 100, 137, 138]. This research has been discussed in section 1.3.1. Hsu and Lehnert's original work considered the generalised QPSK signal formats, i.e. QPSK, OQPSK and MSK. Other publications by them in relation to this include [69, 70]. For the sake of brevity, this technique will be referred to as Özlütürk and Lam's, as this was the only one that the author of this thesis was aware of until Hsu and Lehnert's 1990 paper was highlighted by a reviewer. The reader is reminded however that the technique was developed independently by both sets of authors.

It is this technique, because of its accuracy and direct applicability to the Q-CDMA system, that is applied in this thesis whenever an accurate indication of the bit error probability is required for a set of deterministic sequences. In summary, their technique obtains an expression for the CDF of the total MAI. This is derived from the conditional code-pair interferences and hence is analogous to Morrow and Lehnert's conditional Gaussian approximation to the PBE (discussed in the previous section), the accuracy of which is considered very good for the region of interest.

The average probability of bit error P_e, for BPSK data signalling and a quaternary code alphabet $\{\pm 1, \pm j\}$, is given by equation 2.5 [101, Eq. 2.10]:

$$P_e = \int_{-\infty}^{\infty} f_I(z).\mathcal{Q}\left(\sqrt{\frac{2E_b}{N_o}}\left(1 - \frac{z}{N}\right)\right).dz \tag{2.5}$$

where $f_I(z)$ is the probability density function (PDF) of the MAI. Assuming mutual

independence between all code-pair interferences, the PDF of the MAI is the $(U-1)$-fold convolution:

$$f_I(z) = (f_{I_{2,1}} \star f_{I_{3,1}} \star \ldots f_{I_{U,1}})(z) \tag{2.6}$$

The unconditional PDF of $I_{u,1}$ is related to the PDF of the code-pair interference, conditional on delay and even or odd periodic correlation, as follows:

$$f_{I_{u,1}}(x) = \frac{1}{2N} \sum_{\overline{\phi}=\phi,\widehat{\phi}} \sum_{l_u=0}^{N-1} f_{I_{u,1}|l_u,\overline{\phi}}(x|l_u,\overline{\phi}) \tag{2.7}$$

If the code-chip pulse is rectangular, then Özlütürk and Lam [101] show that:

$$f_{I_{u,1}|l_u,\overline{\phi}}(x|l_u,\overline{\phi}) = \int_0^1 \frac{1}{\pi\sqrt{r^2-x^2}}.d\delta \quad |x| < r \tag{2.8}$$

where

$$\begin{aligned}
r &= \sqrt{E + F.\delta + G.\delta^2} \\
A &= \mathcal{R}e\{\overline{\phi}(l_u)\} \quad B = \mathcal{R}e\{\overline{\phi}(l_u+1)\} \\
C &= \mathcal{I}m\{\overline{\phi}(l_u)\} \quad D = \mathcal{I}m\{\overline{\phi}(l_u+1)\} \\
E &= A^2 + B^2 \\
F &= 2A(B-A) + 2C(D-C) \\
G &= (B-A)^2 + (D-C)^2
\end{aligned}$$

Expressions for the conditional cumulative density function (CDF) of $I_{u,1}$, $F_{I_{u,1}|l_u,\overline{\phi}}(z)$, for all values of the variables A to G are derived in [101].

Having derived an expression for the unconditional CDF of the MAI, $F_{I_{u,1}}(z)$, the PBE can be bounded as discussed below (a summary of [130, 101] based on the original proposal in [108]). Let $[-\sqrt{2}S, \sqrt{2}S]$ denote the maximum range of the PDF of $I_{u,1}$ and define $\Delta = 2\sqrt{2}S/M$ for some even (for convenience) integer M. The CDF of $I_{u,1}$ is then sampled at the locations $z_i = (i - M/2 - 1)\Delta$ for $i \in [1 \ldots M]$. A round-down PDF of $I_{u,1}$ can then be obtained by moving the probability mass of $I_{u,1}$ in (z_i, z_{i+1}) to an impulse of strength $F_{I_{u,1}}(z_{i+1}) - F_{I_{u,1}}(z_i)$ at z_i. Similarly for the round-up PDF, the impulse is located at z_{i+1}. Once the round-down and round-up PDFs of $I_{u,1}$ have been obtained, the round-down and round-up PDFs of the total MAI can be obtained by a discrete convolution. The resultant will be a PDF of $(U-1)(M-1)+1$ impulses

of strength $P_I(k)$ located at $z_k = (k-(U-1)M/2-1)\Delta$ for the lower bound, and at $z_k^{'} = (k-(U-1)(M/2-1)-1)\Delta$ for the upper bound, where $k \in [1 \ldots (U-1)(M-1)+1]$. Since $\mathcal{Q}$ is a monotonically decreasing function the PBE can then be bounded as given below:

$$\sum_{k=1}^{(U-1)(M-1)+1} P_I(k).\mathcal{Q}\left(\sqrt{\frac{2E_b}{N_o}}\left(1-\frac{z_k}{N}\right)\right) \leq P_e \tag{2.9}$$

$$P_e \leq \sum_{k=1}^{(U-1)(M-1)+1} P_I(k).\mathcal{Q}\left(\sqrt{\frac{2E_b}{N_o}}\left(1-\frac{z_k^{'}}{N}\right)\right) \tag{2.10}$$

Whilst techniques which bound the probability of bit error are accurate and highlight the importance of some code properties, they generally do not give a good insight into the relative importance of different code properties and hence how codes should be designed. It could be suggested that to gain such an insight, one should just conduct tests with actual sets of sequences using these approaches. Conclusions on the importance of different code properties could then be based on the results. However if test are conducted in this manner, then one must consider the influence of code phase on the results. The next section discusses and investigates code phase.

Several criteria have been proposed in the literature (mainly as a result of Pursley's standard Gaussian approximation), to select an optimal code phase, but there is no consensus as to which is the most suitable. Further, these criteria employ different merit factors (i.e. emphasize different correlation features), thus if the optimal code phase can be identified, so a preliminary understanding of which correlation features should be given greater emphasis can be obtained. Section 2.2.1 therefore discusses in detail merit factors and criteria for selecting the optimal code phase. Section 2.2.2 then conducts tests on a selection of quaternary codes using the accurate bounding technique of Özlütürk and Lam (reviewed above) in order to determine which criteria (and hence correlation features) should be emphasized. As the discussion in section 2.3 shows however, the results of section 2.2.2 lead to further research on this issue in chapter 3.

2.2 The Influence Of Code Phase On Performance

In the previous section, techniques for determining the performance of a spread-spectrum system have been reviewed. This review highlights the importance of considering not only the peak crosscorrelation of codes, as discussed in the Introduction,

but the occurrence frequencies of the discrete-time (DT) correlation values and the occurrence frequencies of adjacent pairs of DT correlation values, for both even and odd periodic and hence aperiodic correlation.

To develop new code generation techniques, or evaluate existing techniques, the designer requires a thorough understanding of how code properties (correlation features), relate to and influence performance, hence the research question: "What is the relative importance of different code properties on performance?" This then determines which factors are the most important when designing or selecting codes, and which features should be used to compare different code families.

One solution to the research issue, and the commonly employed solution when comparing code families, is to conduct tests with subsets of actual codes. The difficulty with this approach is that there are many factors which can influence performance and it is difficult to maintain control over all of them. The phase of the code, for example, can make drawing conclusions on code properties difficult for the asynchronous environment. This section therefore investigates the influence of the code phase on performance.

Definition 2.2.1 *Code Phase* - *The initial starting point c_0 of the periodic sequence*

$$c = (c_0, c_1, \ldots, c_{N-1})$$

Aperiodic and odd periodic correlation are influenced by the phase of the code, whilst the even periodic correlation is not. In an asynchronous environment, assuming a random binary information sequence, both even and odd periodic correlation are equally important to performance. Thus as the odd periodic correlation varies with the code phase, so will the performance (or PBE) of the system, and this is shown by an example in section 2.2.2.

As mentioned previously, several criteria have been proposed to optimise the code phase, but the literature is not clear as to the most suitable criteria. Many of the criteria were developed from Pursley's standard Gaussian approximation (reviewed in section 2.1.1), and as part of the criteria merit factors are employed. Merit factors emphasize different features of the crosscorrelation spectrum to consider, and the peak value is of course a simple merit factor. However, approximations are often made so that a merit factor may be more easily calculated. Such approximations may include

the use of the Cauchy or Triangle inequalities and therefore whilst the approximations may be accurate in some cases, they can be inaccurate in others. Thus to investigate the influence of code phase on performance, criteria for selecting the code phase must first be reviewed.

Identifying the relative importance of the different criteria, and particularly identifying the optimal criteria for selecting the code phase, therefore provides an insight into which merit factors should be emphasized, because the different criteria for selecting the phase highlight different merit factors. Merit factors and criteria for selecting the code phase are therefore reviewed in detail in section 2.2.1, and tests employing the different criteria are conducted on subsets of codes in section 2.2.2. Finally, it should also be noted that merit factors are often used to select subsets of codes or to compare different code families, because they require substantially less computation than the calculation of the PBE does. This is another reason for their investigation.

2.2.1 Merit Factors

Merit factors are used in spread-spectrum theory to compare code families, select subsets of codes, and to select the phase of the code so that the performance may be optimised. The criteria commonly employed to select the code phase are:

- Least Sidelobe Energy/ Auto-Optimal (LSE/AO) [156]
- Auto-Optimal/ Least Sidelobe Energy (AO/LSE) [156]
- Minimum, Mean-Square Crosscorrelation (MSC)
  or Average Interference Parameter (AIP) [150, 158, 168, 157, 154, 156, 170, 56]

The first two are employed the most in the literature for selecting the phase of a code, the third occasionally and the last infrequently. The reasons for this will become clear in the following discussion, where the above terms are defined for codes a and b.

Definition 2.2.2 *Sidelobe Energy*

$$SE_a = 2\sum_{l=1}^{N-1} C_a(l).[C_a(l)]^\star \quad as\ C_a(-l) = [C_a(l)]^\star. \tag{2.11}$$

Sidelobe energy is a measure of the variance of the out-of-phase discrete-time autocorrelation values and analogously, the mean-square crosscorrelation is a measure of the variance of the aperiodic crosscorrelation values. Sidelobe energy may be defined either with or without the factor of 2 shown in equation 2.11. In this thesis, when the sidelobe energy of the aperiodic autocorrelation is calculated (for example section C.4 of appendix C), the factor of two has been included, as it highlights that the aperiodic correlation is calculated over the delays $(1-N)$ to $(N-1)$ and it shows the analogy with the MSC better. When the sidelobe energy of the even or odd periodic autocorrelation is calculated however, the factor of two is not included. Similarly the MSC in those cases is only calculated over the delays 0 to $N-1$. This discussion is important as some of the original papers for the latter equations define the sidelobe energy of the aperiodic autocorrelation without the factor of 2. Those equations have been suitably modified here for consistency in this thesis.

Definition 2.2.3 *Mean-square crosscorrelation*

$MSC = \mu_{a,b}(0)$ *where*

$$\mu_{a,b}(k) = \sum_{l=1-N}^{N-1} C_{a,b}(l)[C_{a,b}(l+k)]^{\star} \tag{2.12}$$

The importance of the MSC can be seen in Pursley's Gaussian approximation to the PBE, equation 2.1 of section 2.1.1. The calculation of all of the mean-square crosscorrelations, from equation 2.12, between codes in a family involves substantially more computation than the calculation of all of the sidelobe energies of the codes in the family. However, Sarwate and Pursley showed [158, Eq. 5.24] that the MSC can be rewritten in terms of the autocorrelations of the code sequences:

$$\mu_{a,b}(k) = \sum_{l=1-N}^{N-1} C_{a}(l)[C_{b}(l+k)]^{\star} \tag{2.13}$$

This equation substantially reduces the amount of computation required to calculate the MSC as discussed in [171].

The mean-square (aperiodic) correlation given above can also be expressed [156] in terms of the mean-square (even) and mean-square (odd) correlations. An examination of the tabular correlation values given in chapter 5 verifies this equation.

$$\sum_{l=0}^{N-1} |\phi_{a,b}(l)|^2 + \sum_{l=0}^{N-1} |\widehat{\phi}_{a,b}(l)|^2 = 2 \sum_{l=1-N}^{N-1} |C_{a,b}(l)|^2 \tag{2.14}$$

Sarwate and Pursley also showed [158, Eq. 5.26] that by applying the Cauchy inequality to the following equation:

$$\sum_{l=1-N}^{N-1} |C_{a,b}(l)|^2 = N^2 + 2\mathcal{R}e\left\{\sum_{l=1}^{N-1} C_a(l).[C_b(l)]^\star\right\} \tag{2.15}$$

bounds on the MSC could be obtained in terms of the sidelobe energy.

$$N^2 - \sqrt{\mathrm{SE}_a\mathrm{SE}_b} \leq \mathrm{MSC}_{a,b} \leq N^2 + \sqrt{\mathrm{SE}_a\mathrm{SE}_b} \tag{2.16}$$

Similar relations can be found if even or odd periodic correlation replaces aperiodic correlation in the MSC and SE equations.

Thus by minimising the sidelobe energy, the bounds on the mean-square crosscorrelation can be made tight. This is the underlying principle of the least sidelobe energy (LSE) criteria. O'Farrell discussed in [134] how this would not always provide good performance, and subsequently proposed the following criteria:

- Maximum Sidelobe Energy/Auto-Optimal (MSE/AO)

This criteria ensures that the lower bound on the MSC is as low as possible and subsets of codes can then be found which have lower MSC values than those of the LSE phase. If the Gaussian approximation of Pursley is then used to determine the PBE, it can be seen that the MSE phase subset will provide better performance than the LSE subset. A minor disadvantage with the MSE algorithm is the need to sort the codes before selecting the subset, but efficient algorithms exist for this. However, if the entire code family is being considered, the LSE criterion is more important than MSE, as all codes then have a smaller range of MSC values and hence the variation in performance is smaller when different codes are considered.

The least or maximum sidelobe energy phase of a code is not necessarily unique. Massey and Uhran [117] therefore introduced the additional criterion of an auto optimal (AO) phase.

Definition 2.2.4 *Auto Optimal* - *The code phase such that the peak out-of-phase odd periodic autocorrelation is minimised. This phase may not be unique, so the one for which the peak value occurs the least number of times is chosen.*

This phase is important for simple multipath channels where it is desirable to minimise the sidelobes of the autocorrelation. The odd periodic autocorrelation is considered

because even periodic autocorrelation is independent of the phase of the code. The auto-optimal code phase may not be unique either, although in combination with the MSE or LSE phase the resultant generally is.

The selection of AO/LSE or LSE/AO generally depends upon whether multipath propagation, or multiple access interference is perceived as having the greater degradation on performance. The criteria AO/MSE is also worth consideration if subsets of codes are employed. This criteria has not previously been proposed in the literature, but it is a trivial extension of O'Farrell's proposal.

The final merit factor referred to above is the average interference parameter (AIP).

Definition 2.2.5 *Average Interference Parameter*

$$AIP = r_{a,b} = 2\mu_{a,b}(0) + \mathcal{R}e\{\mu_{a,b}(1)\} \tag{2.17}$$

The average interference parameter (AIP) was derived in Pursley's Gaussian approximation to the PBE (discussed in section 2.1.1), and is a component of the average SNR another merit factor used by Pursley and commonly used in the literature to compare subsets of codes. The definition of the AIP is dependent upon the code-chip pulse shape, and the above definition is for a rectangular pulse shape. If the code-chip pulse shape is sinusoidal, as for MSK spread-spectrum, then [152] defines the AIP as:

$$\text{AIP}_{MSK} = \frac{(15+2\pi)}{12\pi^2}.\mu(0) + \frac{(15-\pi)}{12\pi^2}.\mu(1) \tag{2.18}$$

Clearly the AIP is dependent on the mean-square crosscorrelation, but not only does it consider the occurrence frequencies of the discrete-time crosscorrelation values, but also the occurrence frequencies of the adjacent pairs of values. Pursley and Garber [154] also related the AIP to the mean-square difference, a parameter often employed in RADAR systems where spread-spectrum also finds application.

In summary therefore, the review of merit factors has highlighted different criteria, or features of the crosscorrelation spectra that should be considered when designing or evaluating spreading codes. The reader is reminded of the discussion in the Introduction on the desired code properties, and in particular the inadequacy of the definition of the correlation properties. Consideration must clearly be given to the MSC and AIP to better define this.

In the next section, section 2.2.2, the PBE of a subset of different codes is calculated with each of the different criteria for selecting the code phase: LSE/AO, AO/LSE, MSE/AO, AO/MSE, minimisation of the AIP, and minimisation of the MSC. The reason for this is to identify, if possible, an order of importance of the different criteria, which then identifies an order of importance of the merit factors: sidelobe energy, peak value, MSC and AIP, since they comprise the phase selection criteria. Certainly the discussion in this section suggests an order, especially if Pursley's standard Gaussian approximation is used to calculate the PBE, but there is the question of the accuracy of the Gaussian approximation (see section 2.1.1), and the Cauchy and Triangle inequalities. The tests in section 2.2.2 therefore use the accurate bounding technique of Özlütürk and Lam (see section 2.1.2), to compare the criteria and give an indication of the relative importance of each, something the discussion in this section cannot provide.

2.2.2 Variation In Performance

This section illustrates the influence of code phase on the performance of the system by testing the different criteria for selecting the code phase on a subset of sequences. Özlütürk and Lam's accurate technique for bounding the PBE has been employed in the tests and the sequences are random quaternary codes. The codes were generated by a computer program[1] which simulates the tossing of fair q-sided dice. These codes have been employed so as to avoid any potential bias in the results which may have occurred if a specific code family had been employed (i.e. many commonly used code families have well defined correlation properties and relationships).

To digress slightly, whenever tests are conducted in this thesis they generally employ codes of period $N = 63$. There are several reasons for this: Firstly, maximal-length codes are defined in chapter 4 as those with a period of $N = q^m - 1$, for the q-ary alphabet and where m is an integer. Thus 63 is a length consistent with this. Many code generation techniques produce codes of this period hence the comparison is easier, and fairer because the PBE of the system is strongly dependent upon the period of the codes. Secondly, the selection of the code period must be sufficiently large to provide meaningful results without requiring excessive computation times for analysis programs, and in the author's

[1] A modification to the algorithm *ran0*, given in [149, p.216], to generate uniformly distributed integer [0..3] values, and map these values to $\{\pm 1, \pm j\}$.

opinion 63 is a suitable length for this. Finally, Chan and Lam commented [22, p.540] that *"... commercially available parallel correlation-type receivers can only handle from 8 to 64 chips simultaneously. Thus the period of spreading sequences is limited to a small number in practice."* This is also consistent with the choice of 63 as the code period.

Returning to the examination of variations due to code phase, figures 2.1 and 2.2 for $U = 5$ and $U = 10$ users, provide three important conclusions.

Conclusion 2.2.1 *There is no single optimal criteria when LSE/AO, AO/LSE, MSE/AO and AO/MSE are considered.*[2]

That is, in figure 2.1 the LSE/AO phase has the worst performance, then AO/LSE and AO/MSE which both have similar performance. The MSE/AO phase selections are the best of these four criteria. In figure 2.2 however, the MSE/AO phase is now the second worst selection after the LSE/AO phase. The AO/LSE and AO/MSE phases still have a similar level of performance. Thus it is not possible to conclude that any of these four criteria is the optimal choice of phase selection in the multiple access environment, or to determine the order of their importance. The LSE/AO phase is the worst in both tests here, but it would not be difficult to find another subset of codes which perform better with the LSE/AO phase than the MSE/AO phase. The discussion on O'Farrell's development of the MSE/AO criteria shows that this statement is true. The results of Kärkkäinen and Leppänen in [80] for binary sequences support the conclusions above:

> *"It was found that use of AO/LSE and LSE/AO phase optimisation criteria did not give any significant advantage in decibels as compared to randomly selected sequence phases, as the criteria do not minimise crosscorrelation functions directly."*

Conclusion 2.2.2 *The minimum AIP phase is the phase most likely to ensure optimal performance, and the minimum MSC phase is only slightly worse in comparison.*

[2] A point to note with figures 2.1 and 2.2 is that the phase of each of the codes was adjusted to satisfy the LSE/AO, MSE/AO, and AO/LSE criteria, as these involve autocorrelations. In selecting the minimum or maximum MSC (and AIP) phase, the phase of the first code was fixed and that of the remainder varied. The results therefore show how the performance is influenced when a property of the code family is adjusted, rather than showing how the alteration of the phase of one code in the family influences its performance.

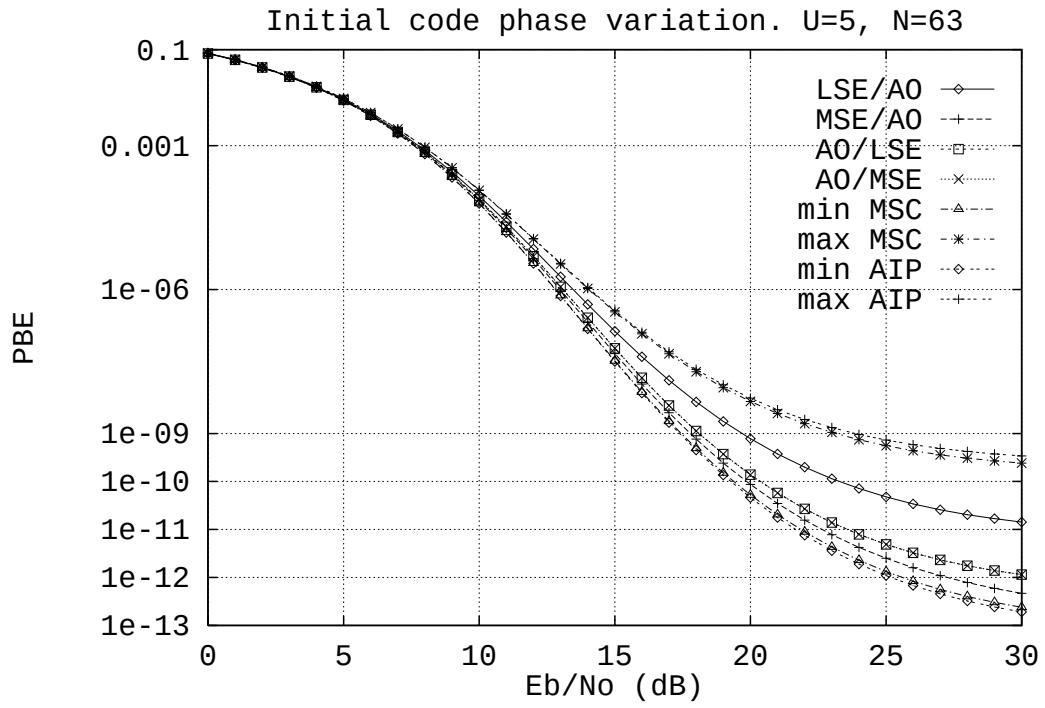


Figure 2.1: The influence of code phase. Five users.

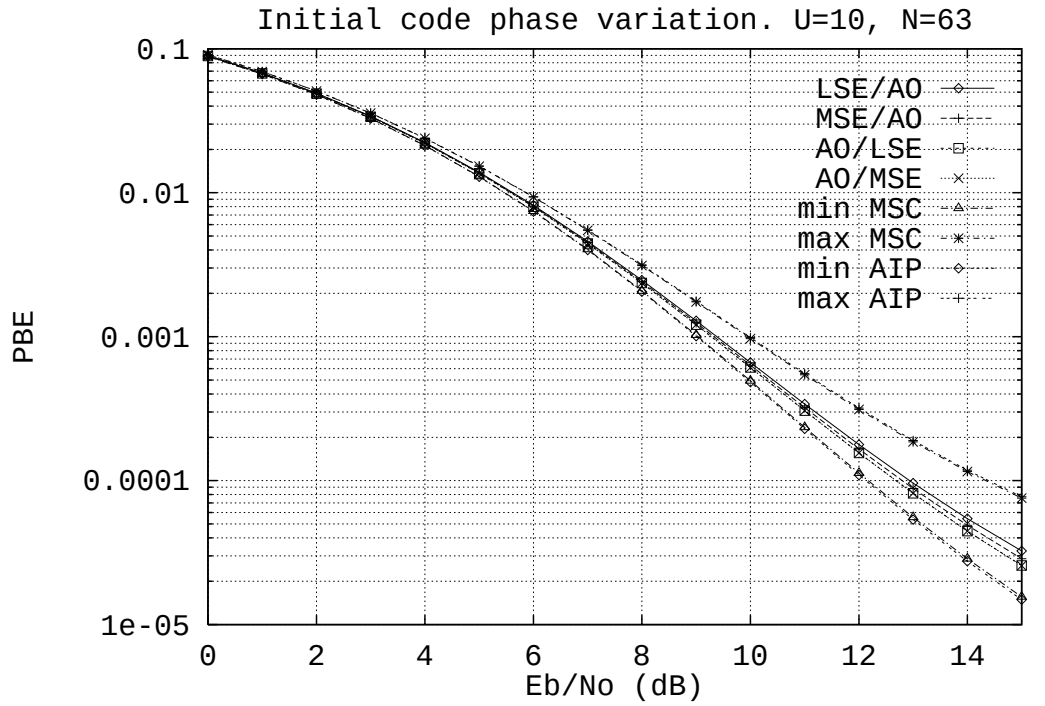


Figure 2.2: The influence of code phase. Ten users.

Figures 2.1 and 2.2 further show that minimising the average interference parameter provides the best performance in both cases, as this does directly minimise the cross-correlation functions, unlike the criteria involving the sidelobe energy. Minimising the MSC also results in a performance level which is only slightly worse than that for the minimised AIP curves. This is important as section 2.2.1 has discussed how the MSC can be computed with substantially less operations than the AIP. The AIP and MSC may therefore be regarded as important merit factors, certainly more so than the sidelobe energy for this situation. Conclusions cannot be drawn on the relative importance between the peak (odd periodic) crosscorrelation value and the sidelobe energy from these tests. The even periodic crosscorrelation is of course independent of the code phase.

The small difference between the AIP and MSC phases is consistent with the comments of Pursley and Sarwate [158, p.802]: *"For most applications, however, the approximation* $r_{x,y} \approx \tilde{r}_{x,y} = 2\mu_{x,y}(0)$ *is quite satisfactory."* The results of Kärkkäinen [77, 78, Table 1] for binary codes, which show that the percentage of $\mu(1)$ to $r_{a,b}$ tends to zero as N becomes large, also support the result here, as does an examination of the tabular values given in chapter 5. Furthermore, the expectation of $\mu(1)$, $\mathcal{E}\{\mu(1)\}$, is equal to zero, the proof of which for non-binary codes can be seen from equation 2.16 and [136, p.70], hence $\mathcal{E}\{\text{AIP}\} = 2\mathcal{E}\{\text{MSC}\}$, i.e. the average value of the AIP is approximately equal to twice the average value of the MSC, hence the minimised AIP and minimised MSC phases should provide a similar level of performance. Ideally a proof that the variance of $\mu(1)$ is small in comparison with $\mu(0)$ is also required to ensure that the MSC and AIP phases produce similar results, but the author of this thesis is not aware of any proof of this.

There is one further point to make in regard to the use of the AIP and MSC as merit factors. The reader may be concerned with their use since they were derived as part of Pursley's Gaussian approximation to the PBE, and section 2.1.1 has discussed that this approximation may not be accurate in the regions where the codes are the dominant influence on performance. However, the MSC and AIP were derived by considering the variance of MAI between two users, and hence derived directly from the interference expressions which are dependent on the crosscorrelations. The Gaussian approximation has therefore not been made at this stage of the analysis.

The MSC and AIP also relate to the second moment in Yao's bounding technique which is discussed in section 2.1.2. It is worth considering whether the higher order moments employed in Yao's paper [199], should be employed as merit factors. This has not been done, nor discussed in any prior literature. An examination of the fourth and exponential moments in Yao's paper shows however, that the moments depend only on factors analogous to $\mu(0)$ and $\mu(1)$, with both of equal importance. The previous results (and indeed those in chapter 5) have found $\mu(0) \gg |\mu(1)|$, hence it is not worthwhile considering these higher order moments as merit factors, as any improvement gained would be expected to be small in relation to the additional computation over the use of the minimum MSC phase.

One further conclusion can be drawn from Figures 2.1 and 2.2:

Conclusion 2.2.3 *The variation in performance (or the PBE) due to the variation in code phase can be significant.*

The large variation in the PBE for the maximum and minimum AIP (or MSC) phases shows that the influence of code phase can be significant for smaller user numbers and a higher E_b/N_o ratio, the region where the code properties have the greatest influence on performance. Pursley et. al. [159, 49] also observed large variations when maximum and minimum average SNR phases were employed in similar tests on binary sequences. Their results thus support the result here for non-binary sequences. Pursley et. al. also found that the difference between the maximum and minimum average SNR phases was greater if the code-chip pulse shape was sinusoidal rather than rectangular, but they did not provide an explanation as to why this was so. Section 3.2.3 explains why the variation should be greater for the sinusoidal code-chip pulse shape. Thus care must be taken when comparing code properties, subsets of codes, or code families from tests conducted on a selection of sequences, because if the phase of the codes is not considered then the conclusions are potentially subjective.

The results of this section have therefore provided three important conclusions, and these conclusions are important to different aspects of the research in this thesis. First, the conclusions assist in resolving the research issue of determining important code properties and their relative importance. Second, the conclusions are important for the research in chapter 5 which compares different code families and generation techniques.

These points are explained further in the next section which provides an overview of this chapter, but the discussions in later chapters best show the significance of these conclusions.

2.3 Discussion

The introduction to this chapter remarks that it serves several distinct but related purposes, and as mentioned previously, some of the conclusions are relevant for the research in later chapters. The conclusions are collected in this chapter however, because they all stem from the same topics or investigations, but they will be discussed again in later chapters. This section therefore provides an overview of the chapter to show how the issues relate and to explain the significance of the conclusions for later chapters.

In section 2.1 literature on different analytical techniques for determining the PBE of spread-spectrum systems is reviewed. Approximations are reviewed in section 2.1.1 and bounds on the PBE are reviewed in section 2.1.2. The review serves several purposes:

1. It provides an insight of important code properties to consider, from a system analysis viewpoint. Specifically, it helps to identify the desirable correlation properties of codes.

2. The review is also used to select the method (used throughout this thesis), of accurately determining the PBE of subsets of deterministic sequences. This method, which is referred to as Özlütürk and Lam's technique, is discussed in detail as part of the review. Furthermore, an aspect of their technique is also employed in the novel analysis developed in chapter 3.

In the development of approximations to the PBE several merit factors have been proposed. Merit factors are commonly used in the criteria to select an optimal code phase, and they highlight important code properties to consider. They may also be used to compare different code families; The peak value is an example of a merit factor commonly used for this second purpose. Section 2.2.2 therefore investigates code phase, because this is a property which can influence the PBE of the system. Section 2.2.1 reviews the different criteria for selecting the code phase and the associated merit factors.

The different criteria emphasize different merit factors (features of the crosscorrelation spectrum), thus if the order of importance and the relative importance of the different criteria is determined, so the same conclusions will apply to the merit factors (or correlation features), and this helps to determine the important code properties and their relative importance.

Section 2.2.2 therefore investigates the different criteria for selecting the code phase by conducting tests on a selection of sequences. The results lead to two important conclusions.

Conclusion 2.3.1 *The minimum AIP phase is the code phase most likely to ensure the best performance, and the minimum MSC phase is a close approximation to this. Criteria minimising the sidelobe energy do not necessarily improve performance.*

This conclusion is relevant to the first research issue of the thesis on determining important code properties and their relative importance. It shows that the AIP highlights important features of the crosscorrelation spectrum to consider, and that the MSC is a dominant component of the AIP. These conclusions are supported by the results for binary sequences discussed in section 2.2.2.

Conclusion 2.3.2 *The variation in performance (PBE) due to the variation in code phase can be significant.*

This second conclusion is important not only in regard to investigating code properties, but also to how code families should be compared (in chapter 5). To explain further, if two sets of codes with different peak values are compared and the codes have arbitrary phases, then it is not possible to conclude in an unsubjective manner which set of codes is the best, and hence how important the peak value is (i.e. the choice of different code phases would not alter the peak even periodic crosscorrelation value, but it would alter performance and thus perhaps the result). The reader may also recognise that this is how many code families are compared in the literature (i.e. by a single merit factor, usually the peak even periodic crosscorrelation value), and that it is not a sufficient comparison.

Another manner in which code families (or codes with different peak values for example) could be compared is by conducting tests on subsets of sequences and comparing their PBE. Conclusion 2.3.2 above shows that if this approach is to be employed then:

1. The code phase must be suitably chosen so that it does not influence the results (on how important the peak value is, or which set of codes is the best). The results suggest that the minimum AIP phase is the most appropriate.

2. The conclusion of which set of codes is the best, or if a property is important or not, only apply to the situation considered. Generalisations should be made with the utmost care because other code selections may provide different conclusions.

Comparing code families, or determining if a property is important (in general, not for the specific situation tested), is therefore difficult and potentially subjective if tests involving actual sequences are conducted, because there are many factors which can influence performance and it may not be possible to control or understand the influence of the different factors.

To overcome the first part of the problem, whenever comparisons are made between different code families (in chapter 5), the PBE is compared for the minimum (and maximum) AIP phases and it is stressed that the conclusions only apply to that specific situation. Chapter 5 explains this further and shows that it is an acceptable approach to meet the requirements in that chapter. Before considering the second part of the problem one final remark on code phase is made. It could be suggested that the variation in code phase should be averaged out but this is not feasible, because in a system of U users with codes of period N there are N^{U-1} combinations of phase to consider.

To overcome the second part of the problem the next chapter develops a novel analytical approach to investigate code properties. The method does not employ actual sequences and therefore eliminates the need to consider variations caused by code phase on the results. It also provides a better understanding of how different factors influence the performance. Amongst other properties, the technique is used to investigate the peak and mean-square values and resolve the importance of these. This is because as the Introduction and chapter 4 discuss, spreading code designers concentrate on the peak value, but the system analysis suggests that the mean-square value or AIP should be emphasized. The next chapter therefore completes the investigation of the first research issue: the determination of important code properties and their relative importance.

Chapter 3

The Influence Of Code Properties On Performance

Whilst much research has been conducted on evaluating the bit-error probability of spread-spectrum systems, this does not provide a good insight into how to design codes. The techniques for random codes are often used to provide an initial system design to indicate the tradeoffs between system parameters (code period, PBE, number of users and E_b/N_o ratio). The paper by Geraniotis and Ghaffari [48] considers random codes for the following reasons[1]:

> *"First, random signature sequences are often used in an attempt to match certain characteristics of extremely complex signature sequences with a very long period. Second, random signature sequence models may serve as substitutes for deterministic models when the communications engineer is given little or no information about the structure of the signature sequences to be used in the system. Finally, in cases where the number of active users is very large, the required computational effort for evaluation of the conditional error probability — given the number of interfering users — may become prohibitive when different deterministic sequences are used by the different users."*

Random code models do not provide the code designer with an insight into properties to consider, or how to select subsets of codes from a code family.

[1] Minor grammatical corrections have been made to the quote.

Analytical techniques for deterministic sequences, although highlighting some code properties to consider (more specifically features of the crosscorrelation spectra), do not always give an indication of the relative importance of different factors, such as whether the peak or mean-square crosscorrelation is more important. The results of the previous chapter also show that determining the relative importance of code properties (or features of the crosscorrelation spectra) on performance is potentially subjective if tests are conducted with actual codes. This is because it is difficult to control or understand the influences of all the different factors on performance. The variation due to some factors such as code phase can be significant.

The code designer therefore requires a model between these two extremes. The model needs to eliminate the variance in the PBE which can be caused by the choice of the phases of the codes, but it must be more accurate than models for random codes so that the variation in the performance (PBE) can be observed as a property of the codes (or a feature of the crosscorrelation spectrum) is varied.

A model of this nature, and the associated system analysis has been developed by this author and published in [163] and [162]. Section 3.1 and 3.2 of this chapter further refine the research of those listed publications, resolving some important research issues which had been posed but not investigated at the time of publication. The reader should note that the conclusions drawn from the novel analysis in this chapter are more important than the model and analysis on which they are based.

Section 3.3 develops some additional novel analysis to relate the randomness and correlation properties of codes. Whilst only approximate, it does help to unify these properties, which although conceptually related are often treated as independent entities in the literature.

The conclusions drawn from the investigations in sections 3.2 and 3.3 have important ramifications on the code design philosophy. Section 3.4 shows the significance of the conclusions drawn from the research in those sections, and it also shows the significance of some of the conclusions at the end of chapter 2.

3.1 Analysing System Performance: Virtual Codes

The need to develop a model between the one used for random codes and accurate ones for used deterministic codes, has been recognised in the introduction to this chapter. The purpose of the model is to allow the variations due to one code (or correlation) property on performance to be observed, whilst maintaining control over others. The conclusions drawn from the analysis will then help to identify the relative importance between code properties. This understanding is important when considering how to design codes, or for comparing different code families. To develop this model the abstract concept of a virtual set of codes is introduced, and the system analysis for this developed.

Definition 3.1.1 *Virtual Set of Codes*

A set of codes, that may or may not exist, which satisfy a defined set of properties.

A virtual set of codes is a set of codes which satisfy specific code properties. Their generation method is not defined, but because their properties have been defined, the influence of one factor on performance (such as the peak value), can be observed whilst maintaining control over others (such as code phase).

The classic example of a set of virtual codes is the *ideal* (or truly *random*, orthogonal) set. The autocorrelation function of each of the codes in the set is a delta function, and the crosscorrelation function between each pair of codes in the set is the zero function. This set does not exist (it violates the Welch bound given in section 3.4), but a virtual set of codes could equally well be defined to satisfy less restrictive criteria, such as having:

- a three-valued crosscorrelation spectra, or
- a specified mean-square crosscorrelation value.

A set of Gold codes satisfy the first criteria and a search of random codes (generated by the dice tossing analogy), could produce a set satisfying the second.

In this thesis, the properties which are defined for the virtual set of codes are:

- the code alphabet is quaternary $\{\pm 1, \pm j\}$ and
- the probability density functions (PDF) of the real and imaginary, even and odd periodic continuous-time (CT) crosscorrelation spectra, are specified.

Several different mathematical methods could be employed to determine the PBE once the PDFs have been appropriately defined. In the theory here, the analysis operates on the PDFs directly (with suitable coordinate transformations), to obtain an expression for the cumulative density function (CDF) of the total multiple access interference (MAI). An alternative approach, as employed in some of the techniques reviewed in section 2.1 of chapter 2, would have been to use the characteristic functions of the PDFs. This was the approach taken by Cowl, Squires and Shafi in [28], which the author of this thesis became aware of after the publication of these ideas in [163, 162]. Cowl et. al. only considered binary codes, and the emphasis in their paper was on features of the channel: multipath and fading, not features of the codes. The important issue however, is the expression for the CDF of the MAI, the manner in which it is obtained is less important.

Once an expression for the CDF of the MAI has been derived, the technique reviewed in detail in section 2.1.2 for bounding (or more precisely bounding the approximation to) the PBE can then be utilised. A simple example to illustrate the analysis is given in section 3.1.1. The example although simple, is not without merit, as discussed in section 3.1.2.

3.1.1 Example - Symmetric Uniform PDF

The analysis for a virtual set of codes is illustrated in this section by way of a simple example: all of the relevant probability density functions (PDFs) are assumed to be uniform. The example is not without merit, and it will be employed in section 3.2 to draw conclusions on the relative importance of different correlation features. The discussion in section 3.1.2 will also show that if the analysis is modified to consider asymmetric, stepped PDFs that contain spikes at discrete locations, then the method could provide an accurate (bounded) approximation to the bit-error probability of a deterministic set of codes. However, the reader is reminded that the technique has not been developed for that purpose. It has been developed to allow conclusions to be drawn on the relative importance of different code properties, without the results being influenced by the choice of code phase. Some of the techniques reviewed in section 2.1 are far more amenable if an accurate determination of the PBE of a set of actual codes is required.

Example 3.1.1 *Symmetric Uniform PDF*

The real and imaginary components for both the even and odd periodic continuous-time crosscorrelation between a pair of codes, have a PDF which is uniform over the region $[-S, S]$ *and zero outside of that region.*

In section 1.2 of chapter 1, the contribution of the normalised code-pair interference to the receiver's decision statistic is given (equation 1.8) as:

$$I_{u,1} = \mathcal{R}e\{\overline{\phi}_{CT}(\tau_u).\mathrm{e}^{j\theta_u}\} \tag{3.1}$$

where

$$\theta_u = \xi_u - \omega_o.\tau_u \tag{3.2}$$

with for a rectangular code-chip pulse shape,

$$\begin{aligned} \overline{\phi}_{CT} &= \overline{\phi}(l_u) + (\overline{\phi}(l_u+1) - \overline{\phi}(l_u)).\delta_u & (3.3)\\ l_u.T_c &\leq \tau_u \leq (l_u+1).T_c & (3.4)\\ \delta_u &= (\tau_u - l_u.T_c)/T_c & (3.5) \end{aligned}$$

Thus:

$$I_{u,1} = \overline{\phi}_{CT}^{\mathcal{R}e}.\cos\theta - \overline{\phi}_{CT}^{\mathcal{I}m}.\sin\theta \tag{3.6}$$

where $\overline{\phi}_{CT}$ is a convenient notation which expresses that the correlation is either even periodic (ϕ_{CT}) or odd periodic ($\widehat{\phi}_{CT}$), depending upon whether the two information bits impressed onto the received sequences spanning the despreading code are the same sign or different. The superscripts indicates the real and imaginary components of $\overline{\phi}_{CT}$, hence $\overline{\phi}_{CT}^{\mathcal{R}e} = \mathcal{R}e\{\overline{\phi}_{CT}\}$. A final point to note with equation 3.6 is that Krone and Sarwate define their initial signal phase (θ_u here) as the negative of equation 3.2. This explains why there is a negative in equation 3.6 above and not in the corresponding equations given by Krone and Sarwate [95, Eq. 13,14].

In [101, p.1608], Lam and Özlütürk showed that θ and τ may be regarded as independent if the carrier frequency ω_o is sufficiently large, which is true of any practical system. Pursley [152, p.159] proved the independence of θ and τ by an alternate means, whilst also showing that θ is uniform over $[-\pi, \pi]$ if ξ is uniform over $[-\pi, \pi]$ and ξ and τ are independent. The common assumption that ξ is uniformly distributed over $[-\pi, \pi]$ is acceptable, as Torrieri states [186], due to the instability of the oscillator.

Recognizing that $I_{u,1}$, $\overline{\mathcal{R}e}_{\phi_{CT}}$, $\overline{\mathcal{I}m}_{\phi_{CT}}$, and θ are all random variables, equation 3.6 may be rewritten as equation 3.7, with obvious associations for notational simplicity and where each random variable is shown in bold.

$$z = x\cos(\boldsymbol{\theta}) - y\sin(\boldsymbol{\theta}) = r\cos(\boldsymbol{\theta} + \boldsymbol{\varphi}) \tag{3.7}$$

where $r = \sqrt{x^2 + y^2}$ and $\boldsymbol{\varphi} = \arctan(y/x)$.

As discussed above, $\boldsymbol{\theta}$ is uniform over $[-\pi, \pi]$ and for this example the probability density function of x and analogously y is given by:

$$f_x(x) = \begin{cases} \dfrac{1}{2S} & |x| \leq S \\ \\ 0 & \text{otherwise} \end{cases} \tag{3.8}$$

Using these PDFs an expression for the cumulative density function (CDF) for the code-pair interference $F_z(z) \equiv F_{I_{u,1}}$ can be obtained. The derivations for these equations are provided in section A.1 of appendix A. That analysis, which differs from existing approaches, raises several issues concerning independence and conditional independence of different random variables. Section 3.1.3 discusses these independence issues in detail.

Once an expression for $F_z(z)$ has been obtained, Özlütürk and Lam's technique (reviewed in section 2.1.2) for obtaining bounds on the PBE can then be utilized to determine bounds on the approximation to the probability of bit-error P_e, which for a Q-CDMA system is given by equation 2.5 of chapter 2, repeated below:

$$P_e = \int_{-\infty}^{\infty} f_I(z).\mathcal{Q}\left(\sqrt{\frac{2E_b}{N_o}}\left(1 - \frac{z}{N}\right)\right).dz \tag{3.9}$$

where $\mathcal{Q}(.)$ is the Gaussian tail probability and $f_I(z)$ is the PDF of the MAI, which is the $(U-1)$-fold convolution between the PDFs of the code-pair interferences:

$$f_I(z) = (f_{I_{2,1}} \star f_{I_{3,1}} \star \ldots f_{I_{U,1}})(z) \tag{3.10}$$

3.1.2 The Probability Density Function Of The Continuous-Time Crosscorrelation Spectra

Example 3.1.1 of the previous section illustrates the analysis for a virtual set of codes for a mathematically simple case. The example is not without merit however, as the discussion in this section will show. Figure 3.1a shows as approximation to the PDF of $\phi_{CT}^{\mathcal{R}e}$, the real component of the even periodic crosscorrelation (figure 3.1b) between a pair of codes. The codes are the quaternary maximal-length sequences (expressed in polynomial form) $D^3 + 3.D^2 + 3.D + 3$ and $D^3 + 3.D^2 + 2.D + 3$. Chapter 4 provides an explanation of maximal-length sequences and their polynomial representation.

