CHANNEL CODING FOR TIME SELECTIVE FADING CHANNELS

By

NICK ANDREW VAN STRALEN, B.Eng., M.Eng..

A Thesis
Submitted to the School of Graduate Studies
in Partial Fulfilment of the Requirements
for the Degree
Doctor of Philosophy

McMaster University

DOCTOR OF PHILOSOPHY (1994) MCMASTER UNIVERSITY
(Electrical & Computer Engineering) Hamilton, Ontario

TITLE: Channel Coding for Time Selective Fading Channels

AUTHOR: Nick Andrew Van Stralen
B.Eng. (Electrical Engineering) McMaster University.
M.Eng. (Electrical Engineering) McMaster University.

SUPERVISOR: Dr. Desmond P. Taylor

NUMBER OF PAGES: xiv, 117

CHANNEL CODING FOR TIME SELECTIVE FADING CHANNELS

Abstract

The purpose of this thesis is to design bandwidth efficient codes for use in a time selective fading channel. A time selective fading channel, the correlated Rayleigh fading channel, is analyzed and criteria for the design of bandwidth efficient codes are presented. These criteria are used to design new codes which are inherently resistant to Rayleigh fading. The new codes are analyzed and a decoding algorithm for the codes is presented. Simulations of the performance of the codes and the decoding algorithm are then presented. Finally, a channel estimator that generates the necessary information for decoding is presented, analyzed, and simulated.

Acknowledgment

I would like to thank my supervisor Dr. Desmond P. Taylor for his help and support in preparing this thesis. His guidance and suggestions during the initial stages of this work were invaluable. His comments and criticisms of the early drafts of this report greatly improved its quality. I would also like to thank the members on my Ph.D. committee for their help in completing this work

Thanks goes to the staff in room 102 and in room 110 for their help with the more mundane problems that inevitably occur with the day to day operations of the Communications Research Laboratory.

I would like to acknowledge the help of my fellow graduate students for their help with computer, research and other technical problems throughout the preparation of this thesis. I would especially like to thank Fergus Ross and Bob Dingman for their enlightening conversation and for their friendship. Andy Ukrainic gave me help with computer and other technical problems many times.

I would like to thank Thérèse for her patience and understanding throughout the course of my work during the past 4 years.

Contents

List of Figures

List of Tables

List of Symbols

$\mathcal{R}(a)$	Real part of a
$\mathcal{I}(a)$	Imaginary part of a
$\hat{a}$	Estimate of a
$\dot{a}$	Time derivative of a
a^*	Complex conjugate of a
$\|a\|$	Magnitude of a
ED$[a, b]$	Euclidean distance between a and b
GF(q)	Galois Field of q elements
$R_{f(x)}[g(x)]$	Remainder of $\frac{g(x)}{f(x)}$
LCM$[f_1(x), f_2(x)]$	Lowest common multiple of arguements

Chapter 1

Introduction

1.1 Bandwidth Efficient Codes for Digital Mobile Radio

In recent years, there has been a trend toward personal communication systems and services. Digital mobile radio is the primary technology that will enable reliable personal communications to become a global reality. However, communicating digital information through a communications channel when the transmitter and receiver are in motion with respect to one another is not trivial. One artifact of this relative motion is multi-path fading. Multi-path fading is a serious channel impairment in the mobile radio environment. The land mobile channel and the satellite mobile channel are two important channels that exhibit multi-path fading. Fading is caused when the antenna on the receiver picks up multi-path or reflections of the transmitted signal. If the receive antenna is in motion the received signal energy will be time varying. Periodically, the received energy drops to a such low level that all communication is impossible.

Transmission of digital information allows one to code the information in such a way so that you can detect and correct corrupted data. This must be done by introducing redundancy in the transmitted signal so that the receiver can detect and remove the effect of the communications channel. The introduction of redundancy

into the communication signal is generally referred to as error control coding. Often this redundancy is accomplished by reducing the overall rate of information transmission through the channel. In the last decade, there has been interest in developing codes that do not decrease the rate of information transmission or increase the required bandwidth [26]. These advanced schemes combine the coding and modulation stages of the transmitter resulting in properties that minimize the effects of channel noise. Only lately has there been an effort to develop advanced coding and modulation schemes for the flat fading channel [23, 7, 6]. The thrust of this effort has been in developing trellis codes that are optimized for use on the fading channel. There has been little work in devising new signaling methods or coding schemes for this channel. Furthermore, there has has been little analysis of the channel characteristics in an effort to devise general guidelines for designing codes in the fading channel. In the AWGN channel, it has been known for years that the minimum free distance of the code when looked at in signal space is the parameter that must be optimized. The understanding of code design for the Rayleigh channel is not as well understood as is for the AWGN channel.

In addition, in code design for the Rayleigh channel, it has often been assumed that the fading is independent from symbol to symbol [7, 23]. In reality, the fading is highly correlated between symbols. Independence can be approximated if the channel symbols are sufficiently interleaved. One would usually prefer that the interleaving be kept small. This is because interleaving introduces a time delay at the transmitter and at the receiver. For voice channels, the delay must be kept below a tight constraint, otherwise the delay will start to interfere with normal conversation. One would prefer that the channel codes for the fading channels require little or no interleaving and also be decoded with very little delay.

Most channel coding schemes to date have tacitly assumed that channel state information is available at the receiver for decoding purposes. If this information is not available, the power of the coding scheme will be lost or severely curtailed. This information will only be available to the receiver if it is tracking the channel to determine the channel state. There will always be some error when estimating the channel state information. The effect of inaccuracies in the channel estimates will

have some effect on the power of the error control coding scheme. These effects have not been evaluated for most coding schemes that are designed for the Rayleigh fading channel. Furthermore, the understanding of how these estimates may be formed is not good and the quality of the channel state Estimator is not known.

In this thesis, the flat fading channel is investigated in an attempt to develop guidelines for designing block coding signaling schemes for this channel model. The guidelines lead directly to a powerful block coding method for signaling through the flat fading channel. The coding scheme is based on a well known class of algebraic codes. A decoding algorithm for this class of block codes is then developed and analyzed. The problem of correlated fading and channel estimation are also addressed. The performance of the block coding signaling scheme is analyzed in the presence of correlated fading and in a finite interleaving environment. Finally a method for channel estimation is introduced. Mean squared estimation error curves for this estimation strategy are presented and results on the performance of the block codes with the presence of the channel estimator are given.

1.2 Status of Work on Codes for Digital Mobile Radio

There has been much work done in the area of analyzing and modeling the multipath communications channel. The physics of why multipath fading occurs is quite well understood. Original work on fading channels was concentrated on determining the statistics of the channel [15] and developing models for these channels [16]. Although communication through the additive white Gaussian noise (AWGN) has been developed mathematically with the concept of signal space [2], the understanding of communication through the fading channel has not been developed to the same extent. A simple analysis of communication through a time selective fading channel has been done for a "fast fading" channel, where the channel introduces a random amplitude and phase that is modeled as complex Gaussian and independent between symbols [29].

Work on understanding the problem of designing codes for use on the multipath fading channel has been done more recently. Divsalar and Simon [7] have developed a method for evaluating the performance of trellis codes when used on the multipath fading channel. Bounds on the error probability of trellis codes through multipath fading channels have also been investigated [6].

There also has been work done recently in developing bandwidth efficient codes for use in the fading channel. The traditional approach to designing codes for fading channel has been to optimize known classes of codes for use on the fading channels [6, 23].

There is essentially nothing in the literature that discusses the effect of imperfect channel estimates on the performance of codes when used in the Rayleigh fading channel. Most of the work assumes that the receiver has perfect knowledge of the channel state. Furthermore, it also assumes that the symbol sequence is sufficiently interleaved so that the fading parameters are essentially independent. These assumptions must be investigated before the true performance of the coding schemes can be evaluated.

The problem of channel estimation has been investigated to some extent. In 1960 Kailath [14] wrote a paper that characterized the fading channel in digital form. This led to the idea of using a pilot tone to estimate the channel for demodulation purposes. There have been no explicit receivers designed for coherent demodulation of amplitude/phase modulated signals. There are realizations of receivers for demodulating a differential phase shift keyed (DPSK) signal in the correlated Rayleigh channel [28, 5]. The receivers are not designed for explicit channel estimation, but in performing maximum likelihood demodulation, the channel needs to be tracked or estimated.

1.3 Scope of Thesis

In chapter 2, the necessary background for the understanding and development of this thesis is reviewed. First there will be an introduction into the causes and problems associated with fading channels. Then the concept of signal space is introduced. Signal

space theory gives the footing on which communication in the Gaussian channel can be evaluated. It also provides insight into the effect fading introduces on the received communication signal. In section 2.3 we give a brief review of coding for the purposes of forward error correction. The difference between block and convolutional codes will be discussed. Also, bandwidth efficient coding will be introduced. Bandwidth efficient codes have been the focus of most of the error control coding research in the past decade. Finally, Reed-Solomon codes will be discussed in greater depth.

Chapter 3 will start with an investigation into signaling on the Rayleigh fading channel. This will lead to criteria for evaluating codes that are to be used on this channel. Reed-Solomon signal space codes are then introduced. Reed-Solomon codes are used for the base codes because they naturally maximize one of the performance criteria for evaluating codes on the Rayleigh fading channel. This follows directly from their property of being maximum distance separable. Section 3.3 will give some examples of different Reed-Solomon signal space codes and discuss their properties. In the final section of chapter 3, we will discuss the possibility of extending the idea of Reed-Solomon signal space codes to signal space codes based on Bose-Chauduri-Hocquenghem codes. This extends the class of Reed-Solomon signal space codes to include many interesting codes for signaling on the Rayleigh fading channel.

Theoretical performance of the Reed-Solomon signal space codes is discussed in chapter 4. First, we determine the pairwise error probability of the codes. Then, in section 4.4, we develop a useful upper bound on the error probability of these codes. In the next section, we introduce a decoding algorithm for decoding the Reed-Solomon signal space codes. The algorithm is not a maximum likelihood decoder, but can decode the Reed-Solomon signal space codes with performance approaching that of a maximum likelihood decoder. In the last sections of chapter 4, we present simulation results for the codes. The simulation results include both the results with simulated interleaving on a correlated channel and infinite interleaving. The goal of these simulations is primarily to test the power of the Reed-Solomon signal space codes used on a Rayleigh fading channel. Also, there are simulations results presented directed at testing the decoding algorithm. We vary some of the parameters of the decoding algorithm and compare these results to a maximum likelihood decoder.

Chapter 5 is primarily concerned with the problem of estimating the channel state information that is needed for the decoder. In section 5.1, an algorithm for channel estimation is presented. The performance of the channel estimator will then be discussed in the following section. Finally, simulation results of joint channel estimation and Reed-Solomon decoding will be presented.

The final chapter of this thesis summarizes the main results of the thesis and discusses some of the open issues that might be researched further.

Chapter 2

Review of Necessary Principles

This chapter reviews the basic principles required for the understanding of the theoretical development of this work. The first section discusses the channel model that is used throughout this work. The theoretical development of the channel model is followed and any assumptions made are stated. The next section introduces signal theory. Signal theory is a viewpoint of the communications problem that provides insight into the causes of unreliable communication. Next, in section 2.3 channel coding is introduced. The differences between block and convolutional codes are stated. Also the difference between algebraic codes and signal space codes is discussed. Finally, in the last section of this chapter, the Reed-Solomon codes and Bose-Chaudhuri-Hoquenghem classes of algebraic codes are discussed in more detail.

2.1 Communication in a Mobile Channel

The fading in a communications channel is caused by the receiver antenna simultaneously receiving multiple signals from the same source via different paths. The channel can be envisioned as containing many reflecting objects or particles. These objects could be buildings, automobiles or ionized particles in the atmosphere. Figure 2.1 is a pictorial representation of a radio communications channel.

The following analysis closely follows that of [5]. When the transmission rate is relatively low, then the propagation time through the transmission medium is much

less than the duration of one symbol. Therefore, on the time scale of the symbols, the various reflections will arrive at the receiver almost simultaneously. However, if the carrier frequency is much higher than the symbol rate, then the different paths may have a different relative phase with respect to one another. The effect of this phase difference will be either constructive or destructive interference. In general, each path will arrive at the receiver with a phase that is statistically independent to that of all other paths.

Each path will also introduce a delay $T_i(t)$ distributed around some nominal propagation delay. The nominal propagation delay can be assumed to be zero without loss of generality. The time delay introduced by each path will itself be a function of time because of the motion of the particles. Since the scatterers do not move significantly during one symbol period, the time delay introduced resulting from a scatterer may by linearly approximated as

$$T_i(t) = \tau_i + \dot{\tau}_i t \tag{2.1}$$

where τ_i is the initial time delay and $\dot{\tau}_i$ is the rate of change of the time delay. The rate of change of the time delay is proportional to the radial velocity of the scatterer with respect to the receiver.