The form of the PDF in figure 3.1a is essentially uniform, hence the merit of example 3.1.1, because the basic form of the equations and integrals solved will be applicable to more realistic examples. The form of figure 3.1a will be discussed in greater detail shortly, but first it is best to clarify figure 3.1a so that the reader understands that it is a PDF in the true mathematical sense (its area is equal to one), but it is an approximation to the PDF of the continuous variable $\phi_{CT}^{\mathcal{R}e}$. Two additional points should also be made:

1. The PDFs shown in this thesis are for illustrative purposes only, they are not used in any numerical calculations.

2. For reasons explained in the next section (in regard to conditional independence), it is not possible to derive an expression for these PDFs unless the codes are assumed to be completely random. The results would then no longer apply to specific deterministic sequences as is required for illustration of the key points.

The Probability Density Function

Figure 3.1a was obtained by sampling the continuous-time (CT) crosscorrelation function $\phi_{CT}^{\mathcal{R}e}$ of figure 3.1b. Each sampled value of the CT crosscorrelation was then quantised with a quantisation step size of Δ_q. The sampling rate was sufficiently high to avoid aliasing. The quantisation step size (or number of quantisation steps) was chosen by trial and error in order to reduce the impact of quantisation error effects on the figure, given that the true form of the PDF was known in advance, as a latter discussion explains.

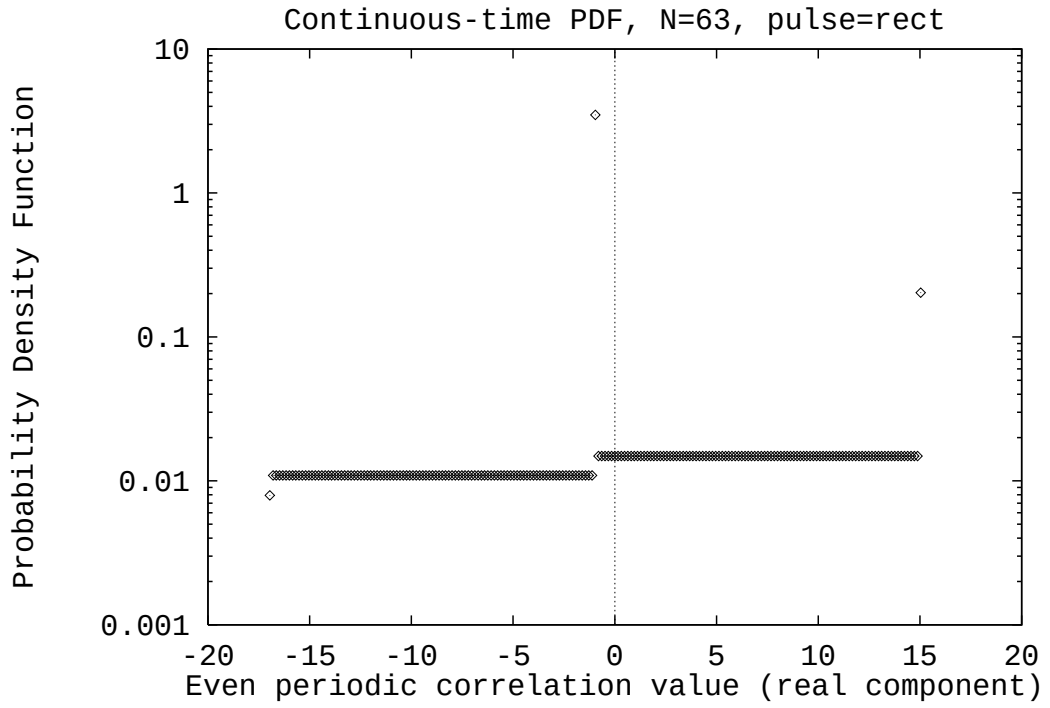


Figure 3.1a: Probability density function of the continuous-time crosscorrelation spectra.

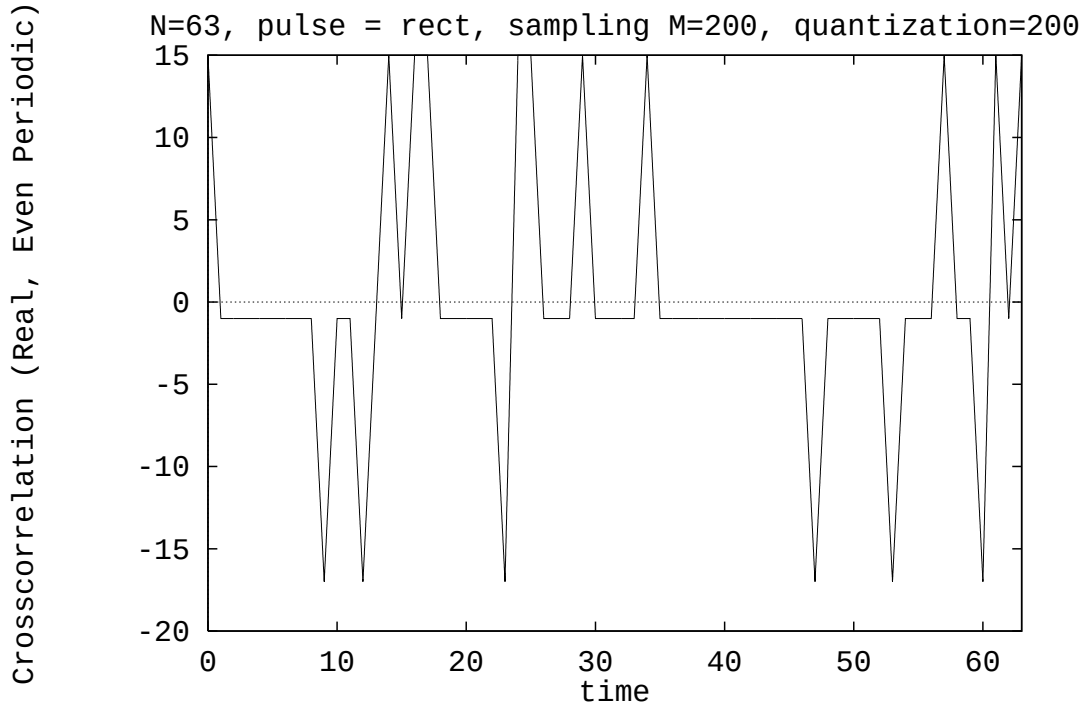


Figure 3.1b: Continuous-time crosscorrelation spectra.

The process of quantisation leads to the use of the term 'approximation' in regard to the PDF.

After sampling and quantisation, an occurrence frequency diagram (or histogram) of the (sampled and quantised) CT crosscorrelation values was produced. The reader may find it helpful to visualise this as analogue-to-digital conversion of the CT crosscorrelation spectrum. Connected to the output of the A/D converter are counters to record how many times each distinct digital output number occurs. This analogy will be extended shortly.

To convert the histogram, or occurrence frequency diagram into a continuous function (the PDF), an assumption needed to be made. The assumption was that the value at each quantisation step along the correlation axis, could be uniformly distributed over the quantisation interval, a reasonable assumption. Thus each discrete value in the histogram has been divided by the quantisation width in order to produce the approximation to the PDF. Note that this explains why the value in the PDF near the correlation value of minus one is greater than one; The discrete value is less than one as it has to be, but in distributing it over Δ_q (with $\Delta_q < 1$), the resultant is greater than one. The reader may again find it helpful to view this process in terms of digital to analogue conversion and the operation of a sample-and-hold circuit to reproduce the waveform. That is, each previously referred to counter (representing how many times a CT crosscorrelation value has occurred), is polled in turn, input to the D/A converter and the PDF constructed via the sample-and-hold circuit. Alternatively, this process may be viewed as the reverse of an aspect of the method used by Özlütürk and Lam to bound the PBE, the technique which section 2.1.2 describes in detail. The specific aspect of the method is the conversion of the continuous PDF to the probability mass impulses. The reverse process has been described above.

Figure 3.1a is therefore a PDF in the mathematical sense as it has an area equal to one, but it is an approximation because of the quantisation process and the assumption involved in converting the impulses at a point to a value over the range of width Δ_q.

The Significance Of The Simple Example

Figure 3.1a shows that the approximation to the PDF of the continuous variable $\phi_{CT}^{\mathcal{R}e}$ in figure 3.1b (a plot of the real component of the continuous-time even periodic crosscorrelation), consists of uniform regions and spikes. The term 'spike' is used fairly loosely and will be explained further shortly.

The shape of this PDF is easily explained by examining the continuous-time crosscorrelation spectrum of the two codes shown in figure 3.1b. Notice that the discrete-time crosscorrelation values are $-1, 15$ and -17. Consider first two values between, but not including minus one and fifteen. All of those values will occur the same number of times in the crosscorrelation spectrum. Hence the PDF is uniform between minus one and fifteen. Similarly it will be uniform between minus one and minus seventeen. The discrete-time crosscorrelation values occur a different number of times to those above however, and this causes the spike at those locations. The height of each uniform region and spike is determined by the occurrence frequencies (or discrete PDF) of adjacent pairs of the discrete-time crosscorrelation values, which is of course dependent on the occurrence frequencies of the discrete-time crosscorrelation values themselves. Thus as minus seventeen always occurs in isolation, a minus fifteen pair occurs only twice, and a minus one pair regularly, so the height of the spike for minus one is much greater than for minus fifteen, which is greater than for minus seventeen.

Thus the shape of the PDF for any continuous-time crosscorrelation spectrum can be obtained, given the discrete-time correlation spectrum and assuming a rectangular code-chip pulse shape. In section 3.2.3 a sinusoidal pulse shape is also considered.

The form of the PDF also means that the analysis for example 3.1.1 need only be modified to consider an asymmetric, stepped PDF that contains spikes at discrete locations to be applicable to actual codes. The extension to allow asymmetry is relatively straightforward, the only difference is that each integration quadrant (figure A.1 in section A.1 of appendix A) is no longer the same. Similarly the extension to consider stepped PDFs is also straightforward. The incorporation of spikes into the analysis although conceptually simple, is difficult in practice, not only with the direct approach given here, but also using characteristic functions and other methods.

Discussion of the term 'spike'

The term 'spike' is used loosely in the above discussion. In figure 3.1a the term spike refers to a uniform region of width Δ_q and height h which has a uniform region of a different height on both sides. Spikes only occur at values corresponding to the discrete-time correlation values $(-1, -17, +15)$. It is not clear whether the spikes are due to delta functions or infinities in the PDF. Lehnert's 1987 paper [108] includes delta functions (hence the term spike above) in the PDF of the CT crosscorrelation at the locations corresponding to the discrete-time correlation values. Significant effort was devoted to modifying the analysis to include these delta functions, but a satisfactory result could not be produced. The best approach was to model the spike by using a uniform region of width ϵ and the height some factor of $1/\epsilon$ and let ϵ tend to zero. This meant that the mathematics was tractable and straightforward, but due to the very large number of terms in the equations, the symbolic mathematics package employed was not able to produce a result. The same limitation in the symbolic mathematics package is also encountered if the spike is treated as a uniform region of width Δ_q.

The inability to extend the analysis to consider delta functions (or spikes) in the distribution should not be seen as a disadvantage for several reasons:

1. The extension would be important if the approach was intended to determine the PBE for actual sets of codes. This is not the reason it has been developed, as the techniques reviewed in section 2.1 are far more amenable for determining the performance of actual codes.

2. Consideration of spikes would allow the influence of occurrence frequencies of adjacent pairs of correlation values on performance to be observed. However this is not recommended, the results and discussions in section 2.2.2, and particularly the results of Kärkkäinen [78, Table 1] show that for most cases, the occurrence frequencies of adjacent pairs of correlation values have little influence on performance. Recall, that section 2.2.2 shows that the AIP $= 2\mu(0)+\mathcal{R}e\{\mu(1)\} \approx 2\mu(0) = 2\text{MSC}$, because $\mu(0) \gg |\mu(1)|$ in most cases. The mean-square crosscorrelation $\mu(0)$ is dependent only on the occurrence frequencies of the correlation values. The occurrence frequencies of adjacent pairs of correlation values are represented by $\mu(1)$.

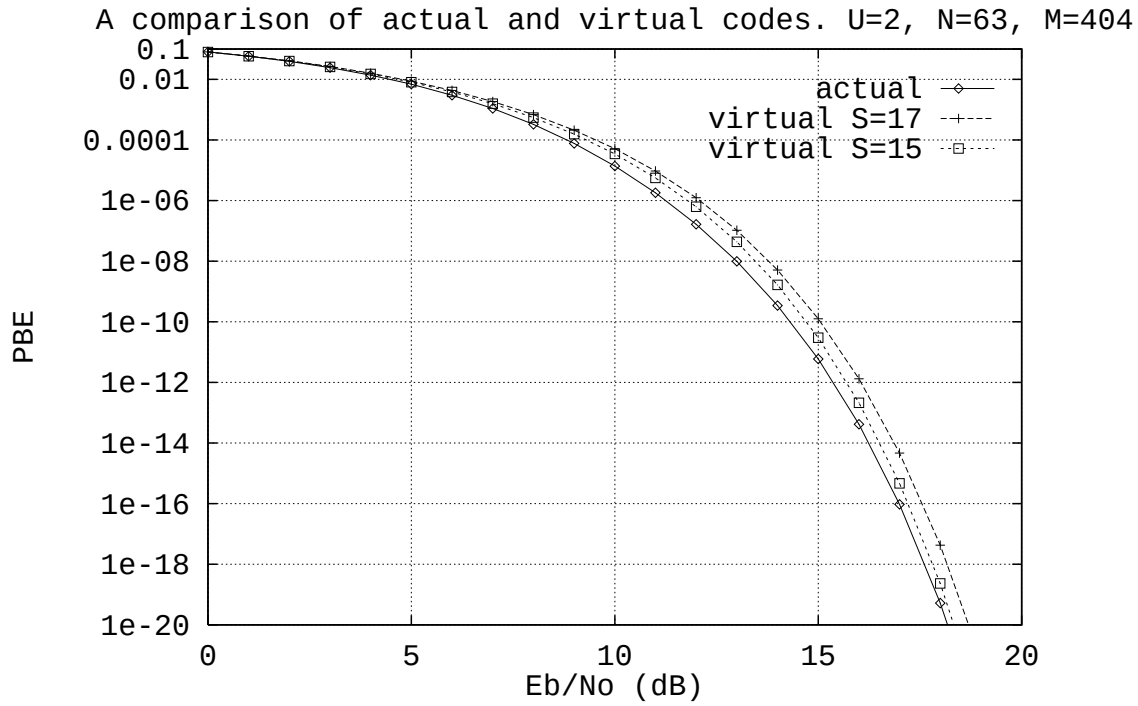


Figure 3.2: A comparison of actual and virtual codes - uniform distribution.

Thus there is little benefit in knowledge to be gained by extending the analysis to investigate this property.

Summary of this section

This section has shown the merit of the example considered in section 3.1.1 because, in developing the analysis for a uniform distribution, the basic forms of the solutions of the equations (integrations) can be applied in more complicated examples (ones which model the PDF of actual sequences to a greater extent).

As an aside, figure 3.2 plots the PBE as a function of E_b/N_o for the two actual codes used in figure 3.1a. Also shown in this figure are curves obtained from the analysis of example 3.1.1 for a virtual set of two codes. This figure shows that there is a close correspondence (over a large range) between the results of the virtual set of codes and the accurate determination of the PBE.

The present state of the analysis for a virtual set of codes is therefore sufficient for the purposes for which it is intended. Its intention is to provide qualitative, not quan-

titative comparisons. This will become clearer in the remainder of this chapter. In section 3.2 it is used to draw conclusions on features of the continuous-time crosscorrelation spectrum which can influence performance, and to observe the tradeoff between them. The features of the continuous-time crosscorrelation spectrum are related to features of the discrete-time crosscorrelation spectrum (including the MSC, the AIP, and the peak value). Resolving whether the peak or MSC is more important has important ramifications for code generation as section 3.4 shows. The resultant codes (emphasizing the appropriate property) can then be optimised by choosing the minimum AIP phase as section 2.2.2 has shown. It is not feasible to design codes to have a given AIP value. Section 3.4 therefore relates the results of this chapter and chapter 2 to refine the philosophy of code generation.

Finally, to complete section 3.1 and the development of the analysis for a virtual set of codes, the issues of independence which have not been discussed in the development of the analysis are treated in the following section.

3.1.3 Questions On Independence

When the code-chip pulse is rectangular, the continuous-time (CT) crosscorrelation can be expressed in terms of the discrete-time (DT) values via:

$$\overline{\phi}_{CT}(\tau) = \overline{\phi}(l) + (\overline{\phi}(l+1) - \overline{\phi}(l)).\delta \tag{3.11}$$

where $\delta = (\tau - l.T_c)/T_c$, as has been shown before. This shows the dependence of $\overline{\phi}_{CT}$ on both $\overline{\phi}(l)$ and $\overline{\phi}(l+1)$, i.e. an adjacent pair of DT correlation values, as well as even or odd periodic correlation. Deriving an expression for the PDF of the CT crosscorrelation spectrum from equation 3.11 is therefore difficult unless random codes are assumed, or the PDF is conditioned on the correlation values as in Lam and Özlütürk's or Nazari and Zeimer's analysis, discussed in section 2.1.2.

In the analysis of example 3.1.1 however, the dependence of $\overline{\phi}_{CT}$ on the adjacent pair of correlation values is not explicitly explained. This is because the reliance of the CT crosscorrelation spectrum on an adjacent pair of DT crosscorrelation values is implicit in the consideration of the form of the appropriate PDFs. This can be seen from the discussion in regard to figure 3.1a. The discussion shows that the PDF of the CT

crosscorrelation spectrum consists of: spikes at the locations of the DT crosscorrelation values, and uniform regions in between. The height of each spike and the uniform region is dependent upon the occurrence of values and adjacent pairs of values in the DT crosscorrelation spectrum. The dependence of the CT crosscorrelation spectrum on adjacent pairs of DT crosscorrelation values is therefore implicit in the analysis employed in section 3.1. The conditioning on even and odd periodic crosscorrelation is also implicit, but this may be made explicit in the following manner if required. Analogously to the approach of Lam and Özlütürk and assuming a random binary information sequence,

$$f_{\overline{\phi}_{CT}} = \frac{1}{2}\left(f_{\phi_{CT}} + f_{\widehat{\phi}_{CT}}\right) \tag{3.12}$$

where $f_{()}$ indicates the PDF of the subscript correlation.

Two remaining questions of independence arise with the analysis:

1. The independence between the code-pair interferences (i.e. $I_{m,1}$ and $I_{n,1}$ where $(m \neq n) \neq 1$).

2. The independence between the real and imaginary components of the CT crosscorrelation, i.e. $\overline{\phi}^{\mathcal{R}e}_{CT} \equiv x$ and $\overline{\phi}^{\mathcal{I}m}_{CT} \equiv y$.

Clearly $\boldsymbol{\theta}$ is independent of x and y. In the analysis of section 3.1, independence has been assumed to hold for both points above. To prove independence for either case appears difficult. It could be argued that independence should not hold for the first point due to the reliance of $I_{m,1}$ and $I_{n,1}$ on the deterministic despreading code of user 1. However, if the codes are random then the lemma given by Torrieri in [186, p.772] could be used to argue the independence of $\overline{\phi}_{m,1}$ and $\overline{\phi}_{n,1}$ and hence the code-pair interferences, but this assumption is not suitable here.

Lemma 3.1.1 Extension of Torrieri's theorem to non-binary codes.
Suppose that $\{\alpha_i\}$ *and* $\{\beta_j\}$ *are statistically independent random non-binary sequences. Let 'a' and 'b' denote arbitrary constants. Then* $\alpha_i\beta_j a$ *and* $\alpha_i\beta_k b$ *are statistically independent random variables for* $j \neq k$.

The author of this thesis is not aware of any analytical technique that does not assume mutual independence between $I_{m,1}$ and $I_{n,1}$ for pseudorandom codes, nor any literature which discusses the validity of this. Similarly, independence may not necessarily hold for

the second point with deterministic quaternary codes. The assumption is obviously not required in any analysis for binary codes, but like the first point is required in order to simplify the analysis.

To examine the validity of the second assumption, statistical tests for independence have been conducted on the crosscorrelation spectra of deterministic sequences, since the author was not able to rigorously prove independence by argument. This need to rigourously prove independence is not important, provided that the assumption is acceptable (which the statistical tests will indicate), because the technique developed in this chapter is intended to provide qualitative (not quantitative) conclusions on how correlation features influence performance. The validity of the assumptions, whilst important, are therefore not crucial.

The statistical method used to examine the independence of the real and imaginary components of the CT crosscorrelation spectrum, was contingency table (or crosstabulation) analysis [149, p.524]. This is a commonly employed technique which is a modified form of the Chi-square test. Appendix B provides the relevant information on this test.

Consider first the real and imaginary components of the even periodic correlation for a pair of random (dice toss) codes shown in figure 3.3. The chi-square test found that the components could be regarded as independent, at a 95% confidence level. Next, consider the real and imaginary components for the maximal-length sequences employed in the previous section: $D^3 = 3D^2 + 3D^1 + 3$ and $D^3 = 3D^2 + 2D^1 + 3$. The chi-square test classified the components of the even periodic crosscorrelation as dependent. This is an expected result, because the discrete-time crosscorrelation spectrum of each component takes only three values. In contrast, the odd periodic crosscorrelation components were classified as independent on a 99.5% confidence level. This is also an expected result, because the odd periodic crosscorrelation contains a substantial range of values.

Thus the more restrictive the criteria on the form or values that the crosscorrelation can take, the less likely is the assumption of independence between the real and imaginary components to be valid. Note that this does not mean that the more restrictive the criteria on the PDFs the less likely is independence, so the assumptions in the analysis are acceptable. This is also shown by the closeness of the results of figure 3.2 (given previously), which compares the PBE for two deterministic sequences with the results

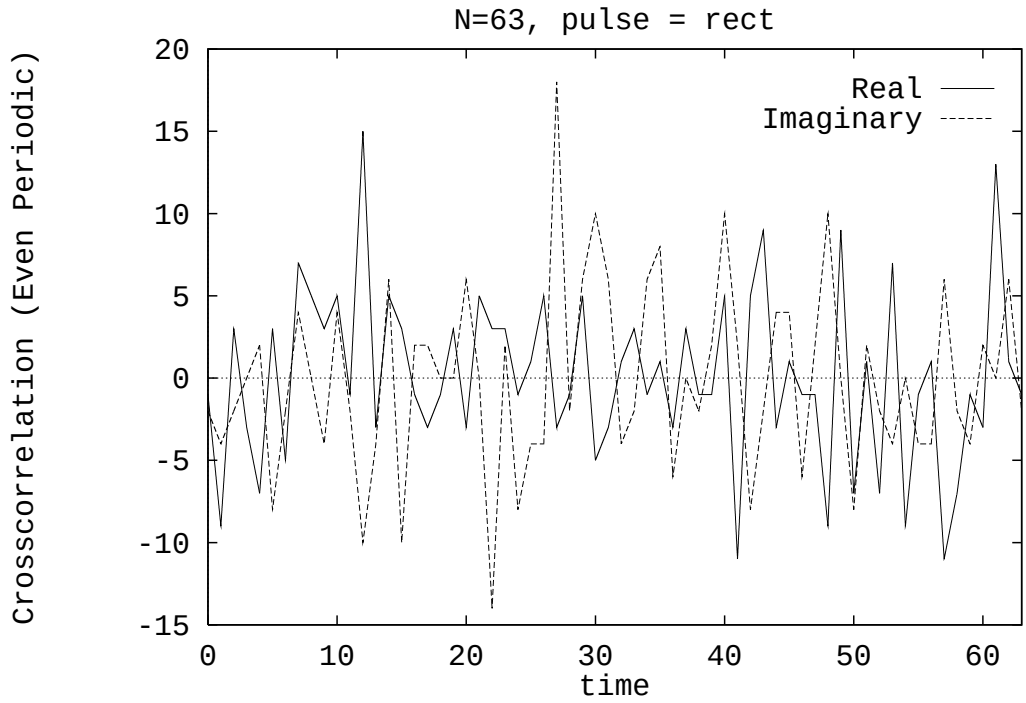


Figure 3.3: Real and Imaginary Components

from the analysis of two virtual codes. For the two deterministic sequences the real and imaginary components of the even periodic correlation were considered dependent, whereas those of the odd periodic correlation were considered independent.

3.2 Other Factors Influencing System Performance

Section 3.1 has developed an analytical technique which allows the influence of features of the crosscorrelation spectrum to be observed without having to conduct tests with actual sequences. This is because of the large variation in performance (PBE) that is possible for different code phase selections, as the results of section 2.2.2 have shown.

In this section, the analysis for a virtual set of codes is applied to resolve the relative importance between the peak correlation value and the mean-square value, thus helping to resolve the first research issue posed in the Introduction: identification of the important code properties and their relative importance. This issue is resolved in the following manner. Section 3.2.1 examines the influence on performance of the peak value, for a

given CT crosscorrelation distribution. This test is to confirm that the analysis produces an expected result, i.e. for a reduction in the peak value, with a given correlation distribution, the performance must improve. In the next subsection 3.2.2, the peak value is fixed and the CT crosscorrelation distribution shape is varied. The results of this section resolve the research issue, because the MSC is related to the shape of the CT crosscorrelation distribution. The author does not derive a mathematical relationship between the MSC and for example, the variance of the CT crosscorrelation distribution, but this could be considered in future research. The results of section 3.2.2 have important ramifications on code generation and these are discussed further in section 3.4.

The CT crosscorrelation distribution is also influenced by the code-chip pulse shape $\Psi(t)$, and this is investigated in section 3.2.3. This section shows that the analysis for a virtual set of codes can be used to provide conclusions on the influence of different code-chip pulse shapes on performance. The results of section 3.2.3 also provide an explanation for a previously unexplained result in the literature.

The discussions on the importance of the results in this section and its three subsections are relatively brief, this is because collectively the results have important ramifications on the code design philosophy. Section 3.4 therefore discusses the results in detail (along with those of section 3.3 and chapter 2), and shows how together, these separate results indicate that the conventional code design philosophy is inappropriate. This then provides the motivation for the different code design philosophy developed and applied in chapter 4.

3.2.1 Peak Crosscorrelation Value

Using the results of example 3.1.1 (i.e. a symmetric uniform PDF for the crosscorrelation values), figure 3.4 shows that as the peak (even or odd) crosscorrelation value (S) is reduced, performance improves. Alternatively, figure 3.5 shows that a reduction in the peak value allows a greater number of active users for a given level of performance. These are expected results consistent with those observed for actual codes.

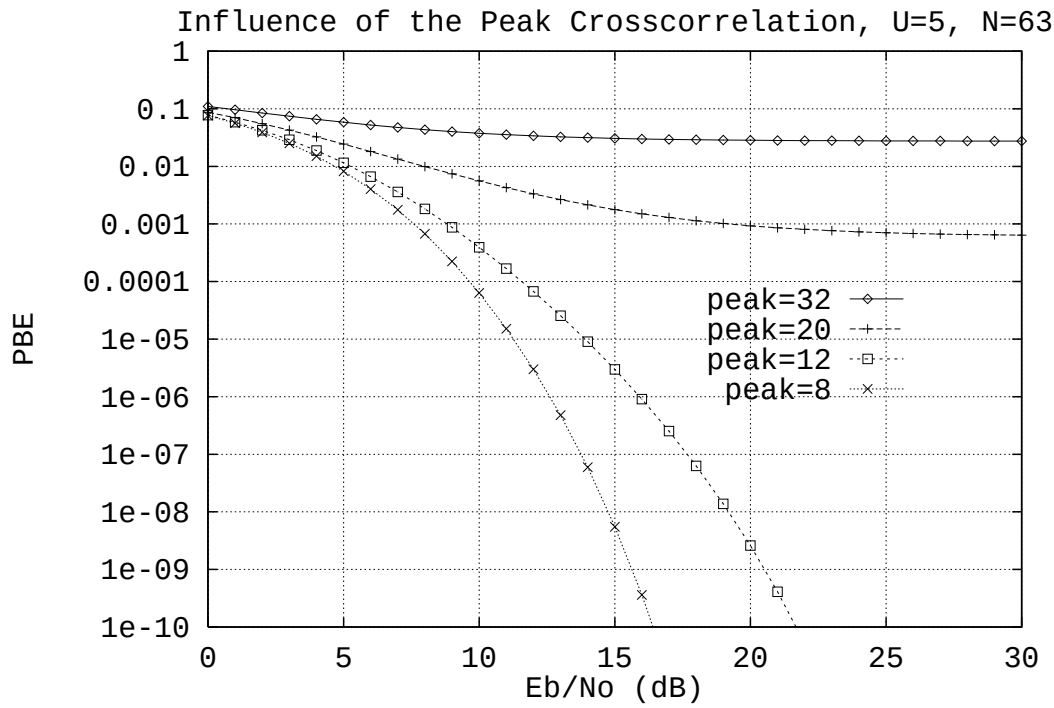


Figure 3.4: The influence of the peak crosscorrelation value.

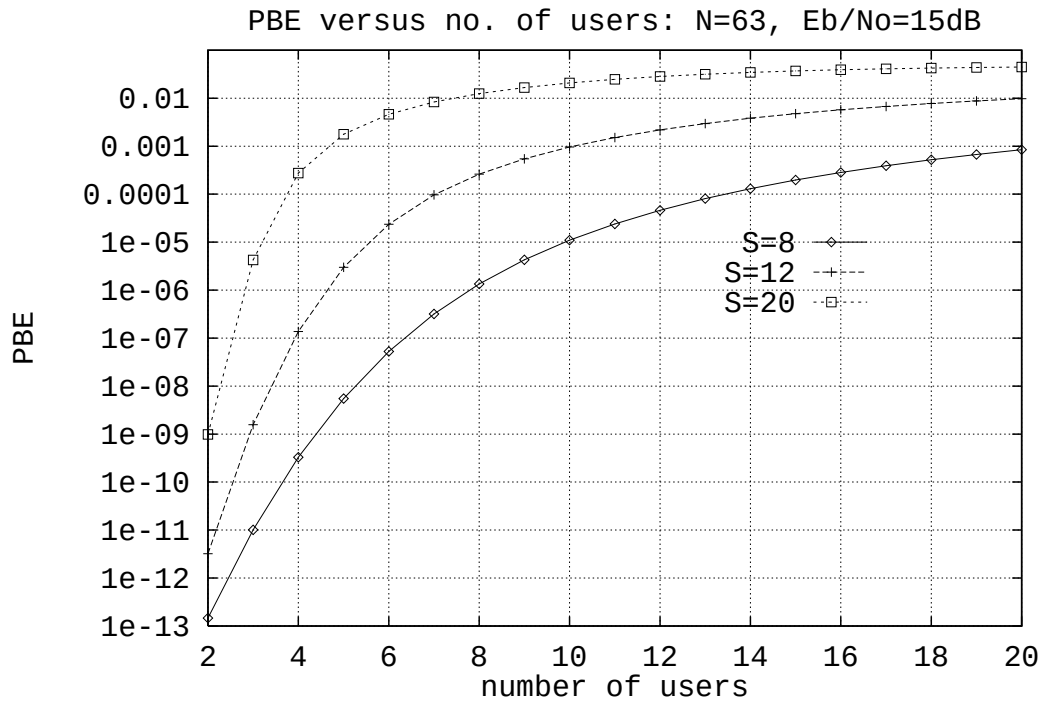


Figure 3.5: Bit Error Probability as a function of the peak value and number of users

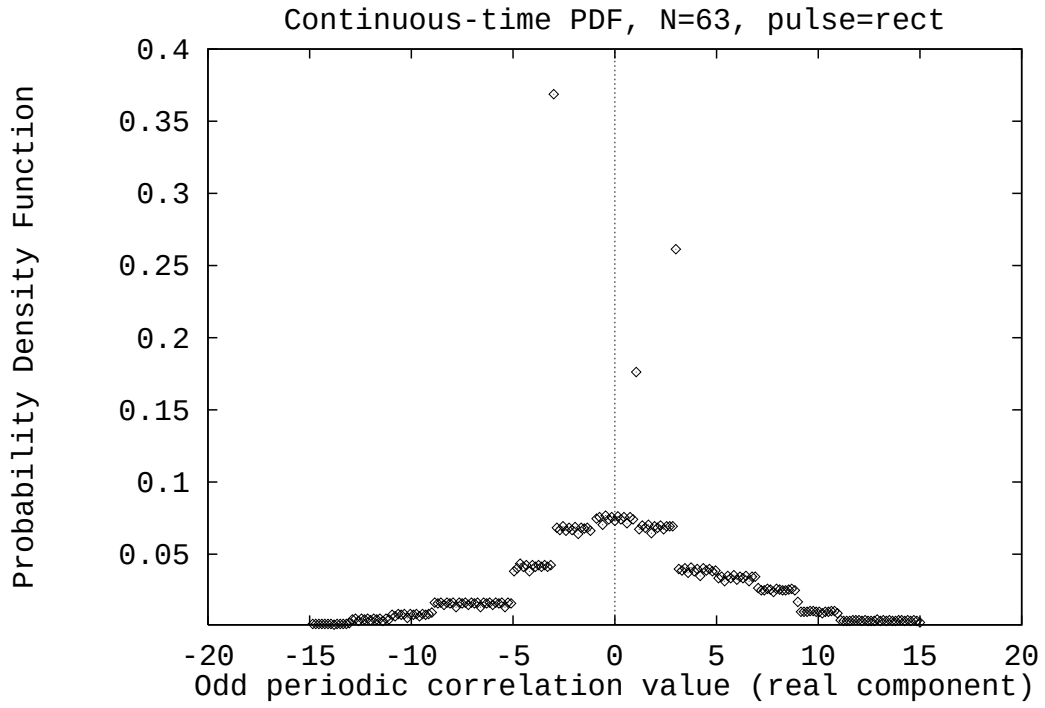


Figure 3.6: PDF of the odd periodic crosscorrelation between a pair of m-sequences

3.2.2 Correlation PDF Shape

The analysis in this chapter has been concerned with the PDFs of the continuous-time (CT) crosscorrelation spectra. In the previous subsection, the influence of the peak value on performance has been observed for a given distribution shape. This section considers a given peak crosscorrelation value (S) and investigates the influence of different distribution shapes. Those considered are the symmetric uniform PDF of example 3.1.1 and a symmetric triangular PDF, which is analysed in section A.2 of appendix A. Figure 3.6 shows[2] the PDF of the real component of the odd periodic crosscorrelation of the maximal-length sequences employed previously. A rough approximation to PDFs of this form could be a triangular distribution. A truncated and normalised Gaussian PDF has also been considered, but this leads to an integral which cannot be expressed in a closed form[3] and needs to be solved numerically. Figure 3.7 also shows the very close

[2]The spike at minus one is off the scale.

[3]No closed form solution is given in [57], which is an extensive catalogue of integrals and their solutions.

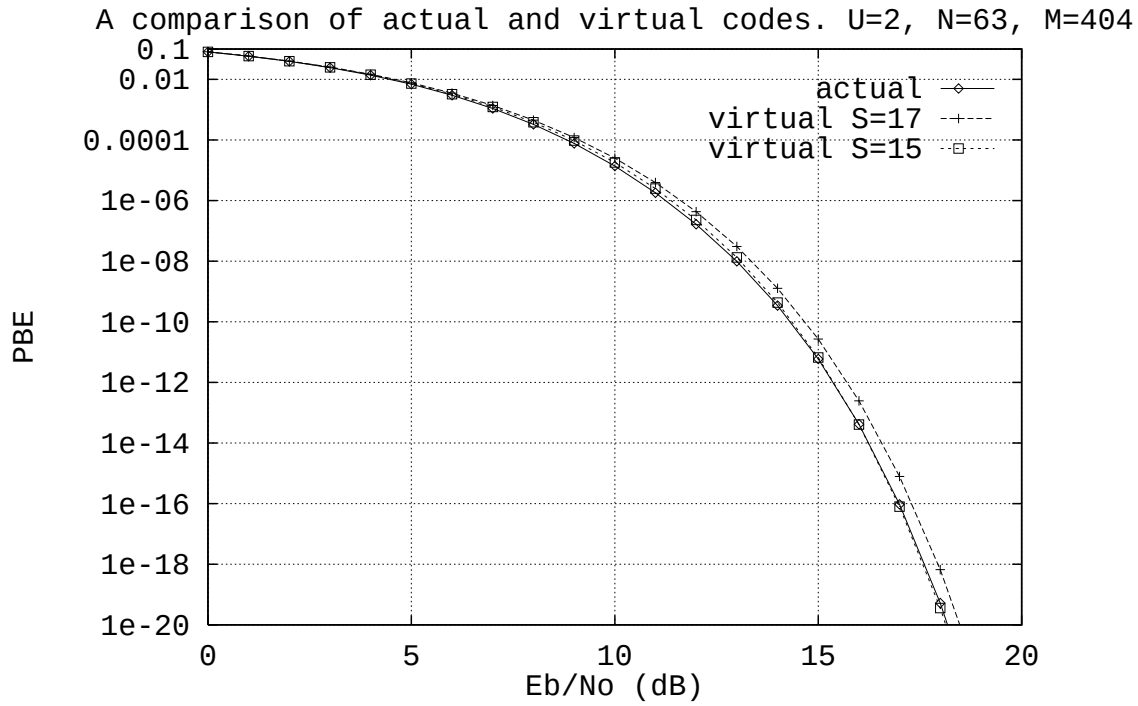


Figure 3.7: A comparison of actual and virtual codes - triangular distribution.

correspondence between the PBE for the pair of actual codes, with the PDF shown in figure 3.6, and the curves resulting from the analysis for two virtual codes with triangular PDFs. The triangular distribution can therefore be used as an acceptable approximation to the stepped PDF in some cases.

Considering triangular and uniform distributions for the same peak crosscorrelation value, figure 3.8 shows that the virtual set of codes with the triangular PDF perform better than those with the uniform PDF. This is an expected result, because the triangular PDF is closer to a delta function PDF, for which the crosscorrelation would be the desired zero function. More importantly however, this figure shows that it is not sufficient to only minimise the peak crosscorrelation value, as the triangular distribution with the larger peak value still performs better than the uniform distribution.

This tradeoff is important for two reasons. Firstly, the tradeoff means that a potentially greater number of codes can be considered than previously. This will be shown in the discussion in section 3.4. Secondly, the tradeoff favours the importance of the mean-square crosscorrelation (MSC) over the peak value. This is because the mean-square

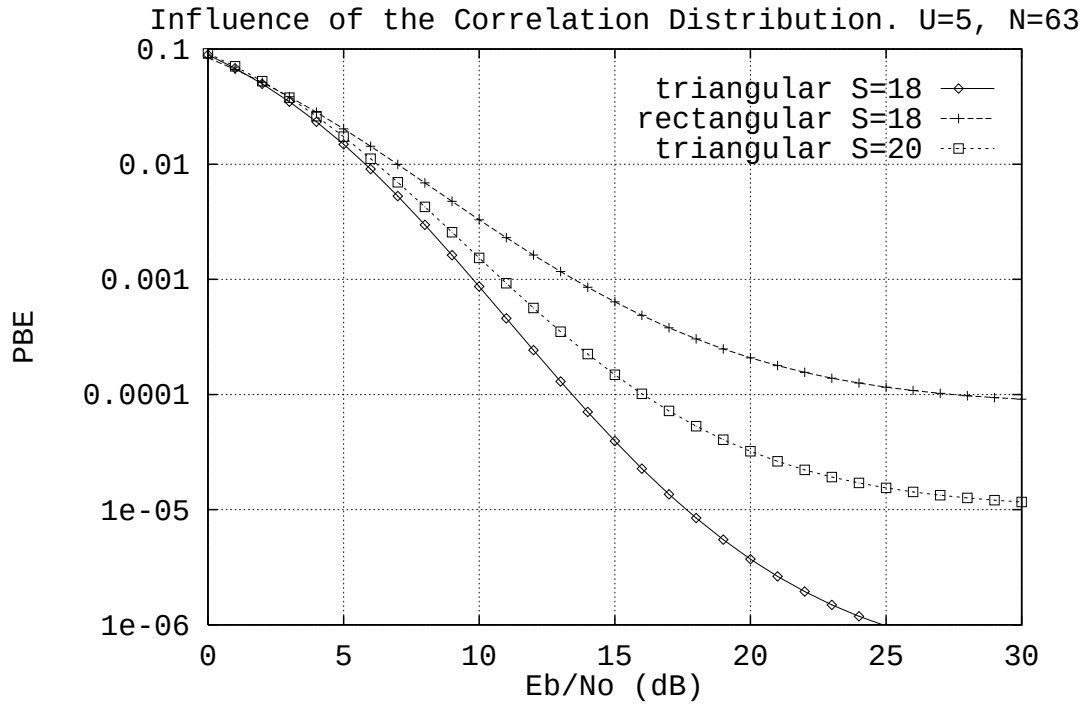


Figure 3.8: The influence of distribution shape on performance.

crosscorrelation is a measure of the variance of the discrete-time (DT) crosscorrelation PDF, which is related to the variance of the CT crosscorrelation PDF. Thus the virtual set of codes with the lower MSC perform better, for a given peak value, than those with the higher MSC. This will also be discussed in greater detail in section 3.4, and in particular the ramifications on the code design philosophy are explained.

In the next subsection the analysis for a virtual set of codes is used to examine the influence of the code-chip pulse shape on performance. The results are not applicable to code generation, but the selection of the code-chip pulse shape can influence performance so it is investigated for completeness.

3.2.3 Code-Chip Pulse Shape

The multiple-access capability of a spread-spectrum system is dependent not only on the code sequence, but also the code-chip pulse shape. In this section the influence of the code-chip pulse shape on the PDF of the continuous-time (CT) crosscorrelation is examined. The results are not directly applicable to code generation, but they do

illustrate that the analysis for a virtual set of codes can be applied to investigate this issue. This is because the basic (not specific) form of the CT crosscorrelation PDF is independent of the code-chip pulse shape, i.e. the basic form still consists of uniform regions and spikes, and the analysis developed in section 3.1 (in particular the solution of the equations and integrals) is therefore applicable. To reiterate, this section qualitatively discusses the influence of the code-chip pulse shape on performance. It should also be noted that the code-chip waveform (and indeed code sequence) determine the spectral properties of the transmitted signal. Spectral properties are not investigated in this thesis, but an interesting topic for future research might be to investigate the influence of the different code properties (e.g. Balance, Run, and Window) of the code sequence on the spectral density of the transmitted signal.

The CT crosscorrelation is related to the DT crosscorrelation by equation 1.9 (of section 1.2) repeated below:

$$\overline{\phi}_{CT} = \overline{\phi}(l).\widehat{\mathcal{R}}_{\Psi}(\tau - l.T_c) + \overline{\phi}(l+1).\mathcal{R}_{\Psi}(\tau - l.T_c) \tag{3.13}$$

where $\widehat{\mathcal{R}}_{\Psi}$ and $\mathcal{R}_{\Psi}$ are factors dependent upon the code-chip pulse shape. Most of the research (and analysis) into spread spectrum-systems employs rectangular code-chip pulse shapes because of their ease of generation. It is well known however, that other pulse shapes can have improved spectral properties. Minimum shift-keyed (MSK) spread-spectrum for example, uses a sinusoidal code-chip pulse shape, and for this case:

$$\widehat{R}_{\Psi}(s) = -s.\cos(\pi s/T_c) + (T_c/\pi).\sin(\pi s/T_c) \tag{3.14}$$

$$R_{\Psi}(s) = (T_c - s).\cos(\pi s/T_c) + (T_c/\pi).\sin(\pi s/T_c) \tag{3.15}$$

The inphase and quadrature channels are also offset by $T_c/2$ in a MSK system. The sinusoidal code-chip waveform and offset between the inphase and quadrature carriers ensures smooth phase transitions in the transmitted signal, and this improves its spectral properties. Additional information on MSK spread-spectrum and its spectral properties can be found in [107] for example.

Figure 3.9a shows an approximation of the PDF of the CT crosscorrelation when a MSK code-chip waveform is employed. The true form is easily discerned from the previous discussions and the correlation spectrum shown in figure 3.9b. These two figures

have been generated by the same two codes used for the PDF and crosscorrelation of figures 3.1a and 3.1b in section 3.1.2.

Comparing the PDF of figure 3.9a with the PDF of figure 3.1a, the main differences are the new uniform region between 9.5 and 15, the additional spike at approximately 9.5 and the narrow uniform region close to minus one. These features arise because of the influence of the sinusoidal waveform on adjacent pairs of the same correlation value. Thus the variance of the CT crosscorrelation and hence the system performance is more likely to be influenced by the occurrence frequencies of adjacent pairs of correlation values (especially the same correlation value occurring twice in succession) for a sinusoidal code-chip pulse shape, than for a rectangular one. This result is consistent with a comparison of the average interference parameter (AIP) for rectangular and sinusoidal code-chip pulse shapes.

$$\text{AIP}_{rect} = 2.\mu(0) + 1.\mathcal{R}e\{\mu(1)\} \tag{3.16}$$

$$\begin{aligned} \text{AIP}_{MSK} &= \frac{(15+2\pi)}{12\pi^2}.\mu(0) + \frac{(15-\pi)}{12\pi^2}.\mu(1) \\ &\approx 0.18\,(2\mu(0) + 1.114\mu(1)) \end{aligned} \tag{3.17}$$

Examining equations 3.16 and 3.17 it can be seen that the relative importance of $\mu(1)$ in relation to $\mu(0)$ is greater for the sinusoidal waveform. Thus $\mu(1)$, which is dependent on adjacent pairs of correlation values, will have a greater relative influence on performance for the sinusoidal code-chip pulse shape. This explains the results of Geraniotis and Pursley [49] who found that the selection of the phase of the code (which changes the odd periodic correlation spectrum) is more important for a sinusoidal than rectangular waveform. This result has not previously been explained in the literature.

The basic (not specific) form of the PDF, which consists of uniform regions and spikes, is clearly independent of the code-chip pulse shape. Thus the results of the analysis for a virtual set of codes could also be applicable to MSK spread-spectrum, provided that the analysis is modified to include the offset between the inphase and quadrature channels.

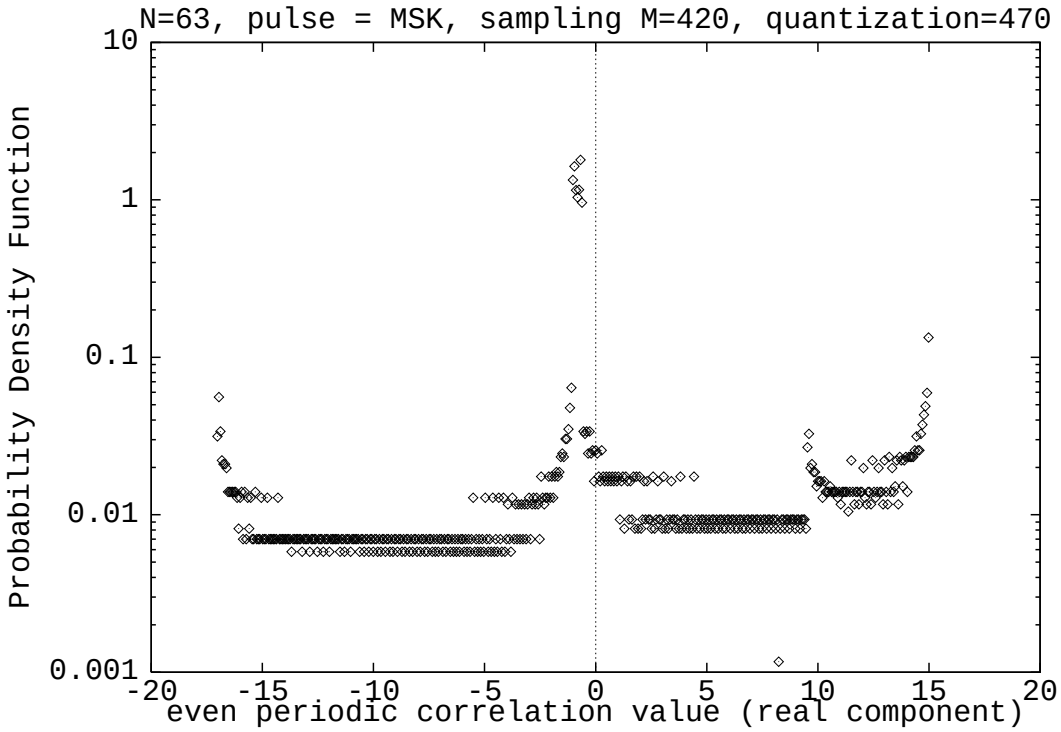


Figure 3.9a: Probability density function of crosscorrelation spectrum: MSK code-pulse shape.

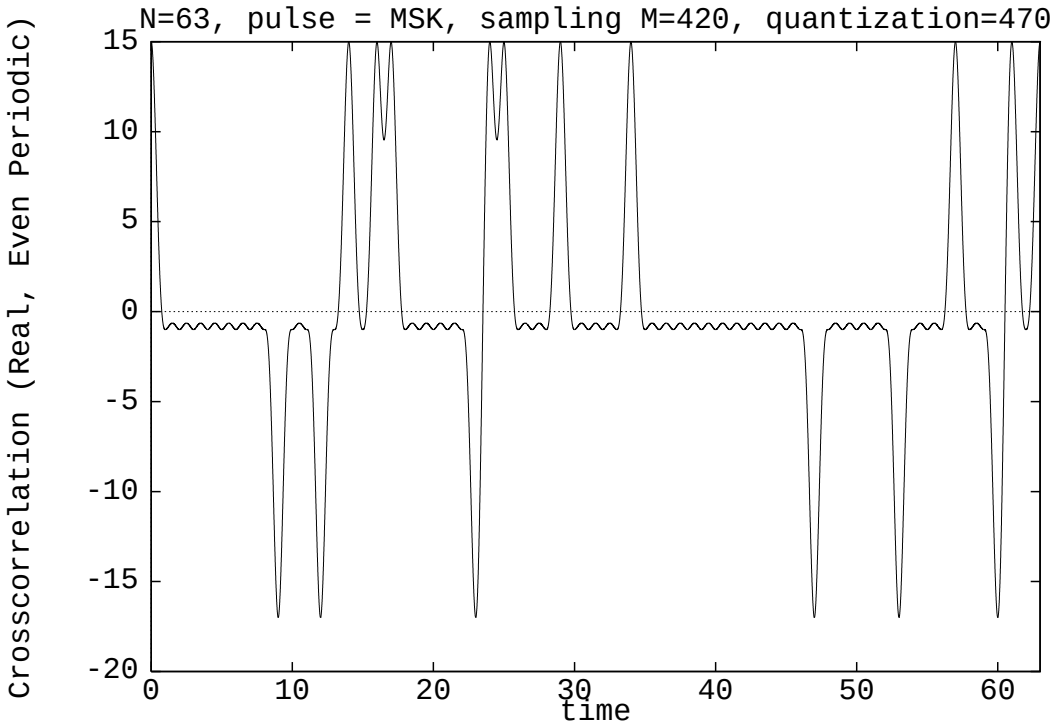


Figure 3.9b: Crosscorrelation spectrum: MSK code-pulse shape.

3.3 Code Symbol Occurrence

In previous sections the influence of features of the crosscorrelation spectrum on performance has been investigated using the idea of virtual codes. The results show that the shapes of the relevant continuous-time (CT) crosscorrelation PDFs have the most influence on performance. Further, these shapes are determined by features of the discrete-time (DT) crosscorrelation spectrum, as well as the code-chip pulse shape. Thus the system analysis does not consider the randomness properties of codes (Balance, Run, and Window), even though conceptually one would expect them to be related to the correlation properties.

The only prior theory relating randomness and correlation properties, that this author is aware of, is for binary sequences. In 1975, Fredricsson [42] showed that the weight distribution of r-tuples of m-sequences can be related to the Hamming code that is the dual of the m-sequence. Fredricsson also showed that the higher order autocorrelations are related to the properties of the dual Hamming code. This section is therefore concerned with the relationship between the randomness and crosscorrelation properties.

This section develops some novel analysis to relate the two types of properties. Specifically, the following research question is investigated: "Do codes which satisfy the Balance property have better correlation properties than codes that do not?" Whilst the novel analysis is only approximate (the assumptions and their acceptability is explained), it does serve to mathematically relate the two classes of properties. This is desirable from a code designer's viewpoint, because it provides an understanding of the relative importance of the properties, and how the alteration of one influences the other and of course performance.

In the previous sections, the analysis has found that the PDFs of the separate real and imaginary components are important. Hence an expression is required for the PDF of a sum of N random variables, where $+1$ has probability α, -1 has probability β and 0 has probability γ. These are the contributions to the real or imaginary components of the crosscorrelation summation and they can be related to the probabilities of a code

symbol occurring as follows:

$$\begin{aligned} p_1^c &= (p_1)^2 + (p_{-1})^2 + 2p_j.p_{-j} \\ p_{-1}^c &= (p_j)^2 + (p_{-j})^2 + 2p_1.p_{-1} \\ p_j^c &= 2p_1.p_j + 2p_{-1}.p_{-j} \\ p_{-j}^c &= 2p_{-1}.p_j + 2p_1.p_{-j} \end{aligned} \tag{3.18}$$

In the above equations, p_j for example, represents the probability of the code symbol j (indicated by the subscript) occurring and p_j^c for example, represents the probability that the contribution to the crosscorrelation summation (indicated by the superscript c) is the complex number j (indicated by the subscript). Hence, if the PDF for the real component of the crosscorrelation is considered, then: $\alpha = p_1^c$, $\beta = p_{-1}^c$ and $\gamma = p_j^c + p_{-j}^c$, where the probabilities (e.g. p_1^c) are defined in the equation set 3.18. Analogous expressions can be obtained if the imaginary component of the PDF is considered: $\alpha = p_j^c$, $\beta = p_{-j}^c$ and $\gamma = p_1^c + p_{-1}^c$.

The even periodic crosscorrelation value of N (or jN), has a probability α^N of occurring. The crosscorrelation value of $N-1$ requires the summation to contain $N-1$ ones and one zero, which has a probability of $N\alpha^{N-1}\gamma$. Similarly $N-2$ requires $N-1$ ones and a minus one, or $N-2$ ones and two zeros as contributions to the summation. An expression for the PDF at any correlation value is readily observed by continuing the series and using the theorem of permutations [94, Theorem 2, p.908] to obtain a multinomial distribution.

Theorem 3.3.1 *If n things can be divided into c classes, such that things belonging to the same class are alike while things belonging to different classes are different, then the number of permutations of these things taken all at a time is*

$$\frac{n!}{n_1!n_2!\cdots n_c!} \qquad (n_1 + n_2 + \cdots + n_c = n) \tag{3.19}$$

where n_m is the number of things in the mth class.

Thus for a crosscorrelation value (real or imaginary) of $N - m : 0 \leq m \leq N$, the value of the PDF at that point is

$$\sum_{k=0}^{\lfloor m/2 \rfloor} \frac{N!}{(N-(m-k))!(m-2k)!k!} \alpha^{N-(m-k)} \gamma^{m-2k} \beta^k \tag{3.20}$$

and for the crosscorrelation value of $-N+m$, the PDF value at that point is

$$\sum_{k=0}^{\lfloor m/2 \rfloor} \frac{N!}{(N-(m-k))!(m-2k)!k!} \beta^{N-(m-k)} \gamma^{m-2k} \alpha^k \tag{3.21}$$

The assumption with the above equations is that the code symbols are independent. This is not true for deterministic sequences, but it may be an acceptable approximation for reasonable code lengths if the deviation from equilikely code symbol occurrence is small. Ronse, who has conducted a significant amount of research into shift-register sequences, states that for codes which satisfy a generalised version of the Run property [164, Second Randomness Postulate p.89]: "*... the value of an element of a cycle is nearly independent of its k predecessors*". The generalised run property requires the number of occurrences of an element of the code, as a function of the sequence length, to be nearly uniform. Thus if the deviation from equilikely symbol occurrence is small, the generalised Run property may be satisfied as well and the assumption of independence is then acceptable. Clearly however if the deviation is large, then the generalised Run property cannot be satisfied, and independence may not hold. Section 4.4.2 investigates the generalised Run property for a selection of deterministic sequences.

Figure 3.10 plots the discrete PDFs of the DT crosscorrelation components for equilikely symbol occurrence probabilities. The real and imaginary components of the PDFs are identical. In contrast, figure 3.11 shows the situation where the code symbol occurrence probabilities (given in brackets for each symbol) are: $-j(0.1), -1(0.1), 1(0.4)$ and $j(0.4)$. The mean-square (even periodic) crosscorrelation is greater for this second set of probabilities. Indeed in extensive tests the author could find no probability set with a lower mean-square (even periodic) crosscorrelation than that for balanced codes (i.e. codes with an equilikely symbol occurrence). Previous results (section 2.2.2) show that reducing the mean-square (aperiodic) crosscorrelation improves performance, and the mean-square (aperiodic) crosscorrelation is related by equation 2.14 to the mean-square (even periodic) and mean-square (odd periodic) crosscorrelations. As a first order approximation therefore, codes which satisfy the Balance property may be expected to perform better than those that do not. Ideally the analysis should be extended to consider not only the Balance property, but also the Window property (for pairs of code symbols), and derive expressions for the continuous-time even and odd periodic PDFs, but this is left as future work as it is by no means a simple task.

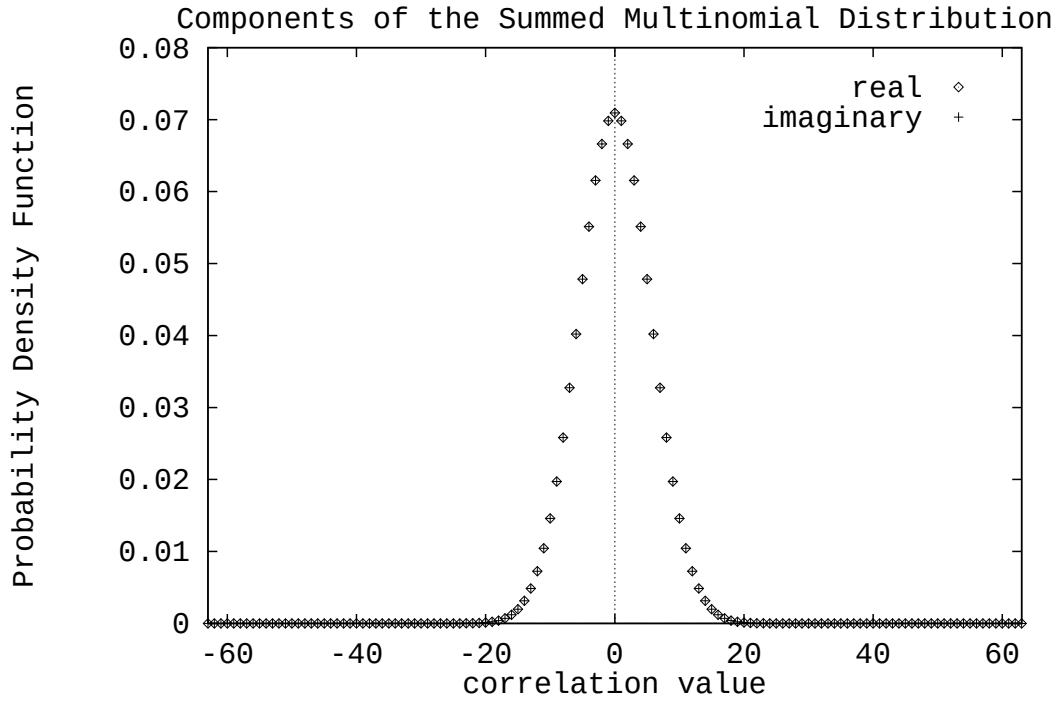


Figure 3.10: Equilikely code symbol occurrence probabilities

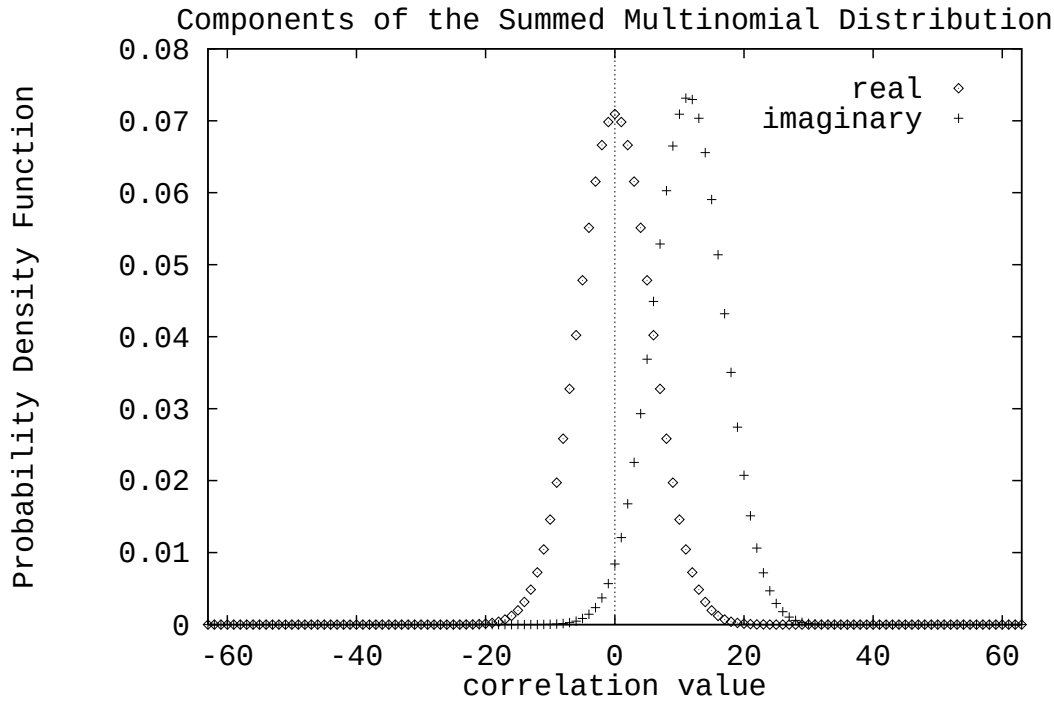


Figure 3.11: Not equilikely code symbol occurrence probabilities

3.4 The Ramifications For Code Generation

This chapter and the previous one have served to resolve many of the issues which need to be considered before the generation of spreading codes can be investigated. The reason for this is because of the disparity in the literature between the properties code designers emphasize and the properties the system analysis emphasizes. This has been previously discussed in this thesis as the inadequacy of the desired crosscorrelation properties, or the issue of the mean-square crosscorrelation versus the peak crosscorrelation. Only a small amount of literature for binary codes has previously been devoted to this topic and that literature is discussed below. This thesis, to the best of the author's knowledge, is the first to examine the issue for non-binary codes. The results of chapters 2 and 3 have led to several conclusions in relation to code properties. Those conclusions will now be brought together and their ramifications for code generation discussed.

Many papers on code generation have investigated only the peak even periodic crosscorrelation and this provides an indication of the worse case system performance as mentioned before. There is the question however, of how likely is the peak value to occur? In a practical system, error correcting codes would be employed with the information sequence, as well as spreading it for transmission, and this would overcome errors generated by a large but infrequent peak value. Designing codes to minimise the peak crosscorrelation value may therefore be overly conservative and not allow the maximum number of users or codes the system is capable of. Rather, the codes should be designed for the average performance level. Error correction coding would then be used to improve performance. When the average system performance is considered, the investigation in this thesis has shown the need to consider not only the peak value, but also the shape of the distribution of the CT crosscorrelation PDFs. That shape is dependent upon:

- the code-chip pulse shape
- the occurrence frequencies of correlation values and
- the occurrence frequencies of adjacent pairs of correlation values.

In chapter 2 the merit factor referred to as the average interference parameter (AIP) is shown to consider all of these factors. Minimising the AIP also improved the performance

of the system in all of the tests conducted in section 2.2.2. This is in contrast to some of the other criteria (and their associated merit factors) used to select the code phase. The results of section 2.2.2 also show that minimising the MSC provides only a slight degradation to performance, but with substantially reduced computation.

The mean-square crosscorrelation considers only the occurrence frequencies of correlation values. Recent research by Chen and Oksman for binary codes [24] has also identified the importance of the occurrence frequencies of the DT crosscorrelation values to performance. Testing sets of deterministic sequences, their paper showed that in some applications codes with more ideal occurrence frequencies out performed those of the same peak value. This result is in agreement with the results of this thesis. In particular, Chen and Oksman considered binary codes with a four or five valued crosscorrelation spectrum, and compared these with binary Gold codes which have only a three-valued spectrum. They found that in some cases codes with a higher peak value and four or five valued crosscorrelation performed better than Gold codes. Chen and Oksman recognised the importance of this to code generation, because they found that there were many more seed-polynomial pairs which could be used to generate such sequences. For the reader not familiar with the generation of Gold codes, they are generated by a preferred pair of m-sequences, which can be represented as polynomials. Only a relatively small number of preferred pairs of m-sequences exist. Thus Chen and Oksman found that more codes could be considered than previously recognised. Detailed information on Gold codes can be found in for example, Sarwate and Pursley's paper [171]. The importance of Chen and Oksman's result and the conclusion of section 3.2.2 that codes with a higher peak but lower MSC can in some cases perform better than those of a lower peak value, can also be seen by considering the Welch bound derived in [193]. Sarwate generalised this in [169] to give a relationship between the peak crosscorrelation ($\overline{\phi}_c$), peak out-of-phase autocorrelation ($\overline{\phi}_a$), number of codes (U) and code period (N), where $\overline{\phi}_a(0) = N$.

$$\left(\frac{\overline{\phi}_c^2}{N}\right) + \frac{N-1}{N(U-1)}\left(\frac{\overline{\phi}_a^2}{N}\right) \geq 1 \tag{3.22}$$

Mow in a later publication [128] discussed some problems with the reasoning in Sarwate's paper, but the resultant equations as originally given were shown to be correct. Other researchers have also derived bounds on the crosscorrelation and autocorrelation of a given number of sequences, such as Sidelnikov [178] and Levenstein [109]. Kumar and

Liu [97] also examined the specific case of non-binary roots-of-unity (r.o.u.) sequences, giving a small improvement over Sidelnikov's bounds. However, the above equation adequately highlights the important results.

Sarwate commented in [169] that tradeoffs are possible between $\overline{\phi}_a$ and $\overline{\phi}_c$. He noted that, because of the steepness of the curve[4] relating them, a small increase in $\overline{\phi}_c$ can lead to a substantial reduction in $\overline{\phi}_a$. The reduction in $\overline{\phi}_a$ can lead to improved synchronisation and tracking performance of the system.

In this thesis, the emphasis is on increasing the number of potential codes which can be considered. Rearranging equation 3.22 therefore (for $\overline{\phi}_c \leq \sqrt{N}$ otherwise a sensible solution is not obtained) gives:

$$U \leq 1 + \left(\frac{N-1}{N}\right)\left(\frac{\overline{\phi}_a^2}{N}\right)\left(1 + \frac{\overline{\phi}_c^2}{N} + \frac{\overline{\phi}_c^4}{N^2} + \cdots\right) \tag{3.23}$$

Thus an increase in $\overline{\phi}_c$, the peak even or odd periodic crosscorrelation, for a fixed $\overline{\phi}_a$ and code period can increase the maximum number of codes which simultaneously satisfy both criteria. The increase in $\overline{\phi}_c$, which could be obtained by choosing codes with better correlation distribution shapes (or smaller MSC for comparable peak values), therefore increases the number of potential which can be considered.

Thus changing the code design philosophy from the min-max criteria (minimise the peak correlation), to minimising the mean-square crosscorrelation or choosing codes with better correlation distributions, can lead to a greater number of codes that can be employed in the system for a given level of performance. It also means that a greater number of codes and code generation techniques can be considered for the system, as Chen and Oksman found for binary codes with the use of non-primitive polynomials in [24], and similarly for Kumar et. al.'s nested chain technique in [96]. This issue will be discussed in more detail shortly.

Although an examination of the system analysis highlights the importance of the mean-square crosscorrelation value, very few authors have examined it for sets of codes. Those who have however, have drawn some important conclusions and their results are now discussed. Perhaps the first author to question the emphasis on the peak crosscorrelation value was Hui [72, footnote 2]:

[4] Actually a plot [169, Fig.2] of C_a^2/N versus C_c^2/N for the bound relating aperiodic cross- and autocorrelation. The same conclusion holds for a plot of $\overline{\phi}_c^2/N$ versus $\overline{\phi}_a^2/N$.

> "*There is the question of whether specifically designed PN sequences (such as the Gold codes) may achieve a higher capacity than sequences that are generated randomly. The answer is no, due to the asynchronism of the transmitters. The proof of this statement follows from a coding theorem for the asynchronous multiple access channel ...*"

The proof by Hui is given in his Ph.D. dissertation: "Fundamental issues of multiple accessing", Massachusetts Institute of Technology, Cambridge MA, 1983. The author of this thesis was unable to obtain this dissertation, so the result has not been extended to non-binary sequences, but it is not unreasonable to expect that the proof could be extended to alphabets other than binary.

In [72] Hui proposed that it is better to search for good convolutional encoders in order to improve the total throughput and decrease the error probability, rather than trying to design PN sequences with good auto- and cross-correlations, which is difficult because of the asynchronous nature of the channel. Hui is therefore indirectly (as it is not stated explicitly in his paper), supporting the use of random codes and the selection of subsets of those codes with suitable correlation properties; Certainly he is not supporting the min-max approach to code design. Improvements are then obtained by error correction coding on the data bits. This then leads to the research issue of the tradeoff between the amount of spreading and error coding which should be employed if the bandwidth is to remain constant. Hui concluded that the best case was all error coding and no PN spreading. The author of this thesis did not investigate this tradeoff in detail and therefore cannot make an informed comment, except that one would intuitively expect the result to be somewhere in the middle if all factors are considered for the mobile channel. As an example, removal of the PN sequence means that a Rake receiver cannot be used in the multipath environment and this is well known to provide an improvement in the performance of the system. One employing coding only would suffer intersymbol interference (ISI) problems with a multipath channel.

Burr [19] also showed that there are situations in which the mean-square crosscorrelation is more important than the peak value. Further, Burr found that for many binary codes the mean-square correlation is similar, even though the peak value of one is much better than the other. The mean-square crosscorrelation of many codes has also been

found to be approximately equal to that expected for random codes. Burr therefore states that it is worthwhile considering using random codes. The obvious disadvantage that he notes, is that there is no limit (other than the trivial value of $\pm N$) on the peak crosscorrelation value. To eliminate the potential for very poor interference, codes with these properties should therefore be removed.

Kärkkäinen's research (sometimes in association with Leppänen), into the mean-square crosscorrelation as a measure for comparing binary code families has also produced analogous results. Kärkkäinen commented in [80] that:

> *"... there are no appreciable differences in SNR performance between sets of Gold, Kasami and m-sequences of equal period and set size.*
> *... the result is somewhat surprising, as it calls into question the accepted belief that some code families are superior for DS/SSMA systems due to the small absolute values of their maximum periodic (even) crosscorrelation. In addition, the SNR performance curves of sets of Gold, Kasami and m-sequences of sufficiently long periods were found to be very close to those of purely random, independent binary spreading codes of equal length.*
> *... Thus the mean square cross-correlation (or cross-correlation spectrum) is perhaps a more realistic performance measure of a code family than a good bounded maximum crosscorrelation. "*

Extensive tabular results comparing the MSC for sets of binary: Gold, Kasami and m-sequences, given in [77, 78, Table 1], show the similarity for a variety of code lengths. Hammons and Kumar provided an explanation as to why this occurred in [63] using results by Massey, and Kumar and Liu, referenced in their paper. The similarity of the MSC values is explained using information theory relationships, and the interested reader is referred to Hammons and Kumar's paper and consequently to Massey's work. Mowbray, Pringle and Grant [129] also found similar performance for different code families when simulating an asynchronous DS/SS system, and they also recognised that it was because of the similar mean-square crosscorrelation values of the sequences employed.

In conclusion therefore, as most code generation techniques produce codes with similar mean-square crosscorrelation values and values comparable to random codes, Burr's philosophy is worthwhile pursuing. That is, the use of random codes and then the se-

lection of subsets with the desirable correlation properties which have been previously highlighted. However, recommending the use of random codes (a mathematical concept) does not resolve the issue of code generation, but this is easily overcome. Rather than designing for the correlation properties, the emphasis should be on designing for the randomness properties. This is researched in the next chapter, where a novel code generation technique is developed.

A final point to note before code generation is investigated, is that the expectations of the mean-square crosscorrelation values for binary and quaternary codes are equal: $\mathcal{E}(\mathrm{MSC})_{\mathrm{binary}} = \mathcal{E}(\mathrm{MSC})_{\mathrm{nonbinary}}$. Thus similar performance would be expected on average between binary and non-binary systems. Non-binary coded spread-spectrum is still worthwhile pursuing however, because of the greater number of potential codes and the reduction in the worse case performance. Ideally, an expression should also be derived for the variance of the MSC for binary and non-binary codes. This may then illustrate in a manner similar to the result for the peak value (section 1.3), the advantage to performance of non-binary codes. The Introduction suggested that the work of Rowe [165] may assist with this, and this could be investigated as a topic of future research.

Chapter 4

Pseudorandom Code Generation

In the previous chapters of this thesis, the research investigates different properties of pseudorandom codes and how those properties influence the performance in an asynchronous multiple-access environment. The reason for this is because of the discrepancy (see for example [95]) between the properties suggested by the analysis of the system, and those emphasized by the literature on spreading-code generation. There is also the additional issue of whether the separate real and imaginary components or the absolute magnitudes of the correlation values should be considered for non-binary codes. The two prior chapters have researched code properties and resolved the important issues. Further, they show that the conventional code design philosophy may be inappropriate for the asynchronous multiple-access channel.

A large majority of the literature on pseudorandom codes (binary or non-binary) emphasizes only the peak even periodic crosscorrelation value. Subsets with a small peak odd periodic crosscorrelation value are then searched for. Recently, a small number of researchers have also proposed techniques to minimise the peak even and odd periodic crosscorrelation simultaneously, and these are discussed later in this chapter. However, the results of the prior chapter show that designing codes to minimise the peak value can lead to overly conservative designs. The shape of the relevant continuous-time crosscorrelation PDFs should also be considered, because in some cases they can be more important than the peak values. The discussions in the prior chapters also relate the PDF shape to the merit factors: mean-square crosscorrelation (MSC) and average interference parameter (AIP), factors other researchers have found to be important.

Designing codes to have a given (or range) of MSC or AIP values is a very difficult task however, particularly when the alphabet is to be constrained to binary or quaternary. Several authors have recognised the importance of the MSC or AIP, and the difficulty in designing for these properties, and therefore suggested that random codes should be used in the system. Subsets with good correlation properties could then be selected from the set of random codes. Other research has also illustrated that many code families have similar MSC values (when not optimised) and that the value is similar to that for random codes. Subsets can of course be optimised for better performance under specific conditions. The use of random codes is therefore a valid proposal, but it does not resolve how the codes are to be generated. How does one obtain (generate, select) random codes? Randomness is an ensemble property. The performance of random codes is obtained by making assumptions of the mathematical expectation of certain properties, not from actual sequences. There are conceptual difficulties in defining a finite-length sequence as random, as sections 1.4 and 4.4.2 discuss. Thus recommending the use of random codes (the mathematical concept) does not explain how suitable codes (actual sequences) can be obtained. The solution is an obvious one, that is, the codes should be designed to satisfy the randomness properties given in section 1.4: Balance, Run, and Window. Literature on code design (particularly m-sequences) has highlighted these as important for PN codes, but in many cases spread-spectrum code designers consider only the correlation properties. The randomness properties may be mentioned, but usually codes are only designed to satisfy those properties when they are used in applications other than spread-spectrum multiple-access communication (e.g. in cryptography, or as random sequences for Monte-Carlo simulation). The design philosophy in this thesis is therefore:

Design Philosophy

- The code family should contain a large number of codes (in comparison with the code period).
- The codes should satisfy the desired randomness properties: Balance, Run and Window.
- Subsets of codes with suitable correlation properties are then selected.

- For ease of implementation and speed, a shift register configuration should be retained for generation of the codes.

Notice, that by relaxing the constraints on the correlation of the codes, a greater number of codes in the family is possible. The research in the previous chapters also shows that the constraints on the peak correlation value can be relaxed without necessarily compromising performance. A novel method of code generation based on this philosophy is discussed in this chapter. The original proposal of this method was published by this author in [161]. It is extended here and new results are presented.

Many code generation methods, including the novel one of this chapter, rely on an understanding of Group theory. The relevant terms are therefore summarised in section 4.1. An extensive literature review on non-binary code generation techniques is given in section 4.2. This review highlights the techniques which are directly applicable to Q-CDMA. Section 4.3 then develops the novel approach in detail. The randomness, stability and security of the new codes is investigated in section 4.4. A brief comparison with other code generation techniques is given in chapter 5, where the emphasis is on the system performance (or PBE), for subsets of codes.

4.1 Fundamental Principles

Many pseudorandom code generation techniques utilise the principles and terminology of Group theory, specifically those relating to Galois fields. This section provides the definitions of terms from Group theory which are discussed and used in this chapter. These definitions are based on those given in [16, chpt. 2,4,5] and [5, chpt. 3]. The definitions of the terms, symbol, code and operator, may appear unnecessary, but it is important that they are clearly stated so that confusion does not arise between, for example, the addition operators defined in this chapter and conventional addition.

Definition 4.1.1 *A* **symbol** *is an element of an* **alphabet***; its only property is that it can be distinguished from all other symbols of the alphabet.*

Symbols will be shown as emphasized text, e.g. *2*, in this thesis. For an alphabet of cardinality q, the symbols are *0, 1, 2,* $\cdots$*, (q-1)*. These symbols will be defined to be

points of the signal constellation, or mapped onto the complex alphabet and they should not be confused with the numbers $0, 1, 2$, etc.

Definition 4.1.2 *A* **code** *or* **sequence** *of length N, is an ordered set of N elements each of which is a symbol of the same alphabet.*

A code will be designated by a tilde over its name, e.g. $\tilde{A}$. Only periodic codes are considered.

Definition 4.1.3 *An* **operation** *on a pair of symbols is an arbitrarily defined function that returns a symbol of the same alphabet.*

Operations are defined by a table (often termed a specification), which gives the returned symbol for each symbol pair. Only two operations are discussed in this paper: addition and multiplication. In the same manner that symbols and numbers should not be confused, the addition and multiplication operations should not be confused with integer, modulo-q, or GF(q) arithmetic, however the last one will arise as a special case of the new approach in section 4.3.

Definition 4.1.4 *A* **maximal-length sequence** *has a period of $N = q^m - 1$, where m is the symbol memory order of the shift-register configuration, and q is as previously defined.*

Definition 4.1.5 *An* **algebraic system** *denoted $\langle \mathcal{S}_\mathcal{E}, \mathcal{S}_\mathcal{O} \rangle$ consists of a finite set of elements $\mathcal{S}_\mathcal{E}$ and a set of operations $\mathcal{S}_\mathcal{O}$ on elements or pairs of elements of $\mathcal{S}_\mathcal{E}$.*

Definition 4.1.6 *A* **group** *is a set together with an operation (denoted by $\bullet$) on pairs of elements in the set satisfying four properties:*

1. **Closure**: *For every* A,B *in the set,* C=A$\bullet$B *is in the set.*
2. **Associativity**: *For every* A,B,C *in the set,* A$\bullet$(B$\bullet$C)=(A$\bullet$B)$\bullet$C.
3. **Identity**: *There is an element* E *called the identity element which satisfies* A$\bullet$E=E$\bullet$A=A, *for every* A *in the set.*
4. **Inverses**: *If* A *is in the set, then there is some element* B *in the set called an inverse of* A, *such that* A$\bullet$B=B$\bullet$A=E.

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Table 4.1: Arithmetic for a Galois field of four elements, GF(4).

Definition 4.1.7 *An* **Abelian group** *satisfies the additional property of* **commutativity**, *where* A•B=B•A.

Definition 4.1.8 *A* **quasigroup** *is an algebraic system* $\langle \mathcal{S}_\mathcal{E}, \bullet \rangle$ *if there is a binary operation* • *defined in* $\mathcal{S}_\mathcal{E}$, *and when two elements* A,B$\in \mathcal{S}_\mathcal{E}$ *are given, then the equations* A•X=B *and* Y•A=B *have a unique solution.*

Definition 4.1.9 *A* **loop** *is a quasigroup with an identity element* E.

Definition 4.1.10 *A* **finite field** *is a set of finite size which has two operations defined on it: addition and multiplication, such that the following axioms are satisfied:*

1. *The set is an Abelian group under addition.*
2. *The field is closed under multiplication, and the set of non-zero*[1] *elements is an Abelian group under multiplication.*
3. **Distributivity**: A∗(B+C)=A∗B+A∗C *and* (B+C)∗A=B∗A+C∗A.

Table 4.1 defines addition and multiplication for a Galois field of four elements, designated as GF(4).

Definition 4.1.11 *If there exists a given one-to-one correspondence,* A $\leftrightarrow \overline{\text{A}}$, *between the set of all elements of the group (field/operator specification) G, and the set of all elements of the group (field/operator specification)* $\overline{G}$, *then if it preserves the operator (field) structure, an isomorphic correspondence exists, and the two groups (fields/operator specifications) are* **isomorphic**. *Hence if any relation of the form* A•B=C *holds between the elements of G, then* $\overline{\text{A}} \bullet \overline{\text{B}} = \overline{\text{C}}$ *(where* A$\leftrightarrow \overline{\text{A}}$, B$\leftrightarrow \overline{\text{B}}$,C$\leftrightarrow \overline{\text{C}}$*), holds for the elements of* $\overline{G}$.

[1] The arithmetic of GF(4) denotes the identity element under addition as "zero".

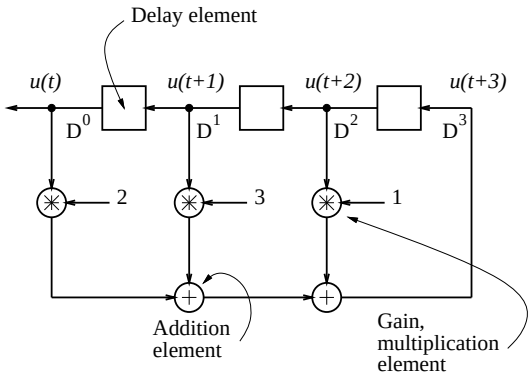


Figure 4.1: Example Feedback Shift Register Configuration

In this thesis, pseudorandom codes are generated by a feedback shift-register configuration, an example of which is shown in figure 4.1. The recurrence relation defining the operation of the shift register, $u(t+3) = 1 * u(t+2) + 3 * u(t+1) + 2 * u(t)$, may be expressed as $D^3 = 1 * D^2 + 3 * D^1 + 2 * D^0$, where D represents the memory element. This latter notation, which is used throughout the thesis, may also be expressed for Galois or linear arithmetic as the polynomial $f(D) = D^3 + D^2 + 3D + 2$, upon which mathematical manipulations may be performed to derive results about the codes. Reference will often be made in coding theory to primitive, irreducible and minimal polynomials. These polynomials are referred to in this chapter, but their definitions are not provided here due to their reliance on many prior definitions. An understanding of the terms is also not required to understand the theory or references to the polynomials in this chapter. The reader interested in the definition of minimal, primitive, and irreducible polynomials is referred to the introductory texts referenced previously on Group and coding theory.

4.2 Review Of Code Generation Techniques

In the review of non-binary code generation techniques it is convenient to divide the designs into two classes. The first class is concerned with those techniques where the code alphabet does not (in general) contain four symbols. The second class of sequences consists of those designs that produce codes from an alphabet of four elements. The non-binary code designs have been divided in this manner because the second class are often directly applicable to a Q-CDMA system and the first are not. There are exceptions to

this, for example quinary m-sequences could be mapped to the alphabet $\{\pm 1, \pm j, 0\}$ and possibly applied in a Q-CDMA system, but this is not investigated in this thesis.

A brief review of codes in the first class was conducted by Kumar and Moreno in 1991, [98]. Similarly Krone and Sarwate [95] reviewed those techniques applicable to the second class in 1984. Many new techniques, particularly those of the second class, have been proposed since those reviews. This section therefore reviews non-binary code generation techniques to the present. The emphasis of this thesis is on Q-CDMA systems, so the review of non-binary codes which cannot be applied to such a system is not as complete as the review of codes which can. The review of the first class of codes therefore concentrates on techniques which were not discussed in [98], except for some such as the Frank-Zadoff-Chu (FZC) design, which are often referred to in literature on non-binary spread-spectrum communications (and have been discussed in section 1.3.1 in relation to the results of Lam et. al.). Thus the reader interested in other code generation techniques of this class is referred to [98] and the recent works [74] and [176].

Table 4.2 summarises a selection of techniques for generating non-binary codes with an alphabet of, in general, more than four symbols. The majority of these designs produce polyphase codes. A polyphase code by definition is one in which all the elements have the same magnitude. Thus p^{th} roots of unity (r.o.u) codes are also polyphase codes. An example of a polyphase code family is the Frank, Zadoff, Chu (FZC) code family. FZC sequences have an ideal even periodic autocorrelation function, and the peak magnitude of the even periodic crosscorrelation between codes is equal to the square root of the code period. FZC sequences are therefore optimal with respect to the Welch lower bound. The total number of codes in the FZC family is given by the Euler totient function $\varphi(N)$, which is the number of integers relatively prime to N. Other polyphase code generation techniques can produce families containing a greater number of codes. However, the discussion in the Introduction shows that the use of polyphase codes with $p > 4$ can lead to practical problems, particularly in a mobile telecommunications environment, hence the concentration on quaternary spreading codes.

The non-binary code generation techniques which can produce quinary codes could possibly be employed with a Q-CDMA system if the elements of the codes can be mapped to the alphabet $\{\pm 1, \pm j, 0\}$, rather than the 5^{th} roots of unity. The techniques of table 4.2

Name	References	Family	Period	Alphabet
Frank	[64, 40, 38]	1	q^2	q^{th} r.o.u.
Frank, Zadoff, Chu	[25, 39, 169, 33]	$\varphi(N)$	N	polyphase
Lee	[105]	code transform[a]	$\frac{(p^m-1)}{(p-1)}$	$\{0, \pm 1, \pm j\}$
m-sequence GF(p)	[23, 50, 61, 103]	$\varphi(p^m-1)/m$	p^m-1	GF(p)
m-sequence GF(p^k)	[61, 65, 144, 142] [143, 88, 55]	$\varphi(p^{m.k}-1)/m$	p^m-1	GF(p^k)
Gold	[51, 103]	p^m+1	p^m-1	GF(p)
complex GMW	[9]	[b]	p^m-1	p^{th} r.o.u.
Alltop quadric	[6]	$p-1$ [c]	≥ 3, odd	N^{th} r.o.u.
Alltop cubic		p	$p \geq 5$	p^{th} r.o.u.
Alltop power residue		M [d]	N	p^{th} r.o.u.
Lüke	[112]	p^m-1	p^m-1	polyphase
Fan *et. al.*	[35, 34]	p	p	p^{th} r.o.u.
Kasami GF(p)	[111]	p^m	$p^{2m}-1$	GF(p)
Kirimoto/Oh-Hashi	[84, 85]	code transform[e]	q^m-1	complex
R.V. Bent function	[118]	not given	not given	$p.q$ phase
Kumar/Moreno	[98]	p^m; $(p \neq 2)$	p^m-1	polyphase
Scholtz/Welch	[175, 169]	[f]	any	polyphase
Popović	[148]	code transform[g]	$k.m^2$	polyphase
Modulatable orthogonal	[183]	$p-1$	p^2	polyphase
pseudo-polyphase	[182]	N	N [h]	complex

[a] Usually on an m-sequence.

[b] $\sum_{1<J<m} \left(\frac{\varphi(p^J-1)}{J}-1\right)\left(\frac{\varphi(p^m-1)}{m}\right) + \frac{\varphi(p-1).\varphi(p^m-1)}{m}$; J a divisor of m.

[c] Where p is prime and the smallest divisor of N.

[d] Where $p = M.N+1$ is prime.

[e] Transform on an m-sequence of GF(q).

[f] If the period is an odd prime p, then $p-2$ codes exist. Family size is not given for other periods.

[g] Transform on a FZC code of the period given. Usually the period is selected to be odd and a set of $m-1$ sequences using $m-1$ different primitive N^{th} roots of unity are generated.

[h] Period of base m-sequence.

Table 4.2: Non-binary codes: (p prime; m, k, q integers).

Name	References	Family	Period
Abbasi/Ghani	[1]	code transform	
m-sequence	[14, 95, 88, 143, 103]	$\varphi(4^m-1)/m$	4^m-1
BTQ	[184, 8],[95, A,B], [44, 45]	code transform	
Barker	[54, 188]	[a]	≤ 15 [b]
Novosad	[133]	$2^{m/2}$	2^m-1, $m=2(\text{mod } 4)$
R.V. Bent function	[118]	$2^{m/2}$	2^m-1, $m=0(\text{mod } 4)$
Mow	[127]	[c]	≤ 24
Solé	[180],[17, $\mathcal{A}$],[63]	2^m+1	2^m-1
Boztaş,Hammons,Kumar	[17, $\mathcal{B}$]	2^{m-1}	$2(2^m-1)$
Welti	[194]	$\leq 2^m$	2^m
Gold	[51],[95, C]	4^m+1	4^m-1
Lerner/Sidelnikov	[95, D]	2	$p\neq 2$
Sidelnikov	[95, E]	4(2)	p^k-1
Krone/Sarwate	[95, F]	$M(4M)$	$(p^k-1)/M$, M a divisor of p^k-1
Krone/Sarwate	[95, G]	$2q+2$	$q-1$
Nested chain	[96]	[d]	2^m-1

[a] One is found by an exhaustive search.
The remainder are found using Barker preserving transformations.
[b] Not all code periods exist.
[c] Found by exhaustive search. Hence dependent on code period.
[d] See [96, Table 1]

Table 4.3: Quaternary codes: (p prime; m, k integers).

which have this potential are m-sequences, Gold and Kasami sequences, and the method developed by Lee. Unlike the binary m-sequences or Gold and Kasami codes, there is no longer an isomorphic correspondence between GF(5) and $\{\pm 1, \pm j, 0; +, *\}$. Thus while such codes may have for example a near-ideal autocorrelation if the mapping is from GF(5) to the 5^{th} roots of unity, this may not directly translate into a near-ideal autocorrelation spectrum if the mapping is from GF(5) to $\{\pm 1, \pm j, 0\}$. This issue and quinary codes are not investigated in this thesis, but they could be examined as part of further research. The important issue of which mapping from quaternary symbols to the complex numbers $\{\pm 1, \pm j\}$, should be employed is treated in chapter 5.