The transmitted signal itself is a complex band limited signal modulated on a sinusoidal carrier. If the complex baseband signal is $b(t)$ then the transmitted signal is

$$s(t) = \Re[b(t)e^{j\omega_o t}] \tag{2.2}$$

where ω_o is the carrier frequency. Using the approximation of equation 2.1, the received signal due to scatterer i is then

$$r_i(t) = \rho_i b(t - \tau - \dot{\tau}_i t)e^{j\omega_o(t-\tau-\dot{\tau}_i t)} \tag{2.3}$$

where ρ_i is the received signal strength due to scatterer i. It was assumed that the delay introduced due to the i^{th} scatterer is small compared to the symbol period. Therefore, the delayed baseband signal $b(t-\tau_i-\dot{\tau}_i)$ will not change significantly from $b(t)$ and the envelope delay will be ignored. If we define the Doppler shift due to the i^{th} scatterer to be

$$\omega_i = \omega\dot{\tau}_i \tag{2.4}$$

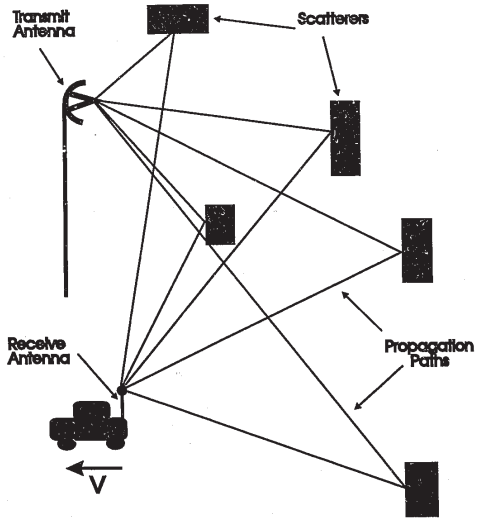

Figure 2.1: A Typical Mobile Communications Channel

then the received signal due to the i^{th} scatterer is well approximated by

$$r_i(t) = \rho_i b(t) e^{-j\omega_o \tau_i} e^{j(\omega_o - \omega_i)t} \tag{2.5}$$

After demodulation, the received signal due to the i^{th} scatterer is,

$$r_i(t) = b(t)\rho_i e^{-j\omega_o \tau_i} e^{-j\omega_i t} \tag{2.6}$$

Letting $\tilde{\rho}_i = \rho_i e^{-j\omega_o \tau_i}$, $\tilde{\rho}_i$ itself is a complex random variable. The received signal due to the i^{th} scatterer can be viewed as the desired baseband signal modulated by a complex sinusoid with unknown frequency ω_i and unknown amplitude $\tilde{\rho}_i$.

There is a near infinite number of paths to the receiver in a scattering channel. The received signal will be the sum of the individual components from all of the different paths. Summing equation 2.6 over all possible paths results in,

$$\begin{aligned} r(t) &= \sum_i b(t)\tilde{\rho}_i e^{-j\omega_i t} && (2.7) \\ &= b(t)\sum_i \tilde{\rho}_i e^{-j\omega_i t} && (2.8) \end{aligned}$$

The received baseband signal is the transmitted baseband signal modulated by a sum of complex sinusoids of unknown complex amplitude and frequency. For each specific frequency, ω_k there will be many scatterers at that particular frequency. If we sum the contributions only from that frequency we get,

$$\begin{aligned} r_k(t) &= b(t) \sum_{i|\omega_i = \omega_k} \tilde{\rho}_i e^{-j\omega_i t} && (2.9) \\ &= b(t) e^{-j\omega_k t} \sum_{i|\omega_i = \omega_k} \tilde{\rho}_i && (2.10) \end{aligned}$$

Although the distribution of the $\tilde{\rho}_i$ is unknown, by the central limit theorem [29], the distribution of their sum will approach Gaussian. If we let,

$$\alpha_k = \sum_{i|\omega_i = \omega_k} \tilde{\rho}_i \tag{2.11}$$

then equation 2.8 can be rewritten as,

$$r(t) = b(t)\sum_k \alpha_k e^{-j\omega_k t} \tag{2.12}$$

where the sum is now over all the possible different frequencies, ω_k. The distribution of the α_k's is estimated as Gaussian with zero mean. If we define a fading process, $a(t)$, to be,

$$a(t) \triangleq \sum_k \alpha_k e^{-j\omega_k t} \tag{2.13}$$

then the distribution of $a(t)$ will also be Gaussian and zero mean since it is itself a sum of Gaussianly distributed random variables with zero mean.

The autocorrelation of the function $a(t)$ is given by

$$\begin{aligned} R_a(t,\tau) &= \overline{a(t)a^*(\tau)} && (2.14) \\ &= \overline{\sum_k \alpha_k e^{-j\omega_k t} \sum_l \alpha_l^* e^{j\omega_l \tau}} && (2.15) \\ &= \overline{\sum_k \sum_l \alpha_k \alpha_l^* e^{-j(\omega_k t - \omega_l \tau)}} && (2.16) \\ &= \sum_k |\alpha_k|^2 e^{-j\omega_k (t-\tau)} && (2.17) \end{aligned}$$

where in going from 2.16 to 2.17 we have assumed that the scatterers are independent and therefore the α_k's are independent. It can be observed that the process, $a(t)$, is stationary and hence its autocorrelation function is the Fourier transform of the power spectral density of the $a(t)$.

The received baseband signal may thus be described as being the baseband transmitted signal modulated by a stationary zero mean complex Gaussian process, $a(t)$. The channel model that we use in this thesis is shown in figure 2.2. The noise is assumed to be generated at the input into the receiver and is modeled as additive, spectrally flat and Gaussian (AWGN). The autocorrelation function, $R_a(t,\tau)$ or equivalently the power spectral density completely characterizes the fading channel. The width of the power spectral density of the process, $a(t)$, is determined by the largest Doppler shift that is present due to the scatterers. In the digital mobile radio channel, the Doppler shift is usually caused by the motion of the vehicle. For a vehicle with a velocity, v with respect to a given transmitter/receiver, and a carrier wavelength, λ, the maximum Doppler shift is,

$$f_D = \frac{v}{\lambda}\cos(\phi) \tag{2.18}$$

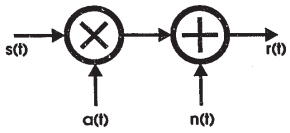

Figure 2.2: Scattering Channel Model

where ϕ is the angle between the velocity vector of the vehicle and the direction vector along the line between the vehicle and the base station.

As an example, for a vehicle traveling with relative velocity of 200km/h and a carrier frequency of 1GHz, $f_D \approx 200$Hz, and assuming that the symbol transmission rate for this channel is 2400 baud, then the fading time bandwidth product of the channel is $BT \approx 0.08$ This is typical for a mobile channel [16]. Figures 2.3 and 2.4 show a typical realization of the magnitude and phase of a fading process, $a(t)$, with a time-bandwidth product of 0.08. These plots were obtained by simulating a fading process on a digital computer. Note that there exist extreme variations in the magnitude of the fading process with quasi-periodic nulls. Extreme nulls occurs with some regularity in this channel and it is at these times when communication is difficult. Note also, that along with these magnitude nulls, there is a possibility of severe phase changes in the fading process. These rapid phase swings make coherent reception of the information bearing signal extremely difficult.

2.2 Signal Theory

A pictorial representation of a communication system is presented in Figure 2.5. The encoder and modulator form the transmitter, while the decoder and demodulator together are the receiver. The channel is any medium in which signals propagate.

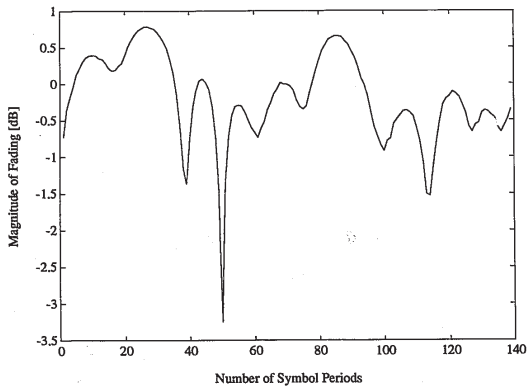

Figure 2.3: Magnitude of a Realization of a Fading Process with Time-Bandwidth Product of 0.08

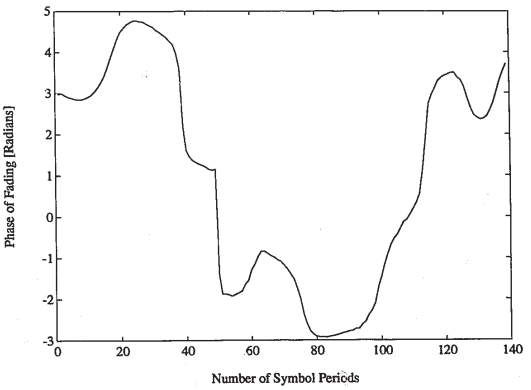

Figure 2.4: Phase of a Realization of a Fading Process with Time-Bandwidth Product of 0.08

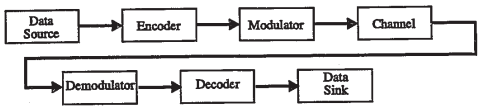

Figure 2.5: A General Communications System

The data source is assumed to generate a stream of independent bits, equally probable to be 1 or 0. It is the job of the transmitter and receiver to communicate the information generated by the data source to the sink. This would not be a problem if the signal arriving at the receiver were identical to that produced at the transmitter. Unfortunately, the channel introduces uncertainties into the signal so that the actual transmitted signal is not known with certainty at the receiver.

The signal out of the transmitter can be expressed as a combination of linearly independent signals. The number of linearly independent signals needed to describe the signal is the dimensionality of the signal [29]. Normally, the signal is transmitted as a sine wave.

$$s(t) = \sqrt{2E}\cos(\omega_o t + \phi) \tag{2.19}$$

Such a signal has two linearly independent components. These basis components are the in-phase and quadrature components.

$$\Phi_I(t) = \sqrt{2}\cos(\omega_o t) \tag{2.20}$$

$$\Phi_Q(t) = \sqrt{2}\sin(\omega_o t) \tag{2.21}$$

Two is the maximum number of dimensions that can be transmitted by a signal of the form of equation 2.19 in a given time period. Higher dimensional signals can be formed by using successive time slots or by using other modulation formats such as frequency shift keying (FSK).

In any event, once the basis of the signal space is found, any signal can be represented. For example, assume the transmitter maps a pair of bits on to one of

the four signals according to the following rule.

$$00 \Rightarrow \sqrt{2E}\cos(\omega_o t + \frac{\pi}{4}) \tag{2.22}$$

$$01 \Rightarrow \sqrt{2E}\cos(\omega_o t + \frac{3\pi}{4}) \tag{2.23}$$

$$10 \Rightarrow \sqrt{2E}\cos(\omega_o t + \frac{5\pi}{4}) \tag{2.24}$$

$$11 \Rightarrow \sqrt{2E}\cos(\omega_o t + \frac{7\pi}{4}) \tag{2.25}$$

The basis of the above set is the linearly independent set of functions 2.20 and 2.21. Each signal can be expressed as a linear combination of the basis set as

$$00 \Rightarrow +\sqrt{\frac{E}{2}}\Phi_I(t) + \sqrt{\frac{E}{2}}\Phi_Q(t) \tag{2.26}$$

$$01 \Rightarrow -\sqrt{\frac{E}{2}}\Phi_I(t) + \sqrt{\frac{E}{2}}\Phi_Q(t) \tag{2.27}$$

$$10 \Rightarrow -\sqrt{\frac{E}{2}}\Phi_I(t) - \sqrt{\frac{E}{2}}\Phi_Q(t) \tag{2.28}$$

$$11 \Rightarrow +\sqrt{\frac{E}{2}}\Phi_I(t) - \sqrt{\frac{E}{2}}\Phi_Q(t) \tag{2.29}$$

This is represented graphically in the signal space of the in-phase and quadrature components in Figure 2.6.

Similarly, the noise generated at the input of the receiver can be represented as a sum of linearly independent components. If we assume that the power spectrum of the noise is white, it would take an infinite set of orthonormal components to completely describe it.

$$n(t) = \sum_{j=1}^{\infty} n_j \Phi_j(t) \tag{2.30}$$

Let the first two basis functions be the same basis functions used to represent the signal. All other basis functions will be orthonormal to these. Then the received signal, $y(t)$, can be represented as a summation of the in-phase, quadrature and other components.

$$y(t) = \Phi_I(t)\,(s_I + n_I) + \Phi_Q(t)\,(s_Q + n_Q) + \sum_{j=3}^{\infty} n_j \Phi_j(t) \tag{2.31}$$

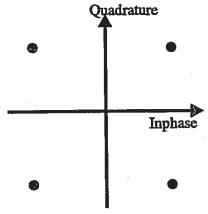

Figure 2.6: Signal Space for 4-PSK

In the above expression, S_I and S_Q denote the signal component in the in-phase and quadrature components respectively. The last term of the above equation contains no information of use in making a decision on $s(t)$. This is called irrelevant information and may be disregarded by the optimum receiver [29].