Table 4.3 summarises quaternary code generation techniques. Maximal-length sequences (m-sequences) and Gold codes exist over GF(4) and are generated in an analo-

gous manner to their binary counterparts. That is, a quaternary m-sequence is generated by the linear feedback shift-register (LFSR) implementation of a primitive polynomial over GF(4), and quaternary Gold codes $G^{(k)}$ are constructed from the quaternary m-sequences M_1 and M_2 via:

$$G^{(k)} = M_1 + T^k.M_2 \tag{4.1}$$

where T is the sequence left-shift operator. Section 5.1 discusses the special requirements on M_1 and M_2.

To digress slightly, there is often confusion in the literature as to whether m-sequences are generated from primitive, irreducible, or in some rare erroneous cases, minimal polynomials, all of which are related. In the original paper on binary m-sequences [200], Zierler defined them as being generated from primitive polynomials. Zierler also proved that m-sequences satisfy the Balance, Run and Window properties; have a constant out-of-phase autocorrelation of -1; and satisfy the shift-and-add property. The shift-and-add property means that an m-sequence added to a time-shifted version of itself (another code phase) is equal to some phase of a different m-sequence. This latter property is important in proving many of the properties of m-sequences and Gold codes.

Irreducible polynomials will also produce maximal-length sequences and this often leads to the confusion in the literature. On this point Pickholtz [146] makes the following comment: If the linear-feedback shift-register (LFSR) is described by the characteristic polynomial $f(D)$, then

> "*A necessary condition that the LFSR is maximal length is that $f(D)$ is irreducible. A sufficient condition is that $f(D)$ is primitive.* "

Hence a maximal length sequence implies that $f(D)$ is irreducible and $f(D)$ irreducible gives a maximal length sequence. If $f(D)$ is primitive a maximal length sequence is obtained, but a maximal length sequence is not necessarily generated from a primitive polynomial.

Confusion also arises between the terms irreducible and primitive, because the number of q-ary m-sequences is often defined as $\varphi(q^m - 1)/m$, where $\varphi(.)$ is the Euler-totient function discussed previously. For quaternary alphabets and codes of period 63, this implies that there are 12 irreducible polynomials which can produce maximal-length sequences of period 63. Table 4.4 gives the 12 irreducible polynomials (from Green and

polynomial			polynomial		
D^3+D^2+D+2	I	P	D^3+2D^2+3D+2	I	
D^3+D^2+D+3	I	P	D^3+2D^2+3D+3	I	
D^3+D^2+2D+3	I	P	D^3+3D^2+D+2	I	P
D^3+D^2+3D+2	I	P	D^3+3D^2+2D+2	I	
D^3+2D^2+D+3	I	P	D^3+3D^2+2D+3	I	
D^3+2D^2+2D+2	I		D^3+3D^2+3D+3	I	

Table 4.4: Polynomials which generate maximal length sequences.

Taylor [61]) and highlights the 6 primitive polynomials (as given by Balza et. al. in [14, Table 1]) for codes of period 63. Thus the use of a primitive or irreducible polynomial to produce an m-sequence is acceptable, even though by Zierler's original definition only primitive polynomials should be considered.

Returning to the discussion, the properties of quaternary m-sequences and Gold codes are analogous to those of the binary versions, except for some important differences as highlighted by Krone and Sarwate in [95]. For example, the autocorrelation of binary m-sequences is:

$$\phi(l) = \begin{cases} N & l \bmod N = 0 \\ -1 & \text{otherwise} \end{cases} \tag{4.2}$$

but the autocorrelation of quaternary m-sequences is given by:

$$\phi(l) = \begin{cases} N & l \bmod N = 0 \\ -1 \pm j(N+1)/2 & \text{if } l = \pm N/3 (\bmod N) \\ -1 & \text{otherwise} \end{cases} \tag{4.3}$$

Testing both the primitive and irreducible polynomials, it was verified that they have an autocorrelation of the above form.

Very little research has been specifically conducted into quaternary m-sequences (or quaternary Gold codes) because the alphabet is not prime and some of the good properties of binary codes are therefore altered for the quaternary sequences, as discussed above. In this thesis, all twelve polynomials in table 4.4 may be referred to as m-sequences for the reasons given below. However, the tests conducted in chapter 5 are restricted to only those generated by primitive polynomials. The autocorrelation of all of the sequences (irreducible or primitive) is the same. However, interesting results were obtained when

the crosscorrelations were tested. Certain pairs of sequences produce even periodic crosscorrelations which are purely real-valued. This is not restricted to only pairs of primitive, or pairs of irreducible polynomials, as both classes can in some instances produce this result, as can some irreducible and primitive combinations. Other combinations have the classic three-valued even crosscorrelation spectra for both the real and imaginary components. Thus, in the consideration of the randomness and correlation properties, the use of the term m-sequence for both irreducible and primitive polynomials is acceptable for quaternary codes. The author has not investigated them in relation to the shift-and-add property, because this is not of importance to the research of this thesis.

Another technique for generating quaternary codes and perhaps an obvious way, is to combine binary sequences. The quaternary sequence a can be formed from the binary $\{\pm 1\}$ base sequences b and c, via for example:

$$a_i = \frac{1}{2}(1+j)b_i + \frac{1}{2}(1-j)c_i \tag{4.4}$$

Relationships can also be found between the quaternary and binary correlation functions with this approach. This can provide a large number of codes [95, Table I] (260 of period 63), but although the properties of the lower-level sequences may be good, after their combination and subsequent mapping to quaternary symbols, the new sequence cannot be guaranteed to have good (as considered in the previous chapters) properties. For example, Hammons and Kumar [63, p.222] note that the combination of two independent Gold codes can produce a resultant quaternary code that has a peak even periodic crosscorrelation which is twice as large as the peak of the binary Gold sequences from which it is formed.

Several quaternary code generation techniques which do produce a family of codes with good crosscorrelation properties (usually only the peak even periodic crosscorrelation is considered), suffer from the expected problem of an insufficient number of codes in the family, e.g. Barker codes; Sidelnikov sequences; real-valued (R.V.) Bent function sequences; Novosad sequences; and the 4-phase near-optimal sequences of Boztaş, Hammons and Kumar, family $\mathcal{B}$. This is expected from the Welch/Sarwate bounds which show how the family size and peak correlation may be traded off. A reduction in the peak crosscorrelation leads to a smaller number of codes in the family. This is most clearly illustrated by Kumar et. al.'s nested chain technique [96] which transforms a binary code

family into a quaternary code family. Table 1 in [96] shows that the code family size decreases as the peak crosscorrelation decreases.

Kumar et. al.'s nested chain technique is analogous to a binary to quaternary (BTQ) transform, i.e. a mapping of binary symbols to quaternary symbols. The BTQ transformations of for example Antweiler et. al. [184, 8] (and the similar technique of Fukumasa et. al. [44, 45]), produce quaternary sequences whose absolute peak crosscorrelation values (even and odd periodic) are smaller than the binary base sequences if the length of the codes is an odd number. Considering the peak of real and imaginary components does not allow the same conclusion to be drawn. The peak correlation value is the same for an even code length and it may or may not be less for an odd code length. The potential drawbacks of binary to quaternary transformations are therefore:

1. The number of quaternary codes is equal to the number of binary codes. However, many binary code families contain an insufficient number of codes, and this was one of the reasons for considering non-binary codes, to obtain larger code families.

2. BTQ transformations may not exploit the increased number of code symbols in the quaternary alphabet to produce codes with smaller peak crosscorrelation values.

In regard to this second point, it has been shown in section 1.3 that a set of non-binary codes should exist, which have a peak crosscorrelation value equal to $1/\sqrt{2}$ of the value for the best binary codes, for a given family size. The only known example of a set of quaternary codes which achieve this in comparison to binary Gold codes are those proposed by Solé [180] and then independently as family $\mathcal{A}$ by Boztaş et. al. in [17]. These codes are often regarded as the best (in terms of the peak value and family size) quaternary codes. Many results on the correlations of these codes are given in [17], along with the characteristic polynomials from which the shift-register recurrence relations can be derived. However, the author feels that the best description of deriving the shift register recurrence relations from the characteristic polynomials is given in [18] where the quaternary codes are used as a base for generating non-linear binary codes. Some points to note in relation to these codes are: firstly, the arithmetic is modulo 4 ($\mathcal{Z}_4$), and secondly the codes are not maximal length.

The literature on the quaternary codes, both family $\mathcal{A}$ and $\mathcal{B}$ of Boztaş, Hammons and Kumar, considers the entire even periodic crosscorrelation distribution. The only

other paper referenced above which also does this is by Matsufuji and Imamura [118] which shows that the real-valued (R.V.) Bent function sequences have a 5-valued even periodic distribution. Matsufuji and Imamura also show that the R.V. Bent sequences are balanced. The remaining papers in most cases consider either only the autocorrelation (and sidelobe energy) of the sequences, or the peak auto- and cross-correlation. The absolute value is often considered rather than the real and imaginary component values as well. The BTQ transformations of Antweiler et. al. and Fukumasa et. al. are also the only ones to consider the odd periodic correlation as well as the even periodic correlation. Similarly, a large proportion of the literature in relation to the non-binary ($q > 4$) sequences reviewed in table 4.2 considers only the minimisation of the absolute peak even crosscorrelation and out-of-phase autocorrelation simultaneously. Thus the reader can now see the discrepancy between the properties emphasized by spreading code designers and the properties highlighted by the system analysis.

4.3 The Dual Problem

The review of existing non-binary code generation techniques in the previous section shows that many, though not all, contain a relatively small number of codes in the family in comparison to the code period. Many have also been designed to simultaneously minimise the non-trivial peak auto- and cross-correlations. Further, although the review does not discuss this in detail, many techniques cannot be easily implemented by a computer or in hardware. In regard to this point, it is considered beneficial at present to retain a shift-register configuration for the generation of the codes due to the expected increased speed of operation in comparison with accessing the code from memory, or generating it via a Fast Fourier Transform (FFT) as Suehiro does.

Very few of the code generation techniques reviewed consider the randomness properties of the codes either. An important exception to this is the theory of m-sequences. Historically m-sequences have formed the basis, or can be related to, many binary and non-binary code generation techniques. Figure 4.2, which is an extension of [132, Fig. 1], illustrates the relationship between m-sequences and other code generation techniques.

The mathematical basis of m-sequences is Group theory over the Galois field GF(2),

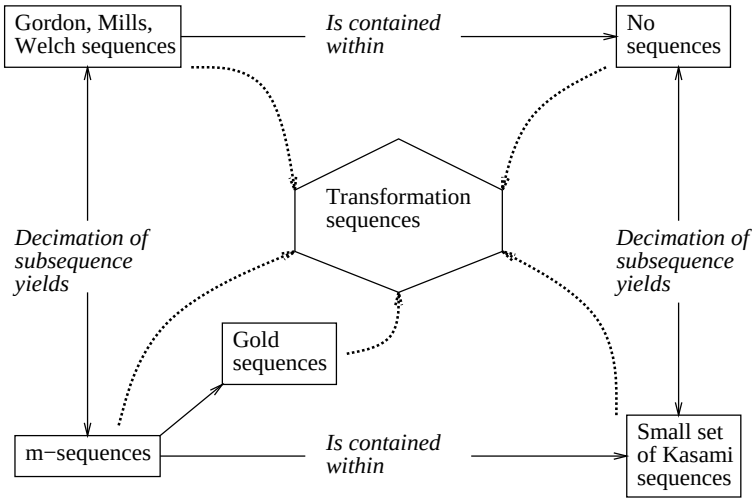


Figure 4.2: Relationships between code generation techniques

a field containing the two binary elements and an operator $\{0, 1, +\}$, which is usually mapped onto $\{+1, -1, *\}$ by isomorphic correspondence. Note that a field contains two operators, but binary multiplication is trivial and can therefore be neglected. To obtain the recurrence relation which defines the shift-register architecture and generates the m-sequence, one needs to find a primitive polynomial over GF(q). GF(q) is defined by the addition and multiplication operations on the symbols of the alphabet. The problem of generating codes could be viewed differently however, i.e. the following research question could be posed: "Is it possible to find an arithmetic (operator definitions) for a given shift-register configuration which will produce a maximal-length sequence?" The investigation of this problem, referred to as the Dual Problem (DP), may be regarded as the converse (or dual) of existing m-sequence theory. Figure 4.3 illustrates the relationship between m-sequence and DP theory. The word dual was proposed because of the analogy with the Primal-Dual problems in Linear Programming, it is not used in the sense of the dual code of coding theory.

The concept of defining an arithmetic is not new and apart from any literature specific to mathematical research topics (e.g. number theory), it was employed by Welti in [194]. The application of this as a method of pseudorandom code generation however, has only been discussed by Kościelny and Mochnacki [90, 89, 125] to the best of the author's knowledge. The author of this thesis became aware of Kościelny and Mochnacki's

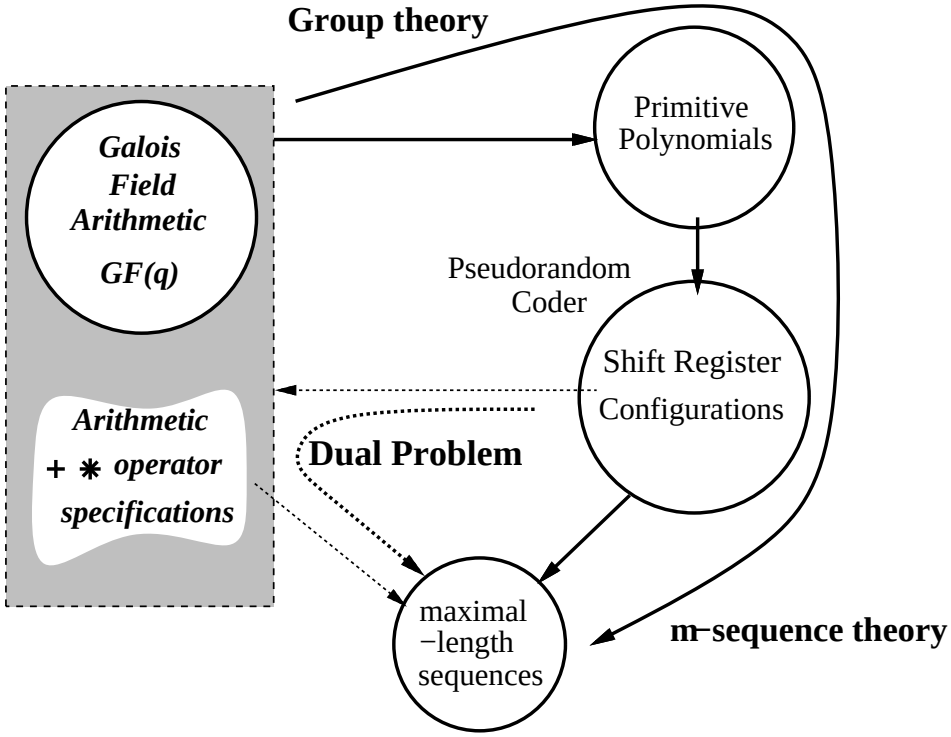


Figure 4.3: The relationship between m-sequence theory and the Dual Problem

work after independently publishing the Dual Problem idea in [161]. However, there are significant differences between the two proposals, and these are discussed in section 4.3.4.

It is also important to realize that the entire essence of the Dual Problem is to provide an alternative view of code generation. Identification of which constraints should be used to define the operators is the research issue, and this is treated in the next section, section 4.3.1. Section 4.3.2 then examines the constraints employed in section 4.3.1 with the Dual Problem to show that it is a valid method of code generation, i.e. they do generate pseudorandom codes. This section also provides an important conclusion in regard to some of the properties satisfied by conventional finite field arithmetic, which the DP arithmetics do not need to satisfy in order to generate PN codes. Section 4.3.3 therefore compares, in greater detail, the properties satisfied by the arithmetics in section 4.3.1 with all of those satisfied by finite field operators. This section is particularly important in the theory of the Dual Problem for PN code generation.

In summary therefore, this section concentrates on the properties of the arithmetics employed in the Dual Problem. An investigation of the properties of the sequences

$\oplus$	*0*	*1*	*2*	*3*
0	A	B	C	D
1	B	E	F	G
2	C	F	H	I
3	D	G	I	J

$\otimes$	*0*	*1*	*2*	*3*
0	*0*	*0*	*0*	*0*
1	*0*	K	L	M
2	*0*	L	N	P
3	*0*	M	P	Q

Table 4.5: Operator Templates: (a) Addition $\oplus$; (b) Multiplication $\otimes$

generated by the Dual Problem is given in section 4.4.

4.3.1 Addition And Multiplication Operators

The previous section introduced the concept of the Dual Problem as a method of code generation. However, the concept of the Dual Problem does not specify which constraints should be placed upon the arithmetic. This section therefore identifies suitable properties for the addition and multiplication operators to constrain the problem.

To define the addition operator $\oplus$, two of the properties of groups are employed: closure, and commutativity to provide symmetry. The other properties of groups: associativity, identity, and inverses, are not made mandatory in defining the operator structure. The only other constraint utilized is the necessary, but not sufficient, condition for the existence of a finite field: Every element should appear once and only once per row and per column of the table defining the group (or the operator). This constraint, referred to as the Balanced Symbol Distribution (BSD), ensures that the distribution of symbols in the operator specification is uniform. It will be shown later that the BSD is important in relation to the stability and randomness of the codes.

Over the quaternary alphabet, a computer search found 96 possible addition operators existed with these constraints. Of these only 16 could form an Abelian group, these 16 result from isomorphic correspondence. Table 4.5(a) is a template for the addition operator. Each element in the following sets is distinct: { A,B,C,D }; { B,E,F,G }; { C,F,H,I }; { D,G,I,J }; with A...J$\in$\{ *0,1,2,3* \}.

To define the second operator multiplication $\otimes$, closure and commutativity are again used as constraints. In order to distinguish the addition and multiplication operators, multiplication employs the extra constraint that $0 \otimes A = 0$, for all symbols A. This is

not necessary, but it retains the similarity to integer and GF(q) multiplication. The constraint used for the addition operator, that each symbol occurs once and only once per row and column, is again employed, but modified to only apply to the non-zero symbols with multiplication. Thus in each row or column (except the one corresponding to the null or zero symbol *0*), each symbol appears once, thus maintaining the balanced symbol distribution. A template of the multiplication operator is shown in table 4.5(b). Each element in the following sets is distinct: { K,L,M }; { L,N,P }; { M,P,Q }; with K...N,P,Q∈{ *1,2,3* }.

Multiplication defines the gains of the feedback path from the shift-register stages. A gain=*0* (the null symbol) is not the same as the case where no feedback from that stage is connected. To avoid confusion a gain=*0* is not used. The operation $0 \otimes 0$ therefore cannot occur by definition and thus although it need not strictly have been defined, it is specified that $0 \otimes 0 = 0$ for completeness.

With these constraints and the four-symbol alphabet, six multiplication operators exist. Three of these satisfy all of the properties of an Abelian group. Therefore the total number of addition/multiplication operator combinations which need to be tested on a given architecture for the production of maximal-length sequences is 576. This value is dependent only on the cardinality of the alphabet and not on the coder memory order m. The complexity of finding primitive polynomials is dependent on the coder memory order. A point to note is that finding the DP addition operators is the "Latin squares" problem from mathematics, with the extra constraint to provide symmetry for the operator. Finding the Dual Problem codes by a computer algorithm is also very simple to implement and this is discussed in the next section.

The next section, section 4.3.2, illustrates the ideas of the Dual Problem with an example. It is also shown that not all of the shift-register configurations can produce maximal-length sequences. This is due to the constraints employed with the Dual Problem, with other constraints this situation may not arise.

4.3.2 Code Existence

To test the validity of the Dual Problem as a method of code generation, a generic feedback shift-register coder was simulated in software. Its operation was verified by hand calculation to ensure correctness. The simulation generated all 576 possible addition and multiplication specification combinations for the quaternary alphabet, and tested these as operators in the feedback configuration employed. A point to note is that GF(4) arithmetic arises as a special case of the 576 possible DP arithmetics. This algorithm, although the simplest, has a high computational complexity for finding all possible DP codes for all possible coder configurations. However this need not necessarily be done, one configuration may be chosen and only the codes for that one found.

Table C.1 given in appendix C shows the number of codes which exist for each monic polynomial (shift-register architecture) for the symbol memory order $m = 3$ (the code period is $N = 63$). This table also shows the number of codes which are distinct for each configuration. The distinctness of the codes could be tested by an order $\mathcal{O}\{N.U\}$ complexity algorithm; U is the number of codes for comparison, N the code period. The reduced complexity of the distinctness test is a direct consequence of the stability of the DP codes (shown in section 4.4.1), which allows the same initial register contents to be used in all tests. Hence in testing the distinctness of the codes, time shifts (different code phases) did not need to be considered.

Over all $m = 3$ shift-register configurations there exist 1692 codes of which 246 are different. This is substantially more than the number of m-sequences of the same code period. A point to note with the Dual Problem is that the emphasis need not be on finding all of the DP codes, rather a shift-register configuration is selected and the codes for that configuration are found. The complexity of the problem is then substantially reduced in comparison with finding Gold codes for example, if one must first find the primitive polynomials and then the preferred pairs of m-sequences.

Some important conclusions have been drawn in obtaining the results of table C.1. Consider first the coder configuration: $D^3 = \mathit{1} \otimes D^2 \oplus \mathit{1} \otimes D^1 \oplus \mathit{1} \otimes D^0$, a non-primitive polynomial over GF(4). This shift-register configuration and the multiplication operator **m1**, given in table 4.6, produce eight distinct DP codes. These codes are labelled $\widetilde{A} \ldots \widetilde{H}$ and the corresponding addition operators are given in section C.2 of appendix C.

$\otimes$	*0*	*1*	*2*	*3*
0	*0*	*0*	*0*	*0*
1	*0*	*1*	*3*	*2*
2	*0*	*3*	*2*	*1*
3	*0*	*2*	*1*	*3*

Table 4.6: Multiplication Operator, **m1**.

Associativity of the addition operator is not necessary for the production of any of these eight DP codes. To show that $\widetilde{A}$ is non-associative it must be shown that there exists A,B,C $\in \{0,1,2,3\}$ such that: (A$\oplus$B)$\oplus$C$\neq$A$\oplus$(B$\oplus$C). Choosing A=*1*, B=*1*, C=*0* gives (A$\oplus$B)$\oplus$C=(*1*$\oplus$*1*)$\oplus$*0*=*0*$\oplus$*0*=*0*$\neq$A$\oplus$(B$\oplus$C)=*1*$\oplus$(*1*$\oplus$*0*)=*1*$\oplus$*2*=*1*. Thus the addition operator for $\widetilde{A}$ is non-associative. Note, that if each symbol is multiplied by *1* using the operator **m1** so as to be consistent with the example shift-register configuration, then associativity still does not hold. This is because $1 \otimes \beta = \beta$ for **m1** and β = {A,B,C} $\in$ {*0,1*} above. It is also possible to verify that the operators $\widetilde{B} \ldots \widetilde{H}$ are non-associative. Further as a group requires associativity to hold, so the addition operator does not need to form a group (or Abelian group) in the production of DP sequences. Neither is the existence of a finite field required, because it relies on the addition operator forming a group. This issue is investigated in greater detail in the next section.

An examination of table C.1 further shows that not all shift-register configurations produce maximal-length sequences. The question arises therefore as to the existence of q-ary DP codes for an arbitrary symbol memory order (m).

Theorem 4.3.1 *DP codes produced by the constraints of section 4.3.1 will exist for all symbol memory orders m.*

Proof:

The Corollary given as [16, Corollary 4.6.14, p.89], proves that for every finite field GF(q) and positive integer m, there exists at least one primitive polynomial $f_q^m(D)$ over GF(q) of degree m. The arithmetic of GF(q) arises as a special case of the set of arithmetics for the Dual Problem, thus there is at least one DP code for every symbol memory order m. That DP code is generated by the configuration $f_q^m(D)$ and the arithmetic of GF(q).

■

It should be noted, that no attempt is made to prove that the DP codes will always produce more codes than m-sequence theory for a given symbol memory order, but it is not unreasonable to accept this as true. A search by the author has also revealed the existence of DP codes of period 255 ($m = 4$). Table C.4 gives the coder configurations which produce DP codes of period $N = 255$ and the number of distinct sequences for each configuration. The complete number of distinct sequences when all configurations are considered could not be determined due to the memory limitations of the software in which the program was implemented.

The results of table C.1 for codes of period 63 and table C.4 for codes of period 255 show, that in most instances, configurations which tap each delay element will produce codes, but some exceptions to this have been found for the codes of period 255.

Thus in summary, this section has shown that the Dual Problem is a valid method of code generation. It has also found that it is possible to relax some of the constraints on the arithmetic used to generate the codes in order to obtain a larger number of sequences. The next section therefore compares the constraints used with the Dual Problem arithmetics, with the properties satisfied by conventional GF(q) arithmetic. This then explains why properties such as associativity can be removed in the production of the DP sequences.

4.3.3 Relationships To Group Theory

The results of section 4.3.2 have illustrated the validity of the Dual Problem for producing quaternary codes. Further, the codes have been produced without the need for a finite field to exist between the addition and multiplication operators. The question arises therefore as to which operator properties are necessary to produce a maximal-length sequence. This question is investigated in this section by considering each of the properties which a finite field operator must satisfy. Those properties were defined in section 4.1.

Associativity

Associativity is not a necessary condition for the production of a maximal-length sequence, as the previous section found. To illustrate why this is so consider the shift-

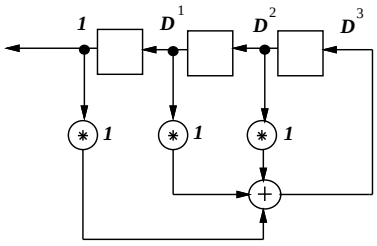


Figure 4.4a: Shift-register schematic $D^3 = 1 \otimes D^2 \oplus 1 \otimes D^1 \oplus 1 \otimes D^0$.

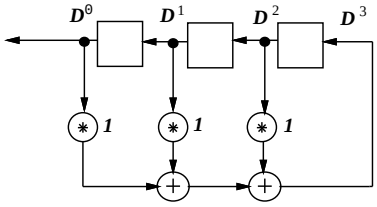


Figure 4.4b: Shift-register implementation $D^3 = 1 \otimes D^2 \oplus 1 \otimes D^1 \oplus 1 \otimes D^0$.

register schematic in figure 4.4a. In this diagram three symbols are added together and the order of application of addition need not be specified, hence suggesting that associativity applies. Figure 4.4b is another interpretation of the same polynomial used for figure 4.4a however, and this is what is implemented in the software simulation, and how the system could be implemented if discrete electronic components are used for a hardware construction. In this second system the order of addition of the three symbols is always defined, hence associativity is not a necessary condition.

Identity

A shift-register of symbol memory order m, can have a maximum period of q^m. With linear feedback (the use of GF(q) arithmetic or m-sequence theory), which is not true for the majority of DP operators considered, this period is reduced by one due to the self-perpetuation of the all-zero state. This occurs because *0+0=0*, and *0*A=0* for all symbols A. Thus it is the use of the addition identity element as the null element in the multiplication operator, which ensures that the period of a maximal-length sequence is $N = q^m - 1$.

For the constraints utilized with the DP codes identity under addition is not strictly specified, and consequently it is not possible to prove that period q^m cycles (referred to as de Bruijn cycles [53, chpt. 6], [41, 198]) do not exist. Golomb [53, Theorem 9,p.124]

states that in order to produce a sequence of length q^m from an m stage shift-register, it is necessary to use all m available tap positions. Unfortunately, no proof was given so this could not be used as a technique to disprove the existence of such cycles here. By incorporating the extra constraint that there exists a symbol $\beta \in \{$ *0,1,2,3*$\}$, such that $\beta \oplus \beta = \beta$ and $\beta \otimes \mathrm{A} = \beta$ for all symbols A, period q^m cycles can be eliminated. The defined maximal-length quaternary sequences would then have a length of $4^m - 1$. Defining such an identity operator is not worthwhile however, as the codes are found by a computer search which can ignore any such sequences. Secondly, if they do exist then they may make good PN sequences. Golomb also showed in [53] that pure cycles do not exist if the feedback configuration can be written in the form $f_b(x_1, \ldots, x_n) = c.x_1 + g(x_2, \ldots, x_n)$, where $g(.)$ represents the non-linear component of the feedback function $f_b(.)$. Thus maintaining Galois arithmetic for the appropriate component of the feedback operation could eliminate these cycles. This is an issue which may be considered in future research.

An identity element under multiplication, which conventional arithmetic denotes as "one", is also unnecessary. Maximal-length sequences exist for those operators which do not satisfy this constraint. The multiplication operator **m1** (given in table 4.6), which is used in the example of section 4.3.2 illustrates this.

Inverses

The existence of an inverse for each symbol relies on the existence of an identity element. Identity does not contribute to the production of maximal-length sequences, as shown above, but indirectly contributes to the period of the PN sequence. Consequently an inverse for each element will not contribute to the existence of a maximal-length sequence. The author has as yet been unable to find any relationship between the properties of pseudorandom sequences and inverses, and therefore considers that this constraint can be removed. Identity and inverse are important in mathematically proving much of the theory associated with linear feedback shift-registers (LFSRs). The removal of these properties therefore means that the proofs of many results are not easily extendable to the Dual Problem.

Distributivity

Distributivity is not a necessary condition by the same reasoning that associativity has been shown to be unnecessary i.e. the order of application of the operators is always specified, hence $(A \otimes B) \oplus (A \otimes C)$ is always performed, never $A \otimes (B \oplus C)$. Distributivity may only be important for minimizing, with some architectures, the number of operators used and hence the number of discrete electronic components in the coder's implementation.

Finite field

The results of section 4.3.2 have found that a finite field is not necessary for the existence of maximal-length sequences. This is expected because definition 4.1.10 shows that for a field to exist, a group must exist. In addition, the above discussion has shown that some of the properties of groups are not necessary in defining the operators so as to produce maximal-length sequences, thus a group and hence a finite field need not exist. However, the existence of a finite field may ensure simplicity in the implementation of the operators. Green and Taylor discuss the relationships between the operational description of the circuit and the algebra employed in [62]. This issue is not investigated in this thesis, but it could be pursued as future research.

The necessary, but not sufficient condition for the existence of a finite field, the requirement of a balanced symbol distribution (where each symbol occurs once and only once per row and per column of the operator specification) is important. Whilst this feature seems to intuitively provide the desired randomness properties of PN sequences, it is shown in section 4.4.1 that it is important in ensuring that the DP codes are stable. The stability of the codes is then shown to be important in proving the randomness properties. Before investigating the stability and other properties of DP codes in section 4.4, the next section digresses slightly. This section has compared the DP arithmetics with arithmetics used in Group theory. The next section compares them with the arithmetics used in Spurious Galois Field theory, an idea proposed by Kościelny and Mochnacki and referred to previously.

4.3.4 Relationships To Spurious Galois Fields

Section 4.3.1 remarks that the author of this thesis became aware of a proposal using arithmetics similar to those of the Dual Problem, after the author published the concept in the journal paper [161]. Whilst similarities can be found between the arithmetics used in the two independent proposals, the overlaying concepts are fundamentally different. The Dual Problem can therefore be regarded as an original contribution to the knowledge of spread-spectrum communications. The relationships between the arithmetics used in the two proposals and their differences are discussed in this section.

In 1989 Kościelny proposed [90], for the field of cryptography, the idea of a Spurious Galois Field SGF(q), which is an algebraic system $\langle \mathcal{S}_{\mathcal{F}}, +, \cdot \rangle$ of q elements satisfying the following axioms [91]:

1. $\langle \mathcal{S}_{\mathcal{F}}, + \rangle$ is an algebraic loop with identity element denoted by *0*.
2. $\langle \mathcal{S}^{\star}_{\mathcal{F}}, \cdot \rangle$ is an Abelian cyclic group, where $\mathcal{S}^{\star}_{\mathcal{F}} = \mathcal{S}_{\mathcal{F}} - \{0\}$.
   Hence $\mathcal{S}_{\mathcal{F}} = \{0, 1, w, \ldots, w^{q-2}\}$, where w is the generator of the multiplicative group and $w^{q-1} = 1$, where *1* is the identity element under multiplication.

The reader may recognise the similarity with Galois field theory with this notation for the code elements.

3. There exists $-1 \in \mathcal{S}_{\mathcal{F}}$, such that $-1 = 1$ if q is even, or $-1 = w^{(q-1)/2}$ if q is odd.
4. For any element $\mathrm{A} \in \mathcal{S}_{\mathcal{F}}$: $\text{-}\mathrm{A} = -1 \cdot \mathrm{A}$ and $\mathrm{A} + (\text{-}\mathrm{A}) = 0$.
5. Distributivity holds.
6. For all elements $\mathrm{A} \in \mathcal{S}_{\mathcal{F}}$, $0 \cdot \mathrm{A} = 0$.

Spurious Galois fields therefore satisfy all of the axioms of Galois fields except for associativity. The multiplication table is the same for all SGF(q), but each has a different addition table. Galois fields are therefore a subset of Spurious Galois fields, which are a subset of the Dual Problem arithmetics proposed in this chapter. Kościelny found that only one Spurious Galois field of four elements existed from which a PN code could be generated. This may be contrasted with the 576 arithmetics for the Dual Problem which can be used to generate quaternary PN codes.

Kościelny and Mochnacki also proposed a more general (than Spurious Galois fields) algebraic system in 1991 as a research note [92], the only publication at present in which they have considered such an algebraic system. Defined as a Spurious ring $\langle \mathcal{S}_{\mathcal{R}}, +, \cdot \rangle$, it satisfies the following axioms:

1. $\langle \mathcal{S}_{\mathcal{R}}, + \rangle$ is an arbitrary additive system.

2. There exists $\mathrm{E} \in \mathcal{S}_{\mathcal{R}}$ such that for all $\mathrm{A} \in \mathcal{S}_{\mathcal{R}}$, $\mathrm{E} \cdot \mathrm{A} = \mathrm{A} \cdot \mathrm{E} = \mathrm{E}$.

3. $\langle \mathcal{S}^{\star}_{\mathcal{R}}, \cdot \rangle$ is an arbitrary multiplicative system, where $\mathcal{S}^{\star}_{\mathcal{R}}$ denotes $\mathcal{S}_{\mathcal{R}} - \{\mathrm{E}\}$.

The term 'arbitrary algebraic system' refers to either an abelian or non-abelian, quasigroup or group. Thus Spurious rings do not necessarily satisfy the property of commutativity. Consideration of definition 4.1.8 for a quasigroup shows that this is equivalent to the requirement of the Balanced Symbol Distribution (BSD): every element should appear once and only once per row and column of the table defining the operator. A Spurious ring with the additional constraint of commutativity is therefore equivalent to the Dual Problem arithmetics with the constraints previously defined. However, the reader is reminded that the Dual Problem can be defined with different constraints on the arithmetics.

Kościelny and Mochnacki investigated Spurious Galois fields and Spurious rings for the purpose of developing cryptographic keys to improve the complexity of stream ciphers (see for example [125, 92, 91]). The PN codes were also generated from a given recurrence relation; notice the difference here with the Dual Problem that finds recurrence relations which produce maximal-length sequences. Thus there are fundamental differences between the two proposals in their development and subsequent application. Kościelny and Mochnacki, who also researched properties important for the use of their codes in stream ciphers, found that their codes had a high linear complexity. This property can also be important in spread-spectrum communications so section 4.4.3 investigates the linear complexity of DP sequences. Kościelny and Mochnacki did not investigate the stability, randomness or correlation properties of their codes. These are investigated for the DP codes in the next section and in chapter 5.

4.4 Properties Of The Dual Problem Codes

This section investigates the stability, randomness and security (or linear complexity) of the new codes. An investigation of the system performance (or correlation) of subsets of codes and a brief comparison between different code generation techniques is given in chapter 5.

4.4.1 Stability

The codes produced by the DP method are for the majority of cases non-linear. That is, in most cases they are generated from a shift-register configuration which does not employ linear (Galois Field arithmetic) feedback.

A desirable property of non-linear codes is the stability of the code sequence. This allows the search for maximal-length non-linear codes to be independent of the initial shift-register contents. Stability is also referred to in the literature as the reversibility of the code and is equated with the state transition diagram of the code being branchless, or containing only a pure cycle [53, p.15]. Each state represents the contents of the shift-register at that time. Figure 4.5a is an example of a state transition diagram for a stable code. All codes generated by a linear feedback shift-register (LFSR) are stable. In contrast, figure 4.5b shows the state transition diagram for an unstable code. With the unstable code several initial sequences need to be considered in the search for maximal-length sequences. This not only increases the complexity of the search algorithm, but also the algorithm for identifying the distinct codes, as time-shifts then need to be considered.

It will now be proven, after some preliminary definitions, that the Dual Problem codes using the constraints discussed previously are stable.

Definition 4.4.1 *For a register symbol memory order m, the contents of the register cells define the* **state s***:*

$$s \triangleq (s_0, s_1, \cdots, s_{m-1})$$

where s_j is a symbol of the alphabet.

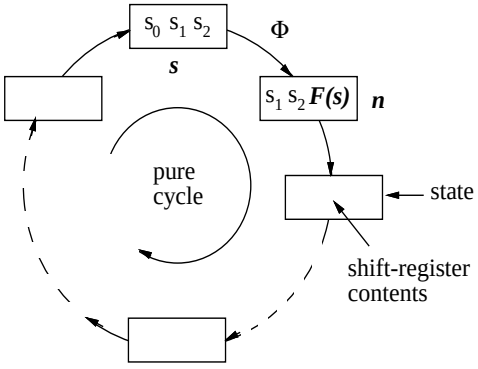


Figure 4.5a: State transition diagram: Stable code

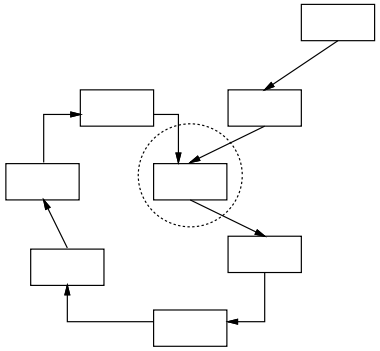


Figure 4.5b: State transition diagram: Unstable code

Definition 4.4.2 *The* **next state function** Φ*, transforms the present state* s*, to the next state* n*.*

$$n = \Phi(s) \stackrel{\triangle}{=} (s_1, s_2, \cdots, s_{m-1}, F(s))$$

where F *is the feedback function.*

Definition 4.4.3 *A code is* **stable** *if the function* Φ *is invertible.*

$$\Phi(s) = \Phi(s') = n \Rightarrow s = s'$$

This last definition can be shown to be equivalent to the statement that no branches exist in the state diagram for the coder. This is also equivalent to the statement that each state has a unique successor and a unique predecessor. Golomb discusses stability and the equivalence of these statements in [53, pp.115–116].

Theorem 4.4.1 *DP codes produced using the addition and multiplication operators defined by the constraints of section 4.3.1 are stable.*

The proof of this theorem is provided below as it highlights the constraints on the arithmetic which are important in ensuring that the codes are stable.

Proof:

(i). The element of the highest order stage is the only different element from one state to the next. This element is uniquely defined by the invariant feedback function, hence the successor of each state is unique.

(ii). To prove that each state has a unique predecessor:

For a given memory order m, and state s, let the feedback symbol be η:

$$\eta = F(s) \stackrel{\triangle}{=} a_0 \oplus \ldots \oplus a_j \oplus \ldots \oplus a_{m-1}$$

where $a_j : j \in \{1, \ldots, m-2\}$ is present if a connection is fedback from that cell of the shift-register. Element a_0 is always present, or the memory order is not m. Also $a_j = g_j \otimes s_j$ where g_j is the gain or multiplier in the feedback segment from stage j.

Assume that the predecessors s, and s' of state n are unique. As the next state is generated from definition 4.4.2 by:

$$n = \Phi(s) = \Phi(s')$$

so

$$s_j = s'_j : j = 1 \ldots m-1 \tag{4.5}$$

and $F(s) = F(s') = \eta$.

But $\eta = g_0 \otimes s_0 \oplus \breve{F}(s) = g_0 \otimes s'_0 \oplus \breve{F}(s')$ where $\breve{F}$ is the feedback operation excluding the first stage. Thus by (4.5), $\breve{F}(s) = \breve{F}(s')$. $\breve{F}(.)$ selects a row of the addition specification. The result symbol η, appears once and only once in that row via the balanced symbol distribution (BSD) constraint, so $g_0 \otimes s_0 = g_0 \otimes s'_0 = \eta_0$. As the non-zero (by definition) symbol g_0 selects a row of the multiplication operation, and each result symbol η_0 appears once and only once in that row (via the BSD), so $s_0 = s'_0$, which implies that $s = s'$. Hence each state has a unique predecessor.

The stability of the codes follows from (i) and (ii).

■

Proving that the Dual Problem codes are stable is a requirement of proving (in the next section) that they satisfy the desired randomness properties: Balance, Run and Window, discussed in the Introduction. Stability is also important in a practical sense as any glitch in the operation of the implemented coder can easily be recovered from with a stable code. This is not true of an unstable code.

4.4.2 Randomness

Section 3.4 modifies the pseudorandom code design philosophy to emphasize the desired randomness properties of codes (discussed in section 1.4). In testing Dual Problem codes of period 63 and 255 all of the codes which have been considered satisfy the Balance, Run and Window properties defined in section 1.4. This section therefore proves that the DP codes satisfy these properties. The proofs are analogous to those of Zierler for m-sequences, [200, Theorem 8 and corollary].

Theorem 4.4.2 *DP codes produced using the addition and multiplication operators defined by the constraints of section 4.3.1 satisfy the Window property defined in section 1.4.*

Proof:

For $r = m$: Every m tuple occurs precisely once in the period, except for one tuple, as the codes are maximal-length and stable.

For $r < m$: By induction, if for $r = k$ each tuple occurs the same number of times, then each tuple of length $r = k - 1$ also occurs the same number of times, unless it is a subtuple of the missing tuple of length m, in which case it occurs one time less than the others.

■

Theorem 4.4.3 *DP codes produced using the addition and multiplication operators defined by the constraints of section 4.3.1 satisfy the Run property defined in section 1.4.*

Proof:

There are q^m possible states when wraparound of the sequence is considered. A run of r symbols has a probability of $1/q^r$ of occurring unless it is part of the single missing m-tuple. Thus the number of times each run occurs is q^{m-r}, unless it is a subtuple of the

run length	$r=2$				$r=3$			
occurrence	symbol							
sequence	*0*	*1*	*2*	*3*	*0*	*1*	*2*	*3*
$\widetilde{A}$	3	4	4	4	0	1	1	1
$\widetilde{B}$	3	4	4	4	0	1	1	1
$\widetilde{C}$	4	3	4	4	1	0	1	1
$\widetilde{D}$	4	3	4	4	1	0	1	1
$\widetilde{E}$	4	3	4	4	1	0	1	1
$\widetilde{F}$	3	4	4	4	0	1	1	1
$\widetilde{G}$	4	3	4	4	1	0	1	1
$\widetilde{H}$	3	4	4	4	0	1	1	1

Table 4.7: Occurrence of runs for sequences $\widetilde{A} \ldots \widetilde{H}$.

missing tuple, in which cases it occurs one time less. Thus a run of r contiguous symbols occurs approximately $N.q^{-r}$ times in the sequence.

■

Corollary 4.4.1 *DP codes produced using the addition and multiplication operators defined by the constraints of section 4.3.1 satisfy the Balance property defined in section 1.4.*

Proof:

Let $r = 1$ in theorem 4.4.3.

■

Table 4.7 shows the number of runs (of length $r = 2$ and $r = 3$) for each symbol for the code sequences $\widetilde{A}$ to $\widetilde{H}$, results which are in agreement with the Run property given previously. Specific details on the generation of these codes has been given in section 4.3.2. Satisfaction of the Window property for sequence $\widetilde{A}$ is shown by table 4.8. Figure 4.6 also shows how the probability of the occurrence of each symbol (in sequence $\widetilde{A}$), as a function of the sequence length, is nearly uniform (apart from the initial transient). This is Ronse's [164, p.89] second postulate, which is a generalisation of the Run property. Ronse's property is discussed in section 3.3 in relation to an element of a code being nearly independent of its predecessors. Similar results have been obtained for all other sequences tested.

To complete this section a few final comments need to be made. This section has investigated several a posteriori tests for randomness, of which the Balance property

occurrence	symbol			
	0	*1*	*2*	*3*
0	3	4	4	4
1	4	4	4	4
2	4	4	4	4
3	4	4	4	4

Table 4.8: Symbol pair occurrence for sequence $\tilde{A}$.

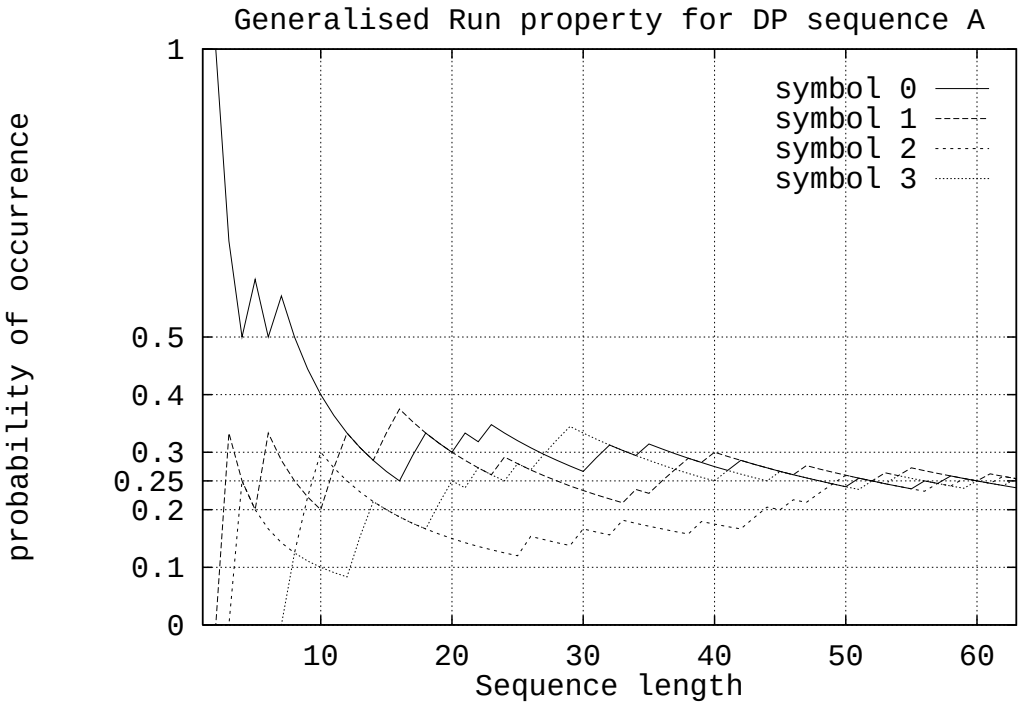


Figure 4.6: Examination of the generalised Run property of Ronse, for sequence $\tilde{A}$.

has the most practical importance (as the Introduction discusses). There is however no universally accepted test for randomness based on the properties of a finite length sequence, nor can there be. The Introduction discusses this in some detail, as does Knuth in [87, chapter 3]. Knuth also proposed a test for randomness referred to as the Spectral test [87, pp.82–97], which Fredriccson [42] showed could be related to the higher-order autocorrelations of the sequences. The spectral test and higher-order autocorrelations are not investigated in this thesis. However, they could be considered in future research as they provide a relationship between the randomness and correlation properties, and relating these properties is important. Randomness could also be expected to be related

to the degree of non-linearity of the sequence. In the next section the linear complexity of the DP sequences is investigated. Linear complexity provides a good insight into equivalent coders capable of generating the sequence. It is also important when the codes need to be secure (i.e. they are not easy to crack). Secure codes are of primary importance to military applications, but if the codes are secure then data encryption need not be employed for public systems. Data encryption may reduce the effective information rate. Linear complexity can therefore be an important property for spreading codes in some applications.

4.4.3 Linear Complexity

In the previous section the randomness properties of the DP codes have been proven to hold, and those of a subset of the sequences have been investigated. The randomness of a code really reflects the possibility of predicting the next element in the sequence given the previous elements, not the properties of the sequence generated. Thus one manner in which randomness could be measured for a sequence is by how easy (or difficult) it is to predict the next element given previous elements. If for example a binary m-sequence is considered, then only $2m-1$ elements of the sequence (of period 2^m-1) are required in order to predict the entire sequence. The Berlekamp-Massey algorithm, given as Theorem 2 of [116], can be used to reveal the structure of the m-sequence generator from $2m-1$ elements of the sequence. However, m-sequences satisfy the Balance, Run, and Window properties. Clearly, there is a conflict between the two methods of measuring the randomness of a sequence. This is discussed in further detail below.

The Berlekamp-Massey algorithm is an efficient technique for synthesising the shortest linear (GF(q) arithmetic) feedback shift register (LFSR) of length L, capable of generating any given sequence (the actual generation method of which may be unknown). Edwin Key employed this as the definition of the linear complexity of a nonlinear sequence in [82]. That is, the linear complexity of a sequence c, is defined as to be the length $L = \lambda(c)$ of the shortest LFSR capable of generating the sequence.

Thus from a military communications point of view, high linear complexity is important in relation to the security of the system; "How easy is it to crack the codes?" This issue is not as important for mobile or personal communications, but linear complexity

can be interpreted as a measure of the randomness of the sequence as the first two paragraphs above show. However, high linear complexity on its own does not guarantee good randomness, for example the sequence consisting of all zeros except the last element has a high linear complexity, but it does not satisfy the Balance, Run or Window properties. Rueppel [166] therefore used the linear complexity profile, a plot of the linear complexity $\lambda_n(c)$ as a function of the number of elements n of the sequence c that have been processed, to indicate randomness. Rueppel states that a good random sequence generator should have a linear complexity profile which closely, but irregularly follows the $n/2$ line.

Using the distribution of the number of binary sequences with a given linear complexity, Rueppel derived expressions for the expected step heights and lengths in the profile. Rueppel commented that the distribution of the number of q-ary sequences with complexity L, was given in "Gust 76". Unfortunately, this reference was not defined in Rueppel's paper, so the results have not been extended here to q-ary sequences.

Figures 4.7 and 4.8 show the linear complexity profiles of the DP sequences $\widetilde{A}$ and $\widetilde{B}$. It is clear from these diagrams that by Rueppel's definition these sequences are random, as their linear complexity profiles follow the $n/2$-line in an irregular manner.

Employing the Berlekamp-Massey algorithm with the DP codes $\widetilde{A}$ to $\widetilde{H}$, each has been found to have a linear complexity of 32, and an irregular $n/2$-line profile as desired. Thus DP codes can have high linear complexity, an expected result given the non-linear nature of the feedback connections in some cases. DP codes may therefore be suitable for applications other than as spreading codes, such as for use in stream ciphers. Future research could therefore investigate different applications for the DP sequences. Two additional points should be also noted. Firstly, a linear complexity of 32 means that 63 elements of the sequence are required to predict the next element, which is the entire sequence length. Secondly, although DP codes can have high linear complexity, because m-sequences are a subset of the DP codes, the linear complexity can be very low, $L = m = 3$, if the DP codes analysed are the m-sequences over GF(4). If high linear complexity is important, then a subset of codes can be found by neglecting GF(4) and its isomorphic fields when searching for codes.

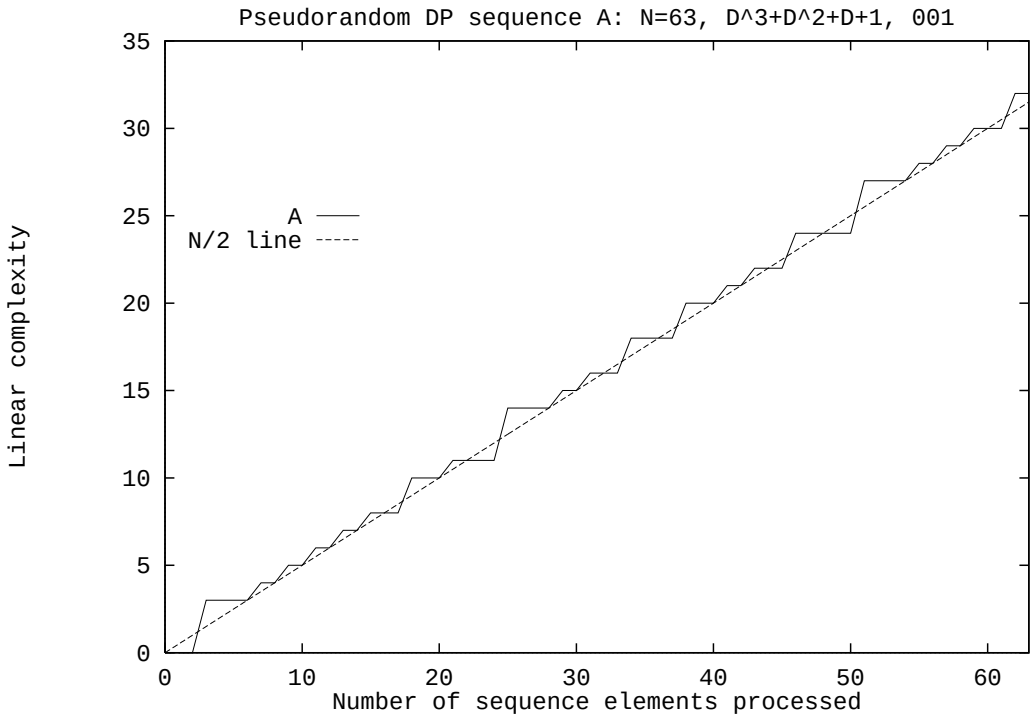


Figure 4.7: Linear complexity profile of DP code $\tilde{A}$

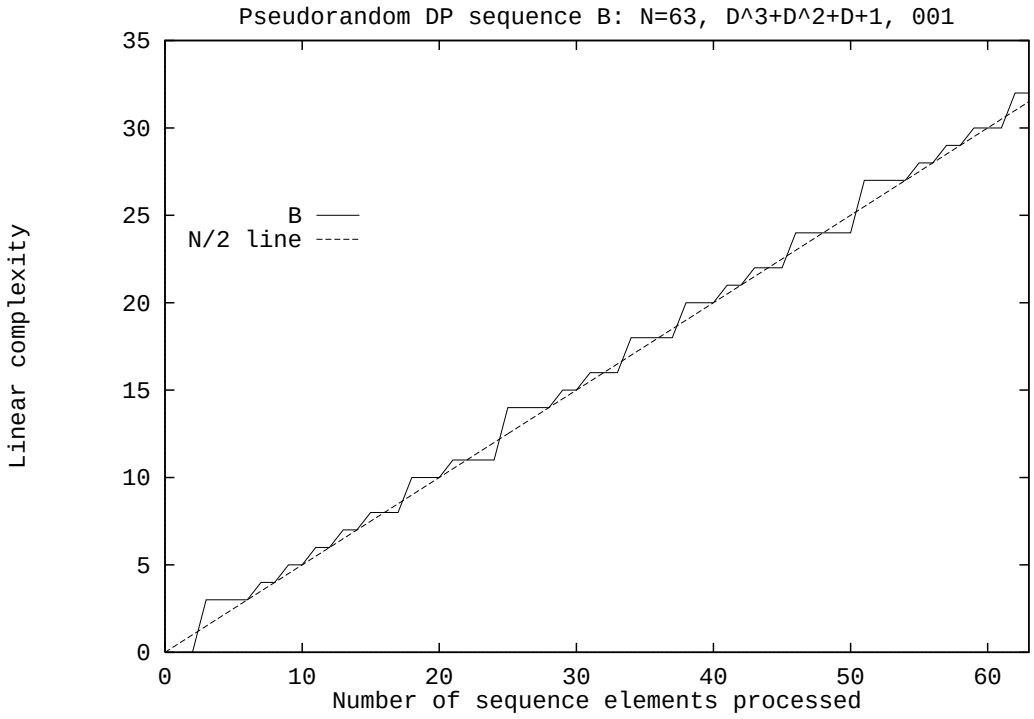


Figure 4.8: Linear complexity profile of DP code $\tilde{B}$

4.5 Overview

This chapter on code generation is an important component of the thesis. It provides the motivation for the research of the first two chapters, and for the investigation in the next chapter. Further, it provides the impetus for many future research topics, and these are discussed in chapter 6. This section therefore provides an overview of this chapter and summarises its key points.

The Introduction of this thesis discusses how very little prior research has been conducted into non-binary, and specifically quaternary, code generation. However, as the Introduction also shows, quaternary codes can provide many advantages for spread-spectrum communications, hence their investigation in this thesis. Before code generation may be considered however, the code designer must have a good understanding of code properties and how they influence performance. An examination of the existing literature on CDMA does not provide the necessary understanding, rather it shows a disparity between the properties emphasized by spreading code designers and those highlighted by the system analysis. This disparity has also been observed by others such as Kärkkäinen in [78]. Chapters 2 and 3 have therefore investigated code properties and they provide the necessary understanding for the system considered in this thesis. The results in those chapters also support a different, from the conventional min-max criteria, spreading code design philosophy. Rather than designing codes to minimise the peak cross- and auto-correlation simultaneously, which restricts the number of codes in the family, the codes are designed to satisfy the randomness properties. This then allows a greater number of potential codes to be considered. Subsets of codes satisfying other important properties can then be selected. This alternate code design philosophy has been discussed in the introduction to this chapter.

To develop a novel method of code generation for this approach, the author researched existing non-binary (and indeed binary) code generation techniques. Section 4.2 is a literature review of the different methods used to generate non-binary spreading codes. The review is separated into those techniques which are capable of generating quaternary $\{\pm 1, \pm j\}$ codes, and those which are not. One technique reviewed, m-sequence generation, provides the initiative for the development of the novel approach (the Dual Problem) in section 4.3.

In the theory of m-sequences an arithmetic is chosen (GF(q)), and the primitive polynomials found. A primitive polynomial can then be implemented by a shift-register configuration, which will generate a maximal-length sequence (an m-sequence), for any non-zero initial condition. In contrast, the Dual Problem considers a given shift-register configuration and then finds an arithmetic (the operators used in the feedback path of the shift-register architecture), so that the coder produces a maximal-length sequence. Thus the Dual Problem views m-sequence theory in reverse, and this is perhaps best illustrated by figure 4.3.

The main research issue however, is to identify the constraints on the arithmetic, i.e. to identify what properties the arithmetic operators must satisfy. This has been discussed in section 4.3.1, where the constraints specified for the operators are closure and commutativity, and that the operators satisfy the balanced symbol distribution (BSD). The balanced symbol distribution requires that every symbol should appear once and only once per row and per column in the table defining the operator. For the multiplication operator this only applies to the non-zero symbols. This property, the BSD, has been shown to be important in proving the stability and subsequently the randomness properties of the DP sequences, as discussed below.

Section 4.3.2 then shows that the Dual Problem (with these constraints), is a valid approach to code generation. This has been done by proving that with these constraints DP sequences exist for all code periods $q^m - 1$, where m is an integer and q is the alphabet size. What is more important however, is that section 4.3.2 shows that:

1. The DP arithmetics do not need to form a finite-field, and the two operators of the arithmetic do not need to form a group (in Group theory terminology).

2. The Dual Problem produces a substantially greater number of codes (for a given code period), than m-sequence theory does.

To explain the first point, the relationships between the Dual Problem arithmetics and finite-field arithmetics are discussed in detail in section 4.3.3. That discussion verifies that some of the properties satisfied by finite-field arithmetics can be removed for PN code generation. The removal of these properties is the reason why the Dual Problem generates more codes than m-sequence theory. However, if the sequences generated by

the Dual Problem are to be successfully applied in spread-spectrum communications, then it is their properties which are important. Thus the investigation of some of their properties in section 4.4.

The nature of the Dual Problem makes it difficult to prove general results on the properties satisfied by DP sequences, particularly in relation to their correlation, but there are two important properties which can be proven.

1. It is possible to prove that the Dual Problem sequences are stable. The proof of the stability of the DP sequences is given in section 4.4.1, and this proof relies upon the codes satisfying the balanced symbol distribution. Stability is important for non-linear codes (which the DP sequences are in general), because it allows the search for maximal-length sequences to be independent of the initial shift-register contents. Thus it reduces the search space or computational complexity of finding the codes. Further, stability is also important in proving the second series of properties below.

2. It is possible to prove the randomness properties of the DP sequences, i.e. the Balance, Run, and Window properties have been proven in section 4.4.2; These are properties which the code design philosophy of chapter 4 emphasizes.

To complete the investigation (in this chapter), of properties satisfied by the DP sequences, section 4.4.3 investigates a property related to randomness, linear complexity. Linear complexity is an important property when PN codes are used in cryptography applications, but it can also be important for spread-spectrum communications because it is a measure of how secure a code is. In section 4.4.3 the linear complexity and linear complexity profiles of a selection of DP sequences have been investigated. The results in this section show that DP sequences can have high linear complexities, hence they are very secure, and they may be considered for different applications in future research.

As mentioned above however, it is very difficult to prove any results about the correlation properties of DP sequences. Consequently, the correlation properties of a selection of DP sequences are investigated in the next chapter. The investigation concentrates on the crosscorrelation properties of the codes, and specifically it compares the performance of subsets of DP sequences with the performance of subsets of other quaternary sequences

(i.e. sequences generated by some of the techniques reviewed in section 4.2). Tabular values of the autocorrelation of selected DP sequences are given in appendix C.4. They have been included as an appendix because the important features of the autocorrelation spectrum have not been investigated as they have for the crosscorrelation spectrum. To determine the important features of the autocorrelation spectrum, the issues of synchronisation, acquisition and tracking, or transmission over a multipath channel need to be investigated. This thesis does not investigate those issues, but concentrates instead on transmission over the multiple-access channel. These issues can of course be investigated further in future research.

Chapter 5

Code Generation Comparisons

In the previous chapter a new approach to code generation has been developed and implemented, and properties relevant to the randomness of individual sequences have also been investigated. In this chapter, using the knowledge of chapters 2 and 3 in relation to system performance and code properties, the new code generation technique is evaluated against some of the other existing approaches reviewed in section 4.2 of chapter 4. The comparison is by no means exhaustive; nor is the intention to specify which is the *best* code generation technique, as clearly that is subjective and dependent upon many issues which have been researched and discussed in this thesis. It is also dependent upon the specific transmission channel that is employed and this thesis considers only a simple model, without several features of actual channels. The importance of this chapter is therefore to show that subsets of Dual Problem codes can perform comparably to other techniques, thus verifying that the refined code design philosophy, and specifically the Dual Problem approach to generating codes, is an acceptable technique.

The Dual Problem codes are compared with several other techniques in this chapter, including: Boztaş, Hammons and Kumar (family $\mathcal{A}$), or Solé codes; Novosad sequences; random codes generated by a program which simulates the tossing of four-sided dice; codes obtained by a binary to quaternary (BTQ) transformation on binary Gold codes; quaternary m-sequences and Gold codes. The period of all codes considered is 63. The Nested chain technique could also have been used for comparison, but those discussed above adequately illustrate the necessary results. Methods of code generation which do not produce sequences of period 63 have not been considered, because the system

performance is strongly dependent upon the choice of code period, and a comparison between sequences of different length would therefore be unfair. Specific details on the generation of the codes employed in the tests are provided in section 5.1.

Although the emphasis of this chapter is a comparison of the performance using codes generated by different techniques, the randomness and linear complexity properties of the codes are also compared in section 5.2 for completeness. However this chapter does not compare the autocorrelation properties of the codes and this is for a deliberate reason. The autocorrelation properties of different codes are not compared because the emphasis is on the multiple-access channel. Furthermore, the issues of synchronisation, acquisition and tracking, or transmission over a multipath channel are not investigated in this thesis, and it is for these issues that the autocorrelation properties are important. Thus future research is required to investigate these issues for the Q-CDMA system before a comparison of the autocorrelation properties of different techniques can be made. However for the interested reader, the literature reviewed in section 4.2 does provide some information on the autocorrelation properties of each technique. This information is usually only the magnitude of the peak (even periodic) out-of-phase autocorrelation value, or the sidelobe energy, but in some cases more detailed on the autocorrelation spectrum is provided. Section C.4 of appendix C also provides tabular information on the peak values and sidelobe energies for a selection of DP sequences. The author compared the magnitudes of these values with those expected an obtained for random sequences in [161]. The comparison concluded that the DP sequences have autocorrelation properties consistent with those of random codes. Certainly some of the other techniques reviewed do have better properties, but that is to be expected given their design approach which emphasized this property.

As mentioned above, the aim of this chapter is to compare the performance of subsets of codes generated by different techniques with subsets of DP sequences, and section 5.3 does this. The random or dice toss codes are employed to provide a comparison for average performance, following the philosophy of some authors that random codes should be used in the system. The codes developed by Solé and independently by Boztaş, Hammons and Kumar (family $\mathcal{A}$), simply referred to as Boztaş codes, are employed because they were expected to provide very good system performance. These codes are

held in high regard in the small but expanding literature on non-binary spread-spectrum. They are perhaps regarded analogously to the use of binary Gold codes as a benchmark for comparisons in binary spread-spectrum systems. The Boztaş codes have also been shown to have the optimal (in relation to the Welch bound) peak even periodic crosscorrelation value. The mean-square (aperiodic) crosscorrelation of these codes is also very good, i.e. it is generally less than the expected value of the MSC for random codes, $\mathcal{E}(\text{MSC})$. Özlütürk and Lam [136] have shown that $\mathcal{E}(\text{MSC}) = N^2$ for random non-binary codes, thus for codes of period 63, $\mathcal{E}(\text{MSC}) = 3969$.

The other code families are compared for completeness, and they provide some interesting results. Of more importance however are the results of section 5.3 in regard to the selection of subsets of the DP sequences. The selection of subsets of sequences is part of the code design philosophy of chapter 4, hence these results should be considered when applying DP codes in spread-spectrum communications. This is explained further in the summary of the chapter given in section 5.4.

5.1 Quaternary Codes Employed For Comparison With The Dual Problem Codes

This section provides the specific details on the generation of the codes used for comparison with those of the Dual Problem in the following two sections.

The Boztaş codes (family $\mathcal{A}$) of period 63, can be generated from the recurrence relations provided below, where the characteristic polynomial $f(x) = x^6 + 2x^3 + 3x + 1$, or 1002031 from [17, Table 1], is expressed as the recurrence relation $D^6 = 2D^3 + D + 3$ in the notation of this thesis. In a short hand notation this may be expressed as 002013. Notice the difference between the two notations is primarily that 1 and 3 are replaced by each other. This is because in modulo-4 arithmetic ($\mathcal{Z}_4$) minus one is equal to three, minus two is equal to two etc.

The six possible coder configurations for this period (expressed in the shorthand notation of this thesis), are: 002013, 330213, 103323, 102003 and 120333. Each of these configurations is capable of generating 65 distinct codes. These sequences are not maximal-length however, so $4^6 - 1$ initial conditions need to be considered in finding the codes

for a given configuration. Boztaş, Hammons and Kumar found the distinct sequences by loading the shift register with states not previously seen during the generation of prior sequences. It would be an interesting aside to directly compare the computational complexity of finding the Dual Problem codes with the computational complexity of finding all of the codes of family $\mathcal{A}$. The two techniques may well have a similar complexity.

In this chapter, the coder configuration employed is 120333, or $D^6 = D^5+2D^4+3D^2+3D^1+3$. The first initial condition is $\{3,3,1,0,0,0\}$, where the last element a zero is loaded into the delay element from which the output is tapped. The remaining initial conditions are $\{2,1,1,0,0,0\}$, $\{1,1,1,0,0,0\}$, $\{1,2,0,0,0,0\}$, $\{3,1,0,0,0,0\}$,$\{2,1,0,0,0,0\}$, $\{3,0,0,0,0,0\}$ and $\{1,0,0,0,0,0\}$. Each of these initial conditions corresponds to a code labelled $\widetilde{\mathcal{B}}_{A1}$ to $\widetilde{\mathcal{B}}_{A8}$ respectively.

The eight Novosad sequences of period 63 used in the tests of this chapter are given in [133, p.1085]. The four m-sequences used are the first four primitive polynomials given in table 4.4 of section 4.2.

Binary Gold codes, which are well known in the literature, can be generated using equation 4.1, given a preferred pair of m-sequences. A preferred pair of binary m-sequences are a pair which have a specific three-valued even periodic crosscorrelation spectrum. Sarwate and Pursley's paper [171] discusses this in detail. The even periodic crosscorrelation of binary Gold codes (and the preferred pair of m-sequences) of period 63 takes only the values from the set $\{-17,-1,+15\}$.

The only papers published on quaternary Gold codes are by Robert Gold in a company report [51] which the author of this thesis was not able to obtain, and by Krone and Sarwate in [95] which was based on Gold's report. In [95] two primitive polynomials, m-sequences U and V over GF(4) were considered. Each quaternary m-sequence was decomposed into two binary m-sequences $U = [W,X]$ and $V = [Y,Z]$ by [95, Eq. 17]. The quaternary Gold codes were then defined to be those for which W and Y formed a preferred pair of binary m-sequences. No similar statement was made concerning the selection of X and Z.

This thesis takes a slightly different approach which is more analogous to binary Gold code generation. To generate quaternary Gold codes the two primitive polynomial m-sequences $f(D) = D^3 + D^2 + D + 2$ and $f(D) = D^3 + D^2 + 3D + 2$ (initial conditions

$\{1, 0, 0\}$) are employed as the preferred pair. This is because in testing the even periodic crosscorrelation of these two codes it was found that the real component of the correlation is three valued $\{-17, -1, +15\}$ and the imaginary component also three-valued $\{0, \pm 8\}$. Thus because the components have a three-valued crosscorrelation spectrum, so the two sequences above were selected as the preferred pair. The quaternary Gold sequences are generated from these two sequences in the same manner as binary Gold codes are generated from a preferred pair, i.e. using equation 4.1. Testing the even periodic crosscorrelations of the first eight sequences it has been found that the real component takes values from the set $\{-17, -1, +15\}$ and the imaginary component values from the sets $\{0, \pm 8\}$ or $\{0, \pm 16\}$ or $\{0, \pm 8, \pm 16\}$.

The reader can recognise that just as there were similarities between the binary and quaternary m-sequences, there are similarities between binary and quaternary Gold codes. However, there are also important differences as has been shown and previously discussed. Krone and Sarwate discussed this in further detail and showed (based on Gold's report), that depending upon the binary base sequences employed, the family of quaternary Gold codes either had poor crosscorrelation properties or poor autocorrelation properties. Quaternary Gold codes and indeed quaternary m-sequences are therefore rarely investigated in the literature, as they are not as highly regarded as their binary counterparts. Indeed, of the techniques discussed here and in chapter 4, including the BTQ transform below, only the codes of Boztaş, Hammons and Kumar (or Solé), have been considered in any detail as they provide a large family of codes with good correlation properties.

The binary to quaternary (BTQ) transform discussed in [184] and [9] is applied to a family of binary Gold codes to generate the BTQ codes used in this chapter. The binary Gold codes are generated from the preferred pair of m-sequences $D^6 = D^5 + D^3 + D^2 + 1$ and $D^6 = D^5 + 1$ as given by [171, Figure 5]. The initial condition employed for both sequences is $\{1, 0, 0, 0, 0, 0\}$, and the variable 's' in the BTQ transformation, which is defined in the papers referenced, has been set equal to one. Specific information on the generation of the DP codes is provided in the sections in which they are discussed.

The following two sections compare the properties of a selection of codes for the different techniques, with subsets of DP codes. Section 5.2 compares the randomness

code	max	min
DP	32	3
m-sequences	3	3
Gold	6	3
BTQ (Gold)	15	9
Boztaş	21	21
Novosad	31	19

Table 5.1: Linear complexity of quaternary sequences of period 63

and linear complexity properties, and section 5.3 provides comparisons of the system performance (PBE). These two sections provide some important results.

5.2 Randomness And Complexity

In section 4.4 the randomness and linear complexity properties of the Dual Problem codes have been investigated. In this section those results for the DP sequences are compared with the corresponding results (for those properties), for the other quaternary code generation techniques considered.

Considering first the linear complexity of the codes, table 5.1 shows that the Dual Problem codes can have the highest linear complexity, a maximum value of 32. However, their minimum value can be very low (equal to 3), because the quaternary m-sequences are a subset of the DP codes. The linear complexity of m-sequences of period $q^m - 1$ is well known to be m, which equals 3 for quaternary codes of period 63. Similarly, the linear complexity of Gold codes is known to be $2m$, or 6 for codes of period 63. The minimum value of 3 occurs only for the first two Gold codes as these are the preferred pair of m-sequences. These generalisations have been verified for the codes employed in the tests. A general result for the linear complexity of the BTQ transformation, given that of the binary base sequence, is not available, however the tests conducted on the codes considered show that it has increased from a maximum of 12 and minimum of 6 for the binary Gold codes to a maximum of 15 and minimum of 9 for the transformed codes. An increase in complexity may or may not hold for other base sequences.

Examining the Boztaş codes produces an interesting result. All eight sequences considered have the same linear complexity and can be generated from the same recurrence

code	Balance	Run	Window
DP	Yes	Yes	Yes
m-sequences	Yes	Yes	Yes
Gold	Yes	No	No
BTQ (Gold)	No	No	No
Boztaş	No	No	No
Novosad	Yes	Yes	No

Table 5.2: Randomness properties of quaternary sequences of period 63

relation (or polynomial) over GF(4). This is an interesting result which the author has not seen reported in any prior literature concerning these sequences, and it may assist in furthering the understanding of these codes and their relationships with other families.

The results of table 5.1 therefore indicate that the DP, Boztaş and Novosad sequences can have good linear complexities and are thus secure codes. Additional data encryption may not be necessary therefore when these codes are employed as spreading codes. This is an advantage because data encryption can reduce the information rate or the throughput of the system.

Comparisons may also be made between the linear complexity of the quaternary codes and several binary codes of the same period ($N = 63$) using table 1 in No and Kumar's paper [132]. Binary No sequences have a linear complexity of at least 12; binary Gold codes have a complexity of exactly 12; the small set of Kasami sequences 9; and the large set of Kasami sequences 15. Thus the quaternary sequences perform well in comparison with these binary sequences of the same code period.

The next series of properties by which the different code families are compared are the randomness properties. Table 5.2 shows the results of testing subsets of the codes for the three randomness properties: Balance, Run and Window. These properties have been proven for m-sequences and DP codes. General results are unavailable for the other code families, so these results only apply to the specific sequences tested. The importance of the Balance property has been discussed in section 1.4. If the codes are not balanced then the resultant transmitted signal has a d.c. offset and this is commonly regarded as a disadvantage in spread-spectrum communications. The importance of the remaining two randomness properties for comparing the structure of the PN code (or pseudonoise

signal), with the structure of true noise has also been discussed. In addition, section 3.3 also relates (in an approximate manner), the correlation of the codes to the Balance property. The results suggest that it is important to retain the balance property, but the approximate nature and assumptions involved in obtaining the result must be considered. Certainly the next section shows that Boztaş codes, which do not satisfy the Balance property, have very good correlation properties.

5.3 System Performance

The research in this thesis has investigated the use of non-binary codes for spread-spectrum multiple-access communication. This research has focussed on the spreading codes and their properties, and how those properties influence the performance as measured by the probability of bit error (PBE). Indeed, this research led to the development of an alternate (to the conventional) code design philosophy in chapter 4. A novel method of code generation, the Dual Problem, has also been developed in that chapter for this design philosophy.

In this section, the performance of subsets of the DP codes is compared with the performance of subsets of codes generated by other means (as discussed in section 5.1). This comparison has carefully considered the results and conclusions of earlier chapters, and in particular section 2.2. To explain further, the codes are not compared via tabular values of crosscorrelation merit factors, instead their PBE versus E_b/N_o curves are compared. The maximum and minimum AIP phases are also used for the comparison to avoid potentially subjective conclusions, which can arise if arbitrary code phases are employed.

Before comparing the performance of different subsets of codes however, it is important to reiterate one comment. The intention of this section is not to determine which is the *best* code generation technique. Rather, the intention is to show that the performance of subsets of DP sequences can be comparable to the performance of subsets of other code generation techniques. This then means that the Dual Problem sequences are acceptable for use as spreading codes for non-binary spread-spectrum communication.

In considering the correlation of the codes an important issue, with some quaternary

generation techniques, is the mapping between the code symbols and the complex numbers. For example, the mapping between GF(4) symbols for m-sequences and Gold codes or modulo-4 ($\mathcal{Z}_4$) symbols for Boztaş codes, and the complex numbers $\mathcal{C}_4 : \{\pm 1, \pm j\}$. In the literature, the mapping from GF(2), which is equal to modulo-2 ($\mathcal{Z}_2$) arithmetic, to the real numbers $\{\pm 1\}$, is via the isomorphic mapping: $\{0, 1\} \rightleftharpoons \{1, -1\}$. The literature is not clear on the mapping from GF(4):$\{0, 1, 2, 3\}$, which is not equal to $\mathcal{Z}_4 : \{0, 1, 2, 3\}$, to the complex numbers $\mathcal{C}_4 : \{\pm 1, \pm j\}$. This is because a large proportion of the research into non-binary codes, which in itself is very small, concentrates on those of prime cardinality, in which case GF(p)=$\mathcal{Z}_p$, for all prime numbers p. Further, if correlation is discussed it is generally only the even periodic correlation and more specifically the peak value which is considered. The importance of this particularly in relation to m-sequences is discussed shortly.

The mapping between the symbols of the code and the complex numbers is important as it can in some cases affect the crosscorrelation of the codes. Clearly this mapping is important when codes have been designed to satisfy specific crosscorrelation properties; Boztaş codes are an example of one such technique. Boztaş, Hammons and Kumar, employed the mapping from $\mathcal{Z}_4$ to $\mathcal{C}_4$ of $\mathcal{M}_B : \{0, 1, 2, 3\} \rightleftharpoons \{1, j, -1, -j\}$. That is, an element s of $\mathcal{Z}_4$ is given by the complex number w^s, where $w = \sqrt{-1}$. This is consistent with the mapping used from GF(2)=$\mathcal{Z}_2$ to $\{\pm 1\}$, with $w = -1$. With the above mapping from $\mathcal{Z}_4$, the maximum magnitude of the even periodic crosscorrelation $|\phi_{max}|$, of Boztaş codes can be shown to be $|\phi_{max}| \leq 1 + \sqrt{N+1}$, or for codes of period $N = 63$, $|\phi_{max}| \leq 9$. Boztaş, Hammons and Kumar have also derived expressions for the occurrence frequencies of the even periodic correlation of the family with this mapping (see for example [17]). In testing the eight Boztaş codes $\tilde{\mathcal{B}}_{A1}$ to $\tilde{\mathcal{B}}_{A8}$ discussed previously, the expressions for $|\phi_{max}|$ and the values that can occur in the correlation spectra have been verified. The correlation properties of the Boztas codes are regarded as very good, especially considering the large family size.

If a different mapping from $\mathcal{Z}_4$ to $\mathcal{C}_4$ is employed, then the Boztaş codes no longer have such good crosscorrelation properties. Indeed for the mapping $\mathcal{M}_R : \{0, 1, 2, 3\} \rightleftharpoons \{-j, -1, 1, j\}$, the peak even periodic crosscorrelation of the eight codes considered is 31, a large value. The mean-square crosscorrelations and average interference parameters are

also significantly worse. Figures 5.1 and 5.2 show the difference in performance for the two mappings. Using the incorrect mapping significantly degrades performance at higher ($>$ 10dB) E_b/N_o ratios. The analytical technique of Özlütürk and Lam [101], which is reviewed in chapter 2, was employed to calculate the probability of bit-error for these sets of deterministic sequences. It should be noted when viewing these figures that a PBE of 10^{-20} for example, could not be observed in practical situations. The assumption of the analysis that the channel is stationary for this time would not be true. However, the figures have included these values so as to highlight the differences between the different code generation techniques.

When the two different mappings are tested on m-sequences, the peak and mean-square values for the even periodic correlation remain unchanged. This is perhaps expected given that the codes satisfy all of the randomness properties. The change of mapping would have little influence on the structure of the codes in relation to the even periodic correlation equation. Differences occur in the peak and mean-square values with odd and aperiodic correlation for different mappings, but this is again expected (i.e. the situation is analogous to the influence of code phase). The differences are not as substantial as for the Boztaş sequences however.

With the Dual Problem method, the arithmetic can vary with each code. Two techniques can therefore be used in transforming the symbols $\{0,1,2,3\}$ to the complex numbers $\{\pm 1, \pm j\}$. Firstly, a single mapping could be used, regardless of the arithmetic of the coder. This is the approach employed by the author in this thesis. The mapping is $\mathcal{M}_R : \{0,1,2,3\} \rightleftharpoons \{-j, -1, 1, j\}$, which was arbitrarily chosen. Testing this mapping and that used by Boztaş et. al. on the four DP codes $\widetilde{A}$ to $\widetilde{D}$, figures 5.3 and 5.4 show that there is little variation in performance.

This is expected, given that DP codes are designed to satisfy the randomness properties and not specific correlation properties, and the discussion above for m-sequences.

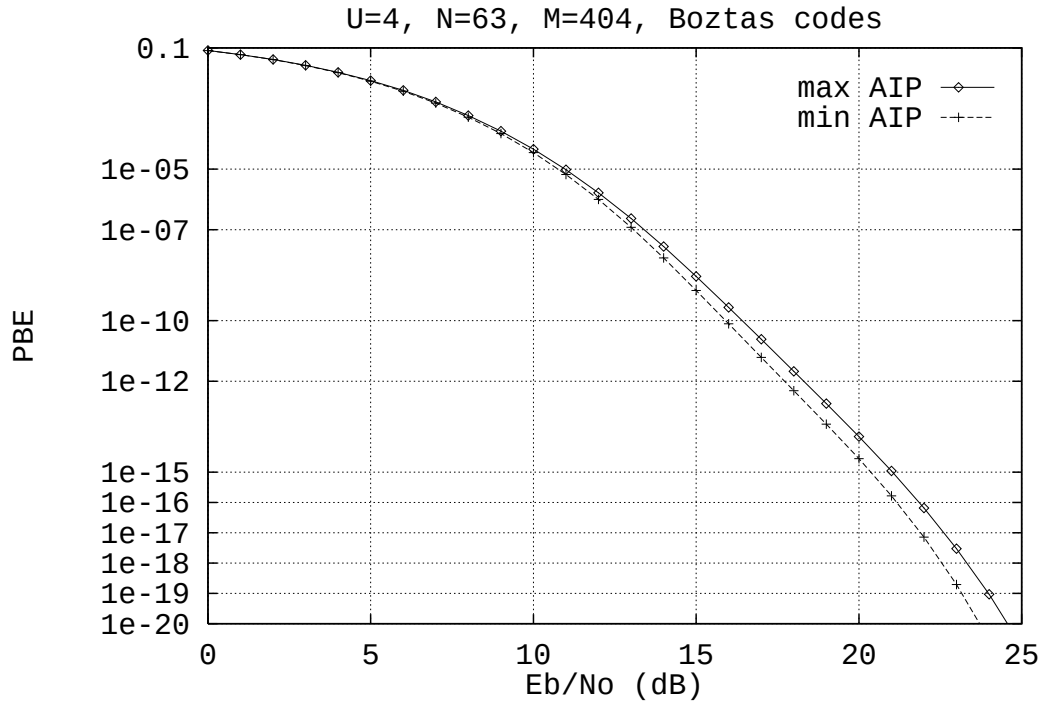


Figure 5.1: The performance of Boztaş codes with the mapping $\mathcal{M}_B$ from $\mathcal{Z}_4$ to $\mathcal{C}_4$. Four Users

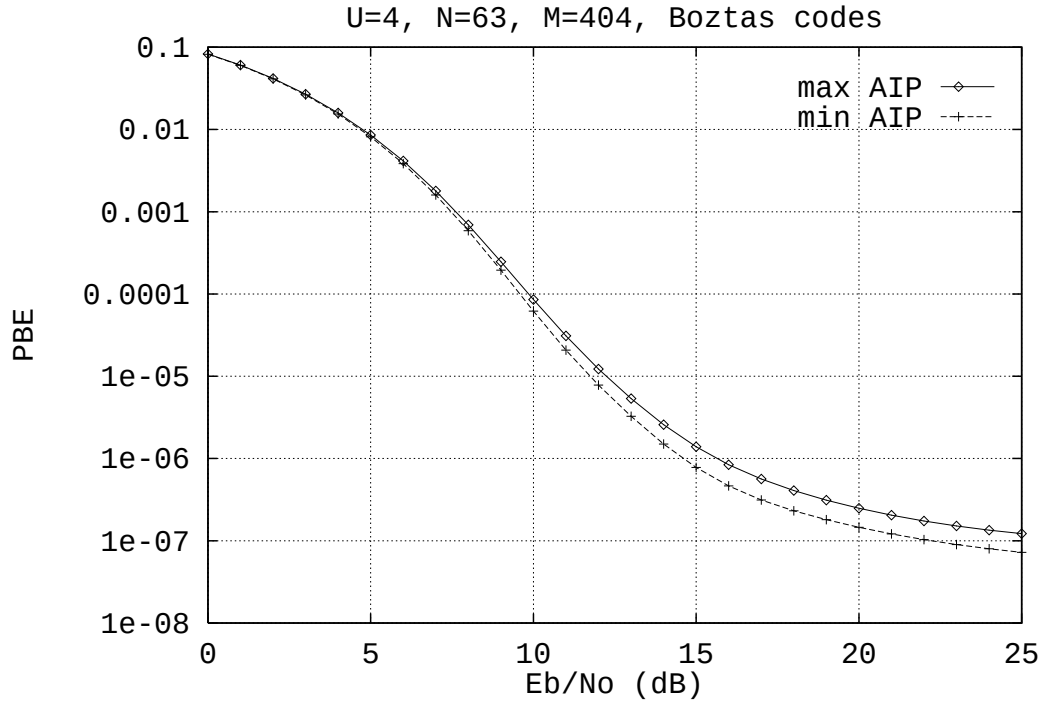


Figure 5.2: The performance of Boztaş codes with the mapping $\mathcal{M}_R$ from $\mathcal{Z}_4$ to $\mathcal{C}_4$. Four Users

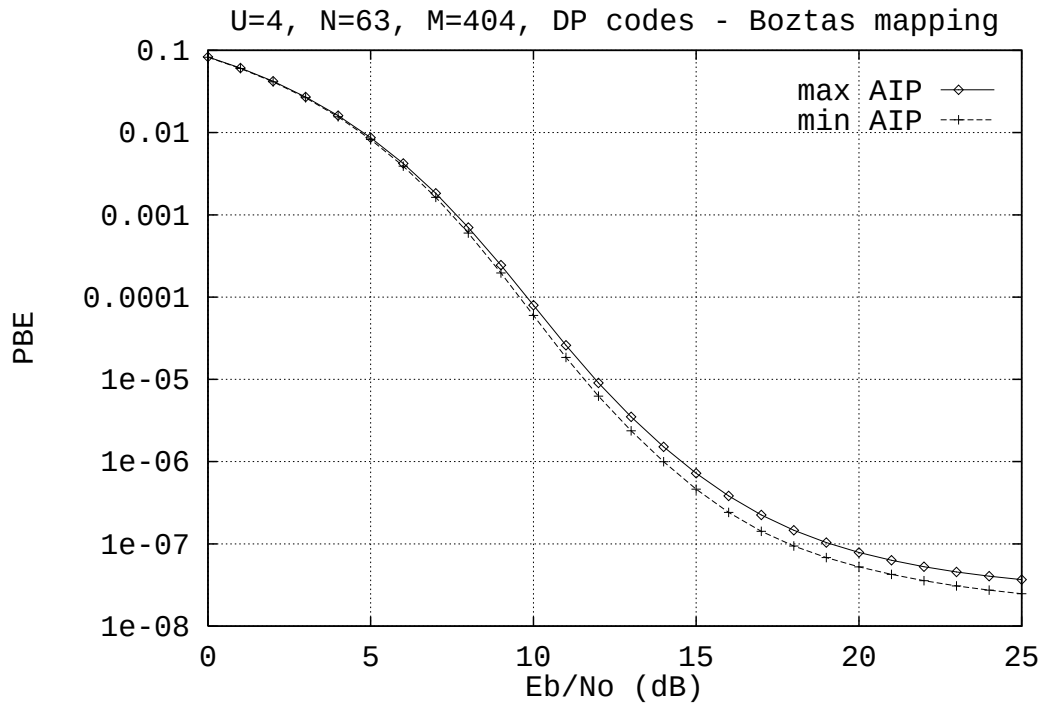


Figure 5.3: The performance of the DP codes $\widetilde{A}\ldots\widetilde{D}$ with the mapping $\mathcal{M}_B$ used by Boztaş et. al. Four Users

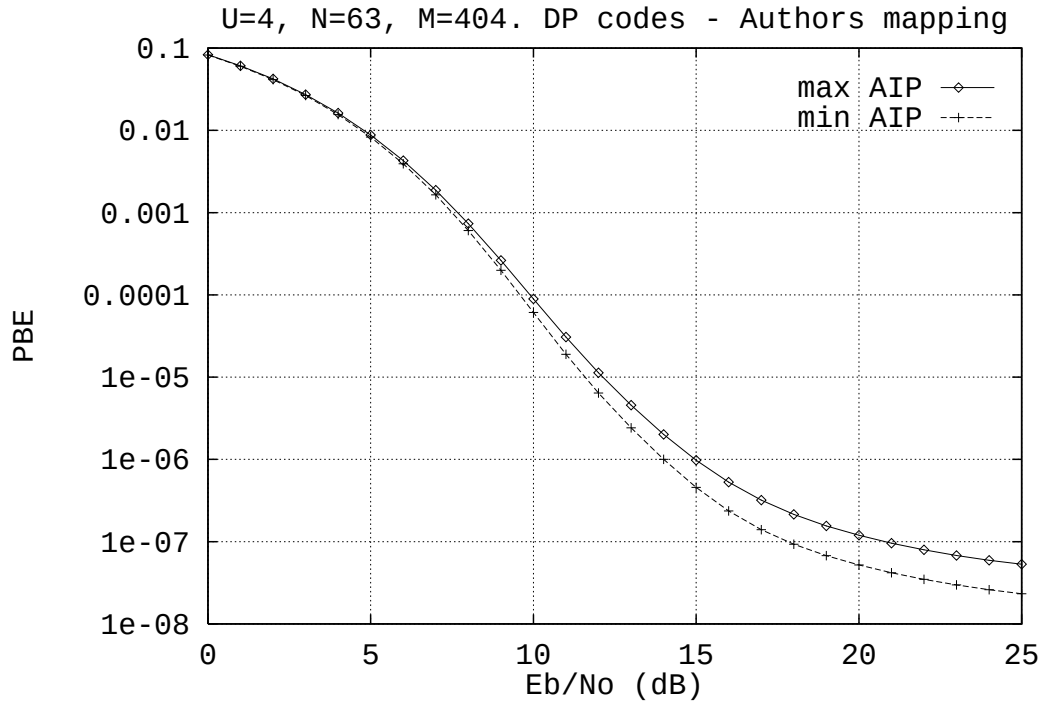


Figure 5.4: The performance of DP codes $\widetilde{A}\ldots\widetilde{D}$ with the mapping $\mathcal{M}_R$. Four Users

codes	peak		MSC
	Re	Im	
$\widetilde{B},\widetilde{A}$	31	18	4423
$\widetilde{C},\widetilde{A}$	32	17	4423
$\widetilde{D},\widetilde{A}$	10	13	3615
$\widetilde{E},\widetilde{A}$	14	63	7615
$\widetilde{F},\widetilde{A}$	13	10	3615
$\widetilde{G},\widetilde{A}$	12	31	3959
$\widetilde{H},\widetilde{A}$	17	32	5495
$\widetilde{C},\widetilde{B}$	10	17	3727
$\widetilde{E},\widetilde{D}$	13	10	3615
$\widetilde{H},\widetilde{G}$	14	11	3087
$\widetilde{F},\widetilde{D}$	14	63	7615
$\widetilde{F},\widetilde{E}$	10	13	3615

codes	peak				MSC	
	max		min		max	min
	Re	Im	Re	Im		
$\widetilde{B},\widetilde{A}$	31	20	11	10	4751	3387
$\widetilde{C},\widetilde{A}$	32	21	12	11	5055	3631
$\widetilde{D},\widetilde{A}$	16	17	10	9	4463	3223
$\widetilde{E},\widetilde{A}$	18	63	10	9	7287	3315
$\widetilde{F},\widetilde{A}$	17	16	9	10	4463	3223
$\widetilde{G},\widetilde{A}$	20	31	10	11	4859	2851
$\widetilde{H},\widetilde{A}$	21	32	11	14	4695	3751
$\widetilde{C},\widetilde{B}$	18	21	8	9	4619	2835
$\widetilde{E},\widetilde{D}$	17	18	11	12	4999	3311
$\widetilde{H},\widetilde{G}$	18	17	12	9	4539	3051
$\widetilde{F},\widetilde{D}$	20	63	12	11	8047	3791
$\widetilde{F},\widetilde{E}$	16	17	10	11	4479	3547

Table 5.3: a) Even Periodic b) Odd Periodic Crosscorrelation

The second approach is to search for a mapping that is consistent between the DP arithmetic and the complex correlation operation, analogous to the mapping used for binary codes. This has not been investigated in this thesis as it requires a much greater mathematical treatment of the DP arithmetics, which is discussed as part of possible future research in section 6.2 . The author is also not aware of any prior research into this issue, except for a comment made by Krone and Sarwate [95] in relation to a private communication between them and Alltop. They remarked that Alltop had examined the autocorrelation of quaternary m-sequences and found it to be independent of the mapping from GF(4) to $\mathcal{C}_4$, a result which has been verified by the author of this thesis. This result, and because research into quaternary codes is still in its infancy, are perhaps two reasons why this issue has not previously been researched or discussed.