The receiver must make an estimate of the transmitted data from the received in-phase and quadrature components of the received signal. Again, if we assume AWGN, the in-phase and quadrature components are each perturbed by an additive zero mean, independent, normally distributed noise sample of variance σ^2. For any of the transmitted signals, $s_I + js_Q$, the probability density that the received signal is y is

$$Pr(y|s_I + s_Q) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left(\frac{-\mathrm{ED}^2[y, s_I + js_Q]}{2\sigma^2}\right) \tag{2.32}$$

where ED[•] is the Euclidean distance between the arguments. Since $Pr(y|s_I + js_Q)$ decreases monotonically with increasing Euclidean distance, the optimum receiver in an uncoded environment chooses the signal point, s_k, that is closest to the received signal y. An error is made if the noise introduced is such that the received signal is closer to a point in the signal set other than the actual transmitted signal. An

estimate of the error rate can readily be calculated for an uncoded system. Consider the quadrature phase shift keyed (QPSK) signal set with $-\sqrt{\frac{E}{2}}\Phi_I(t) - \sqrt{\frac{E}{2}}\Phi_Q(t)$ as the actual transmitted signal. An error would be made if the in-phase noise were larger than $\sqrt{\frac{E}{2}}$ or if the quadrature noise were larger than $\sqrt{\frac{E}{2}}$. Thus the probability of symbol error for this transmitted signal is

$$Pr(e) = 2Q\left(\frac{\sqrt{\frac{E}{2}}}{\sigma}\right) - Q^2\left(\frac{\sqrt{\frac{E}{2}}}{\sigma}\right) \tag{2.33}$$

where $Q(\bullet)$ is the Gaussian Q function.

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty \exp\left(\frac{-z^2}{2}\right) dz \tag{2.34}$$

By symmetry, the error rate for the other three points is the same, therefore the overall error rate is also given by equation 2.33. In general, a good high signal to noise ratio approximation to the symbol error rate in any system is

$$Pr(e) = N_{d_{min}} Q\left(\frac{d_{min}}{2\sigma}\right) \tag{2.35}$$

where d_{min} is the smallest pairwise distance between any two signals and $N_{d_{min}}$ is the number of pairs at the minimum distance.

2.3 Channel Coding

To obtain an arbitrarily low error rate, the signal to noise ratio in equation 2.35 would have to be made arbitrarily high. It was for this reason that researchers thought that the random nature of the channel put a limitation on the reliability of communications. Claude Shannon showed that this is not the case. In papers published in the late forties [24, 25], Shannon showed that the random channel limits the rate of communication, not the reliability. As long as the rate of transmission is less than the channel capacity, C, error–free communications can be accomplished. In Gaussian noise, channel capacity is given by

$$C = \frac{1}{2}D\log_2\left(1 + \frac{S}{N}\right) \qquad \frac{\text{bits}}{\text{T}} \tag{2.36}$$

where $\frac{S}{N}$ is the signal to noise power ratio and D is the number of available dimensions per second. The number of dimensions a channel may accommodate for fixed bandwidth and time is approximately [29]

$$D \approx 2.4WT \qquad W, T \text{ large} \tag{2.37}$$

Recently, a capacity estimate was developed for the Rayleigh fading channel [17]. In this paper, it was shown that capacity in the Rayleigh fading channel approaches channel capacity in a Gaussian noise environment when the number of diversity branches becomes large. Diversity can be achieved by a number of different methods. Space diversity, time diversity and frequency diversity three common methods of achieving diversity.

It is the aim of channel coding to convey information at a rate near capacity with minimum effort. After Shannon's results were published there was great interest in the development of coding schemes to meet the limits promised. There was work done in two main areas. One is called block coding and the other is termed convolutional coding.

Block coding essentially encodes a finite-length block of data into a finite-length codeword. Successive blocks are coded independently of one another. The original codes developed within this class of codes are the Hamming codes [10]. Hamming codes are a class of single error correcting codes. Another important class of block codes are the Bose-Chauduri-Hocquenghem codes [4, 11]. These codes are a large class of multiple error correcting codes and play a large role in the understanding of error control codes. Furthermore, efficient and practical decoding algorithms have been devised for these codes. A subclass of these codes, developed by Reed and Solomon [21], found a class of non-binary codes that have the property of being maximum distance separable.

Convolutional codes can be viewed as the output of a system in which the data sequence is convolved with an encoder [27]. Convolutional codes are the most important codes of a larger class of tree codes. Convolutional codes are popular because they can be decoded with a simple algorithm, the Viterbi algorithm [8]. However, the Viterbi algorithm is useful for only the lower complexity codes because

the complexity of the Viterbi algorithm grows exponentially with the number of states in the convolutional code.

A major advance in coding theory occurred with the development of Ungerboeck codes [26]. Ungerboeck described a class of error control codes that did not necessitate the expansion of the required bandwidth of the communications link. This is the case with previously known coding structures. The most important concept that resulted from his work was that the coding and modulation stages of the transmitter could be combined. With the coding and modulation combined, the codes could be designed and analyzed with the concept of signal space being applied to the code and not just at the symbol level. Prior to Ungerboeck's work, codes were designed and analyzed algebraically, with Hamming distance being the foremost criteria. After Ungerboeck's work, there has been much work done in this area. The codes that are based on Ungerboeck's concepts are generally referred to as trellis codes.

There also exist block codes that use the concept of combining the coding and modulation. These codes are often based on sphere packings known as lattices and are referred to as lattice codes. Advanced modulation and coding refers to the bandwidth efficient coding schemes, either trellis codes or lattice codes. Much of the research into coding theory in the last few years has been in the development of these advanced modulation techniques.

2.4 Bose-Chaudhuri-Hocquenghem and Reed-Solomon Codes

A discussion of Reed-Solomon codes would not be complete without an introduction to Bose-Chauduri-Hocquenghem codes. BCH codes are a large class of multiple error correcting codes. BCH codes form a subclass of cyclic codes. Cyclic codes themselves are a subclass of all linear codes obtained by imposing a strong structural requirement on the codes. We begin our discussion of BCH and Reed-Solomon codes with a definition of linear codes. Then we will define cyclic codes and BCH codes. For the development of this theory, the reader is assumed to be familiar with Galois field

theory. Appendix A gives discussion of the necessary theory of Galois fields for the understanding of this thesis. For a more detailed treatment of Galois field theory, the reader is referred to [12].

Definition 2.1 *A linear code is a subspace of* $GF(q)^n$.

By definition 2.1, a linear code is the set of n-tuples such that the sum of any two codewords is another codeword. Also, the product of any codeword by a field element of GF(q) results in a codeword. As a further result of this definition, the all zero n-tuple will also be a codeword. This is because, if $\mathbf{c}$ is a codeword then $-\mathbf{c}$ is also a codeword, and hence $\mathbf{c} + -\mathbf{c}$ is a codeword. Due to the linearity of the code, all codewords have an equivalent arrangement of codewords surrounding them. Hence, if we know the arrangement of the codewords around the all zeros codeword, we then know the arrangement of codewords around all other codewords. By this knowledge, we can determine the minimum distance of the code. To this end, we define the Hamming weight.

Definition 2.2 *The Hamming weight of a codeword is the number of non-zero elements in the codeword.*

If we can identify the minimum weight codeword in the code, then using definition 2.2, we also know the minimum Hamming distance between codewords. The minimum Hamming distance of a linear code is the Hamming weight of the minimum weight codeword in the code.

Definition 2.3 *A linear code over GF(q) is a cyclic code if whenever* $\mathbf{c} = (c_0, c_1, c_2, ..., c_{n-1})$, *then* $\mathbf{c}' = (c_{n-1}, c_0, c_1, ...c_{n-2})$ *is also a codeword.*

The class of cyclic codes is a subset of the linear codes with this cyclic property.

Each codeword in a cyclic code can be represented in an alternative way. The codeword is a vector on $GF(q)$, and can be represented as a polynomial in x of degree equal to or less than $n-1$. Therefore the codeword $\mathbf{c} = (c_0, c_1, c_2, ..., c_{n-1})$ will be represented by $c(x) = c_0 + c_1x + c_2x^2 + ... + c_{n-1}x^{n-1}$. Note that we may add two polynomials corresponding to two codewords and the result will be a polynomial

corresponding to another codeword. The set of all possible polynomials that exist on a vector space on $GF(q)^n$ forms a ring. This ring can be denoted as

$$GF(q)\frac{[x]}{(x^n-1)} \tag{2.38}$$

A cyclic shift of a polynomial can be written as a multiplication within this ring,

$$x \cdot c(x) = R_{x^n-1}[xc(x)] \tag{2.39}$$

where $R_a[b]$ is the remainder of $\frac{a}{b}$. It follows that we may multiply any codeword polynomial by any polynomial in the ring $GF(q)\frac{[x]}{(x^n-1)}$ and the result will be a codeword polynomial.

Suppose we choose a codeword polynomial of minimum degree. Denote this minimum degree by $n-k$. Note that $n-k$ will always be of degree less than or equal to $n-1$. Multiply this minimum order polynomial by a field element such that the term of highest degree has a coefficient of 1. This monic minimum degree codeword polynomial is defined as the generator polynomial, $g(x)$. Then all the codeword polynomials can be found by multiplying $g(x)$ by all polynomials in the ring $GF(q)\frac{[x]}{(x^n-1)}$ of degree $k-1$ or less [3]. We can write this as

$$c(x) = g(x)i(x) \tag{2.40}$$

where $i(x)$ is the information polynomial. The generator polynomial, $g(x)$ will also divide into the polynomial x^n-1 [20]. We will denote this polynomial as the parity check polynomial,

$$h(x) = \frac{x^n-1}{g(x)} \tag{2.41}$$

Now, the product of any codeword polynomial and the parity check polynomial will result in 0 in the ring of polynomials,

$$\begin{aligned} R_{x^n-1}[h(x)c(x)] &= R_{x^n-1}[h(x)g(x)i(x)] && (2.42)\\ &= R_{x^n-1}[(x^n-1)i(x)] && (2.43)\\ &= 0 && (2.44) \end{aligned}$$

If we denote the received polynomial by $v(x)$ then the error introduced by the channel will be

$$e(x) = v(x) - c(x) \tag{2.45}$$

where $e(x)$ is also a polynomial in the ring of polynomials. Errors in cyclic codes are identified by calculating the syndrome. The syndrome is calculated as the remainder of the received polynomial divided by the generator polynomial. Recall, if there is no error induced by the channel then the generator will divide the received codeword and the syndrome polynomial will be zero. We will denote the syndrome polynomial as

$$\begin{aligned} s(x) &= R_{g(x)}[v(x)] && (2.46)\\ &= R_{g(x)}[c(x)+e(x)] && (2.47)\\ &= R_{g(x)}[i(x)g(x)+e(x)] && (2.48)\\ &= R_{g(x)}[e(x)] && (2.49) \end{aligned}$$

An important property of cyclic codes is that if the minimum distance of the code is d^*, than every error polynomial of weight less than $\frac{d^*}{2}$ has a unique syndrome polynomial [3]. This property enables one to correct up to $\frac{d^*}{2}$ channel errors. Decoding is the process of finding the minimum weight polynomial $e(x)$ that satisfies 2.49. Decoding is maximum likelihood if the errors are randomly occurring.

A problem that remains is to find generator polynomials that will result in a given minimum distance. Bose-Chaudurі-Hocquenghem codes provide a method of constructing such generator polynomials. A general generator polynomial, $g(x)$, can often be factored into minimal polynomials as,

$$g(x) = \text{LCM}[f_1(x), f_2(x), \ldots f_r(x)] \tag{2.50}$$

where LCM denotes least common multiple and $f_i(x)$ are the minimal polynomials of the zeros of $g(x)$. The zeros of the minimal polynomials will, in general, not be on the same field as the symbol field, $GF(q)$. They will however, always be contained on an extension field, $GF(q^m)$, of the symbol field where m is an integer. Rewriting equation 2.45 as,

$$v(x) = c(x) + e(x) \tag{2.51}$$

and evaluating the polynomial, $v(x)$, at a zero, γ_j, of the generator polynomial will result in

$$\begin{aligned} v(\gamma_j) &= c(\gamma_j) + e(\gamma_j) && (2.52)\\ &= e(\gamma_j) && (2.53) \end{aligned}$$

because $g(x)$ is a factor of $c(x)$ and γ_j is a zero of $g(x)$. Now, $g(x)$ has r roots and therefore we have r syndromes,

$$\begin{aligned} S_j &= v(\gamma_j) \qquad j=1,\ldots,r && (2.54)\\ &= e(\gamma_j) \qquad j=1,\ldots,r && (2.55)\\ &= \sum_{i=0}^{n-1} e_i\gamma_j^i \qquad j=1,\ldots,r && (2.56) \end{aligned}$$

These syndromes have different values from the syndrome polynomial discussed earlier, but contain the same information about the errors [3]. In fact, the syndromes S_j will be normally be elements of the extension field $GF(q^m)$, whereas the coefficients of the syndrome polynomial will be on $GF(q)$.

BCH codes choose the zeros of the generator polynomial so that if there are fewer than t errors, the syndromes can be used to calculate the errors. If α is a primitive element of the extension field $GF(q^m)$, then

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t} \tag{2.57}$$

are a set of zeros that can be used to form the generator polynomial.

The general construction procedure for BCH codes is as follows:

1. Choose a block length for the code such that the block length $n = q^m-1$, where q is the symbol field of the code and m is an integer.
2. Choose t, the minimum number of errors that the code must correct.
3. Choose a prime polynomial of degree m and construct the field $GF(q^m)$.
4. Choose α, a primitive element of $GF(q^m)$.
5. Find the minimal polynomial, $f_j(x)$, of α^j for $j = 1,\ldots,2t$.

6. Construct the generator polynomial as $g(x) = \text{LCM}[f_1(x), f_2(x), \ldots f_{2t}(x)]$

This construction will always result in a code that is capable of correcting t errors. The minimum distance of BCH codes is therefore at least $2t+1$. Sometimes, the true minimum distance of the code is even higher. A distinction should be made between the true minimum distance of the code, d^*, and the designed distance, $d = 2t+1$. The length of the BCH codes when constructed in this manner will be q^m-1. This length is called the primitive block length of the code.