The figures for the DP and Boztaş codes also show that the set of four DP codes $\widetilde{A}$ to $\widetilde{D}$, perform poorly in comparison with the four Boztaş codes. Similarly a comparison (see figures 5.11 and 5.14 provided later) of the eight Boztaş codes $\widetilde{\mathcal{B}}_{A1}$ to $\widetilde{\mathcal{B}}_{A8}$, with the eight DP codes $\widetilde{A}$ to $\widetilde{H}$, shows the performance of the Boztaş codes to be significantly better. Tables 5.3 and 5.4 show the correlation properties of this subset of DP codes, and provides an explanation of the poor performance of these codes. They show, that in some cases, pairs of the DP sequences $\widetilde{A}$ to $\widetilde{H}$ have very poor crosscorrelation properties. One such example is for the codes codes $\widetilde{A}$ and $\widetilde{E}$, which have the maximum possible peak

codes	peak				MSC		AIP	
	max		min		max	min	max	min
	Re	Im	Re	Im				
$\widetilde{B}$,$\widetilde{A}$	31	19	16	11	4587	3905	9274	7704
$\widetilde{C}$,$\widetilde{A}$	32	17	16	10	4739	4027	9190	7884
$\widetilde{D}$,$\widetilde{A}$	13	15	9	10	4039	3419	8158	6562
$\widetilde{E}$,$\widetilde{A}$	16	63	10	32	7451	5465	14310	10448
$\widetilde{F}$,$\widetilde{A}$	15	13	10	9	4039	3419	8158	6562
$\widetilde{G}$,$\widetilde{A}$	13	31	10	16	4409	3405	8592	6684
$\widetilde{H}$,$\widetilde{A}$	19	32	11	16	5095	4623	10120	8922
$\widetilde{C}$,$\widetilde{B}$	13	19	8	11	4173	3281	8346	6472
$\widetilde{E}$,$\widetilde{D}$	14	14	10	10	4307	3463	8452	6744
$\widetilde{H}$,$\widetilde{G}$	15	13	11	7	3813	3069	7242	5868
$\widetilde{F}$,$\widetilde{D}$	17	63	11	32	7831	5703	15114	10952
$\widetilde{F}$,$\widetilde{E}$	12	15	9	11	4047	3581	8156	6900

Table 5.4: Aperiodic Crosscorrelation

crosscorrelation value. This was a reservation expressed by Burr in relation to employing random codes, and clearly this pair would not be considered in a practical system.

The reason why this code pair has such poor crosscorrelation properties has been explained by the author of this thesis in [161]. These two codes are isomorphic (allowing for time shifts), i.e. each symbol of one code has a one-to-one mapping to a symbol of the second code, and for the two codes above the mapping is $\{0,1,2,3\}_{\widetilde{A}} \Leftrightarrow \{1,3,0,2\}_{\widetilde{E}}$. Further to this, when the above symbols are mapped to the complex alphabet, the two real-valued symbols of one code must map to the two imaginary-valued symbols (or two real-valued symbols) of the other, so that the complex even periodic crosscorrelation at some delay is -63, or $0 \pm j63$. This is not necessarily a disadvantage however, as it may be possible to partition this set of codes into subsets, and an example of this would be the partitions $\{\widetilde{A}, \widetilde{E}\}$ and $\{\widetilde{D}, \widetilde{F}\}$. Tables 5.3(a) and (b) show that there is poor crosscorrelation within each of these subsets, but good crosscorrelation between subsets, and this could possibly be beneficial to multiuser CDMA systems. Indeed, the author has had some correspondence with researchers of multiuser CDMA on this topic. Future research proposed in chapter 6 in relation to the structure of the DP codes could also alleviate the above problem, and the analogy with preferred pairs of m-sequences may be of assistance.

To digress slightly, the values given in these tables can also be used to verify some of the relationships discussed in chapter 2. Firstly, these tables numerically verify equation 2.14, which shows that the sum of the even and odd periodic mean-square cross-correlations is equal to twice the mean-square aperiodic crosscorrelation, e.g. for codes $\tilde{A}$ and $\tilde{B}$: $4423 + 4751 = 2 \times 4587$. Secondly, they show agreement with the comment that the AIP can be approximated by twice the MSC, e.g. for codes $\tilde{A}$ and $\tilde{B}$, the AIP=9274$\approx 2 \times 4587 = 9174$.

The performance of the set of DP sequences $\tilde{A}$ to $\widetilde{H}$ is poor because the codes are too similar, which is not surprising since they are generated by the same shift-register configuration and multiplication operator, only the addition operator is different for each sequence. A second approach to selecting a subset of DP sequences is therefore investigated. For this second set the DP sequences are generated by different shift-register configurations, but the same arithmetic (the addition operator of sequence $\tilde{A}$ and the multiplication operator **m1**). The shift-register configurations for the codes in this set are $D^3 = 1 \otimes D^2 \oplus 1 \otimes D \oplus 1 \equiv 111$ and *112,221*, and *332*. A comparison of figure 5.5 with figure 5.1 (given previously), shows that the performance with these four DP codes is only slightly worse than the performance with the 4 Boztaş codes. The difference is less than 1dB for a PBE less than 10^{-12}, and to see the significance of this recall that voice transmissions often require a PBE of only 10^{-3}. The reader may also recognise that the selection of a subset of DP codes in this manner is analogous to the generation of m-sequences, and this generalisation could be investigated further in future research.

Notice also that the difference in performance between the maximum and minimum AIP phases of the Boztaş codes in figure 5.1 is less than for the set of DP codes in figure 5.5. This may be considered a possible advantage for the Boztaş codes as it reduces the need to find the optimal code phase. On this point, figure 5.6 shows that the four BTQ(Gold) codes have the smallest variation in performance between the maximum and minimum AIP phases. However, their performance is worse than the Boztaş or DP (same arithmetic, different polynomial) codes at higher (> 10dB) E_b/N_o ratios. This is an expected result and it is discussed further in section 5.4. Tests on the first four m-sequences also found that their performance is very poor in comparison with

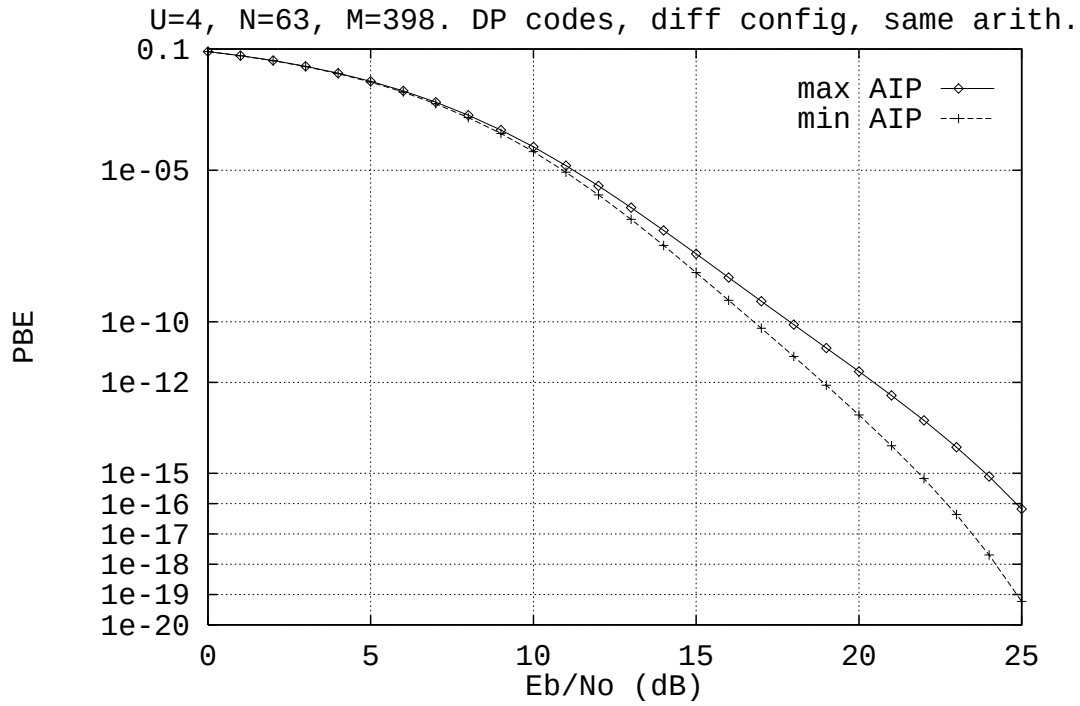


Figure 5.5: The performance of DP codes. (same arithmetic, different polynomial). Four users.

other techniques, but this result can be explained by considering the average interference parameter (AIP) of these sequences. The AIP of one pair of sequences (min 9350, max 11208) is much greater than the expected value of the AIP for random codes ($2N^2 = 7938$), and this significantly degrades the performance for four users. Note that the peak even periodic crosscorrelation for this pair is only 17, thus highlighting the importance of considering factors other than the peak value. The first four Novosad and the first four random (or dice toss) sequences also have, like the BTQ codes, a large difference in performance between the maximum and minimum AIP phases. Figures 5.7 and 5.8 show the performance for four Novosad and the four random sequences respectively. Note that the BTQ(Gold) and Novosad sequences were generated or given directly with elements of $\mathcal{C}_4 : \{\pm j, \pm 1\}$, hence the issue of which mapping to employ does not arise.

The reader should also recognise that at lower (< 10 dB) E_b/N_o ratios the the performance of all of the different code families is comparable. This is expected because this is a region in which the performance is determined more by the noise rather than the code

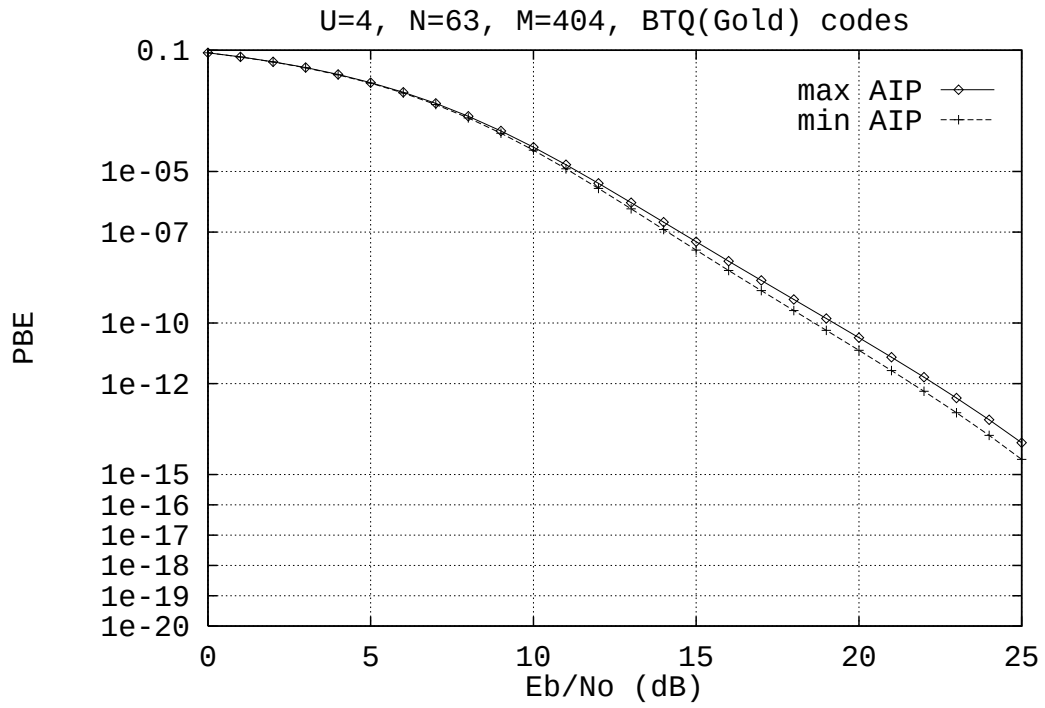


Figure 5.6: The performance of BTQ(Gold) codes. Four users.

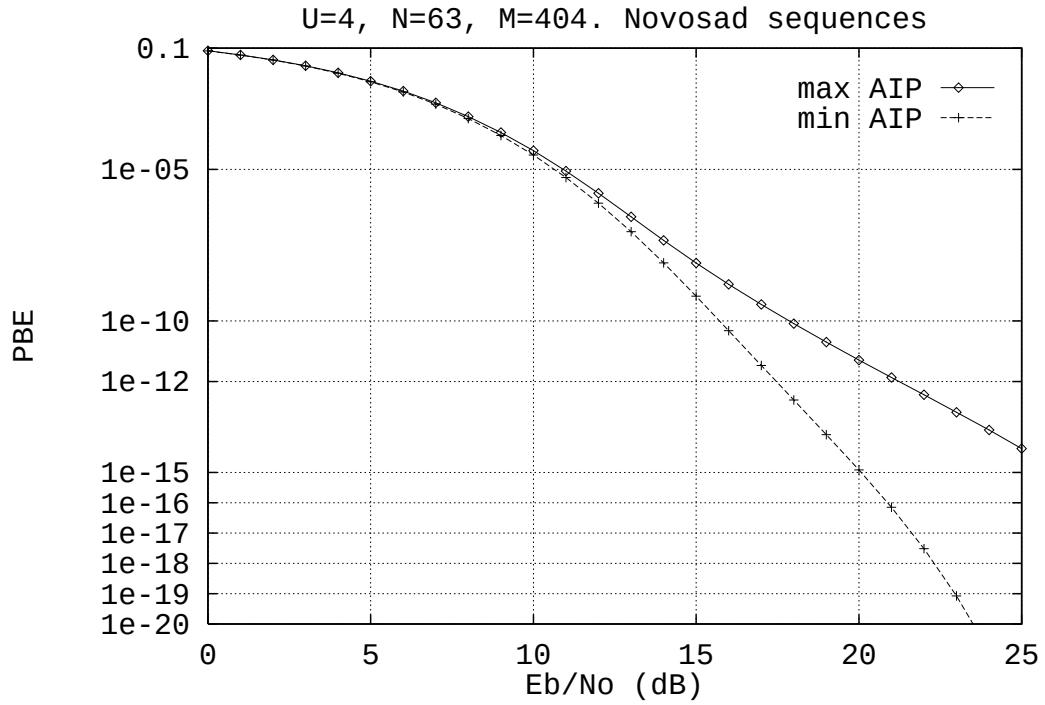


Figure 5.7: The performance of Novosad codes. Four users.

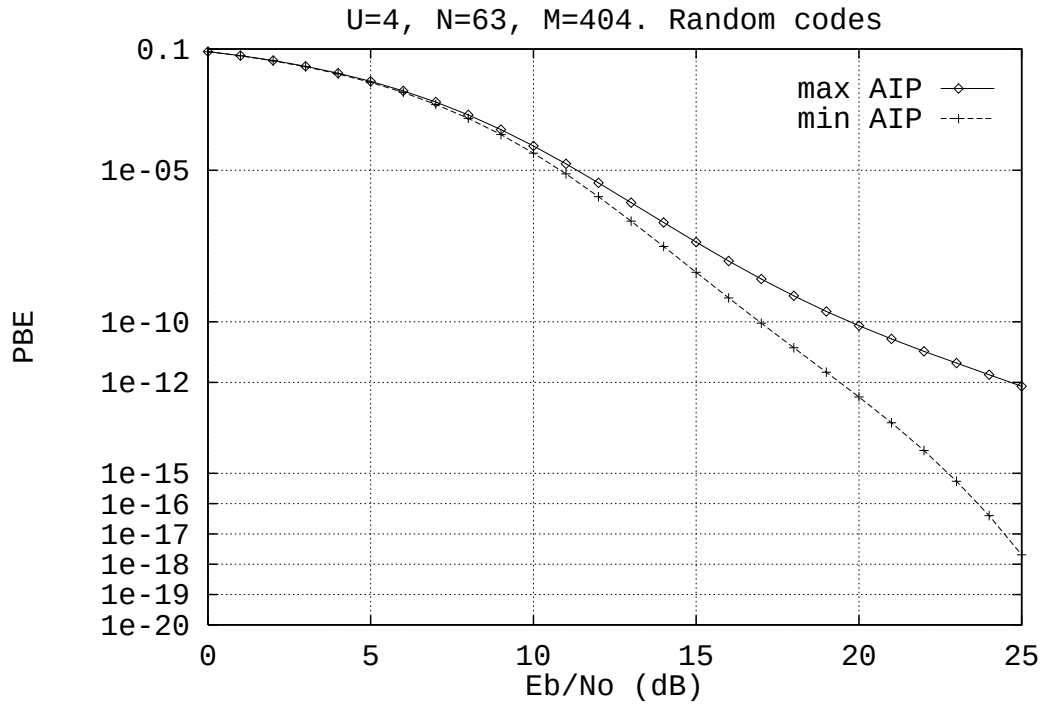


Figure 5.8: The performance of random codes. Four users.

properties. Commercial systems for personal or mobile communication may well operate in this region (e.g. higher user numbers, or lower E_b/N_o ratios), because they may only require a PBE of 10^{-3} for voice transmission. The code design philosophy used in this thesis and the notion of using random (or Dual Problem) codes is then appropriate.

Another alternative to using DP codes of the same arithmetic, but different shift-register configurations, is to consider subsets of DP codes generated by different arithmetics and using different shift-register configurations. As an example, the following eight coder configurations produce DP codes, if the addition operators correspond to those of $\widetilde{A}$ to $\widetilde{H}$ (given in appendix C.2), and the multiplication operator is **m1**: *111,113,–23,112,121,223,–32* and *332*. The shorthand notation *–23* corresponds to the polynomial $D^3 = 2 \otimes D^1 \oplus 3 \otimes D^0$. Figure 5.9 shows the performance for the first four of these codes, and it can be seen that the performance for the minimum AIP phase is comparable with that of the Boztaş codes for four users.

Comparisons may also be made for eight users between this subset of DP codes and Boztaş, Novosad, random, BTQ(Gold) and Gold codes. Figures 5.10 to 5.16 provide the

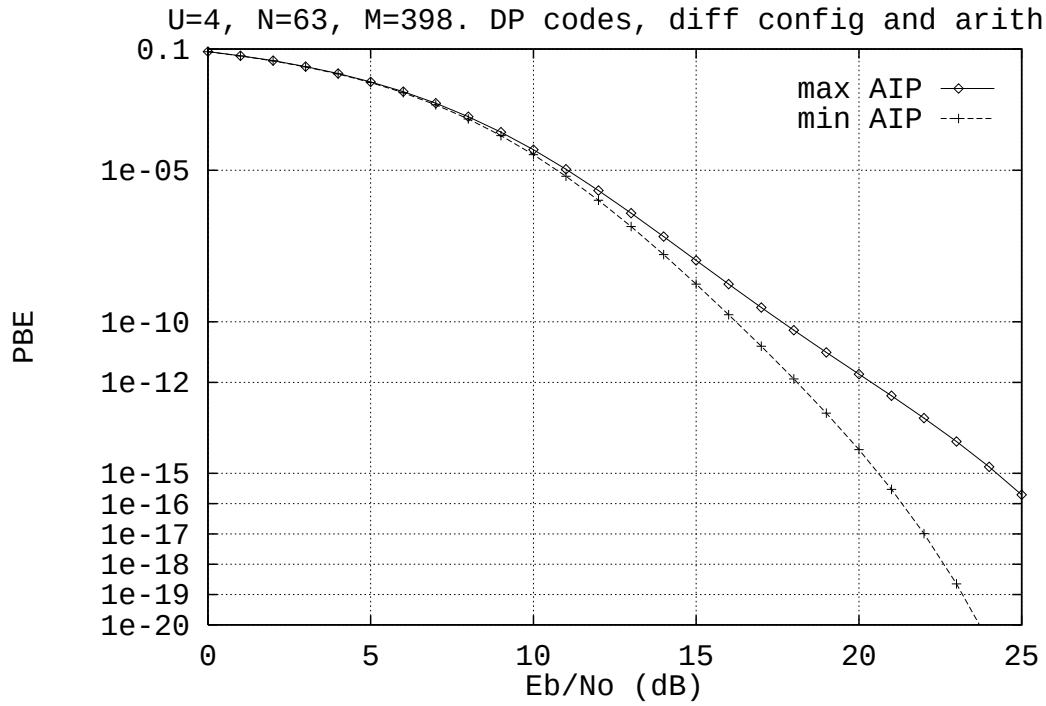


Figure 5.9: The performance of DP codes (different arithmetics and polynomials). Four users.

performance of each subset respectively. Note that only four codes exist for the specific example considered of a subset of DP codes using the same arithmetic and different shift-register configurations. Only six m-sequences generated by primitive polynomials exist as well.

Figures 5.10 to 5.16 show that the Novosad sequences perform slightly better with the minimum AIP phase than the Boztaş sequences, but slightly worse with the maximum AIP phase. However, at a PBE less than 10^{-6} the difference is negligible between these techniques. The subset of DP sequences considered above, and the random (or dice toss) codes, have only slightly poorer performance with their minimum AIP phases. The BTQ(Gold) and quaternary Gold sequences perform poorly, as do the DP sequences $\widetilde{A}$ to $\widetilde{H}$. These results are expected given prior discussions. The selection of the maximum and minimum AIP phases is also less significant with the BTQ(Gold) codes than for the other techniques. The random (or dice toss) codes have the largest variation in performance between the maximum and minimum AIP phases.

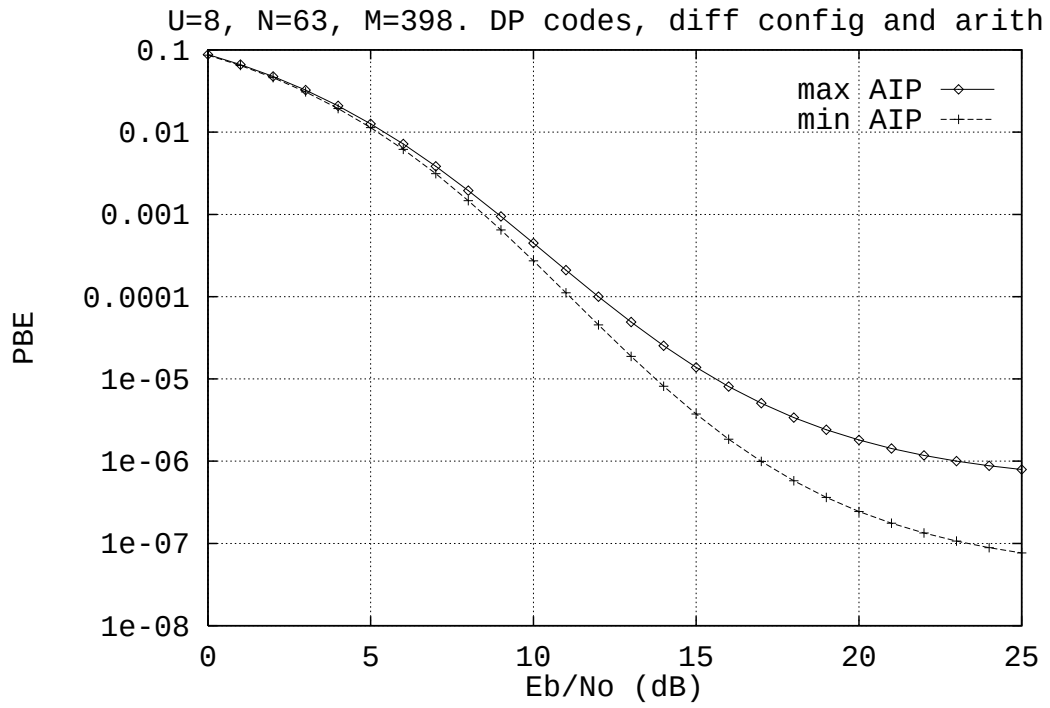


Figure 5.10: The performance of DP codes (different arithmetics and polynomials). Eight users.

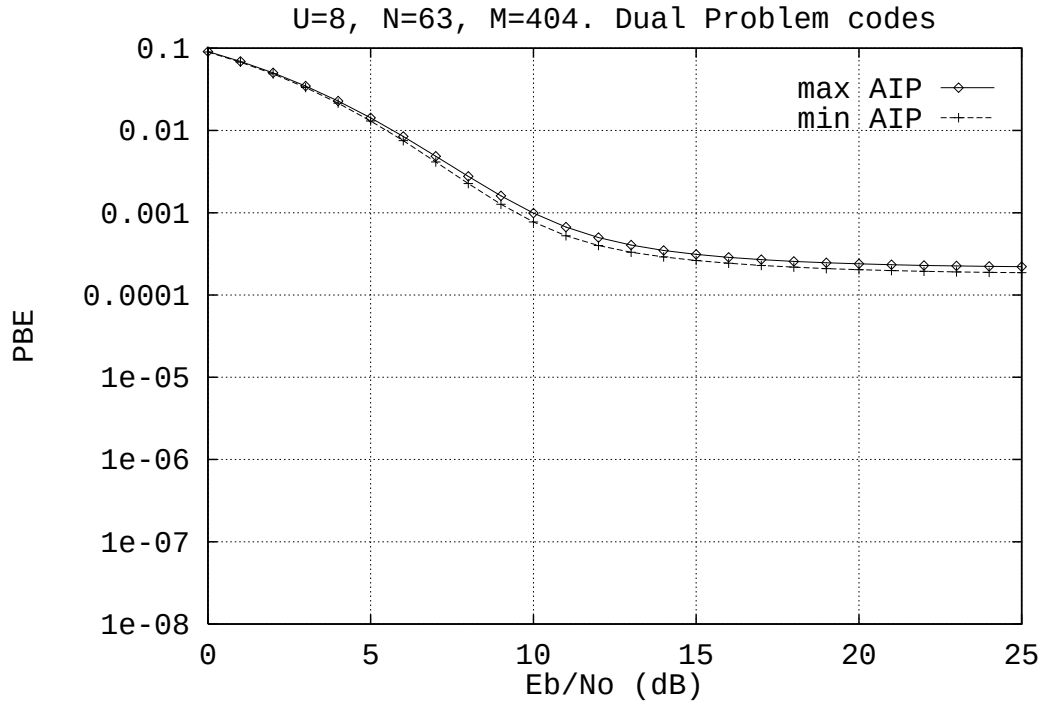


Figure 5.11: The performance of DP codes of the same class. Eight Users

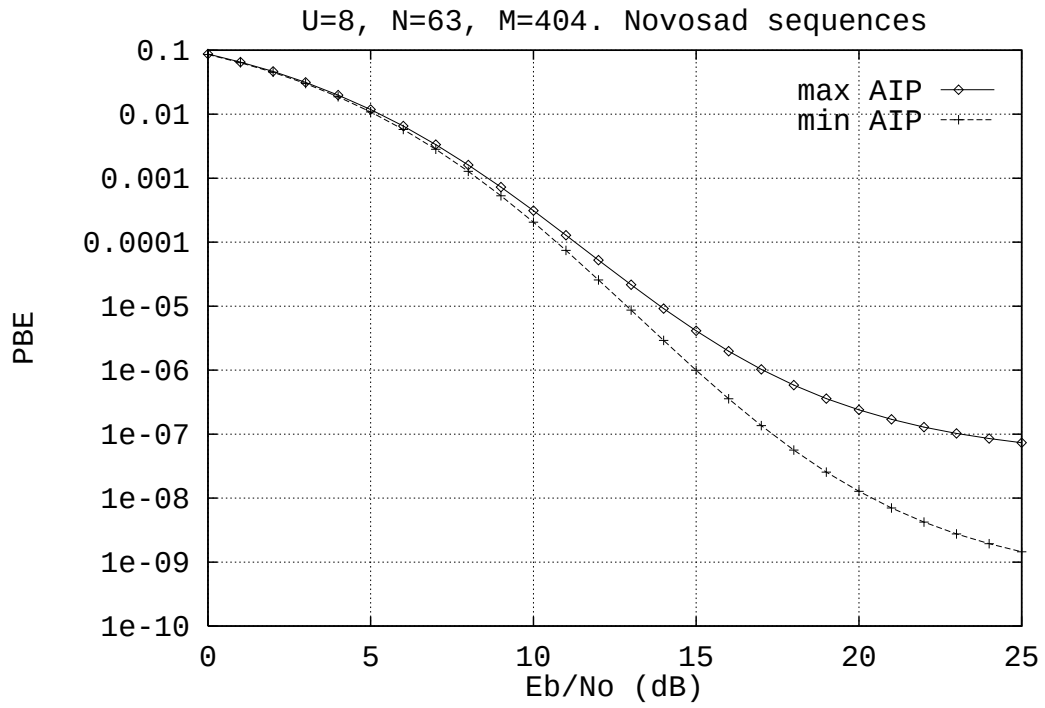


Figure 5.12: The performance of Novosad codes. Eight users.

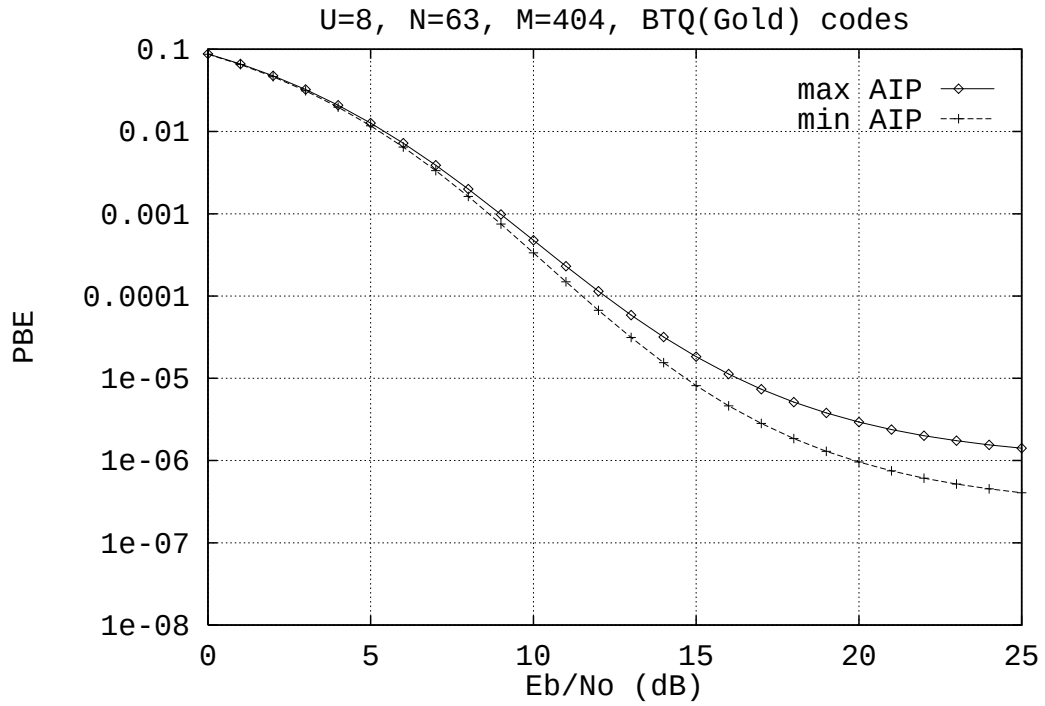


Figure 5.13: The performance of BTQ(Gold) codes. Eight users.

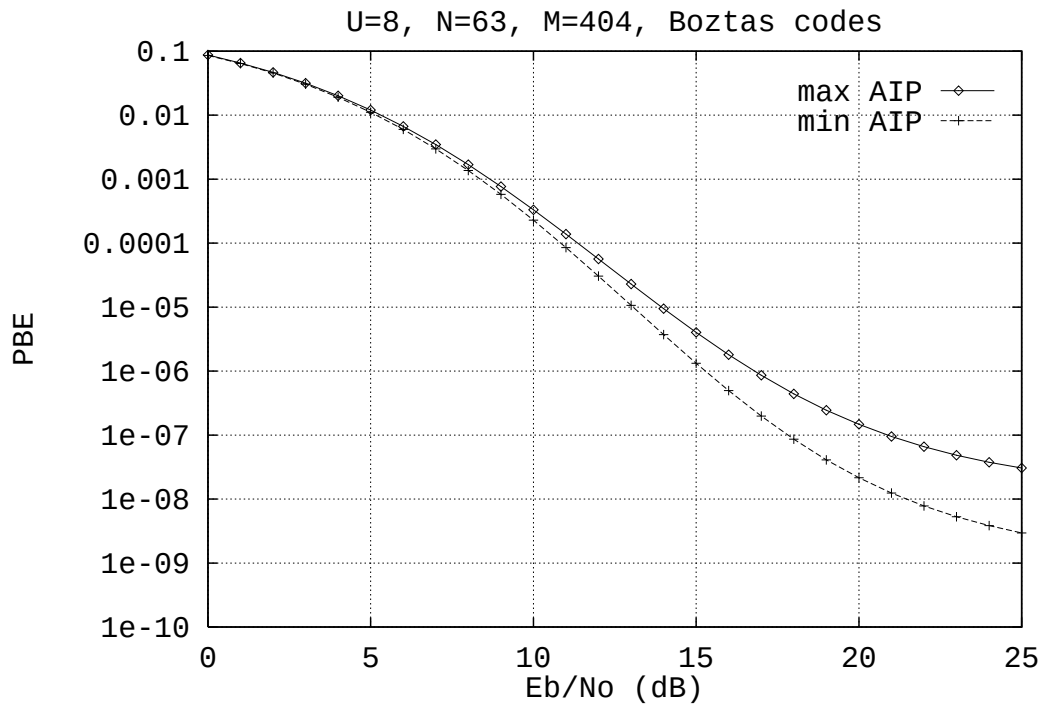


Figure 5.14: The performance of Boztas. Eight Users

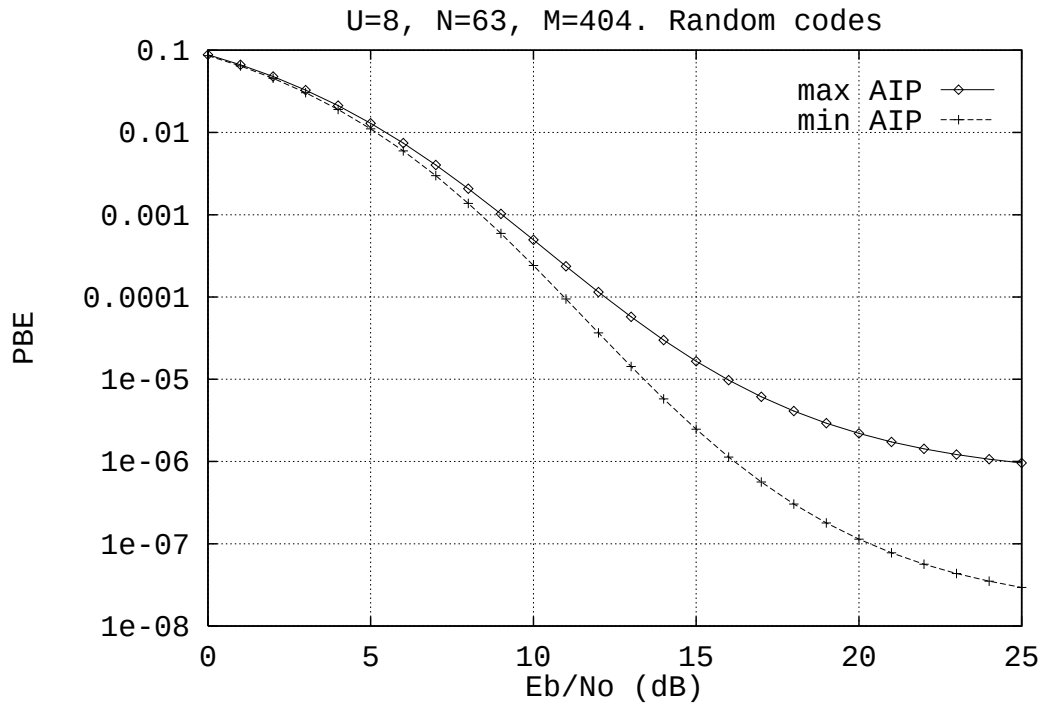


Figure 5.15: The performance of random codes. Eight users.

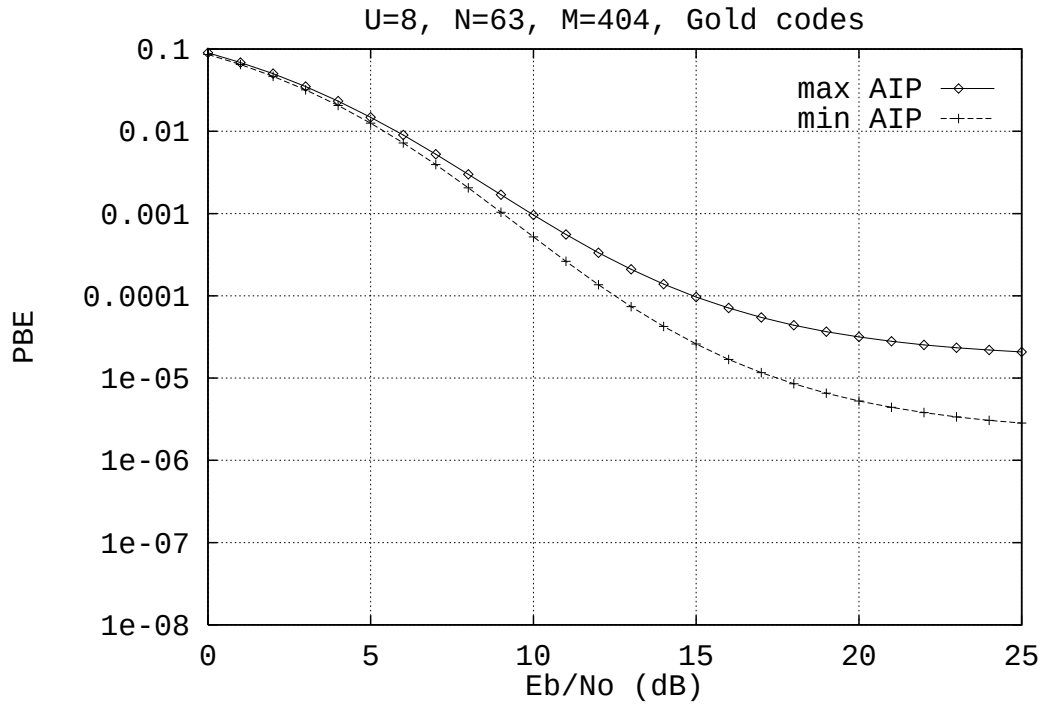


Figure 5.16: The performance of Gold codes. Eight users.

In summary therefore, the Dual Problem of code generation is a suitable method for designing spreading codes, because subsets of sequences can be found for which the performance is comparable to random codes, and indeed to the other quaternary code generation methods considered here. Some subsets of DP sequences can result in very poor performance, but the investigation in this chapter has explained how this can occur, and hence this problem can be avoided. This is explained further in the next section which provides an overview of this chapter. The next section also explains many of the results of this section in further detail. However, there is one point which should be restated. It is very difficult to make generalisations on the relative merits of a code family from tests which compare the PBE of subsets of codes. The conclusions drawn from the tests are only valid for the specific situations considered, and tests with other code could lead to a different code family being regarded as the *best*. The results in the latter part of chapter 2 emphasized this point. Thus the intention of this section has been to show that the DP codes provide an acceptable level of performance, and this is true provided that subsets of the sequences are chosen with care.

5.4 Discussion

The aim of this chapter has been to show that sequences generated by the Dual Problem are suitable for use in spread-spectrum multiple-access communications. As the research in the latter part of chapter 2 illustrated however, comparing code families is a difficult task. Certainly they should not be compared by a single merit factor alone, such as by their peak or mean-square value. Rather, the performance of subsets of codes should be compared, but again as results in chapter 2 illustrate, this comparison should employ the maximum and minimum AIP phases to allow for variations due to code phase. Further, it must also be recognised that the conclusions only apply for the specific situation considered. Thus instead of attempting to show that there is an optimal code generation technique, the intention in this chapter has been to identify situations which will result in an unacceptable level of performance, i.e. a level of performance which is significantly worse than for random codes, and this has been done for the DP sequences. Further, in recognising the ways in which the subsets have been selected and the resultant performance, a deeper mathematical investigation of the relationship between the arithmetic and the coder configuration might lead to a refinement of the Dual Problem. Specifically it could lead to a reduction of the search space for DP codes, and the removal of the problem encountered for the subset $\widetilde{A}$ to $\widetilde{H}$. This is discussed in detail along with other recommendations for future research in section 6.2.

With these comments in mind, the results of section 5.3 may now be summarised. The Boztaş codes have been found to provide good system performance, and this technique is particularly important because of the large number of codes in the family in comparison to the code period. The Novosad sequences also provide good performance (comparable to Boztaş codes), but only eight Novosad sequences of period 63 exist, and this may be an insufficient amount. The similarity of performance between these techniques can also be expected because they have comparable peak and mean-square values for even, odd and aperiodic crosscorrelation. The mean-square crosscorrelation values for the subsets of sequences tested are also, in general, less than for those expected for random codes (see chapter 3), hence the better performance than random codes.

In examining the results for the binary to quaternary transformation, it can be concluded that although this approach ensures that the peak even and odd periodic cross-

correlation magnitudes are the same, this may not necessarily improve the performance in general. This result again illustrates the importance when designing codes of considering other factors as well as the peak value. The BTQ transformation does not exploit the additional number of symbols available in the quaternary code in order to reduce the crosscorrelations and hence improve performance. The quaternary Gold codes and quaternary m-sequences tested have also been found to provide poor performance, but again this result is expected as those techniques are really designed for alphabets of prime cardinality.

The results of the previous section also show, that when subsets of Dual Problem codes are chosen with care their performance can be comparable to the other code generation techniques considered, and that was the aim of this chapter. In addition, the results of section 5.2 show that subsets of the Dual Problem codes can also be used where secure codes are required, because they can have a high linear complexity. This is perhaps a property more important for a military communication system than a public system, but it also means that future research may consider other applications for the DP sequences, for example in cryptography. Section 5.3 also shows that the Dual Problem codes satisfy the Balance property, unlike Boztaş codes and those of many other techniques, and this may be important in a practical system.

Hence the refined code design philosophy and the novel technique of code generation developed in chapter 4, can (with care) provide codes suitable for non-binary spread-spectrum communications. The technique does not provide the *best* level of performance, but it is comparable to that of random codes. The difference between the code families also became comparable at lower bit-error probabilities, and a commercial mobile or personal communication system would generally operate in this region, thus supporting the refined code design philosophy. Certainly the Dual Problem technique, which has been developed as part of this philosophy, is worth pursuing in future research, particularly because of the understanding it might provide to the theory of generating pseudorandom codes.

Chapter 6

Conclusions And Recommendations

6.1 Conclusions

After reviewing the literature on spread-spectrum communications, the author of this thesis (like others) recognised the potential advantages of CDMA for the growing mobile or personal communications market. However, an investigation of binary code generation techniques shows that many provide an insufficient number of codes for this application. Using non-binary codes has been recognised as one solution to this problem, and this is the solution which this thesis has investigated for the reasons given below.

1. Firstly, a detailed literature review shows that only a small amount of research has been conducted into non-binary spread-spectrum systems, but that this is increasing. Chapter 1 in this thesis summarises the different types of non-binary systems which are discussed in the literature. An examination of the literature also shows that, as well as providing more codes, the best non-binary codes have a peak crosscorrelation value which is less than that of the best binary codes, and the proof of this is given in chapter 1, the Introduction. Sets of non-binary codes which provide better performance than sets of binary sequences can therefore be found, and the literature confirming this is also referenced in the Introduction. In addition, the Introduction also explains the importance of restricting the codes to the quaternary alphabet when transmission is over the mobile communication channel. Practical reasons have been given for this.

2. Secondly, a detailed review of non-binary code generation techniques, given in

chapter 4, shows that:

(a) literature and research into non-binary codes is very small (in relation to that for binary codes), and

(b) often this research is concerned with alphabets other than quaternary.

Hence, the advantages of using non-binary codes in spread-spectrum communications, and the small amount of prior research into the topic, have provided the motivation for the research in this thesis, of which a summary is now given.

The early sections in the Introduction discuss the advantages and disadvantages of spread-spectrum communication, and in particular non-binary code spread-spectrum. They also summarise the current state of commercial proposals for CDMA, and introduce the basic theory and key equations. Section 1.4 also reviews the properties of pseudorandom (PN) codes which are commonly discussed in the literature, and this leads ‘ to the first area of investigation. The review in section 1.4 of PN code properties and consideration of the operation of the system given in the section 1.2 shows a disparity between the properties many code designers consider important and those that the analysis of the system emphasizes. Kärkkäinen had also commented on this in [78] in relation to binary codes. Two possible reasons can be suggested for this disparity in the literature. Firstly, it is difficult to design code families to satisfy the properties emphasized by the system analysis, and secondly, very little research has been conducted on the relative importance of different code properties on performance, even for binary codes. This thesis is the first to have investigated this second issue for non-binary codes. An investigation of the important properties (and specifically features of the crosscorrelation of spectrum) of the codes needed to be undertaken before code generation could be considered. The early chapters in this thesis therefore research this issue.

Chapter 2 commences the investigation by reviewing the literature on techniques for determining the probability of bit error (PBE) of the system. The PBE is the measure of system performance used throughout this thesis. The review is divided into two and considers techniques which approximate the PBE and techniques which bound the PBE. The former are easier to calculate and provide a better insight into important features of the crosscorrelation spectra than the latter, but the latter are more accurate. This review also serves two other important purposes:

1. It describes in detail the accurate analytical technique used throughout the thesis to determine the PBE of sets of deterministic sequences. Simulation is not considered because of the typically long run times that would be required to produce results in the region of interest, which are the regions where the codes have the dominant influence on performance.

2. That accurate technique also forms the basis for the development of a novel method in chapter 3, which is used to examine the relative importance of different features of the crosscorrelation spectrum on performance.

The methods for approximating the PBE propose several merit factors. These merit factors, such as the average signal to noise ratio (SNR), average interference parameter (AIP), and mean-square crosscorrelation (MSC), emphasize the properties which system designers consider important. Hence the discussion on these in section 2.2.1. Primarily, merit factors form the basis of criteria used to select the appropriate code phases which optimise performance. The phase or starting point of the code is important because the transmission is over an asynchronous channel, where both odd and even periodic correlation are equally important. The odd periodic correlation and consequently the performance of the system are influenced by the phase of the codes. There is, however, no consensus in the literature on which criteria should be used, but this needs to be resolved before different code properties or families are compared. The following two points may clarify why this is so.

Firstly, in researching different methods of code generation one must have a method of comparing them. The initial intention was to do this by conducting tests to determine the PBE of sets of sequences, and then compare the results. This approach was also considered initially as a means of comparing code properties, but as a later discussion shows this simple approach is naive. An understanding of the relative importance of different code properties on performance is required before new codes can be designed.

The second reason for investigating code phase is because the different criteria for selecting the phase employ different merit factors, and these merit factors highlight different correlation features. Thus if the relative importance of the different criteria (or at least the optimal criteria) could be determined, then this would provide an insight into the relative importance of different correlation features (or at least highlight those of the

most importance).

Section 2.2.2 therefore investigates the different criteria for selecting the phase of the codes. It is shown that the criteria commonly used, LSE/AO and AO/LSE, do not guarantee that the performance will be better than for randomly selected code phases. Nor is it possible to conclude, for example, that the AO/LSE phase is better than the LSE/AO or MSE/AO phases. The criteria of minimising the AIP (or the close approximation, minimising the MSC) does ensure the best performance in all of the tests of this thesis. The discussion in chapter 2 shows that these results are expected. The results of section 2.2.2 also show that the variation in the PBE between the maximum and minimum AIP phases can be substantial in regions where the codes have the dominant influence on performance.

Testing the different criteria for selecting the code phase, therefore provides several important conclusions (additional to those above):

1. The AIP is a merit factor which highlights the properties of the codes (or their crosscorrelation spectra) which have an important influence on performance.

2. If different code families or subsets of codes are to be selected from tests comparing their PBE, then the conclusions are only applicable to that specific situation. Any generalisation will be subjective because of the variation possible in the PBE with different phases.

3. It is not possible to determine the relative importance of different code properties by conducting tests on specific subsets of sequences. This is because it is not possible or practical to average out the variations in the PBE which different factors can cause, and these variations can be significant.

The results of chapter 2 therefore show that a different approach is required to determine the relative importance of different code properties on performance. The simple approach is not satisfactory. Chapter 3 therefore discusses a proposal by the author which has been published in [163], refined in [162] and is further refined in this thesis, to achieve this. The proposal considers a virtual set of codes and develops the appropriate system analysis for them. The virtual code model can be regarded as lying between the extremes of those used for random codes and deterministic sequences. A virtual set of

codes is defined to be a set which may or may not exist, whose correlation properties are appropriately defined. Thus the influence of different factors on performance can be observed in a less subjective manner. The technique is in effect a simplification of an accurate technique for bounding the PBE given in section 2.1.2. The new technique is illustrated by an example in section 3.1.1. The accuracy of the method and the assumptions involved are also investigated in chapter 3, and it is shown that they are acceptable for its intended use.

Virtual codes have been used in this thesis to investigate the influence of the peak value and shape of the continuous-time crosscorrelation distribution on performance. The research confirms the expected result that a reduction in the peak value improves the performance. What is of more importance is that the research shows that in some cases the shape can have a greater influence on performance than the peak value. This is important because as the discussion in chapter 3 shows, the tradeoff between these two factors can allow a greater number of active users. Furthermore, consideration of the Welch bound shows that a greater number of codes can be considered for use in the system than the min-max design criteria suggests. Clearly, these conclusions have important ramifications for the code design philosophy.

The shape of the continuous-time crosscorrelation spectrum is dependent upon:

- the occurrence frequencies of the discrete-time crosscorrelation values,
- the occurrence frequencies of the adjacent pairs of discrete-time crosscorrelation values, and
- the code-chip pulse shape.

The results from the tests conducted in section 2.2.2 highlight the importance of the two merit factors, the AIP and the MSC. The MSC may be regarded as a measure of the variance of the occurrence frequencies of the discrete-time crosscorrelation values, and the AIP is related to the MSC with an additional factor to account for the occurrence frequencies of adjacent pairs of discrete-time crosscorrelation values. The AIP also takes into account the code-chip pulse shape, hence the results at the end of chapter 2 and in chapter 3 are in agreement.

Further support of the conclusion that the shape of the crosscorrelation distribution can be more important than the peak value is given by the conclusions of Chen and Oksman in [24]. In testing sets of deterministic binary sequences, they found that the occurrence frequencies of discrete-time crosscorrelation values could be more important than the peak value. They further recognised (from a different argument to the one given in this thesis) that this result allowed a greater number of code generation techniques (and codes) to be considered than previously thought.

The conclusions in chapter 3 have therefore resolved the first research issue: to determine the important code properties and their relative importance. In addition, resolving the research issue has an important ramification on code design and subset selection. In summary:

1. The AIP illustrates all of the important properties which influence the crosscorrelation spectrum and hence performance.

2. The MSC is often a sufficient approximation to the AIP, as the results of chapter 2 show.

3. The MSC can be more important than the peak value. Consequently, if the min-max criteria is used to select subsets of codes, then this may not produce optimal performance. Furthermore, if the min-max criteria is used to design code families then it may unnecessarily restrict the family size.

Discussions with Kärkkäinen at the International Symposium on Spread Spectrum Techniques and Applications (ISSSTA'94) identified further research on binary spread-spectrum systems supporting these conclusions. The literature pertaining to this, by Kärkkäinen et. al., Burr, Hui, and Grant, is discussed in chapter 3. Specifically, these authors also recognised the importance of the mean-square crosscorrelation value. They also concluded, therefore, that the conventional philosophy of designing codes to have, or selecting codes with, the minimum peak (usually only even periodic) crosscorrelation value is insufficient for the asynchronous multiple-access channel. Further, and perhaps more importantly for code design, these authors found that the MSC of codes from different families is often very similar, for arbitrary code phases, even though the peak values are not. In addition, the MSC values are comparable to those expected of random

codes. Kärkkäinen also discussed in [78] how James Massey had shown this to be an expected result of coding theory.

As a consequence of the similarity (on average) of the MSC value of many codes from different families, and its similarity to the expected value for random codes, the authors listed above suggested that random spreading codes should be used, and subsets of codes with suitable properties selected for the specific application. The results of chapters 2 and 3 show how subsets should be selected, but consideration must also be given to properties important for other issues, e.g. acquisition and tracking. Using random codes may not provide optimal performance for a specific set of circumstances, but it does provide a large code family, and the performance of other code families tends to that of random codes as the number of users is increased, or alternatively, as the E_b/N_o ratio is decreased. However, proposing the use of random codes does not overcome the issue of code generation, and this is perhaps where the thesis makes its most important contribution to the knowledge of the field. Chapter 4 proposes a refined code design philosophy; the code family is to be designed to contain a large number of non-binary sequences, but rather than the conventional conflicting constraint of specifying stringent correlation properties, the codes are to be designed to satisfy the randomness properties (as discussed in section 1.4). The codes are also generated by a shift-register configuration for practical reasons.

As far as the author is aware, the only other pseudorandom codes used in spread-spectrum systems, which emphasize the randomness properties are m-sequences, but the difficulty with employing m-sequences is the small number of codes in the family. Considering the manner in which m-sequences are generated led to the proposal of a novel approach to code generation. This approach, referred to as the Dual Problem, was published by the author of this thesis in [161], and it is further refined in chapter 4. Rather than considering a given arithmetic (e.g. Galois field) and finding shift-register configurations (or primitive polynomials) which produce maximal-length sequences, the new approach considers a coder configuration and finds suitable arithmetics so that the coder generates a maximal-length sequence. Tests in chapter 4 show that a significantly greater number of codes can be produced by this method, and these codes satisfy the desired randomness properties. Although applicable for non-binary codes of any cardinality, the

method is only used to generate quaternary codes in this thesis.

Examination of the properties of these arithmetics, in particular consideration as to which properties of the arithmetic are important, why they are important, and how they influence the operation of the coder, verifies that not all of the properties of finite field arithmetic (from Group theory) are necessary for this application. For example, associativity, distributivity, identity and inverse can be removed. After the publication of the novel proposal in [161], the author became aware of research by Kościelny and Mochnacki who had, in their own words, discovered by accident that associativity of the addition operator could be removed in the generation of PN codes. This supports the conclusions of this author that associativity is not necessary. Unlike [161] however, Kościelny and Mochnacki did not explain why it could be removed. Neither did they consider maximal-length sequences or apply their codes as spreading sequences. Instead, they investigated them for use in stream ciphers and cryptography applications. These and other significant differences have been discussed in chapter 4.

This thesis also provides the proof of the stability of the DP codes and discusses the importance of this. The randomness properties: Balance, Run and Window are also proven, as is the existence of the codes. Kościelny and Mochnacki did not consider these issues, concentrating instead on those relevant to their application. A point to note is that it is very difficult to prove general results in relation to the properties of the DP codes, due to the nature of their generation. Many of the recommendations for future research therefore suggest possible ways of improving the understanding of these codes, and this could then improve the understanding of other techniques.

Chapter 4 also examines the linear complexity of the DP codes, because Kościelny and Mochnacki found that their codes (a special case of the DP codes) could have high linear complexity. Linear complexity is an important property of PN codes in cryptographic applications, and it can also be important for spread-spectrum communications. Subsets of DP codes have been found which have a very high linear complexity, but because m-sequences are a special case of the DP codes, and m-sequences have poor linear complexity, so other subsets of DP codes with low linear complexity can be found.

The last research chapter of this thesis, chapter 5, compares subsets of the DP codes with a selection of other quaternary techniques. The comparison is provided for com-

pleteness and is not intended to show that any given technique is better than another. The research of the early chapters shows that such a comparison is influenced by many factors and conclusions drawn cannot necessarily be generalised from the specific situations considered. The research in chapter 5 therefore intends to show that DP codes perform comparably to random codes, and this is shown to be true in most cases. The selection of a subset of the codes in a certain manner can provide poor performance, but the reasons for this have been recognised and discussed. Other subset selections tested do have performance comparable to random codes and codes from the other quaternary families considered. Thus with care, subsets of Dual Problem codes can be found which are suitable for non-binary spread-spectrum multiple-access. Certainly these novel codes provide many avenues for future research, recommendations for which are given in the next section.

The results of this thesis also provide contributions to the understanding of non-binary coded spread-spectrum multiple-access on several levels, which is important because although the field is still in its infancy, research is increasingly considering it.

6.2 Recommendations For Future Work

The motivation for future research into non-binary coded spread-spectrum communications will be provided by the increasing number of commercial applications of spread-spectrum technology, particularly in the mobile or personal communications market. In such systems, families containing large numbers of codes will be required. The use of *long* codes is discussed in the Introduction as one method of providing for a large number of potential users. The use of non-binary codes, as investigated in this thesis is another, which is also applicable to the former approach. Non-binary codes can provide the additional advantage of potentially reduced correlations and therefore improve performance, or allow a greater number of active users. For this reason they may well be considered for use in spread-spectrum systems employing *long* codes.

The development of commercial systems generates several practical issues which can be researched, for example:

1. A potential problem with quaternary systems is self interference that can arise be-

tween the inphase and quadrature channels, because of the imperfections in practical oscillators and phase-shift circuitry.

2. Consideration could also be given to increasing the code length from $q^n - 1$ to q^n. This then means that the data and code generator clocks can be made coincident, which not only reduces the complexity of the system, but as discussed by Scholtz in [173] can improve the privacy of the system. Fiebig et. al. [37] investigated this issue in relation to m-sequences and found that performance was generally degraded. Investigating the issue for sets of DP sequences may prove to be more worthwhile, since m-sequences have a number of special properties, such as satisfying the randomness properties, the shift-and-add property, and the near-ideal (for binary codes) autocorrelation spectrum. The insertion of a different code symbol into the code would completely disrupt this, as Fiebig et. al. found. A simple approach would be to place an additional memory element at the output of the shift-register (after the feedback tap) which initially contained the additional symbol. This then maintains the shift-register configuration and simplifies the problem that Fiebig considered of determining where to place the additional symbol.

The avenue of investigation for the second point proposed above, the inclusion of an extra memory element at the output of the feedback shift-register configuration, arises in some cases as a solution to the Berlekamp-Massey algorithm. This algorithm is used to determine the linear complexity of the codes as measured by the shortest linear feedback shift-register capable of generating the codes. The algorithm could be employed in future research to investigate the structure of the DP codes in relation to the arithmetic and feedback configuration employed. This may then reduce the search space for finding the codes, overcome problems in the selection of subsets with poor performance, and possibly eliminate the need to test codes for uniqueness.

Research which could assist this investigation includes that by Green and associates [59, 58, 60] in relation to non-linear binary shift-registers and their polynomial representations. Key [82] also investigated the structure of non-linear binary codes and this research could be considered as well. A different approach was employed by Lindholm [110] who researched the weight-tuple distributions of binary codes and related these to the generating polynomial. Pursuing this avenue of research could further the under-

standing of the relationships between the code properties of complexity, randomness and correlation. This would then assist in the understanding of not only the Dual Problem codes, but possibly other code generation techniques as well. It is the author's opinion that the next stage of research into the Dual Problem should be pursued from a more rigorous mathematical viewpoint. This could then refine the arithmetic definition, lead to a reduced search space for finding the codes and assist in the selection of subsets for use in spread-spectrum communications.

Another field of CDMA research receiving increasing attention is multiuser systems. In such systems a smart receiver is employed to reduce the multiple-access interference and improve performance. It has been discussed in the Introduction (section 1.3.1) how the use of non-binary codes with Trellis Coded Modulation (TCM) can improve performance over binary-code spread-spectrum with TCM. There are many parallels between the binary SS/TCM system and multiuser CDMA research, hence the consideration of non-binary codes may provide further areas of investigation and gains for that field.

The research of this thesis therefore contributes to the understanding of direct-sequence spread-spectrum systems employing non-binary codes on several levels, all concerned with the fundamental component of the system, the spreading codes. No prior research has investigated non-binary codes for spread-spectrum systems in such detail, to the best of the author's knowledge. The research required the resolution of many issues in relation to code properties which still cause contention in the literature on binary codes, and are rarely considered in the small amount of literature relating to non-binary codes. The development of the Dual Problem approach to code design also proposes many avenues for future research which the author hopes are pursued because of the potential for improving the overall understanding of code generation and spread-spectrum systems. Thus the work of this thesis provides original contributions to the knowledge of the field, and a promising basis for this future research.

Appendix A

Analysis For The Examples Of Chapter 3

A.1 Symmetric Uniform PDF

This appendix provides information relevant to deriving the CDF of the code pair interference if the PDF of the real and imaginary components of the even and odd periodic crosscorrelation spectra have a symmetric (about the zero value) uniform PDF. This example can be extended to consider the more difficult case of an asymmetric stepped PDF containing spikes at discrete locations, which is the form of the PDF for an actual set of codes.

For the example of section 3.1.1, the probability density function of x and analogously y, is given as:

$$f_x(x) = \begin{cases} \dfrac{1}{2S} & |x| \leq S \\ \\ 0 & \text{otherwise} \end{cases} \tag{A.1}$$

Since $\boldsymbol{\theta}$ is uniformly distributed over $[-S, S]$ and x, y and $\boldsymbol{\theta}$ are assumed independent, so $f_{x,y,\theta}(x, y, \theta)$ is as given as below.

$$f_{x,y,\theta}(x, y, \theta) = \begin{cases} \dfrac{1}{8\pi S^2} & |x| \leq S, |y| \leq S \text{ and } |\theta| \leq \pi \\ \\ 0 & \text{otherwise} \end{cases} \tag{A.2}$$

Converting to polar coordinates $f_{r,\varphi,w}(r, \varphi, w) = r.f_{x,y,\theta}(r\cos\varphi, r\sin\varphi, w)$, defining $\boldsymbol{\alpha} =$

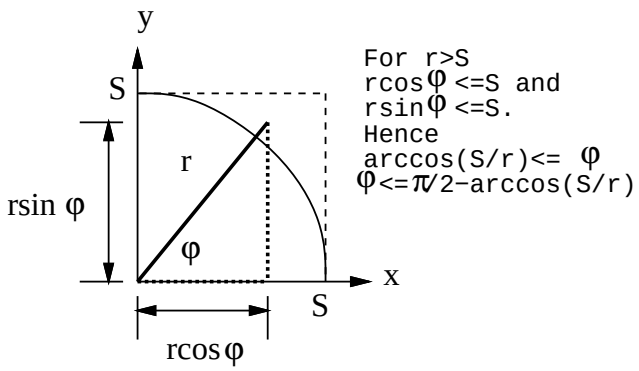


Figure A.1: Integration quadrant.

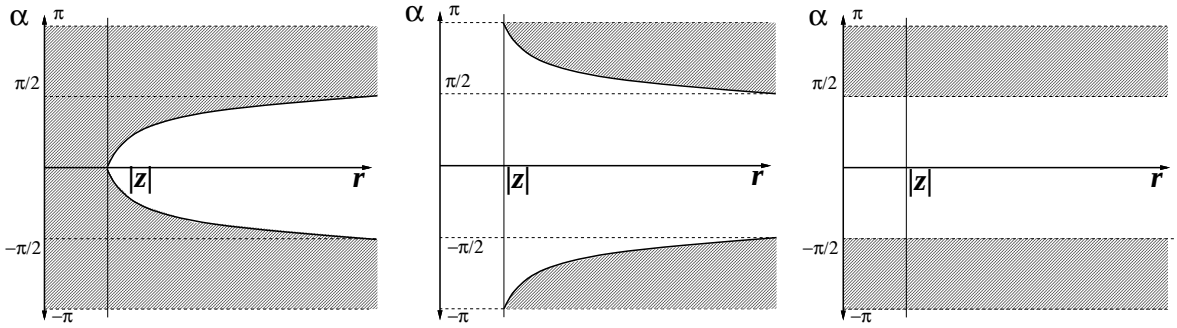


Figure A.2: Integration regions $z \geq 0$, $z \leq 0$ and $z = 0$, with $\alpha = \arccos(z/r)$.

$\boldsymbol{\theta} + \boldsymbol{\varphi}$ and integrating over φ will eliminate the variable φ. Care needs to be taken in the integration in the region $S \leq r \leq \sqrt{2}S$ however, because of the conversion to polar coordinates. Figure A.1 illustrates one of the four symmetrical integration regions.

Thus for $0 \leq r \leq S$:

$$f_{r,\alpha}(r,\alpha) = 4\int_0^{\frac{\pi}{2}} \frac{r}{8\pi S^2}.d\varphi = \frac{r}{4S^2} \tag{A.3}$$

and for $S \leq r \leq \sqrt{2}S$:

$$f_{r,\alpha}(r,\alpha) = 4\int_{\lambda}^{\frac{\pi}{2}-\lambda} \frac{r}{8\pi S^2}.d\varphi = \frac{r}{4S^2} - \frac{\lambda r}{\pi S^2} \tag{A.4}$$

where $\lambda = \arccos(S/r)$. To obtain the CDF of the code-pair interference $F_z(z)$, $f_{r,\alpha}(r,\alpha)$ needs to be integrated over the regions illustrated in figure A.2. The symbolic mathematics program *Mathematica* [195] was employed by the author for this.

It can be shown that:

$$\begin{aligned} F(z|z=0) &= \int_{\frac{\pi}{2}}^{\pi}\int_{0}^{S} f_{r,\alpha}(r,\alpha).dr.d\alpha + \int_{-\pi}^{-\frac{\pi}{2}}\int_{0}^{S} f_{r,\alpha}(r,\alpha).dr.d\alpha \\ &+ \int_{\frac{\pi}{2}}^{\pi}\int_{S}^{\sqrt{2}S} f_{r,\alpha}(r,\alpha).dr.d\alpha + \int_{-\pi}^{-\frac{\pi}{2}}\int_{S}^{\sqrt{2}S} f_{r,\alpha}(r,\alpha).dr.d\alpha \\ &= \frac{1}{2} \end{aligned}$$

$$\begin{aligned} F(z|0\le z\le S) &= \int_{-\pi}^{\pi}\int_{0}^{z} f_{r,\alpha}(r,\alpha).dr.d\alpha + \int_{\arccos(z/r)}^{\pi}\int_{z}^{S} f_{r,\alpha}(r,\alpha).dr.d\alpha \\ &+ \int_{\arccos(z/r)}^{\pi}\int_{S}^{\sqrt{2}S} f_{r,\alpha}(r,\alpha).dr.d\alpha + \int_{-\pi}^{-\arccos(z/r)}\int_{z}^{S} f_{r,\alpha}(r,\alpha).dr.d\alpha \\ &+ \int_{-\pi}^{-\arccos(z/r)}\int_{S}^{\sqrt{2}S} f_{r,\alpha}(r,\alpha).dr.d\alpha \\ &= 1 + \frac{z}{4S}\sqrt{2-\frac{z^2}{S^2}} - \frac{1}{2}\arccos\left(\frac{z}{\sqrt{2}S}\right) + 2\mathcal{I}_1 \end{aligned}$$

$$\begin{aligned} F(z|S\le z\le \sqrt{2}S) &= \int_{-\pi}^{\pi}\int_{0}^{S} f_{r,\alpha}(r,\alpha).dr.d\alpha + \int_{-\pi}^{\pi}\int_{S}^{z} f_{r,\alpha}(r,\alpha).dr.d\alpha \\ &+ \int_{\arccos(z/r)}^{\pi}\int_{z}^{\sqrt{2}S} f_{r,\alpha}(r,\alpha).dr.d\alpha + \int_{-\pi}^{-\arccos(z/r)}\int_{z}^{\sqrt{2}S} f_{r,\alpha}(r,\alpha).dr.d\alpha \\ &= 1 + \frac{z}{4S}\sqrt{2-\frac{z^2}{S^2}} - \frac{1}{2}\arccos\left(\frac{z}{\sqrt{2}S}\right) + 2\mathcal{I}_2 \end{aligned}$$

and $F(z|z\le 0) = 1 - F(z|z\ge 0)$. Where

$$\begin{aligned} \mathcal{I}_1 &= \int_{S}^{\sqrt{2}S} \arccos(s/r)\arccos(z/r)\frac{r}{\pi S^2}.dr \\ &= \frac{1}{2\pi}(\frac{\pi}{2}-1)\arccos\left(\frac{z}{\sqrt{2}S}\right) - \frac{z}{8S}\sqrt{2-\frac{z^2}{S^2}} \\ &+ \frac{z}{2\pi S}\left\{\frac{(S^2+z^2)}{2zS}\ln\left|\frac{S^2-z\sqrt{2S^2-z^2}}{S^2-z^2}\right| + \ln\left|\frac{3S^2-z^2+2\sqrt{S^2(2S^2-z^2)}}{S^2-z^2}\right|\right\} \end{aligned}$$

$$\begin{aligned} \mathcal{I}_2 &= \int_{z}^{\sqrt{2}S} \arccos(s/r)\arccos(z/r)\frac{r}{\pi S^2}.dr \\ &= \frac{1}{2\pi}(\frac{\pi}{2}-1)\arccos\left(\frac{z}{\sqrt{2}S}\right) - \frac{z}{8S}\sqrt{2-\frac{z^2}{S^2}} \\ &+ \frac{z}{2\pi S}\left\{\frac{(S^2+z^2)}{2zS}\ln\left|\frac{S^2-z\sqrt{2S^2-z^2}}{z^2-S^2}\right| + \ln\left|\frac{3S^2-z^2+2\sqrt{S^2(2S^2-z^2)}}{z^2-S^2}\right|\right\} \end{aligned}$$

A bounded approximation to the bit error probability can now be obtained via the method of Özlütürk and Lam reviewed in section 2.1.2.

A.2 Symmetric Triangular PDF

This appendix derives the CDF of the code-pair interference when the real and imaginary components for the even and odd periodic crosscorrelation spectra have a PDF which is triangular in the region $[-S, S]$. That is

$$f_x(x) = \begin{cases} \frac{1}{S} - \frac{|x|}{S^2} & \text{for } |x| \leq S \\ \\ 0 & \text{otherwise} \end{cases} \tag{A.5}$$

and analogously for $f_y(y)$. Following the analysis outlined in the previous section of this appendix, it can be shown that

$$f_{r,\alpha}(r,\alpha) = \begin{cases} \frac{r}{\pi S^2}\left(\frac{r^2}{S^2} - \frac{4r}{S} + \pi\right) & 0 \leq r \leq S \\ \\ \frac{r}{\pi S^2}\left(-2 - \frac{r^2}{S^2} + 4\sqrt{\frac{r^2}{S^2} - 1} + \pi - 4\arccos(s/r)\right) & S \leq r \leq \sqrt{2}S \\ \\ 0 & \text{otherwise} \end{cases} \tag{A.6}$$

From this, expressions for $F_z(z)$ the CDF of the code-pair interference can be derived. Again following the outline in the previous section, it can be shown that $F_z(z|z=0) = 0.5$ and that:

$$\begin{aligned} F(z|0 \leq z \leq S) &= 1 + \frac{1}{3\pi S^3}\left[(3S^2 + 2z^3)\sqrt{1 - \frac{z^2}{S^2}} + (-7S^2 z + 3\pi S^2 z - z^3)\sqrt{2 - \frac{z^2}{S^2}}\right. \\ &\quad -S^3\arccos(z/S) + (18S^3 - 6\pi S^3)\arccos\left(\frac{z}{\sqrt{2}S}\right) \\ &\quad \left. + 4z^3\ln(z) - 4z^3\ln\left(S + S\sqrt{1 - \frac{z^2}{S^2}}\right)\right] - 8\mathcal{I}_3 + 8\mathcal{I}_1 \end{aligned}$$

$$\begin{aligned} F(z|S \leq z \leq \sqrt{2}S) &= 1 - 2\left[\frac{z(2S^2 - 3\pi S^2 + z^2)\sqrt{2 - \frac{z^2}{S^2}}}{6\pi S^3} + \frac{(\pi - 3)\arccos\left(\frac{z}{\sqrt{2}S}\right)}{\pi}\right] \\ &\quad -8\mathcal{I}_4 + 8\mathcal{I}_2 \end{aligned}$$

and $F_z(z|z \leq 0) = 1 - F_z(z|z \geq 0)$ where $\mathcal{I}_1$ and $\mathcal{I}_2$ are as given in the previous section and

$$\begin{aligned}
\mathcal{I}_3 &= \int_z^{\sqrt{2}S} \arccos(z/r) \frac{r}{\pi S^2} \sqrt{\frac{r^2}{S^2} - 1}.dr \\
&= \frac{-z\sqrt{2 - \frac{z^2}{S^2}}}{6\pi S} + \frac{\arccos\left(\frac{z}{\sqrt{2}S}\right)}{3\pi} \\
&+ \frac{z}{6\pi S^3} \left[\frac{S^3}{z} \ln \left| \frac{S^2 - z\sqrt{2S^2 - z^2}}{S^2 - z^2} \right| - \frac{3S^2 - z^2}{2} \ln \left| \frac{3S^2 - z^2 + 2\sqrt{S^2(2S^2 - z^2)}}{S^2 - z^2} \right| \right]
\end{aligned}$$

$$\begin{aligned}
\mathcal{I}_4 &= \int_S^{\sqrt{2}S} \arccos(z/r) \frac{r}{\pi S^2} \sqrt{\frac{r^2}{S^2} - 1}.dr \\
&= \frac{-z\sqrt{2 - \frac{z^2}{S^2}}}{6\pi S} + \frac{\arccos\left(\frac{z}{\sqrt{2}S}\right)}{3\pi} \\
&+ \frac{z}{6\pi S^3} \left[\frac{S^3}{z} \ln \left| \frac{S^2 - z\sqrt{2S^2 - z^2}}{z^2 - S^2} \right| - \frac{3S^2 - z^2}{2} \ln \left| \frac{3S^2 - z^2 + 2\sqrt{S^2(2S^2 - z^2)}}{z^2 - S^2} \right| \right]
\end{aligned}$$

Appendix B

Contingency Table Analysis

This appendix provides information relevant to the statistical independence test: contingency table or crosstabulation analysis. The definitions provided below are taken from [135, p.295–297].

> *"Definition 10.2*
>
> *Two variables that have been categorised in a two-way table are independent if the probability that a measurement is classified into a given cell of a table is equal to the probability of being classified into that row times the probability of being classified into that column. This must be true for all cells of the table.*
>
> *The test statistic is*
>
> $$\chi^2 = \sum_i \sum_j \left[\frac{n_{ij} - E_{ij}}{E_{ij}} \right]^2 \tag{B.1}$$
>
> *where n_{ij} and E_{ij} are respectively the observed and expected number of measurments falling in the cell for the i^{th} row and j^{th} column."*

> *"Definition 10.3*
>
> *The expected number of measurments E_{ij} falling in the i, j cell (cell of the i^{th} row and j^{th} column of the table) is taken to be $E_{ij} = (row\ i\ total)(column\ j\ total)/n$ when the two variables are independent. $[n = \sum_i \sum_j n_{ij}]$ "*

The null hypothesis H_0 is that the two variables are independent, and the alternate hypothesis is that they are dependent. Hypothesis H_0 is rejected if χ^2 exceeds the

tabulated value of chi-square (for example [94, Table A12]), for a significance level of α and $(r-1)(c-1)$ degrees of freedom, where the number of rows in the table is r and the number of columns is c.

Care must be taken when using contingency table analysis however, as [135, p.270] states:

> *"Cochran (1954) indicates that the approximation* [chi-square independence test] *should be good if no E_{ij} is less than 1 and no more than* 20% *of the E_{ij}'s are less than 5. "*

This constraint was adhered to when the test was used in section 3.1.3.

Appendix C

Dual Problem

C.1 DP (N=63) Code Existence

Gain $D^2D^1D^0$	MLS existence	Total No. of codes	Distinct for coder
– 1 1	no	0	0
– 1 2	yes	36	6
– 1 3	yes	36	6
– 2 1	yes	36	6
– 2 2	no	0	0
– 2 3	yes	36	6
– 3 1	yes	36	6
– 3 2	yes	36	6
– 3 3	no	0	0
1 – 1	no	0	0
1 – 2	no	0	0
1 – 3	no	0	0
1 1 1	yes	40	28
1 1 2	yes	88	70
1 1 3	yes	88	70
1 2 1	yes	46	37
1 2 2	yes	40	22
1 2 3	yes	52	19
1 3 1	yes	46	37
1 3 2	yes	52	19
1 3 3	yes	40	22
2 – 1	no	0	0
2 – 2	no	0	0

Gain $D^2D^1D^0$	MLS existence	Total no. of codes	Distinct for coder
2 – 3	no	0	0
2 1 1	yes	40	22
2 1 2	yes	46	37
2 1 3	yes	52	19
2 2 1	yes	88	70
2 2 2	yes	40	28
2 2 3	yes	88	70
2 3 1	yes	52	19
2 3 2	yes	46	37
2 3 3	yes	40	22
3 – 1	no	0	0
3 – 2	no	0	0
3 – 3	no	0	0
3 1 1	yes	40	22
3 1 2	yes	52	19
3 1 3	yes	46	37
3 2 1	yes	52	19
3 2 2	yes	40	22
3 2 3	yes	46	37
3 3 1	yes	88	70
3 3 2	yes	88	70
3 3 3	yes	40	28

Table C.1: Existence and repetition of period 63 DP codes. †

†: The dash indicates no feedback connection

C.2 A Selection Of Addition Operators

This section contains the addition operators used in examples of the Dual Problem codes throughout this thesis.

$\oplus$	0	1	2	3
0	0	2	3	1
1	2	0	1	3
2	3	1	2	0
3	1	3	0	2

$\oplus$	0	1	2	3
0	0	3	1	2
1	3	0	2	1
2	1	2	3	0
3	2	1	0	3

$\oplus$	0	1	2	3
0	1	2	0	3
1	2	1	3	0
2	0	3	2	1
3	3	0	1	2

$\oplus$	0	1	2	3
0	1	3	2	0
1	3	1	0	2
2	2	0	3	1
3	0	2	1	3

Table C.2: Addition operators for codes: $\widetilde{A} \ldots \widetilde{D}$.

$\oplus$	0	1	2	3
0	2	0	1	3
1	0	3	2	1
2	1	2	3	0
3	3	1	0	2

$\oplus$	0	1	2	3
0	2	1	0	3
1	1	3	2	0
2	0	2	3	1
3	3	0	1	2

$\oplus$	0	1	2	3
0	3	0	2	1
1	0	2	1	3
2	2	1	3	0
3	1	3	0	2

$\oplus$	0	1	2	3
0	3	1	2	0
1	1	2	0	3
2	2	0	3	1
3	0	3	1	2

Table C.3: Addition operators for codes: $\widetilde{E} \ldots \widetilde{H}$.

C.3 DP (N=255) Code Existence

This section lists the coder configurations capable of producing Dual Problem codes of period $N = 255$. The notation – *1 1 1* specifies the coder $D^4 = 1 \otimes D^2 \oplus 1 \otimes D^1 \oplus 1 \otimes D^0$. The abbreviation "Tot." specifies the total number of codes found, and "Dist.", the number of distinct sequences for that coder.

Coder	Tot.	Dist.	Coder	Tot.	Dist.	Coder	Tot.	Dist.
– *1 1 1*	16	10	*1 – 1 1*	8	2	*1 2 3 1*	3	3
– *1 1 2*	14	8	*1 – 1 2*	24	21	*1 2 3 3*	15	15
– *1 1 3*	14	8	*1 – 1 3*	24	21	*1 3 – 1*	27	21
– *1 2 1*	8	8	*1 – 2 1*	24	21	*1 3 – 2*	18	15
– *1 2 2*	16	13	*1 – 2 2*	20	17	*1 3 – 3*	8	5
– *1 2 3*	38	20	*1 – 2 3*	27	15	*1 3 1 1*	11	5
– *1 3 1*	8	8	*1 – 3 1*	24	21	*1 3 1 2*	25	25
– *1 3 2*	38	20	*1 – 3 2*	27	15	*1 3 1 3*	37	28
– *1 3 3*	16	13	*1 – 3 3*	20	17	*1 3 2 1*	3	3
– *2 1 1*	16	13	*1 1 – 1*	8	8	*1 3 2 2*	15	15
– *2 1 2*	8	8	*1 1 – 2*	18	9	*1 3 3 1*	25	22
– *2 1 3*	38	20	*1 1 – 3*	18	9	*1 3 3 2*	4	1
– *2 2 1*	14	8	*1 1 1 2*	21	21	*1 3 3 3*	23	20
– *2 2 2*	16	10	*1 1 1 3*	21	21	*2 – – 1*	36	6
– *2 2 3*	14	8	*1 1 2 1*	4	1	*2 – – 3*	36	6
– *2 3 1*	38	20	*1 1 2 2*	32	29	*2 – 1 1*	20	17
– *2 3 2*	8	8	*1 1 2 3*	19	7	*2 – 1 2*	24	21
– *2 3 3*	16	13	*1 1 3 1*	4	1	*2 – 1 3*	27	15
– *3 1 1*	16	13	*1 1 3 2*	19	7	*2 – 2 1*	24	21
– *3 1 2*	38	20	*1 1 3 3*	32	29	*2 – 2 2*	8	2
– *3 1 3*	8	8	*1 2 – 1*	27	21	*2 – 2 3*	24	21
– *3 2 1*	38	20	*1 2 – 2*	8	5	*2 – 3 1*	27	15
– *3 2 2*	16	13	*1 2 – 3*	18	15	*2 – 3 2*	24	21
– *3 2 3*	8	8	*1 2 1 1*	11	5	*2 – 3 3*	20	17
– *3 3 1*	14	8	*1 2 1 2*	37	28	*2 1 – 1*	8	5
– *3 3 2*	14	8	*1 2 1 3*	25	25	*2 1 – 2*	27	21
– *3 3 3*	16	10	*1 2 2 1*	25	22	*2 1 – 3*	18	15
1 – – 2	36	6	*1 2 2 2*	23	20	*2 1 1 1*	23	20
1 – – 3	36	6	*1 2 2 3*	4	1	*2 1 1 2*	25	22

Table C.4: DP coder configurations producing codes of period 255. Part I.

Coder	Tot.	Dist.	Coder	Tot.	Dist.	Coder	Tot.	Dist.
2 1 1 3	4	1	*3 – – 1*	36	6	*3 2 – 2*	8	5
2 2 – 1	18	9	*3 – – 2*	36	6	*3 2 – 3*	27	21
2 2 – 2	8	8	*3 – 1 1*	20	17	*3 2 1 1*	15	15
2 2 – 3	18	9	*3 – 1 2*	27	15	*3 2 1 3*	3	3
2 2 1 1	32	29	*3 – 1 3*	24	21	*3 2 2 1*	4	1
2 2 1 2	4	1	*3 – 2 1*	27	15	*3 2 2 2*	23	20
2 2 1 3	19	7	*3 – 2 2*	20	17	*3 2 2 3*	25	22
2 2 2 1	21	21	*3 – 2 3*	24	21	*3 2 3 1*	25	25
2 2 2 3	21	21	*3 – 3 1*	24	21	*3 2 3 2*	37	28
2 2 3 1	19	7	*3 – 3 2*	24	21	*3 2 3 3*	11	5
2 2 3 2	4	1	*3 – 3 3*	8	2	*3 3 – 1*	18	9
2 2 3 3	32	29	*3 1 – 1*	8	5	*3 3 – 2*	18	9
2 3 – 1	18	15	*3 1 – 2*	18	15	*3 3 – 3*	8	8
2 3 – 2	27	21	*3 1 – 3*	27	21	*3 3 1 1*	32	29
2 3 – 3	8	5	*3 1 1 1*	23	20	*3 3 1 2*	19	7
2 3 1 1	15	15	*3 1 1 2*	4	1	*3 3 1 3*	4	1
2 3 1 2	3	3	*3 1 1 3*	25	22	*3 3 2 1*	19	7
2 3 2 1	25	25	*3 1 2 2*	15	15	*3 3 2 2*	32	29
2 3 2 2	11	5	*3 1 2 3*	3	3	*3 3 2 3*	4	1
2 3 2 3	37	28	*3 1 3 1*	37	28	*3 3 3 1*	21	21
2 3 3 1	4	1	*3 1 3 2*	25	25	*3 3 3 2*	21	21
2 3 3 2	25	22	*3 1 3 3*	11	5			
2 3 3 3	23	20	*3 2 – 1*	18	15			

Table C.5: DP coder configurations producing codes of period 255. Part II.

C.4 Tabular Autocorrelation Values Of Selected Dual Problem Sequences

This section provides tabular information on the autocorrelation properties of a selection of Dual Problem codes. Tables C.6 (a) and (b) and C.7 provide the peak out-of-phase value of the real and imaginary components and the sidelobe energy for even periodic, odd periodic and aperiodic autocorrelation. A detailed comparison of the autocorrelation properties of codes from different families is not provided in this thesis, because it is not relevant to the research which has investigated code properties for the multiple-access channel and subsequently code generation.

The autocorrelation properties of codes are important when transmission is over a multipath channel and in regard to synchronisation, acquisition and tracking. These issues are not investigated in this thesis, thus a comparison using merit factors alone could be misleading without having investigated these properties and situations in detail. However, the reader interested in the autocorrelation properties of different codes is referred to the literature referenced for each technique in chapter 4. The reader is also referred to the prior work by this author in [161] which shows that the peak out-of-phase magnitudes and sidelobe energies of a selection of DP sequences are comparable with those of random codes.