Reed-Solomon codes are a special case of BCH codes, where the symbol field and the field where the zeros of the generator polynomial are located are the same. That is, in part 1 of the construction technique for BCH codes, $m=1$ and the block length of the code is $n = q-1$. The minimal polynomial of an element, γ in $GF(q)$ when γ itself exists in $GF(q)$ is

$$f_\gamma(x) = x - \gamma. \tag{2.58}$$

Since all the zeros of the generator polynomial exist in the symbol field, the generator polynomial is calculated as

$$g(x) = (x-\gamma_1)(x-\gamma_2)\ldots(x-\gamma_{2t}) \tag{2.59}$$

This will always result in a generator polynomial of degree $2t$, and therefore a Reed-Solomon code has

$$n-k = 2t. \tag{2.60}$$

Reed-Solomon codes are BCH codes and therefore the true minimum distance of the code satisfies

$$d^* \geq 2t+1 \tag{2.61}$$

However, for linear codes the Singleton bound [3] says

$$d^* \leq n-k+1 \tag{2.62}$$

Therefore, the minimum distance of Reed-Solomon codes is

$$d^* = n-k+1 \tag{2.63}$$

There do not exist codes that for a fixed (n, k) having a larger minimum distance than Reed-Solomon codes. For this reason, Reed-Solomon codes are said to be maximum distance separable.

A property of Reed-Solomon codes that is useful is the weight distribution. The weight distribution gives information on the distance spectrum of the the code. In general, weight distributions for most codes are not known. However, the weight distribution of Reed-solomon codes is known. The weight distribution of a (n, k) Reed-Solomon code on $GF(q)$ is [20]

$$A_j = \binom{n}{d} \sum_{h=0}^{j-1-(n-k)} (-1)^h \binom{j}{h} \left(q^{j-h-(n-k)} - 1\right) \qquad n-k+1 \le j \le n \quad (2.64)$$

where A_j is the number of codewords in the code with weight j. For $1 \le j \le n-k$, $A_j = 0$ and $A_0 = 1$. Since Reed-Solomon codes are linear, 2.64 is also the distance spectrum for the code.

Decoding of Reed-Solomon codes can be performed with the same decoder as for a BCH code. Appendix B discusses the decoding of BCH and Reed-Solomon codes.

BCH and Reed-Solomon codes may be shortened to smaller block length codes. The shortened codes are generated by finding the equivalent systematic cyclic code and then fixing some of the information symbols. Since the symbols are fixed, they can be known to the receiver and need not be transmitted. The shortened code will have the same minimum distance as the original code. This process will convert an (n, k, d) code into an $(n-l, k-l, d)$ code where l is the degree of shortening. A cyclic code, and hence a BCH and a Reed-Solomon code, can always be made into an equivalent systematic code. This is done by simply inserting the information symbols into the higher order coefficients of the codeword and choosing the other symbols so that the result is a codeword in the code. The codeword is to have the form

$$c(x) = x^{n-k} i(x) + t(x) \quad (2.65)$$

If this is a codeword in the code, then

$$\begin{aligned} 0 &= R_{g(x)}\left[c(x)\right] && (2.66)\\ &= R_{g(x)}\left[x^{n-k} i(x)\right] + \left[R_{g(x)} t(x)\right] && (2.67) \end{aligned}$$

or

$$t(x) = -R_{g(x)}\left[x^{n-k} i(x)\right] \quad (2.68)$$

because the degree of $t(x)$ is $g(x)$. This is a one to one mapping. The codewords in the code of a systematic code are the same as the codewords of non-systematic coding procedure. The only difference is the association between the information polynomial $i(x)$ and the codeword polynomial, $c(x)$.

Chapter 3

Codes Resistant to Rayleigh Fading

This chapter begins with an examination of the Rayleigh channel with particular interest in the effect that the fading has on the Euclidean distance between two channel signals. This leads to some rules for designing block codes for the Rayleigh channel. Next, in section 3.2, we introduce Reed-Solomon signal space codes for use on the Rayleigh fading channel. After some examples of different codes we will extend the idea to include a class of Bose-Chauduri-Hocquenghem signal space codes.

3.1 Signaling on a Rayleigh Fading Channel

The error probability of binary orthogonal signaling on the Rayleigh channel was calculated in [29]. In their calculation, they assume that the fading parameter $a(t)$ is somehow known to the receiver. We will also make this assumption for the moment. The problem of estimating the received fading process will be addressed in chapter 5. Wozencraft and Jacobs [29] evaluate the error probability of binary orthogonal signaling with diversity reception. They show that diversity is an effective method for reducing the error probability in the fading channel. Methods of generating diversity include retransmitting the signal at a later time or simultaneously transmitting it on a different frequency. The problem with these methods of generating diversity is that

the channel data rate is reduced by the same amount as the diversity is increased. This analysis examines the error rate of a signaling scheme that is slightly different than the binary orthogonal case. In this analysis, we are going to determine the pairwise error probability of two signals which have distance that is distributed over many symbol elements. This scheme is equivalent to a binary repetition code modulated on a binary phase shift keyed (BPSK) carrier.

We are going to calculate the pairwise error probability of binary signaling on the Rayleigh channel in which the binary symbols are spread over N symbol periods and each symbol is subject to independent fading. This is a repetition code in which the total power of the N symbols (representing 1 bit) is unchanged, i.e. the bit energy is normalized. Each symbol is subject to Rayleigh fading independent of other symbols. We want to find the distance of the signal points to the origin at the receiver or after fading. If we know this distance, then we can calculate the distance between the two signals and hence the probability of error.

The sequence of symbols transmitted by the receiver representing the bit "1" will be

$$S_i = \frac{1}{\sqrt{N}} \qquad \text{for } i = 1 \cdots N \quad (3.1)$$

and the corresponding sequence for the bit "0" is

$$S_i = -\frac{1}{\sqrt{N}} \qquad \text{for } i = 1 \cdots N \quad (3.2)$$

Signals that are different in N positions will be said to have a time diversity of N. This sequence of symbols is transmitted through a channel subject to independent Rayleigh fading and noise. Each symbol in the sequence representing either "1" or "0" will be received as

$$r_i = a_i S_i + n_i \qquad \text{for } i = 1 \cdots N \quad (3.3)$$

where the probability distribution of the multiplicative fading parameters, a_i is complex Gaussian and the noise, n_i, also has a complex Gaussian distribution. If the receiver has knowledge of the fading process, a_i, the effect of the random phase of each symbol can be unraveled. Then, the received sequence of symbols can be viewed as being the transmitted sequence modulated by a sequence of Rayleigh distributed

real random variables corrupted with noise whose distribution is complex Gaussian. The noise on each symbol is complex, but the optimum receiver will not be affected by noise that is orthogonal to the symbols containing the information. Hence, the receiver will make an estimate of the information based on the received sequence given by

$$R_i = \mathcal{R}\left[\hat{a}_i S_i + \hat{n}_i\right] \qquad \text{for } i = 1 \cdots N \tag{3.4}$$

where $R_i = \frac{r_i |a_i|}{a_i}$, $\hat{a}_i = |a_i|$ and $\hat{n}_i = \frac{n_i |a_i|}{a_i}$. The distribution of $\hat{a}_i$ is Rayleigh and the distribution of $\hat{n}_i$ is Gaussian. Both are real random variables.

The Euclidean distance of the transmitted signal from the all zeros vector can be calculated as

$$\begin{aligned} d_S &= \sqrt{\left(\sum_{i=1}^{N} d_{S_i}^2\right)} && (3.5)\\ &= \sqrt{\left(\sum_{i=1}^{N} \frac{1}{N}\right)} && (3.6)\\ &= 1 && (3.7) \end{aligned}$$

In the absence of fading, the probability of error is calculated by determining the error rate for a specific noise sample, and then integrating over the probability distribution of the noise,

$$\begin{aligned} \mathrm{P}[\mathcal{E}] &= \int_{d_S}^{\infty} \frac{1}{\sqrt{\pi N_o}} \exp^{-\frac{\alpha^2}{N_o}} \mathrm{d}\alpha && (3.8)\\ &= \mathrm{Q}\left(d_S \sqrt{\frac{2}{N_o}}\right) && (3.9) \end{aligned}$$

In the presence of fading, the distance properties of the received signal, prior to the addition of noise, are altered. In any event, the probability of error given a specific distance can be calculated with 3.9. The total Euclidean distance of the received signals from the all zeros vector after fading and before the addition of noise can be calculated as

$$\begin{aligned} d_R &= \sqrt{\sum_{i=1}^{N} d_{R_i}^2} && (3.10)\\ &= \alpha d_S && (3.11) \end{aligned}$$

where $d_{R_i}^2$ is the distance of the i^{th} symbol. Each of the d_{R_i}'s is composed of the product of the distance of the i^{th} symbol of the transmitted signal and a random variable due to fading plus an additive part due to noise. The variable α is a random variable whose distribution is unknown. The probability of error can be calculated by integrating equation 3.9 over the probability distribution of α [29],

$$\mathrm{P}[\mathcal{E}] = \int_{-\infty}^{\infty} \mathrm{Q}\left(\alpha d_S \sqrt{\frac{2}{N_o}}\right) \mathrm{P}_\alpha(\alpha) \mathrm{d}\alpha \tag{3.12}$$

If the probability distribution of α can be determined we can estimate the probability of error using 3.12. The squared distance of the received signal from the all zeros vector is the summation of the squared distance of each dimension. Each dimension is independently perturbed by a multiplicative factor whose distribution is Rayleigh. The distance of the received vector will be

$$d_R = \sqrt{\sum_{i=1}^{N} (d_{S_i} \rho_i)^2} \tag{3.13}$$

The distribution of ρ_i is Rayleigh

$$P_\rho(\rho) = 2\rho \exp\left[-\rho^2\right] \qquad 0 \le \rho < \infty \tag{3.14}$$

Note that $\mathrm{E}[\rho^2] = 1$ so that the average received signal energy is the same as the transmitted signal energy. If the transmitted distance is distributed equally over the N symbols and the transmitter energy is normalized to unity, then $d_{T_i} = \frac{1}{\sqrt{N}}$ and the distance of the received signal from the all zeros vector is

$$\begin{aligned} d_R &= \sqrt{\sum_{i=1}^{N} \frac{1}{N} (\rho_i)^2} && (3.15)\\ d_R &= \sqrt{\sum_{i=1}^{N} \chi_i^2} && (3.16) \end{aligned}$$

where $\chi_i = \rho_i / \sqrt{N}$ is again a Rayleigh random variable with PDF

$$P_\chi(\chi) = 2N\chi exp\left[-N\chi^2\right] \tag{3.17}$$

and $\mathrm{E}[\chi_i^2] = \frac{1}{N}$. Each Rayleigh random variable is itself a function of 2 independent Gaussian random variables

$$\chi_i = \sqrt{\gamma_{i_1}^2 + \gamma_{i_2}^2} \tag{3.18}$$

and $\mathrm{E}[\gamma_{i_1}^2] = \mathrm{E}[\gamma_{i_2}^2] = \mathrm{E}[\frac{\chi_i^2}{2}] = \frac{1}{2N}$. Then the distance of the received signal to the all zeros vector after fading and prior to the addition of noise is

$$d_R = \sqrt{\sum_{i=1}^{2N} \gamma_i^2} \tag{3.19}$$

where γ_i's are independent Gaussian random variables with $\sigma_\gamma^2 = \frac{1}{2N}$. The distribution of the distance is a Chi distribution with $2N$ degrees of freedom. The probability distribution function of this Chi distribution is

$$P_\delta(\delta) = \frac{2}{2^{\frac{n}{2}} \sigma^n \Gamma\left(\frac{n}{2}\right)} \delta^{n-1} \exp\left[-\frac{\delta^2}{2\sigma^2}\right] \tag{3.20}$$

where $n = 2N$ and $\sigma^2 = \frac{1}{2N}$. This density function is plotted in figure 3.1. Note that the area under each curve is the same and the $\mathrm{E}[\delta^2]$ for each curve is 1. The most interesting thing to note about the distributions is that the higher the time spreading, the less the area in the vicinity of $\chi = 0$.

From the distance distributions, we are able to estimate the probability of error for antipodal signaling by [29]

$$P[\varepsilon] = \int_0^{\infty} \mathrm{Q}\left(\delta \sqrt{\frac{2E_s}{N_o}}\right) \mathrm{P}_\delta(\delta) \mathrm{d}\delta \tag{3.21}$$

The four density functions from figure 3.1 were numerically integrated for different values of average signal to noise ratio and plotted. They are plotted in figure 3.2. An increase in transmitter signal power would increase the signal to noise ratio at the receiver for a given noise level. This would result in a decrease in the error rate for the repetition code. One may also increase the length of the repetition code while maintaining the same bit energy to get the same effect. In general, codes designed to be used in the fading channel must be designed with a balance between the Euclidean distance between the nearest neighbors and the time diversity of the codes. Most codes to date have been designed to maximize the Euclidean distance between codewords or code sequences.

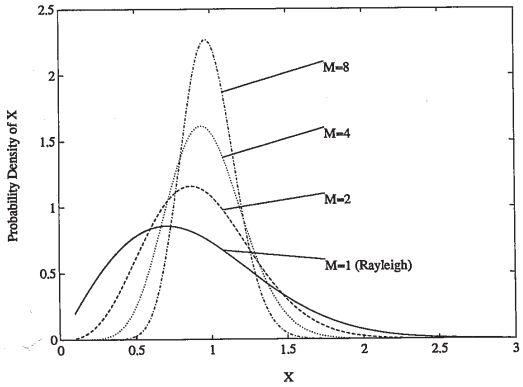

Figure 3.1: Chi distribution with $2N$ degrees of freedom

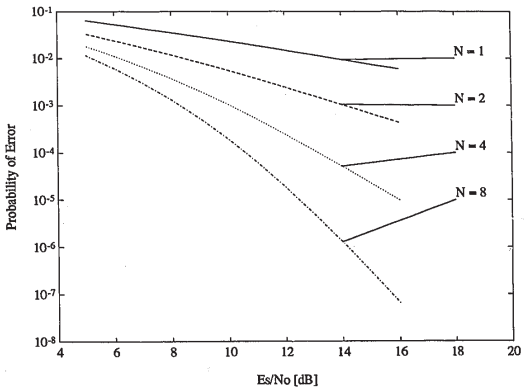

Figure 3.2: Pairwise Error Probability for an Antipodal Signaling Scheme with Time Spreading N

Two criteria for designing codes for fading channels are evident. First, one must try to maximize the Euclidean distance between the codewords. The Euclidean distance is the distance between the two codewords when viewed in signal space. Second, the Euclidean distance between two codewords must be distributed over a maximum number of symbols and this distance should be equally distributed over these symbols. That is, the code should have a large implicit time diversity

The first criterion is to reduce the probability that a large sample of receiver noise causes an error. The second criterion is to introduce diversity into the transmitted signal so that the random nature of the channel is reduced. These two criteria, are in general, conflicting requirements in code design.

3.2 Reed–Solomon based Signal Space Codes

Code design must be concerned with maximizing two parameters, one being the Euclidean distance of the code and the other being the diversity of the code. A good code must also try to maximize the throughput of the channel or to maximize the spectral efficiency. We have developed a class of spectrally efficient signal space codes that have good Euclidean distance properties and also have high diversity. The class of codes is based on well known algebraic codes, the Reed-Solomon codes. The result is a class of signal space block codes that are effective in combating multiplicative fading. Reed-Solomon codes were selected for the contruction of the signal space codes because of their property of being maximum distance separable. The use of RS codes guarantees a minimum amount of diversity. The resultant signal space codes are not the optimum codes that maximize both criteria.

The coding construction is a mapping of a block codeword of an algebraic block code on a field of q elements onto a channel signal set which also contains q elements. The most natural codes to use for the algebraic block codes when designing for Rayleigh fading channels is the class of Reed-Solomon codes. This is because Reed-Solomon codes are maximum distance separable, and the resultant code will have the property of having a large diversity. The channel signal set can be any signal set that contains q elements.

Assume we are using a (N, K, d) Reed-Solomon code on a field of q elements as the base Reed-Solomon code. N is the block length of the code, K is the number of data symbols and d is the Hamming distance of the code. For a Reed-Solomon code $d = N-K+1$ and $N \leq q+1$. The input binary data is interpreted as data on the field of q elements. Let b be the number of bits needed to represent a symbol on the field of q elements. The K data symbols of the Reed-Solomon code are data symbols on $GF(q)$, therefore, the number of data bits in a block can be calculated as the product of K and b. The encoder uses the K data symbols and generates a codeword of block length N, also in $GF(q)$. Each of the N symbols is then independently mapped onto the channel signal set. The channel signal set must contain q elements, the number of field elements.

The channel signal set may be any signal set that contains q elements. We usually choose the signal set to be a two dimensional signal set. A typical choice for the channel signal set would be to use either an appropriate quadrature amplitude modulated (QAM) or amplitude-phase modulated (AMPM) signal set such as 16-QAM when the number of field elements is 16 or 32-AMPM when we are using GF(32). This may be desirable because of existing hardware requirements. However, other signal sets may be used. Another good choice for a two dimensional signal set is to choose the q lowest energy points of the hexagonal lattice. This choice of signal set will generally result in codes that have a slightly larger Euclidean distance than if a QAM type signal set were chosen. If the number of elements in the Galois field of the Reed-Solomon codes is large, higher dimensional signal sets may be used. An example of this would to be choose the 64 lowest energy elements of the 4 dimensional Barnes-Wall lattice. Since it will take two channel symbols to represent a point in 4 dimensions, the block length of the resulting signal space code will be $2N$. In general, for a channel signal set with dimensionality $\mathcal{D}$, the number of channel symbols in the Reed-Solomon signal space code will be $\mathcal{D}N/2$. A quadrature amplitude modulated signal can accommodate 2 dimensions for each channel symbol. The specific mapping from elements in GF(q) to points in the signal set is arbitrary. In general, this mapping cannot be optimized to produce better codes because of the complexity of the Reed-Solomon codes.

The resultant code is a signal space code with $\mathcal{D}N/2$ channel symbols, containing Kb information bits. The spectral efficiency is the average number of information bits transmitted per channel symbol. The spectral efficiency can then be calculated as $\frac{2bK}{\mathcal{D}N}$.

Most of the codes of interest are codes that are based on Reed-Solomon algebraic codes on extension fields of $GF(2)$. Then, there will be an integral number of data information bits needed to represent each information symbol in the code. Other fields may be used, but then the representation of binary information on the code field is not straightforward.

The distance properties of the code can be calculated through knowledge of the Hamming distance of the Reed-Solomon base code and the Euclidean distance properties of the channel signal set. If the squared Euclidean distance of the channel signal set is S^2, then the minimum squared Euclidean distance of the code is at least S^2d. This distance determines the effectiveness of the code on additive white Gaussian noise channels.

3.3 Examples of Different Codes

As an example of the encoding procedure, consider the following scheme using a [14,7,8] Reed-solomon code on the field of 16 elements. Since the field size is 16, it requires that the input binary data be interpreted as information on GF(16). Four bits are necessary to uniquely determine a symbol on GF(16) ($2^4 = 16$). Seven information symbols on GF(16) are input into a Reed-Solomon systematic encoder which generates a block of 14 symbols on GF(16). These 14 symbols are independently mapped onto the channel signal set. Since there are 16 possibilities for these code symbols, the channel signal set must also contain 16 elements. Specifying the channel signal set, (eg. 16-QAM) and a mapping completes the encoder. The spectral efficiency of this code can be determined by multiplying the number of bits of information required to specify a symbol on GF(16) (4) by the number of information symbols in the Reed-Solomon code (7) and dividing by the block length of the code (14). A simple calculation reveals that the spectral efficiency is 2 bits per symbol. Since the

Reed-Solomon Code	Signal Space Code	Gain in dB	Diversity
[16, 8, 9] on GF(16)	Length 16 on 16-QAM	2.55	9
[14, 7, 8] on GF(16)	Length 14 on 16-QAM	2.04	8
[12, 6, 7] on GF(16)	Length 12 on 16-QAM	1.46	7
[10, 5, 6] on GF(16)	Length 10 on 16-QAM	0.79	6

Table 3.1: Reed-Solomon Signal Space codes that use rate one half RS codes on GF(16) and use the 16-QAM signal set

Hamming distance of the Reed-Solomon code is 8, the diversity of the code is 8. The minimum squared Euclidean distance between two codewords is the product of the Hamming distance of the Reed-Solomon code and the minimum squared Euclidean distance between points in the channel signal set. In this case, the minimum squared Euclidean distance of the code is $4 \times 8 = 32$, assuming that the 16-QAM signal set is fixed to integer values of $\pm 3, \pm 1$. Normalizing the average signal energy to unity, the minimum squared Euclidean distance is 3.2. This compares to the uncoded 4-PSK case where the minimum squared Euclidean distance is 2 with an average signal energy of one. This corresponds to a gain of 2.04 dB over uncoded 4-PSK. This value of gain in itself is not impressive, but since the code also gives a diversity factor of 8, the code is quite powerful when used for signaling on the Rayleigh fading channel.

There are many other codes that can be constructed using the code construction method of section 3.2. Other codes that result in a spectral efficiency of 2 bits per symbol and use the 16-QAM signal set are constructed in the same manner using different Reed-Solomon codes as the base codes. These codes will all be rate $\frac{1}{2}$ codes, since we desire a spectral efficiency of 2 bits per symbol and the number of bits needed to represent an element of GF(16) is 4. Table 3.1 indicates the Reed-Solomon base codes which are used to generate the codes. Also included in the table are the Euclidean distance gain over uncoded 4-PSK and the diversity factor of the code.

The codes in table 3.1 can be modified by changing the channel signal set used. The 16-QAM signal set is not the best 2-dimensional signal set in terms of having a large Euclidean distance. The Hexagonal lattice is the best two dimensional packing in this regards. If 16 of the lowest energy signals in the hexagonal lattice were to be used as signal points instead of the 16-QAM signal set, then each of the

Reed-Solomon Code	Signal Space Code	Gain in dB	Diversity
[30, 12, 19] on GF(32)	Length 30 on 32-AMPM	2.58	19
[25, 10, 16] on GF(32)	Length 25 on 32-AMPM	1.83	16
[20, 8, 13] on GF(32)	Length 20 on 32-AMPM	0.93	13
[15, 6, 10] on GF(32)	Length 15 on 32-AMPM	-0.21	10

Table 3.2: Reed-Solomon Signal Space codes that use rate $\frac{2}{5}$ RS codes on GF(32) and use the 32-AMPM signal set

codes in the table would have an extra 0.458 dB of gain.

Rate $\frac{1}{2}$ Reed-Solomon codes on GF(16) are limited to a diversity of 9 if a spectral efficiency of 2 bits per symbol is to maintained, because the block length is limited to 17 symbols. If codes with higher diversity are desired, then one must use Reed-Solomon codes on a larger field. The class of codes on GF(32) also generate interesting signal space codes. On GF(32), the code rate only needs to be rate $\frac{2}{5}$ to result in signal space codes with a spectral efficiency of 2 bits per symbol. The change in field of the Reed-Solomon code requires a change of channel signal set. Since the field now has 32 elements, the channel signal set must also contain 32 elements. We will choose the 32-AMPM signal set as the channel signal set. By 32-AMPM channel signal set, we are referring to the 64-QAM channel signal set with half of the signal elements removed. Table 3.2 shows some of the possible codes of this type.

Again, one could use the 32 lowest energy points of the hexagonal lattice as the the channel signal set to increase the Euclidean distance of the signal space code. Then, each of the codes in the table would have an additional Euclidean distance gain of .76 dB.

Codes can also be constructed that have a higher spectral efficiency. To obtain a spectral efficiency of 3 bits per symbol using Reed-Solomon codes the code rate must be $\frac{3}{5}$. Table 3.3 lists some of the codes constructed with rate $\frac{3}{5}$ Reed-Solomon codes with a channel signal set of 32-AMPM. The gain value quoted is the Euclidean distance gain over uncoded 8-AMPM. These codes have both a large Euclidean distance gain and a large diversity factor.

If we again increase the number of field elements in the Galois field, the construction technique will generate codes of extremely high diversity. Tables 3.4

Reed-Solomon Code	Signal Space Code	Gain in dB	Diversity
[30, 18, 13] on GF(32)	Length 30 on 32-AMPM	4.91	13
[25, 15, 11] on GF(32)	Length 25 on 32-AMPM	4.18	11
[20, 12, 9] on GF(32)	Length 20 on 32-AMPM	3.31	9
[15, 9, 7] on GF(32)	Length 15 on 32-AMPM	2.22	7

Table 3.3: Reed-Solomon Signal Space codes that use rate $\frac{3}{5}$ RS codes on GF(32) and use the 32-AMPM signal set

Reed-Solomon Code	Signal Space Code	Gain in dB	Diversity
[60, 20, 41] on GF(64)	Length 60 on 64-QAM	2.91	41
[45, 15, 31] on GF(64)	Length 45 on 64-QAM	1.69	31
[30, 10, 21] on GF(64)	Length 30 on 64-QAM	0.00	21

Table 3.4: Reed-Solomon Signal Space codes that use rate $\frac{1}{3}$ RS codes on GF(64) and use the 64-QAM signal set

and 3.5 give the code parameters for codes with spectral efficiencies of 2 and 3 constructed with Reed-Solomon codes on GF(64). The channel signal set was taken to be 64-QAM.

3.4 Extension to BCH codes

The code construction technique from section 3.2 describes the construction of Reed-Solomon signal space codes using the known class of Reed-Solomon codes as the base code. An obvious extension to this concept would be to use other codes as the base codes. A good choice for base codes is the class of Bose-Chauduri-Hocquenghem

Reed-Solomon Code	Signal Space Code	Gain in dB	Diversity
[60, 30, 31] on GF(64)	Length 60 on 64-QAM	5.67	31
[50, 25, 26] on GF(64)	Length 50 on 64-QAM	4.91	26
[40, 20, 21] on GF(64)	Length 40 on 64-QAM	3.98	21
[30, 15, 16] on GF(64)	Length 30 on 64-QAM	2.80	16

Table 3.5: Reed-Solomon Signal Space codes that use rate $\frac{1}{2}$ RS codes on GF(64) and use the 64-QAM signal set

codes. This is because they also exist on extension fields of GF(2). BCH codes are a large class of codes and the possibilities for use as signal space codes with large diversity are many.