Future research could therefore investigate the suitability of the DP sequences in relation to the issues of acquisition, tracking, synchronisation and a multipath channel.

code	peak		SE
	Re	Im	
$\widetilde{A}$	11	14	3646
$\widetilde{B}$	9	10	2286
$\widetilde{C}$	9	10	2286
$\widetilde{D}$	11	14	3646
$\widetilde{E}$	11	14	3646
$\widetilde{F}$	11	14	3646
$\widetilde{G}$	11	12	3182
$\widetilde{H}$	11	12	3182

code	peak				SE	
	max		min		max	min
	Re	Im	Re	Im		
$\widetilde{A}$	17	18	9	10	5270	2694
$\widetilde{B}$	15	16	9	8	4070	2118
$\widetilde{C}$	15	16	9	8	4070	2118
$\widetilde{D}$	17	18	9	10	5270	2694
$\widetilde{E}$	17	18	9	10	5270	2694
$\widetilde{F}$	17	18	9	10	5270	2694
$\widetilde{G}$	19	18	9	8	5830	2166
$\widetilde{H}$	19	18	9	8	5830	2166

Table C.6: a) Even Periodic b) Odd Periodic Autocorrelation

code	peak				SE	
	max		min		max	min
	Re	Im	Re	Im		
$\widetilde{A}$	14	16	9	10	4458	3170
$\widetilde{B}$	12	12	6	8	3178	2202
$\widetilde{C}$	12	12	6	8	3178	2202
$\widetilde{D}$	14	16	9	10	4458	3170
$\widetilde{E}$	14	16	9	10	4458	3170
$\widetilde{F}$	14	16	9	10	4458	3170
$\widetilde{G}$	14	15	7	9	4506	2674
$\widetilde{H}$	14	15	7	9	4506	2674

Table C.7: Aperiodic Autocorrelation

Bibliography

[1] Z.A. Abbasi and F. Ghani. Multilevel sequences with good autocorrelation properties. *Electronics Letters*, Vol. 24, No. 7, pp.393–394, Mar. 1988.

[2] A.H. Aghvami. Future CDMA cellular mobile systems supporting multi-service operation. In *Proceedings of the 5th IEEE Personal, Indoor, Mobile Radio Communications Conference*, pp. 1276–1279, The Hague, Netherlands, Sep. 18–22 1994.

[3] M. Ahtee and P.J. White. Spread spectrum communication within EMC regulation. In *Proceedings of the 2nd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 295–302, Yokohama, Japan, Nov. 29–Dec. 2 1992.

[4] J.P. Aldis and S.K. Barton. On the relative power levels required by handsets in DS-CDMA, FH-CDMA and narrowband cellular radio systems. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 362–366, Stockholm, Sweden, Jun. 7–10 1994.

[5] P.S. Alexandroff. *An introduction to the theory of Groups.* Blackie and son, 1968.

[6] W.O. Alltop. Complex sequences with low periodic correlations. *IEEE Transactions on Information Theory*, Vol. 26, No. 3, pp.350–354, May 1980.

[7] P.G. Andermo and G. Brismark. CODIT, a testbed project evaluating DS-CDMA for UMTS/FPLMTS. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 21–25, Stockholm, Sweden, Jun. 7–10 1994.

[8] M. Antweiler, C. Acker, and L. Bomer. New quadriphase sequences with good periodic and odd correlation properties. In *Proceedings of the URSI International Symposium on Signals, Systems, and Electronics*, pp.540–543, 1989.

[9] M. Antweiler and L. Bomer. Complex sequences over GF(p^m) with a two-level autocorrelation function and large linear span. *IEEE Transactions on Information Theory*, Vol. 38, No. 1, pp.120–130, Jan. 1992.

[10] A. Baier, U-C. Fiebig, W. Granzow, W. Koch, P. Teder, and J. Thielecke. Design study for a CDMA-based third-generation mobile radio system. *IEEE Journal on Selected Areas in Communications*, Vol. 12, No. 4, pp.733–743, May 1994.

[11] A. Baier and H. Panzer. Multi-rate DS-CDMA radio interface for third-generation cellular systems. In *Mobile and Personal Communications*, pp.255–260. IEE Conference Publication No. 387, 13–15 Dec. 1993.

[12] P.W. Baier. CDMA or TDMA? CDMA for GSM? In *Proceedings of the 5th IEEE Personal, Indoor, Mobile Radio Communications Conference*, pp. 1280–1284, The Hague, Netherlands, Sep. 18–22 1994.

[13] D.M. Balston and R.V. Macario, editors. *Cellular Radio Systems*. Artech House, 1993.

[14] C. Balza, A. Fromageot, and M. Maniere. Four-level pseudorandom sequences. *Electronics Letters*, Vol. 3, No. 7, pp.313–315, Jul. 1967.

[15] E. Berruto, T. Brännlund, J. Gustafsson, and W. Schott. An SDL methodology used for specifying the radio protocols in a CDMA system. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 554–558, Stockholm, Sweden, Jun. 7–10 1994.

[16] R.E. Blahut. *Theory and Practice of Error Control Codes*. Addison-Wesley, 1984.

[17] S. Boztaş, R. Hammons, and P.V. Kumar. 4-phase sequences with near-optimum correlation properties. *IEEE Transactions on Information Theory*, Vol. 38, No. 3, pp.1101–1113, May 1992.

[18] S. Boztaş and P.V. Kumar. Binary sequences with Gold-like correlation but larger linear span. *IEEE Transactions on Information Theory*, Vol. 40, No. 2, pp. 532–537, Mar. 1994.

[19] A.G. Burr. Codes for spread spectrum multiple access systems. In *Proceedings of the 1st IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 109–115, London, England, Sep. 24–26 1990.

[20] S. Cacopardi, F. Frescura, and G. Reali. 4-Phase DS-CDMA mobile radio receiver in non-Gaussian environment. In *Proceedings of the 3rd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 440–444, Oulu, Finland, Jul. 4–6 1994.

[21] S. Cacopardi, F. Frescura, and G. Reali. Analysis and simulation of DS-CDMA mobile system in non-linear, frequency selective slow fading channel. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 60–64, Stockholm, Sweden, Jun. 7–10 1994.

[22] C-K Chan and W-H Lam. Efficient use of pseudo-noise sequences in synchronous direct-sequence spread-spectrum multiple-access communication systems. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 540–544, Stockholm, Sweden, Jun. 7–10 1994.

[23] J.A. Chang. Generation of 5-level maximal-length sequences. *Electronics Letters*, Vol. 2, No. 7, p.258, Jul. 1966.

[24] X.H. Chen and J. Oksman. BER performance analysis of 4-CCL and 5-CCL codes in slotted indoor CDMA systems. *IEE Proceedings*, Vol. 139, No. 1, Part I, pp.79–84, Feb. 1992.

[25] D.C. Chu. Polyphase codes with codes with good periodic correlation properties. *IEEE Transactions on Information Theory*, Vol. 18, pp.531–532, Jul. 1972.

[26] C.I. Cook. Development of air interface standards for PCS. *IEEE Personal Communications Magazine*, Vol. 1, No. 4, pp.1426–1433, Fourth Quarter 1994.

[27] G.R. Cooper and R.W. Nettleton. Spread spectrum technique for high-capacity mobile communications. *IEEE Transactions on Vehicular Technology*, Vol. 27, No. 4, pp.264–275, Nov. 1978.

[28] D.J. Cowl, P.L. Squires, and M. Shafi. An analytical approach to multipath and inter-user interference in multiple access direct sequence spread spectrum systems. In *Proceedings of the 2nd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 279–282, Yokohama, Japan, Nov. 29–Dec. 2 1992.

[29] R.C. Dixon. Why spread spectrum? *IEEE Communications Magazine*, Vol. 13, pp.21–25, 1975.

[30] R.C. Dixon. *Spread Spectrum Systems*. John Wiley and Sons, 1976.

[31] R. Dou and L.B. Milstein. Error probability bounds and approximations for DS spread spectrum communication systems with multiple tone or multiple access interference. *IEEE Transactions on Communications*, Vol. 32, No. 5, pp.493–502, May 1984.

[32] M. Epstein. Qualcomm CDMA. In *IEEE International Conference on Universal Wireless Access*, key–note speaker, 1994.

[33] P.Z. Fan, M. Darnell, and B. Honary. Crosscorrelations of Frank sequences and Chu sequences. *Electronics Letters*, Vol. 30, No. 6, pp.477–479, 1994.

[34] P.Z. Fan, M. Darnell, and B. Honary. New class of polyphase sequences with two-valued auto- and crosscorrelation functions. *Electronics Letters*, Vol. 30, No. 13, pp.1031–1032, Jun. 1994.

[35] P.Z. Fan, M. Darnell, and B. Honary. Polyphase sequences with good periodic and aperiodic autocorrelations. In *Proceedings of the IEEE International Symposium on Information Theory*, p. 74, Trondheim, Norway, Jun. 27–Jul. 1 1994.

[36] M. Feuerstein, G. Clausius, D. Vendetti, and D. Crews. Design and test of CDMA cellular systems. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 6–10, Stockholm, Sweden, Jun. 7–10 1994.

[37] U.C.G. Fiebig and M. Schnell. Correlation properties of extended m-sequences. *Electronics Letters*, Vol. 29, No. 20, pp.1753–1754, Sep. 1993.

[38] R.L. Frank. Polyphase codes with good nonperiodic correlation properties. *IEEE Transactions on Information Theory*, pp.43–45, Jan. 1963.

[39] R.L. Frank. Comments on Polyphase codes with good correlation properties. *IEEE Transactions on Information Theory*, Vol. 19, p.244, Mar. 1973.

[40] R.L. Frank, S.A. Zadoff, and R.C. Heimiller. Phase shift pulse codes with good periodic correlation properties. *IRE Transactions on Information Theory*, pp.381–382, Oct. 1962.

[41] H. Fredricksen. A survey of full length nonlinear shift register cycle algorithms. *SIAM Review*, Vol. 24, No. 2, pp.195–221, Apr. 1982.

[42] S.A. Fredricsson. Pseudo-randomness properties of binary shift register sequences. *IEEE Transactions on Information Theory*, Vol. 21, pp.115–120, Jan. 1975.

[43] M. Frullone, G. Riva, P. Grazioso, and M. Missiroli. Comparisons of multiple access schemes for personal communication systems in a mixed cellular environment. *IEEE Transactions on Vehicular Technology*, Vol. 43, No. 1, pp.99–109, Feb. 1994.

[44] H. Fukumasa, R. Kohno, and H. Imai. Design of pseudo-noise sequences with good odd and even correlation properties. In *Proceedings of the 2nd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 139–142, Yokohama, Japan, Nov. 29–Dec. 2 1992.

[45] H. Fukumasa, R. Kohno, and H. Imai. Design of pseudonoise sequences with good odd and even correlation properties for DS/CDMA. *IEEE Journal on Selected Areas in Communications*, Vol. 12, No. 5, pp.828–836, Jun. 1994.

[46] F.D. Garber and M.B. Pursley. Performance of offset quadriphase spread-spectrum multiple-access communications. *IEEE Transactions on Communications*, Vol. 29, No. 3, pp. 305–313, Mar. 1981.

[47] E. Geraniotis, Y.-W. Chang, and W.-B. Yang. Multi-media integration in CDMA networks. In *Proceedings of the 3rd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 88–97, Oulu, Finland, Jul. 4–6 1994.

[48] E. Geraniotis and B. Ghaffari. Performance of binary and quaternary direct-sequence spread-spectrum multiple-access systems with random signature sequences. *IEEE Transactions on Communications*, Vol. 39, No. 5, pp.713–724, May 1991.

[49] E.A. Geraniotis and M.B. Pursley. Error probability for direct-sequence spread-spectrum multiple-access communications – Part II: Approximations. *IEEE Transactions on Communications*, Vol. 30, No. 5, pp.985–995, May 1982.

[50] K.R. Godfrey. Three-level m-sequences. *Electronics Letters*, Vol. 2, No. 7, pp.241–242, Jul. 1966.

[51] R. Gold. Study of multistate PN sequences and their application to communication systems. *Rockwell Int. Corp. Rep.*, AD A025137, 1967.

[52] R. Gold. Maximal recursive sequences with 3-valued recursive cross correlation functions. *IEEE Transactions on Information Theory*, pp.154–156, Jan. 1968.

[53] S.W. Golomb. *Shift Register Sequences*. Holden Day, 1967.

[54] S.W. Golomb and R.A. Scholtz. Generalized Barker sequences. *IEEE Transactions on Information Theory*, Vol. 11, No. 4, pp.533–537, Oct. 1965.

[55] G. Gong and G.Z. Xiao. Synthesis and uniqueness of m-sequences over GF(q^n) as n-phase sequences over GF(q). *IEEE Transactions on Communications*, Vol. 42, No. 8, pp.2501–2505, Aug. 1994.

[56] C.S. Goswami and M. Beale. Correlation properties of dual-BCH, Kasami, and other sequences for spread-spectrum multiple-access systems. *IEE Proceedings*, Vol. 135, Part F, No. 1, pp.114–117, Feb. 1988.

[57] I.S. Gradshetyn and I.M. Ryzhik. *Table of integrals, series, and products: Corrected and enlarged edition*. Academic Press, 1992.

[58] D.H. Green and K.R. Dimond. Nonlinear product-feedback shift registers. *IEE Proceedings*, Vol. 117, No. 4, pp.680–686, Apr. 1970.

[59] D.H. Green and K.R. Dimond. Polynomial representation of nonlinear feedback shift registers. *IEE Proceedings*, Vol. 117, No. 1, pp.56–60, Jan. 1970.

[60] D.H. Green and R.G. Kelsch. Some polynomial compositions of nonlinear feedback shift registers and their sequence-domain consequences. *IEE Proceedings*, Vol. 117, No. 9, pp.1750–1756, Sep. 1970.

[61] D.H. Green and I.S. Taylor. Irreducible polynomials over composite Galois fields and their applications in coding techniques. *Proceedings of the IEE*, Vol. 121, No. 9, pp.935–939, Sep. 1974.

[62] D.H. Green and I.S. Taylor. Modular representation of multiple-valued logic systems. *IEE Proceedings*, Vol. 121, No. 6, pp.409–418, 1974.

[63] R. Hammons and P.V. Kumar. On recent 4-phase sequence design. In *Proceedings of the 2nd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 219–225, Yokohama, Japan, Nov. 29–Dec. 2 1992.

[64] R.C. Heimiller. Phase shift pulse codes with good periodic correlation properties. *IRE Transactions on Information Theory*, pp.254–257, Oct. 1961.

[65] T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Mathematics*, Vol. 16, pp.209–232, 1976.

[66] F. Hemmati and D.L. Schilling. Upper bounds on the partial correlation of PN sequences. *IEEE Transactions on Communications*, Vol. 31, No. 7, pp.917–922, Jul. 1983.

[67] J.M. Holtzman. A simple, accurate method to calculate spread-spectrum multiple-access error probabilities. *IEEE Transactions on Communications*, Vol. 40, No. 3, pp.461–464, Mar. 1992.

[68] R.T. Hsu and J.S. Lehnert. A characterization of multiple-access interference in generalized quadriphase spread-spectrum communications. In *Proceedings of the Tactical Communications Conference*, 1, pp.155–163. IEEE, Apr. 1990.

[69] R.T. Hsu and J.S. Lehnert. Continuous phase-coded direct-sequence spread-spectrum multiple-access communications. In *Phoenix Conference on Computers and Communications*, pp.441–447, 1991.

[70] R.T. Hsu and J.S. Lehnert. A characterization of multiple-access interference in generalized quadriphase spread-spectrum communications. *IEEE Transactions on Communications*, Vol. 42, No. 2/3/4, Part III, pp.2001–2010, Feb./Mar./Apr. 1994.

[71] L. Hu. Distributed code assignments for CDMA packet radio networks. *IEEE/ACM Transactions on Networking*, Vol. 1, No. 6, pp.668–677, Dec. 1993.

[72] J.Y. Hui. Throughput analysis for code division multiple accessing of the spread spectrum channel. *IEEE Journal on Selected Areas in Communications*, Vol. 2, No. 4, pp.482–486, Jul. 1984.

[73] K.W. Hung and T.S. Yum. Efficient spreading code assignment algorithm for packet radio networks. *Electronics Letters*, Vol. 28, No. 23, pp.2193–2195, Nov. 1992.

[74] K. Imamura, S. Uehara, and T. Moriuchi. GF(q) sequences of period q^{n-1} with maximum linear complexity and maximum order complexities for minimum changes of m-sequences. In *Proceedings of the IEEE International Symposium on Information Theory*, p. 366, Trondheim, Norway, Jun. 27–Jul. 1 1994.

[75] A. Jirattitichareon and T. O'Farrell. Analysis of DS/SSMA for indoor radio communication in a log-normal fading channel. *Electronics Letters*, Vol.29, No. 13, pp.1204–1206, Jun. 1993.

[76] P. Jung, P.W. Baier, and A. Steil. Advantages of CDMA and spread-spectrum techniques over FDMA and TDMA in cellular mobile radio applications. *IEEE Transactions on Vehicular Technology*, Vol. 42, No. 3, pp.357–364, Aug. 1993.

[77] K.H.A. Kärkkäinen. Mean-square cross-correlation as a performance measure for spreading code families. In *Proceedings of the 2nd IEEE International Symposium*

on Spread Spectrum Techniques and Applications, pp. 147–150, Yokohama, Japan, Nov. 29–Dec. 2 1992.

[78] K.H.A. Kärkkäinen. Meaning of maximum and mean-square crosscorrelation as a performance measure for CDMA code families and their influence on system capacity. *IEICE Transactions on Communications: Special Issue on Spread Spectrum Techniques and Applications*, Vol. E76-B, No. 8, pp. 848–854, Aug. 1993.

[79] K.H.A. Kärkkäinen, M.J. Laukkanen, and H.K. Tarnanen. Performance of an asynchronous DS-CDMA system with long and short spreading codes - a simulation study. In *Proceedings of the IEEE Military Communications Conference*, pp. 780–784, Fort Monmouth, New Jersey, Oct. 2–5 1994.

[80] K.H.A. Kärkkäinen and P.A. Leppänen. Comparison of the performance of some linear spreading code families for asynchronous DS/SSMA systems. In *Proceedings of the IEEE Military Communications Conference*, pp.34.2.1–34.2.7, McLean, Virginia, Nov. 4–7 1991.

[81] M. Kavehrad and B. Ramamurthi. Direct-sequence spread spectrum with DPSK modulation and diversity for indoor wireless communications. *IEEE Transactions on Communications*, Vol. 35, No. 2, pp.224–236, Feb. 1987.

[82] E.L. Key. An analysis of the structure and complexity of nonlinear binary sequence generators. *IEEE Transactions on Information Theory*, Vol. 22, No. 6, pp.732–736, Nov. 1976.

[83] D.I. Kim and R.A. Scholtz. A random spreading code assignment scheme for centralized spread-spectrum packet radio networks. In *Proceedings of the IEEE Military Communications Conference*, pp.6.2.1–6.2.5, McLean, Virginia, Nov. 4–7 1991.

[84] T. Kirimoto and Y. Oh-Hashi. Orthogonal periodic sequences derived from m-sequences on GF(q). In *Proceedings of the IEEE Military Communications Conference*, pp.34.1.1–34.1.5, McLean, Virginia, Nov. 4–7 1991.

[85] T. Kirimoto and Y. Oh-Hashi. Orthogonal periodic sequences derived from m-sequences on GF(q). *IEEE Transactions on Information Theory*, Vol. 40, No. 2, pp.526–532, Mar. 1994.

[86] F. Knebelkamp, B. Eylert, W. Schütters, M. Chang, and K. Gilhousen. Field test of a CDMA system. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 1–5, Stockholm, Sweden, Jun. 7–10 1994.

[87] D.E. Knuth. *The Art of Computer Programming: Volume 2/ Seminumerical Algorithms*. Addison-Wesley, 1969.

[88] J.J. Komo and M.S. Lam. Primitive polynomials and m-sequences over GF(q^m). *IEEE Transactions on Information Theory*, Vol. 39, Nos. 2, pp.643–647, 1993.

[89] C. Kościelny. A cryptographic procedure using latin square spurious Galois fields. In *RELCOMEX'89, Performance evaluation, reliability and exploitation of computer systems*, pp.383–387, Ksiaz Castle, Poland, Sep. 1989.

[90] C. Kościelny. Spurious Galois fields. In *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pp.416–418, Jun. 1989.

[91] C. Kościelny. Spurious Galois fields. *Information and Computation*, To be published, 1994.

[92] C. Kościelny and W. Mochnacki. Cryptographic keys for improving the reliability of ciphers. *Computer Communications*, Vol. 14, No. 9, pp.557–561, 1991.

[93] R. Krenz, F. Muratore, and G. Romano. Channel estimation for a DS-CDMA mobile radio system with a coherent reception. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 724–728, Stockholm, Sweden, Jun. 7–10 1994.

[94] E. Kreyszig. *Advanced Engineering Mathematics, Fifth Edition*. John Wiley and Sons, 1983.

[95] S.M. Krone and D.V. Sarwate. Quadriphase sequences for spread-spectrum multiple-access communication. *IEEE Transactions on Information Theory*, Vol. 30, No. 3, pp.520–529, May 1984.

[96] P.V. Kumar, T. Helleseth, A.R. Calderbank, and A.R. Hammons Jr. Large families of quaternary sequences with low correlation. In *Proceedings of the IEEE International Symposium on Information Theory*, p. 71, Trondheim, Norway, Jun. 27–Jul. 1 1994.

[97] P.V. Kumar and C.M. Liu. On lower bounds to the maximum correlation of complex roots-of-unity sequences. *IEEE Transactions on Information Theory*, Vol. 36, No. 3, pp.633–640, May 1990.

[98] P.V. Kumar and O. Moreno. Prime-phase sequences with periodic correlation properties better than binary sequences. *IEEE Transactions on Information Theory*, Vol. 37, No. 3, pp.603–616, May 1991.

[99] D. Laforgia, A.Luvison, and V.Zingarelli. Bit error rate evaluation for spread-spectrum multiple-access systems. *IEEE Transactions on Communications*, Vol. 32, No. 6, pp.660–669, Jun. 1984.

[100] A.W. Lam and F.M. Özlütürk. Performance bounds for direct-sequence spread-spectrum communications with complex signature sequences. In *Phoenix Conference on Computers and Communications*, pp.408–414, Mar. 1991.

[101] A.W. Lam and F.M. Özlütürk. Performance bounds for DS/SSMA communications with complex signature sequences. *IEEE Transactions on Communications*, Vol. 40, No. 10, pp.1607–1614, Oct. 1992.

[102] A.W. Lam, F.M. Özlütürk, and S. Tantaratana. M-ary DS/SSMA communications with complex signature sequences. In *Proc. of Conf. on Information, Sciences, and Systems, John Hopkins Univ.*, Mar. 1991.

[103] M.S. Lam. *Generation of m-sequences and Gold codes over GF(q).* PhD thesis, Dep. Elec. Comput. Eng., Clemson University, Clemson, SC, Dec. 1988.

[104] W.C.Y. Lee. Overview of cellular CDMA. *IEEE Transactions on Vehicular Technology*, Vol. 40, No. 2, pp.291–301, May 1991.

[105] Y.H. Lee and S. Tantaratana. Sequential acquisition of PN sequences for DS/SS communications: Design and performance. *IEEE Journal on Selected Areas in Communications*, Vol. 10, No. 4, pp.750–761, May 1992.

[106] J.S. Lehnert. An efficient technique for evaluating direct-sequence spread-spectrum multiple-access communications. *IEEE Transactions on Communications*, Vol.37, No. 8, pp.851–858, Aug. 1989.

[107] J.S. Lehnert. Serial MSK spread-spectrum multiple-access communications. *IEEE Transactions on Communications*, Vol. 40, No. 6, pp.119–1127, Jun. 1992.

[108] J.S. Lehnert and M.B. Pursley. Error probabilities for binary direct-sequence spread-spectrum communications with random signature sequences. *IEEE Transactions on Communications*, Vol. 35, No. 1, pp.87–98, Jan. 1987.

[109] V.L. Levenshtein. Lower bounds on the cross-correlation for codes of a given size. In *Proceedings of the IEEE International Symposium on Information Theory*, p. 72, Trondheim, Norway, Jun. 27–Jul. 1 1994.

[110] J.H. Lindholm. An analysis of pseudo-randomness properties of subsequences of long m-sequences. *IEEE Transactions on Information Theory*, Vol. 14, No. 4, pp.569–576, Jul. 1968.

[111] S.C. Liu and J.J. Komo. Nonbinary Kasami sequences over GF(p). *IEEE Transactions on Information Theory*, Vol. 38, No. 4, pp.1409–1412, Jul. 1992.

[112] H.D. Lüke. Families of polyphase sequences with near-optimal two-valued auto- and crosscorrelation functions. *Electronics Letters*, Vol. 28, No. 1, pp.1–3, Jan. 1992.

[113] R.S. Lunayach. Performance of direct sequence spread-spectrum system with long period and short period code sequences. *IEEE Transactions on Communications*, Vol. 31, No. 3, pp.412–419, Mar. 1983.

[114] F.J. MacWilliams and N.J.A. Sloane. Pseudo-random sequences and arrays. *Proceedings of the IEEE*, Vol. 64, No. 12, pp.1715–1729, Dec. 1976.

[115] D.T. Magill, F.D. Natali, and G.P. Edwards. Spread-spectrum technology for commercial applications. *Proceedings of the IEEE*, Vol. 82, No. 4, pp.572–584, Apr. 1994.

[116] J.L. Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, Vol. 15, No. 1, pp.122–127, Jan. 1969.

[117] J.L. Massey and J.J. Uhran Jr. Sub-baud coding. In *Proceedings of the 13th Allerton conference on Circuit and System Theory*, p. 539–547, Oct. 1975.

[118] S. Matsufuji and K. Imamura. Real-valued Bent function and its application to the design of balanced quadriphase sequences with optimal correlation properties. In G. Goos and J. Hartmanis, editors, *8th International Conference, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Tokyo Japan, Edited by S. Sakata. Lecture Notes in Computer Science No. 508*, pp.113–121. Springer-Verlag, 1990.

[119] J.E. Mazo. Some theorectical observations on spread-spectrum communications. *The Bell System Technical Journal*, Vol. 58, No. 9, pp.2013–2023, Nov. 1979.

[120] D.A. McFarlane and M.D. Allkins. Validation of advanced CDMA concepts for UMTS and FPLMTS. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 36–39, Stockholm, Sweden, Jun. 7–10 1994.

[121] J. Millott and T. Guy. Australian CDMA trials. In *IEEE International Conference on Universal Wireless Access*, pp. 17a–17e, Melbourne, Australia, Jul. 4–6 1994.

[122] L.J. Millott and A.J. Guy. CDMA cellular radio trials. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 669–672, Stockholm, Sweden, Jun. 7–10 1994.

[123] L.B. Milstein, D.L. Schilling, R.L. Pickholtz, V. Erceg, M. Kullback, E.G. Kanterakis, D.S. Fishman, W.H. Biederman, and D.C. Salerno. On the feasibility of a CDMA overlay for personal communications networks. *IEEE Journal on Selected Areas in Communications*, Vol. 10, No. 4, pp.655–668, May 1992.

[124] L.B. Milstein and J. Wang. Interference suppression for CDMA overlays of narrowband waveforms. In *Proceedings of the 3rd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 61–68, Oulu, Finland, Jul. 4–6 1994.

[125] W. Mochnacki. An application of periodic sequences over SGF(q) in cryptography. In *RELCOMEX'89, Performance evaluation, reliability and exploitation of computer systems*, pp.389–396, Ksiaz Castle, Poland, Sep. 1989.

[126] R.K. Morrow Jr. and J.S. Lehnert. Bit-to-bit error dependence in slotted DS/SSMA packet systems with random signature sequences. *IEEE Transactions on Communications*, Vol. 37, No. 10, pp.1052–1061, Oct. 1989.

[127] W.H. Mow. Best quadriphase codes up to length 24. *Electronics Letters*, Vol. 29, No. 10, pp.923–925, May 1993.

[128] W.H. Mow. On the bounds on odd correlation of sequences. *IEEE Transactions on Information Theory*, Vol. 40, No. 3, pp. 954–955, May 1994.

[129] R.S. Mowbray, R.D. Pringle, and P.M. Grant. Increased CDMA system capacity through adaptive cochannel interference regeneration and cancellation. *IEE Proceedings*, Vol. 139, Part I, No. 5, pp.515–524, Oct. 1992.

[130] N. Nazari and R.E. Ziemer. Computationally efficient bounds for the performance of direct-sequence spread-spectrum multiple-access communications systems in jamming environments. *IEEE Transactions on Communications*, Vol. 36, No. 5, pp.577–587, May 1988.

[131] P. Newson and M.R. Heath. The capacity of a spread spectrum CDMA system for cellular mobile radio with consideration of system imperfections. *IEEE Journal on Selected Areas in Communications*, Vol. 12, No. 4, pp.673–684, May 1994.

[132] J.S. No and P.V. Kumar. A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span. *IEEE Transactions on Information Theory*, Vol. 35, No. 2, pp.371–379, Mar. 1989.

[133] T. Novosad. A new family of quadriphase sequences for CDMA. *IEEE Transactions on Information Theory*, Vol. 39, Nos. 3, pp.1083–1085, 1993.

[134] T. O'Farrell. New signature code sequence design techniques for CDMA systems. *Electronics Letters*, Vol. 27, No. 4, pp.371–373, Feb. 1991.

[135] L. Ott. *An Introduction to Statistical Methods and Data Analysis*. Duxbury Press, 1977.

[136] F.M. Özlütürk and A.W. Lam. DS/SSMA communications with nonbinary polyphase signature sequences. In *Proc. of Conf. on Information, Sciences, and Systems, Princeton Univ.*, pp.68–73, Mar. 1990.

[137] F.M. Özlütürk and A.W. Lam. Probability of bit error for DS/SSMA systems with MPSK signaling and complex signature sequences. In *Proceedings of the IEEE Military Communications Conference*, pp.35.5.1–35.5.5, Oct. 1992.

[138] F.M. Özlütürk, S. Tantaratana, and A.W. Lam. Performance bounds for ds/ssma systems with binary noncoherent signalling schemes. In *Proceedings of the IEEE Military Communications Conference*, Boston, Massachusetts, Oct. 11–14 1993.

[139] R. Padovani, B. Butler, and R. Boesel. CDMA digital cellular: Field test results. In *Proceedings of the 44th IEEE Vehicular Technology Conference*, pp. 11–15, Stockholm, Sweden, Jun. 7–10 1994.

[140] E.A. Palo. Application of digital signal processing in spread spectrum systems. In *Proceedings of the 3rd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 146–151, Oulu, Finland, Jul. 4–6 1994.

[141] A. Papoulis. *Probability, Random Variables, and Stochastic Processes, Third Edition*. McGraw-Hill, 1991.

[142] W.J. Park and J.J. Komo. The autocorrelation of m-sequences over nonprime finite fields. *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 24, No. 4, pp.459–461, Jul. 1988.

[143] W.J. Park and J.J. Komo. Relationships between m-sequences over GF(q) and GF(q^m). *IEEE Transactions on Information Theory*, Vol. 35, No. 1, pp.183–186, Jan. 1989.

[144] W.J. Park Jr. *An investigation of maximum length linear recursive sequences over finite fields.* PhD thesis, Dep. Elec. Comput. Eng., Clemson University, Clemson, SC, May 1986.

[145] R.L. Pickholtz, L.B. Milstein, and D.L. Schilling. Spread spectrum for mobile communications. *IEEE Transactions on Vehicular Technology*, Vol. 40, No. 2, pp.313–321, May 1991.

[146] R.L. Pickholtz, D.L. Schilling, and L.B. Milstein. Theory of spread-spectrum communications – A tutorial. *IEEE Transactions on Communications*, Vol. 30, No. 5, pp.855–884, May 1982.

[147] A. Polydoros and S. Glisic. Code synchronization: A review of principles and techniques. In *Proceedings of the 3rd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 115–137, Oulu, Finland, Jul. 4–6 1994.

[148] B.M. Popovic. Generalized chirp-like polyphase sequences with optimum correlation problems. *IEEE Transactions on Information Theory*, Vol. 38, No. 4, pp.1406–1409, Jul. 1992.

[149] W.H. Press, B.P. Flannery, S.A. Teukolsky, and W.T. Vetterling. *Numerical Recipes in Pascal: The Art of Scientific Computing.* Cambridge-University Press, 1990.

[150] M.B. Pursley. Performance evaluation for phase-coded spread-spectrum multiple-access communication - Part I: System analysis. *IEEE Transactions on Communications*, Vol. 25, No. 8, pp.795–799, Aug. 1977.

[151] M.B. Pursley. On the mean-square partial correlation of periodic sequences. In *Infomation Science and Systems Conference, John Hopkins University, Maryland, USA*, pp.377–379, Mar. 1979.

[152] M.B. Pursley. Spread-spectrum multiple-access communications. In G. Longo, editor, *CISM Courses and lectures No. 265; Multi-User Communication Systems*, pp.139–199. Springer-Verlag, 1981.

[153] M.B. Pursley. The role of spread spectrum in packet radio networks. *Proceedings of the IEEE*, Vol. 75, No. 1, pp.116–134, Jan. 1987.

[154] M.B. Pursley and F.D. Garber. Quadriphase spread-spectrum multiple-access communications. In *IEEE International Conference on Communications ICC78*, Vol. 1, pp.7.3.1–7.3.5, Jun. 1978.

[155] M.B. Pursley, F.D. Garber, and J.S. Lehnert. Analysis of generalized quadriphase spread-spectrum communications. In *IEEE International Conference on Communications ICC80*, Vol. 1, pp.15.3.1–15.3.6, 1980.

[156] M.B. Pursley and H.F.A. Roefs. Numerical evaluation of correlation parameters of binary shift-register sequences. *IEEE Transactions on Communications*, Vol. 27, No. 10, pp.1597–1604, Oct. 1979.

[157] M.B. Pursley and D.V. Sarwate. Evaluation of correlation parameters for periodic sequences. *IEEE Transactions on Information Theory*, pp.508–513, Jul. 1977.

[158] M.B. Pursley and D.V. Sarwate. Performance evaluation for phase-coded spread-spectrum multiple-access communication - Part II: Code sequence analysis. *IEEE Transactions on Communications*, Vol. 25, No. 8, pp.800–803, Aug. 1977.

[159] M.B. Pursley, D.V. Sarwate, and W.E. Stark. Error probability for direct-sequence spread-spectrum multiple-access communications – Part I: Upper and lower bounds. *IEEE Transactions on Communications*, Vol. 30, No. 5, pp.975–984, May 1982.

[160] Qualcomm. *An Overview of the Application of Code Division Multiple Access (CDMA) to Digital Cellular Systems and Personal Cellular Networks*, May 21 1992. An updated version of the report submitted to the TIA TR45.5 subcommittee on March 28, 1992.

[161] D.P. Rogers. The Dual Problem of pseudorandom code generation for quadriphase spread-spectrum multiple-access. *Australian Telecommunications Research Journal*, Vol. 27, No. 1, pp.19–33, May 1993.

[162] D.P. Rogers and B.R. Davis. Code properties: Influences on the performance of a quaternary CDMA system. In *3rd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 494–499, Oulu, Finland, Jul. 4–6 1994.

[163] D.P. Rogers and B.R. Davis. Correlation features that influence the performance of a Q-CDMA system. In *IEEE International Conference on Universal Wireless Access*, pp. 53–57, Melbourne, Australia, Apr. 18–19 1994.

[164] C. Ronse. *Feedback Shift Registers*. Number 169 in Lecture Notes in Computer Science. Springer-Verlag, 1984.

[165] H.E. Rowe. Bounds on the number of signals with restricted cross correlation. *IEEE Transactions on Communications*, Vol. 30, No. 5, pp.966–974, May 1982.

[166] R.A. Rueppel. Linear complexity and random sequences. In G. Goos and J. Hartmanis, editors, *Advances in Cryptology - Eurocrypt'85, Lecture Notes in Computer Science No. 219*, pp.167–188. Springer-Verlag, 1986.

[167] J.S. Sadowsky and R.K. Bahr. Direct-sequence spread-spectrum multiple-access communications with random signature sequences: A large deviations analysis. *IEEE Transactions on Information Theory*, Vol. 37, No. 3, pp.514–527, May 1991.

[168] D.V. Sarwate. New correlation identities for periodic sequences. *Electronics Letters*, Vol. 13, No. 2, pp.48–49, Jan. 1977.

[169] D.V. Sarwate. Bounds on crosscorrelation and autocorrelation of sequences. *IEEE Transactions on Information Theory*, Vol. 25, No. 6, pp.720–724, Nov. 1979.

[170] D.V. Sarwate. Mean-square correlation of shift-register sequences. *IEE Proceedings*, Vol. 131, Part F, No. 2, pp.101–106, Apr. 1984.

[171] D.V. Sarwate and M.B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *Proceedings of the IEEE*, Vol. 68, No. 5, pp.593–619, May 1980.

[172] D.V. Sarwate, M.B. Pursley, and T.U. Başar. Partial correlation effects in direct-sequence spread-spectrum multiple-access communication systems. *IEEE Transactions on Communications*, Vol. 32, No. 5, pp.567–573, May 1984.

[173] R.A. Scholtz. The spread spectrum concept. *IEEE Transactions on Communications*, Vol.25, No. 8, pp.748–755, Aug. 1977.

[174] R.A. Scholtz. New technology and radio regulation. In *Proceedings of the 3rd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 4–13, Oulu, Finland, Jul. 4–6 1994.

[175] R.A. Scholtz and L.R. Welch. Group characters: Sequences with good correlation properties. *IEEE Transactions on Information Theory*, Vol. 24, No. 5, pp.537–545, Sep. 1978.

[176] H.D. Schotten and B. Liesenfeld. Linear families of code-sequences with optimum corelation properties. In *Proceedings of the IEEE International Symposium on Information Theory*, p. 281, Trondheim, Norway, Jun. 27–Jul. 1 1994.

[177] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, Vol. 27, pp.623–656, 1948.

[178] V.M. Sidelnikov. On mutual correlation of sequences. *Soviet Mathematics Doklady*, Vol. 12, No. 1, pp.197–201, 1971.

[179] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt. *Spread Spectrum Communications. Volumes I, II, III.* Computer Science Press, 1985.

[180] P. Solé. A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties. In G. Goos and J. Hartmanis, editors, *Coding Theory and Applications, 3rd International Colloquim, Toulon France, Edited by G. Cohen and J. Wolfman. Lecture Notes in Computer Science No. 388*, pp.193–201. Springer-Verlag, 1988.

[181] R. Steele. The evolution of personal communications. *IEEE Personal Communications Magazine*, pp.6–11, Second Quarter 1994.

[182] N. Suehiro. Pseudo-polyphase orthogonal sequence sets with good cross-correlation property. In G. Goos and J. Hartmanis, editors, *8th International Conference, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Tokyo Japan, Edited by S. Sakata. Lecture Notes in Computer Science No. 508*, pp.106–112. Springer-Verlag, 1990.

[183] N. Suehiro and M. Hatori. Modulatable orthogonal sequences and their application to SSMA systems. *IEEE Transactions on Information Theory*, Vol. 34, No. 1, pp.93–100, Jan. 1988.

[184] J.W. Taylor Jr. and H.J. Blinchikoff. Quadriphase code - A Radar pulse compression signal with unique characteristics. *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 24, No. 2, pp.156–170, Mar. 1988.

[185] A. Tietäväinen. On the correlation of sequences. In G. Goos and J. Hartmanis, editors, *Algebraic Coding, First French-Soviet Workshop, Paris France, Edited by G. Cohen, S. Litsyn, A.Lobstein, and G. Zemor. Lecture Notes in Computer Science No. 573*, pp.1–4. Springer-Verlag, 1991.

[186] D.J. Torrieri. Performance of direct-sequence systems with long pseudonoise sequences. *IEEE Journal on Selected Areas in Communications*, Vol. 10, No. 4, pp.770–781, May 1992.

[187] D.J. Torrieri. *Principles of Secure Communications, Second Edition.* Artech House, 1992.

[188] R.J. Turyn. Four-phase Barker codes. *IEEE Transactions on Information Theory*, Vol. 20, No. 3, pp.366–371, May 1974.

[189] S. Verdú. Adaptive multiuser detection. In *Proceedings of the 3rd IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 43–50, Oulu, Finland, Jul. 4–6 1994.

[190] A.J. Viterbi. The orthogonal-random waveform dichotomy for digital mobile personal communication. *IEEE Personal Communications Magazine*, pp.18–24, First Quarter 1994.

[191] A.J. Viterbi, R. Padovani, and J-P de Weck. Spread spectrum CDMA system design and comparative testing on two continents. In *Proceedings of the 2nd IEEE International Symposium on Spread Spectrum Techniques and Applications*, p. 1, Yokohama, Japan, Nov. 29–Dec. 2 1992.

[192] A.J. Viterbi, A.M. Viterbi, K.S. Gilhousen, and E. Zehavi. Soft handoff extends CDMA cell coverage and increases reverse link capacity. *IEEE Journal on Selected Areas in Communications*, Vol. 12, No. 8, pp.1281–1288, Oct. 1994.

[193] L.R. Welch. Lower bounds on the maximum cross correlation of signals. *IEEE Transactions on Information Theory*, Vol. 20, No. 3, pp.397–399, May 1974.

[194] G.R. Welti. Quaternary codes for pulsed radar. *IRE Transactions on Information Theory*, Vol. 6, pp.400–408, Jun. 1960.

[195] S. Wolfram. *Mathematica: A System for Doing Mathematics by Computer.* Addison Wesley, 1991.

[196] K.T. Wu. Average error probability for DS-SSMA communications: The Gram-Charlier expansion approach. In *Proceedings nineteenth annual Allerton conference on communication, control, and computing*, pp.237–246, 1981.

[197] K.T. Wu and D.L. Neuhoff. Average error probability for direct sequence spread spectrum multiple access communication systems. In *Proceedings eighteenth annual Allerton conference on communications, control, and computing*, pp.359–368, 1980.

[198] J.H. Yang and Z.D. Dai. Construction of m-ary de Bruijn sequences. In Y. Seberry and Y. Zheng, editors, *Advances in Cryptology - AUSCRYPT'92, Lecture Notes in Computer Science No. 718*, pp.357–363. Springer-Verlag, 1992.

[199] K. Yao. Error probability of asynchronous spread spectrum multiple access communication systems. *IEEE Transactions on Communications*, Vol. 35, No. 8, pp.803–809, Aug. 1977.

[200] N. Zierler. Linear recurring sequences. *Journal of the Society of Industrial Applications of Mathematics*, Vol. 7, p.31, 1959.

Addendum

The author of this thesis has duly noted the comments made by the examiners Professor V. P. Ipatov and Associate Professor E. S. Seumahu. In addition the author thanks them for their careful and thorough examiniation of this thesis, and the worthwhile comments that they made. Based upon those comments the following statements should be considered when reading this thesis.

Ipatov remarked that the following assertion (page 55, paragraph 1), is not correct:
"It is worth considering whether the higher order moments employed in Yao's paper [199], should be employed as merit factors. This has not been done, nor discussed in any prior literature."
Ipatov commented that the Russian researcher L.E. Varakin had written a series of papers in the 1970's on the influence of higher order moments on the PBE. This was detailed in section 4.3 of Varakin's book *Signal Set Theory* (in Russian, Moscow 1978).

Ipatov also noted that the conclusion on page 89, paragraph 3 for the case $\overline{\phi}_c \leq \sqrt{N}$ that it is impossible to estimate a potential number of users is not correct. This is because for $\sqrt{N} < \overline{\phi}_c < \sqrt{2N}$ a more accurate bound than Welch's exists whose inversion gives the necessary upper limit of U. Further information can be found in section 6.1 of the book by Ipatov, *Periodic discrete signals with optimal correlation properties*, (in Russian, Moscow 1992).

In regard to the discussion (pages 102 and 103) on primitive and irreducible polynomials, and in particular Table 4.4, Ipatov rightly pointed out that the six polynomials shown only as irreducible are also primitive. They are the reciprocal (as the paper [14] by Balza et al states), of the six polynomials shown as both irreducible and primitive in Table 4.4. This oversight does not influence the results in this thesis and indeed it explains why no difference was observed between the tests discussed on pages 103 and 104 for polynomials from each set.

In addition Ipatov made two other important observations. Firstly, Ipatov noted that from equation 3.7 under a uniform PDF of θ an overall angle of $\alpha = \theta + \varphi$ also has a uniform PDF. Thus the PDFs of r and φ are sufficient to obtain the PDFs of the interference and there is no need to separately consider the real and imaginary components in the virtual code analysis; the absolute crosscorrelation values can be utilised. Secondly, Ipatov noted that as a consequence of the first point, it is possible to prove, in an analytic way, that a necessary

and sufficient condition for the MSC to be minimal is the Balance property of a code sequence. This is important because it supports the conclusion on page 85 that "... codes which satisfy the Balance property may be expected to perform better than those that do not".