The code construction is a mapping of a codeword of a BCH algebraic block code on a field of q elements onto a channel signal set which also contains q elements. The channel signal set could be any signal set that contains q elements.

Assume we are using a (N, K, d) BCH code on a field of q elements as the base code. Again, N is the block length of the code, K is the number of data symbols and d is the Hamming distance of the code. If b is the number of bits needed to represent a symbol on the field GF(q), the number of data bits in a block can be calculated as the product of K and b. The encoder uses the K data symbols and generates a codeword of block length N, also in $GF(q)$. Each of the N symbols is then independently mapped onto the channel signal set. The channel signal set must contain q elements, the number of field elements.

The choices for the channel signal set are the same as for the Reed-Solomon signal space codes. If a 2 dimensional signal set is used, the result is a signal space code of with N channel symbols, containing Kb information bits. The spectral efficiency is the average number of information bits transmitted per channel symbol. The spectral efficiency can then be calculated as $\frac{bK}{N}$.

The distance properties of the code are calculated with the same procedure as for the Reed-Solomon signal space codes. If the squared Euclidean distance of the channel signal set is S^2, then the minimum squared Euclidean distance of the code is $S^2 d$. This distance determines the effectiveness of the code on additive white Gaussian noise channels. The diversity of the code is the Hamming distance of the base code used to construct the signal space code.

The main advantage of using BCH codes instead of Reed-Solomon codes as the base code for constructing the signal space codes is that for a given field size, BCH codes may have larger block lengths. In a field containing q elements, a Reed-Solomon code is limited in block length to $q + 1$. This restriction will also limit the Hamming distance of the base code, and hence the diversity of the signal space code, if the channel throughput is to be maintained. BCH codes may have extremely large

block lengths and with the increasing block length for a fixed rate code, the Hamming distance of the BCH code will increase. This means that the corresponding signal space codes may have extremely large diversity and Euclidean distance coding gains.

The disadvantage to using BCH codes as the base code for constructing signal space codes is that the complexity of decoding increases with increasing block length.

There are many examples of signal space codes that can be constructed using BCH codes as the base algebraic code. If one wished to use an 8 point channel signal constellation, it is required to use an algebraic code that exists on GF(8). If the channel throughput is to be maintained at 2 bits per channel symbol, then the code rate of the algebraic code must be $\frac{2}{3}$. Primitive BCH codes are rarely rate $\frac{2}{3}$. Primitive block length codes can however be shortened to produce rate $\frac{2}{3}$ BCH codes by finding the equivalent systematic cyclic code and then setting some of the information symbols equal to zero. These known information symbols do not need to be transmitted through the channel and hence the effective block length of the code is reduced. This reduction in block length also reduces the number of information symbols in the code, but the shortened code's Hamming distance will not be decreased. BCH codes exist on GF(q) whose primitive block lengths are $q^n - 1$, where n is any positive integer. Therefore, on GF(8), codes exist whose primitive block lengths are 63 and 511. Tables 3.6 and 3.7 are examples of signal space codes constructed from BCH codes on GF(8) that result in a spectral efficiency of 2 bits per symbol. The value of gain quoted is the Euclidean distance gain over uncoded 4-PSK. The gains quoted in the tables are asymptotic gains and cannot in general be realized due to the error multiplicity of the codes. The diversity and the Euclidean distance gain of these codes is impressive. The codes in table 3.6 offer tremendous potential for use on the Rayleigh fading channel. The complexity of decoding however, increases with increasing block length. Decoding of signal space codes constructed with BCH codes as the base codes is discussed in section 4.3.

There are many other possibilities for signal space codes that are constructed by either using BCH algebraic codes of longer block length or using BCH codes that exist on larger fields. If the signal set were again expanded to include 16 elements, then codes that exist on GF(16) could be used as the base codes for constructing the

Primitive BCH Code	Rate $\frac{2}{3}$ Code	Signal Space Code	Gain in dB	Diversity
[63, 61, 2] on GF(8)	[6, 4, 2]	Length 6 on 8-AMPM	-0.97	2
[63, 59, 3] on GF(8)	[12, 8, 3]	Length 12 on 8-AMPM	0.79	3
[63, 57, 4] on GF(8)	[18, 12, 4]	Length 18 on 8-AMPM	2.04	4
[63, 55, 5] on GF(8)	[24, 16, 5]	Length 24 on 8-AMPM	3.01	5
[63, 53, 6] on GF(8)	[30, 20, 6]	Length 30 on 8-AMPM	3.80	6
[63, 51, 7] on GF(8)	[36, 24, 7]	Length 36 on 8-AMPM	4,47	7
[63, 49, 9] on GF(8)	[42, 28, 9]	Length 42 on 8-AMPM	5.56	9
[63, 48, 10] on GF(8)	[45, 30, 10]	Length 45 on 8-AMPM	6.02	10
[63, 46, 11] on GF(8)	[51, 34, 11]	Length 51 on 8-AMPM	6.43	11
[63, 44, 12] on GF(8)	[57, 38, 12]	Length 57 on 8-AMPM	6.81	12
[63, 42, 13] on GF(8)	[63, 42, 13]	Length 63 on 8-AMPM	7.16	13

Table 3.6: Signal Space codes constructed with BCH codes on GF(8) with primitive block length of length 63, using the 8-AMPM signal set with spectral efficiency of 2 bits per symbol

Primitive BCH Code	Rate $\frac{2}{3}$ Code	Signal Space Code	Gain in dB	Diversity
[511, 472, 15] on GF(8)	[117, 78, 15]	Length 117 on 8-AMPM	7.78	15
[511, 460, 20] on GF(8)	[153, 101, 20]	Length 153 on 8-AMPM	9.03	20
[511, 448, 25] on GF(8)	[189, 126, 25]	Length 189 on 8-AMPM	10.00	25
[511, 433, 30] on GF(8)	[234, 156, 30]	Length 234 on 8-AMPM	10.79	30
⋮	⋮	⋮	⋮	⋮
[511, 342, 74] on GF(8)	[507, 342, 74]	Length 507 on 8-AMPM	14.71	74

Table 3.7: Signal Space codes constructed with BCH codes on GF(8) with primitive block length of length 511, using the 8-AMPM signal set with spectral efficiency of 2 bits per symbol

Primitive BCH Code	Rate $\frac{1}{2}$ Code	Signal Space Code	Gain in dB	Diversity
[255, 227, 15] on GF(16)	[56, 28, 15]	Length 56 on 16-QAM	4.77	15
[255, 220, 20] on GF(16)	[70, 35, 20]	Length 70 on 16-QAM	6.02	20
[255, 210, 25] on GF(16)	[90, 45, 25]	Length 90 on 16-QAM	6.99	25
[255, 200, 30] on GF(16)	[110, 45, 30]	Length 110 on 16-QAM	7.78	30
[255, 185, 40] on GF(16)	[140, 70, 40]	Length 140 on 16-QAM	9.03	40
[255, 169, 51] on GF(16)	[172, 86, 51]	Length 172 on 16-QAM	10.09	51
[255, 152, 60] on GF(16)	[206, 103, 60]	Length 206 on 16-QAM	10.79	60

Table 3.8: Signal Space codes constructed with BCH codes on GF(16) with primitive block lengths of length 255, using the 16-QAM signal set with spectral efficiency of 2 bits per symbol

Primitive BCH Code	Rate $\frac{3}{4}$ Code	Signal Space Code	Gain in dB	Diversity
[255, 227, 15] on GF(16)	[112, 84, 15]	Length 112 on 16-QAM	8.75	15
[255, 220, 20] on GF(16)	[140, 105, 20]	Length 140 on 16-QAM	10.00	20
[255, 210, 25] on GF(16)	[180, 135, 25]	Length 180 on 16-QAM	10.97	25
[255, 200, 30] on GF(16)	[220, 165, 30]	Length 220 on 16-QAM	11.76	30
[255, 195, 35] on GF(16)	[240, 180, 35]	Length 240 on 16-QAM	12.43	60

Table 3.9: Signal Space codes constructed with BCH codes on GF(16) with primitive block lengths of length 255, using the 16-QAM signal set with spectral efficiency of 3 bits per symbol

signal space codes. In this class, we could use the BCH codes that exist on GF(16) whose primitive block length is 255. If we wanted a channel information rate of 2 bits per symbol. The primitive block length codes would be shortened to produce rate $\frac{1}{2}$ codes. Table 3.8 list a few of the possible codes constructed from BCH codes on GF(16) with a primitive block length of 255 which are shortened to produce signal space codes that have 2 bit per channel symbol spectral efficiency.

The BCH codes on GF(16) could also be used to construct signal space codes with 3 bits per symbol spectral efficiency. The primitive block length codes would, in this case, be shortened to produce rate $\frac{3}{4}$ codes. Table 3.9 list a few of the possible signal space codes constructed from algebraic BCH codes that have 3 bit per channel symbol spectral efficiency.

Chapter 4

Performance

In this chapter we will assess the performance of the Reed-Solomon and the BCH signal space codes. In the first section of this chapter we will discuss the pairwise error performance of the codes. Next, we will present some simulations results on the performance of the signal space codes when hard decision decoding is performed. In section 4.3 we will present an algorithm for decoding the Reed-Solomon signal space codes and present results on the combination of the encoding procedure and decoding algorithm when these codes are used for signaling in the Rayleigh channel. Finally, results are presented on the performance of the Reed-Solomon signal space codes in the presence of correlated Rayleigh fading. All error rate curves are plotted as a function of the average channel signal to noise ratio.

4.1 Pairwise Error Probability

In this section we are going to estimate the pairwise error probability of the Reed-Solomon signal space codes when used in the Rayleigh channel. The pairwise error probability will be governed by both the Euclidean distance of the signal space code and the Hamming distance of the base Reed-Solomon code and the average channel receiver signal to noise ratio.

Consider 2 minimum distance codewords from a Reed-Solomon signal space code. Let the base RS code be a $[N, k, d_H]$ code on a field of Q elements. The

minimum Hamming distance of the code is d_H. Let d_{SS}^2 be the minimum squared Euclidean distance between any two signal elements in the channel signal set. The squared Euclidean distance between any two codewords is $d_H d_{SS}^2$. The pairwise error probability of the two codewords depends only on the positions in which the two codewords differ. This is equivalent to the pairwise error probability of a binary repetition code of block length d_H where the two codewords are $C_0 = [d_{SS}/2, d_{SS}/2, ..., d_{SS}/2]$ and $C_1 = [-d_{SS}/2, -d_{SS}/2, ..., -d_{SS}/2]$. We have calculated the probability of error for such a binary signalling scheme in section 3.1. Because of the equivalence, it is also an estimate of the pairwise error probability of the Reed-Solomon signal space codes. An estimate of the pairwise error probability for the Reed-Solomon signal space codes can be calculated with knowledge of the two parameters d_H and d_{SS}^2. The parameter d_H determines the shape of the error rate curve and the Euclidean distance $d_H d_{SS}^2$ determines the position of the curve. A higher Euclidean distance will shift the error rate curves to the left, whereas a higher Hamming distance of the base Reed-Solomon code will result in a steeper asymptotic slope.

Pairwise error estimates of some Reed-Solomon signal space codes are given in figures 4.1 and 4.2. The pairwise error estimates are plotted versus the average channel signal to noise ratio. Figure 4.1 shows the pairwise estimates for rate one half Reed-Solomon signal space codes on Galois fields of 16 elements. These codes have a spectral efficiency of 2 bits per channel symbol. The channel signal set for these codes is the 16-QAM signal set. Figure 4.2 shows the estimates for signal space codes that were constructed from codes on GF(32) mapped to the 32-AMPM channel signal set. The base codes are rate $\frac{2}{5}$ and therefore the signal space codes also have a spectral efficiency of 2 bits per channel symbol.

The figures reveal that these codes have great potential for use on the Rayleigh fading channel. The true error rate for the codes will be higher than the pairwise error estimates because there are many codewords that are at the minimum distance to any codeword. For example, the $[14, 7, 8]$ Reed-Solomon code has 65,024 nearest neighbors. Multiplying the pairwise error curves by the number of nearest neighbors is often done to provide an estimate of the error probability of the code. This procedure does not result in a useful estimate in this case. This is because not all of the nearest

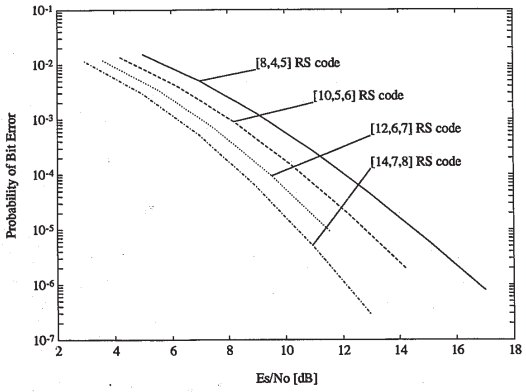

Figure 4.1: Pairwise Error Probability Estimate for Rate $\frac{1}{2}$ Reed-Solomon Signal Space Code Mapped to 16-QAM

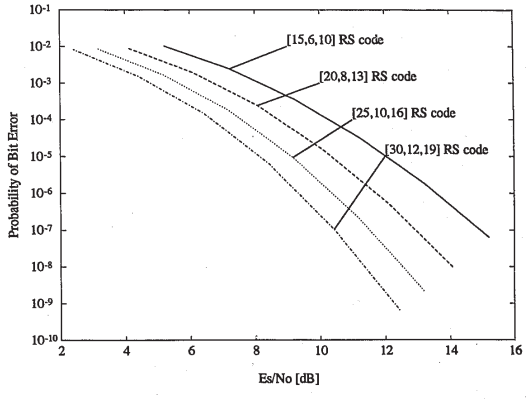

Figure 4.2: Pairwise Error Probability Estimate for Rate $\frac{2}{5}$ Reed-Solomon Signal Space Code Mapped to 32-AMPM

neighbors in the Reed-Solomon algebraic codes become nearest neighbors in the signal space codes. In mapping from the Galois field to the channel signal space, some of the codewords that are algebraic nearest neighbors may not result in signal space nearest neighbor codewords because of the type of channel signal set used. If an AMPM type channel signal set is used, each element of the Galois field will have 4 or fewer nearest neighbors after the mapping onto the channel signal set.

Figure 4.3 shows the pairwise probability estimate for a 3 bit per channel symbol signal space code. The codes used are rate $\frac{3}{5}$ Reed-Solomon codes on GF(32) mapped to the 32-AMPM channel signal set. Figure 4.3 shows that it is possible to signal 3 bits per channel signal through a Rayleigh channel and still maintain a low error rate.

4.2 Hard Decision Decoding of the RS and the BCH Signal Space Codes

This section will discuss hard decision decoding and provide simulation for hard decision decoding of the Signal space codes. First we will discuss the performance of the Reed-Solomon and the Bose-Chauduri-Hocquenghem signal space codes in the independent Rayleigh fading channel. Then in section 4.2.2 we will present results on the performance of the Bose-Chauduri-Hocquenghem signal space codes in the additive white Gaussian noise channel.

4.2.1 Performance of Space Codes in Rayleigh Fading and Hard Decision Decoding

Figure 4.4 shows the performance of Reed-Solomon signal space codes in the presence of fading and additive white Gaussian noise. The simulations presented here are of codes that offer 2 bits per channel symbol spectral efficiency. The codes are derived from Reed-Solomon codes that exist on GF(16) and are mapped to the 16-QAM channel signal set. The curves show that using hard decision decoding with these codes does not offer a performance advantage when compared to trellis codes [23, 13].

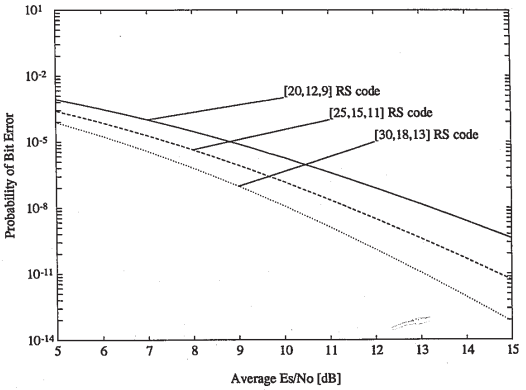

Figure 4.3: Pairwise Error Probability Estimate for Rate $\frac{3}{5}$ Reed-Solomon Signal Space Code Mapped to 32-AMPM

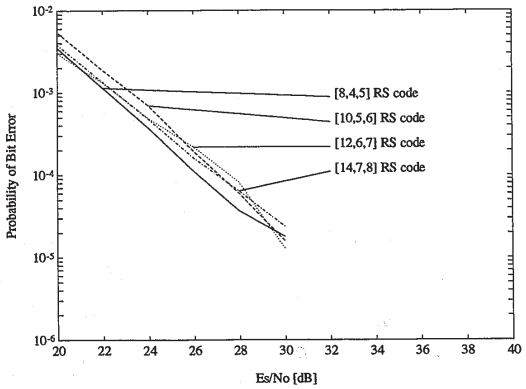

Figure 4.4: Error Performance curves generated by simulation of the Reed-Solomon Signal Space Curves in Fading

If we wished to use hard decision decoding with the signal space codes in the presence of fading and noise, we would probably use a BCH code as the base code. The reasons for this are twofold. BCH codes with large Hamming distance exist on fields with a small number of elements, and therefore more errors may be corrected. The other reason why BCH codes would be preferred is that the channel signal set is expanded only minimally, i.e. has only twice as many signal points as required for uncoded signalling. When there is a smaller number of elements in the channel signal set, there will be a corresponding larger distance between channel symbols and a lower symbol error rate. The lower symbol error rate is particularly desirable when hard decision decoding is performed.

Figures 4.5 and 4.6 show the performance of some Bose-Chauduri-Hocquenghem codes in independent Rayleigh fading and noise.

The simulations presented in both of these charts are of BCH signal space codes that offer 2 bits per channel symbol of spectral efficiency. The curve in figure 4.5 are codes whose primitive block lengths are 63 symbols. The codes have all been shortened to produce signal space codes with the 2 bits per channel symbol spectral efficiency. The codes presented in figure 4.6 are simulations of codes whose primitive block lengths are 511 symbols. The simulations show that BCH codes with hard decision decoding offer good performance considering the simplicity of decoding. No metrics need to be computed and the algebraic decoding need be performed only once per block.

4.2.2 Performance of the Bose-Chauduri-Hocquenghem Signal Space Codes in Additive White Gaussian Noise with Hard Decision Decoding

The tables in section 3.4 indicated that BCH signal space codes can offer a tremendous distance advantage over equivalent uncoded systems. In order to maintain the power of these codes, maximum likelihood decoding would have to be performed. However, if a sub-optimum decoding method could be used without degrading performance significantly, these codes may be attractive for use on the additive white Gaussian

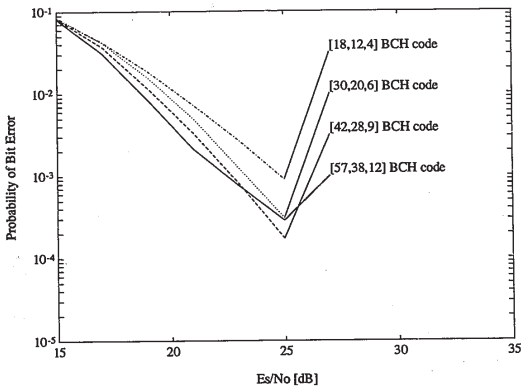

Figure 4.5: Error Performance curves of the Bose-Chauduri-Hocquenghem Signal Space Curves in Fading; Codes with Primitive Block Length of 63 and a Spectral Efficiency of 2 Bits per Channel Symbol

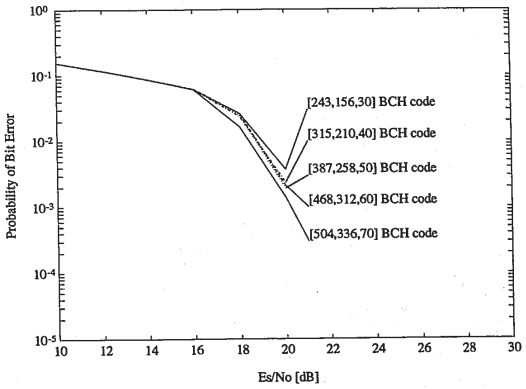

Figure 4.6: Error Performance curves of the Bose-Chauduri-Hocquenghem Signal Space Curves in Fading; Codes with Primitive Block Length of 511 and a Spectral Efficiency of 2 Bits per Channel Symbol

noise (AWGN) channel. It is known that with hard decision decoding of binary codes a performance loss of 3dB can be expected. The tables in section 3.4 seem to indicate that a 3dB loss may be tolerated with these powerful codes.

Figures 4.7 and 4.8 show the performance of BCH codes in additive white Gaussian noise using a hard decision decoder. BCH signal space codes that offer 2 bits per channel symbol of spectral efficiency are shown in both figures. The curves in figure 4.7 are codes whose primitive block lengths are 63 symbols. The codes presented in figure 4.8 are simulations of codes whose primitive block lengths are 511 symbols. The simulations show that, in additive white Gaussian noise, BCH codes with hard decision decoding offer impressive performance.

4.3 Soft Decision Decoding of the Reed-Solomon Signal Space codes

It is the job of the decoder to determine an estimate of the K data symbols with knowledge of only the N complex received signals and the N complex fading parameters. For the purpose of devising a decoding algorithm, we will assume that the receiver has ideal channel state information. In principle, the simplest decoding procedure would be to determine the conditional probability of the received signal given the fading process and a codeword. The receiver would calculate the conditional probability for every codeword in the code and then choose as its guess of the transmitted codeword, that codeword with the highest conditional probability. Divsalar and Simon, [7], have done work on calculating these conditional probabilities. The conditional probability is inversely proportional to the weighted Euclidean distance

$$D_w = \sum_{i=1}^{N} [x_i b_i - y_i]^2 \tag{4.1}$$

where the sum is over all symbols in the codeword and x_i, b_i and y_i are the transmitted signal, the fading and the received signal in the ith position respectively. The receiver would then calculate Equation 4.1 for all possible transmitted codewords and determine the codeword with the minimum D_w. This decoding procedure is maximum likelihood decoding for the Reed-Solomon signal space codes on the Rayleigh

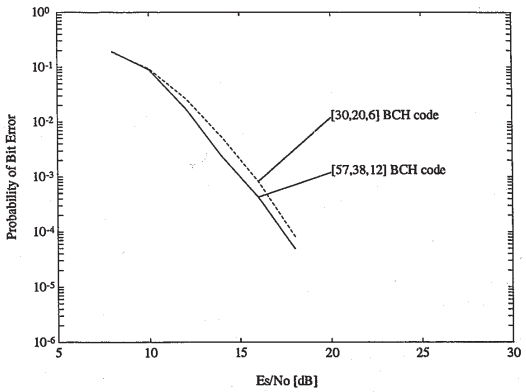

Figure 4.7: Error Performance curves of the Bose-Chauduri-Hocquenghem Signal Space Curves in AWGN; Codes with Primitive Block Length of 63 and a Spectral Efficiency of 2 Bits per Channel Symbol

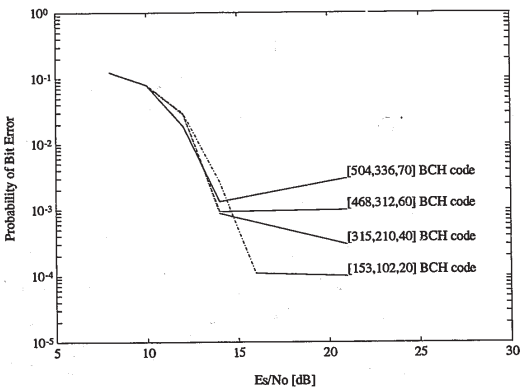

Figure 4.8: Error Performance curves of the Bose-Chauduri-Hocquenghem Signal Space Curves in AWGN; Codes with Primitive Block Length of 511 and a Spectral Efficiency of 2 Bits per Channel Symbol

channel. This procedure is extremely computationally intensive, especially when the number of codewords in the code is large. It is desirable to reduce the computations required in order to decode while maintaining reasonable decoding performance.

The decoding algorithm presented here, attempts to limit the search for the transmitted codeword to codewords that have a high probability of being the maximum likelihood codeword. To do this we exploit the erasure detection properties of Reed-Solomon codes. Reed-Solomon codes are known as erasure correcting codes because with any $[N, K, d]$ code, the codeword can be uniquely determined with knowledge of any K symbols. In our decoding scheme, the K symbols that are used for the purpose of reconstruction are determined by the receiver's knowledge of the fading. The receiver selects the K symbols that are associated with the K largest fading parameters. These symbols are selected because their contribution to the sum in equation 4.1 is usually larger due to scaling by the larger $b_i's$. A maximum likelihood search for the transmitted codeword could be performed in this manner by assigning each of these K symbols one of its q possibilities followed by codeword reconstruction and calculation of 4.1. Note that this will still require q^K codewords to be searched. We limit the search by allowing each of the K symbols to be one of $M < q$ values. The search for the maximum likelihood codeword will then be only over M^K codewords. For each of the K positions, the M values that each symbol may take are the elements associated with the signal points in the channel signal set that have the highest conditional probability of being transmitted given the received symbol. This means that for each of these K symbols,

$$[x_i b_i - y_i]^2 \tag{4.2}$$

is calculated for each of the q field elements and the the M best (lowest) are considered possibilities for that symbol. Note that these calculations and sorting must be done K times per block. The value of M will be denoted as the depth of decoding.

An example will serve to clarify the decoding procedure. Continuing with the example the [14,7,8] Reed-Solomon code mapped onto a 16-QAM signal set. A block diagram of of the decoding process for this example is given in figure 4.9. This example will continue with a decoder whose decoding depth $M = 4$. The information set of

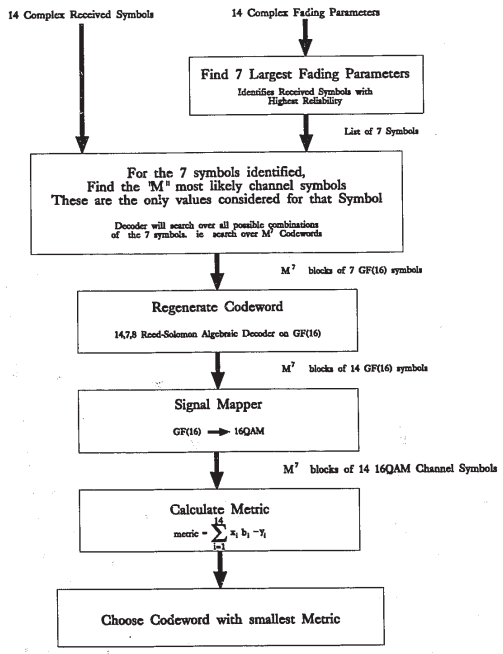

Figure 4.9: Decoding procedure for the [14,7,8] Reed-Solomon signal space code, showing major units

this Reed-Solomon code is 7 symbols. This means that any 7 of the 14 symbols in the block could be used to uniquely determine the whole block. The decoder chooses 7 positions of the block which it deems 'most reliable'. These positions are determined only by the decoders knowledge of the fading process. These positions are identified as the positions corresponding to the 7 largest (in magnitude) fading values. For each of these positions the decoder then chooses 4 (decoding depth) symbols that have the highest conditional probability of being transmitted given the received symbol and the fading for that position. The decoder searches through 7^4 possible codewords by performing a codeword reconstruction and the calculation of 4.1 for every combination of the 4 symbols in the 7 positions. The decoder chooses as its decoded codeword that codeword that is included in the search which has the highest conditional probability of being transmitted. Note that the 7 positions chosen to be the information set must be determined for each block.

4.3.1 Simplifications

There are some practical simplifications of the computation of the values of the the conditional probability that are worthwhile mentioning. Figure 4.9 shows that codeword reconstruction and calculation of equation 4.1 must be performed for each codeword in the search. However, many of the computations need only be calculated once per block. For each position in the block there are only q possible transmitted channel symbols. Therefore the quantity

$$[x_i b_i - y_i]^2 \tag{4.3}$$

may take on one of q different values. For a code with a block length of N, one must perform Nq such calculations. We will denote these values as the symbol conditional probabilities. If these Nq symbol conditional probabilities are precomputed, then the calculation of equation 4.1 can be simplified considerably. After codeword reconstruction, the calculation of 4.1 can be performed as a table lookup of the N symbol conditional probabilities, followed by a summer.

The codeword reconstruction part of the decoding algorithm is also very computationally intensive. This is also because it must be performed M^k times. The decoder may also precompute many of the calculations that are required for codeword reconstruction. Suppose that the decoder were to identify position a as one of the K positions that is to be used for codeword reconstruction. The decoder would compute the codeword in the code that has a 1 in the a'th position, and 0's in all of the other K positions used for codeword reconstruction. This unique codeword will be denoted as the sub-generator codeword for position a given the K positions. We call this the sub-generator codeword because with knowledge of the K sub-generators, $\mathbf{g}_i$, all ot the codewords in the code can be calculated as

$$\sum_i x_i \mathbf{g}_i \tag{4.4}$$

where the sum is over the K sub-generator codewords and x_i is an element of GF(q). The calculation of equation 4.4 requires only $(N-K)K$ multiplications in GF(q) and NK additions in GF(q). The decoder limits the search by limiting each of the x_i's in equation 4.4 to one of M values. The decoder would precompute the K sub-generator codewords and perform codeword reconstruction using 4.4.

4.3.2 Modifications to Decoding Algorithm

The performance of the decoding algorithm may be optimized by reducing the number of codewords that are searched without significantly reducing the probability that the actual transmitted codeword is searched. Let the K positions in the block that are used for codeword reconstruction be denoted as the regeneration set for the block. In the basic algorithm, the decoding depth is the number of possible values that each member of the regeneration set is allowed to take. A simple modification of the basic algorithm is to let different positions of the regeneration set take a different number of possible values. For example, since the element associated with the largest fading parameter is more reliable than the other elements in the block, this element may only be allowed to take on $M-1$ possible values while the other positions of the regeneration set may take on one of M possibilities. This simple change in the rule for including a codeword in the search reduces the number of codeword that

are contained in the search to $M^{K-1}(M-1)$. In general, each of the K different positions in the regeneration set will be allowed to different values, M_i, where M_i is the number of possibilities for the position associated with the i'th largest fading value. The values of M_i will be optimized to offer the best complexity- error rate performance. The total number of codewords in the search for varying values of M will then be

$$\prod_{i=1}^{K} M_i \tag{4.5}$$

4.3.3 Simulations of Code Performance

Figure 4.10 illustrates the performance of Reed-Solomon signal space codes in the presence of fading and noise. The results presented here are of codes derived from Reed-Solomon codes that exist on a field of 16 elements which were shortened to produce signal space codes that have 2 bits per channel symbol spectral efficiency. The parameters of the codes are indicated on the chart. Decoding is performed with the soft decision decoding algorithm presented in section 4.3 with a decoding depth of $M = 4$. The block length 14 Reed-Solomon code based on the algebraic Reed-Solomon code on 16 elements and mapped to the 16-QAM signal set achieves a bit error rate of 10^{-4} at about 15dB average channel symbol to noise ratio.

When the decoding depth of the soft decision decoder is increased, the required signal to noise ratio to a achieve a specific error rate is, in general, decreased. Figure 4.11 shows the results of simulations in which the decoding depth of the soft decision decoder are varied. The results presented are simulations of the block length 14 code derived from the [14,7,8] Reed-Solomon algebraic code on the field of 16 elements. The channel signal set used for the signal space code is again the 16-QAM signal set. The results indicate that there is a practical limit to the depth of decoding required. After this limit is reached, there are diminishing returns in terms of the amount of improvement of the decoder. The required decoding depth for decoding codes on the generated on a field of 32 elements and mapped to the 32-AMPM signal set is usually higher than for the codes that are based on GF(16) Reed-Solomon codes. This is because the channel signal elements become closer together when the change

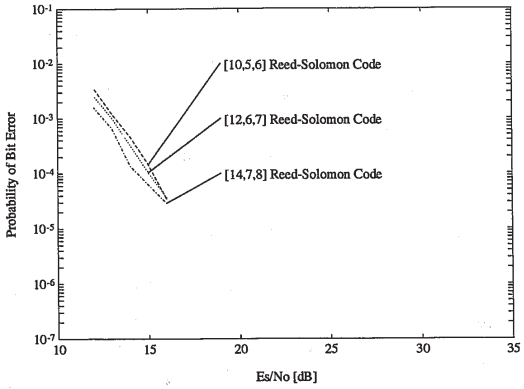

Figure 4.10: Simulations of code and decoder performance in independent Rayleigh fading and noise; Reed-Solomon signal space codes derived from codes in GF(16); Decoding depth = 4

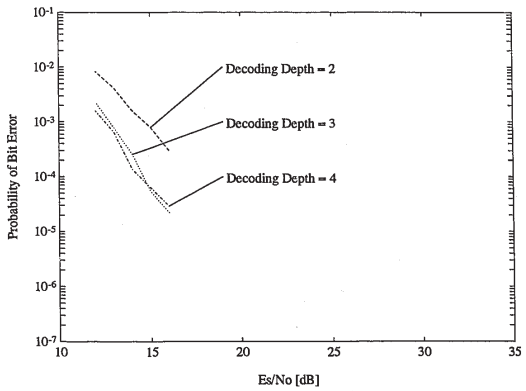

Figure 4.11: Simulations of code and decoder performance in independent Rayleigh fading and noise; Reed-Solomon signal space code derived from the [14,7,8] code in GF(16)

to the 32-AMPM signal set is done. However, when the signal set is changed to the 32 point signal set, the required code rate to achieve a spectral efficiency of 2 bits per channel symbol decreases from $\frac{1}{2}$ to $\frac{2}{5}$. This means that, for the same size block length code, the regeneration set is smaller and also the reliability of the received points in the regeneration set is higher.

Some simulations were performed that were directed at optimizing the soft decision decoder which has a varying decision depth. This modification to the decoding algorithm was discussed in section 4.3.2. These simulations are presented

N'th Largest symbol	1	2	3	4	5	6	7
Number of Different Symbols Considered in Decoder	3	3	3	4	4	5	5

Table 4.1: Decoder depth values for modified decoding algorithm simulation set

in figure 4.12. The code used in the simulations is derived from the [14,7,8] Reed-Solomon algebraic code on the field of 16 elements. Again the channel signal set is the 16-QAM signal set. The values of decoder depth of the regeneration set for the simulation are provided in table 4.1. The results show that there is some optimization that will minimize the number of decoder errors for a fixed number of codewords in the search of the decoder. This optimization will be different for different block length codes and for codes that exist in different fields.

4.4 Bounds on Performance

4.4.1 A Bound on the Block Error rate for Hard Decision Decoding of Signal Space Codes

An upper bound on the block error rate of both Reed-Solomon and Bose-Chauduri-Hocquenghem signal space codes can be evaluated by examining the per symbol error probability of the channel and the code parameters. The per symbol error rate of the channel is determined by the channel model, the channel signal set and the average signal to noise power ratio of the receiver. For the additive white Gaussian noise channel model, this is simply the symbol error rate for uncoded transmission given a channel signal set and specific noise power. Error rate curves for many modulation formats on the AWGN channel are known [29, 18]. In the presence of fading, the per symbol error probability can be estimated as the product of the pairwise error probability and the average number of nearest neighbors. The pairwise error probability in the presence of a known multiplicative fading was evaluated in [29]. The result was stated in section 3.1. The probability of error is calculated by integrating the Gaussian Q-function over the probability distribution of the fading.

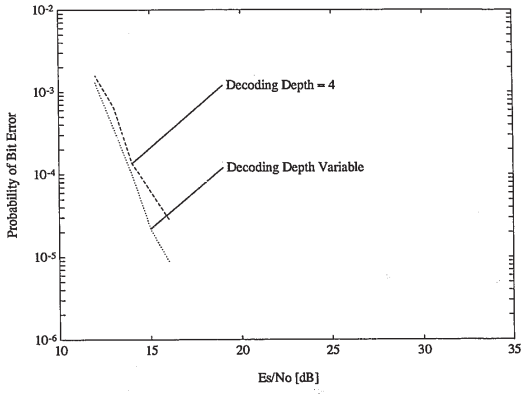

Figure 4.12: Simulations of code and decoder performance in independent Rayleigh fading and noise; Reed-Solomon signal space code derived from the [14,7,8] code in GF(16); Modified soft decision decoder

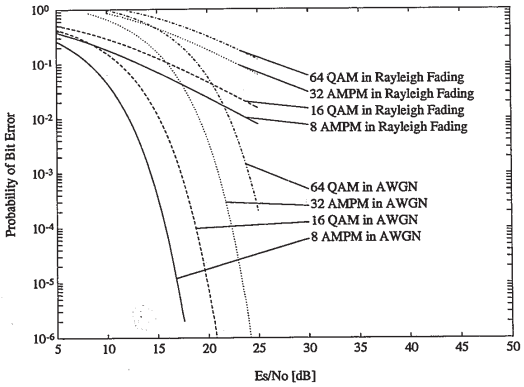

Figure 4.13: Symbol Error Rate Curves of Some Modulation Formats in AWGN and in multiplicative Rayleigh fading

Equation 3.12 is rewritten here for the reader's convenience as

$$P[\mathcal{E}] = \int_0^\infty Q\left(\alpha d_S \sqrt{\frac{2}{N_o}}\right) p_a(\alpha) d\alpha \tag{4.6}$$

Figure 4.13 shows the symbol error rate lower bounds for some different uncoded modulation formats for both the additive white Gaussian noise channel and the independent Rayleigh fading channel with noise.

With knowledge of the per-symbol error rate, a lower bound on the block error rate is easily determined when hard decision decoding is performed. A code that is able to correct up to T errors will make a correct decision if the actual number of errors is between 0 and T. If the block length of the code is N, and the per symbol

error rate is $P[\mathcal{E}]$, then the probability of having exactly t errors is

$$P[\text{number of errors is } t] = \binom{N}{t} P[\mathcal{E}]^t (1 - P[\mathcal{E}])^{N-t} \tag{4.7}$$

If the code can correct up to T errors, then the probability the decoding is correct can be calculated by summing equation 4.7 from $t = 0$ to $t = T$. Therefore the probability of block error is

$$P[\text{Block Error}] = 1 - \sum_{t=0}^{t=T} \binom{N}{t} P[\mathcal{E}]^t (1 - P[\mathcal{E}])^{N-t} \tag{4.8}$$

This will lower bound the block error rate with hard decision decoding because the probability of symbol error estimate is also a lower bound on the symbol error rate. If the per symbol error rate is known exactly, then equation 4.8 will be the block error rate. Equation 4.8 can also be used as a somewhat looser lower bound on the channel bit error rate after decoding.

Figure 4.14 shows the lower bound on error probability for some of the Reed-Solomon signal space codes used on the Rayleigh fading channel and using hard decision decoding. The fading in the simulation was independent Rayleigh fading. The [14,7,8] code uses the 16-QAM signal set, the [30,12,19] code is mapped to the 32-AMPM signal set and the [60,20,41] code employs the 64-QAM channel signal set.

It was stated in section 3.4 that if hard decision decoding were to be performed, then BCH signal space codes would probably be preferred to Reed-Solomon codes. The results are shown in figure 4.15. In this case the codes bounded are the [503,345,70] code on GF(8) and the [63,42,13] code also on GF(8). In both cases the channel signal set is the 8-AMPM signal set. The results for the AWGN channel are shown in figure 4.16.

4.4.2 Lower Bound on the Block Error Probability of the Soft Decision Decoding Algorithm

The probability of block error of the soft decision decoder is lower bounded by the probability that the actual transmitted codeword is in the set of codewords that the

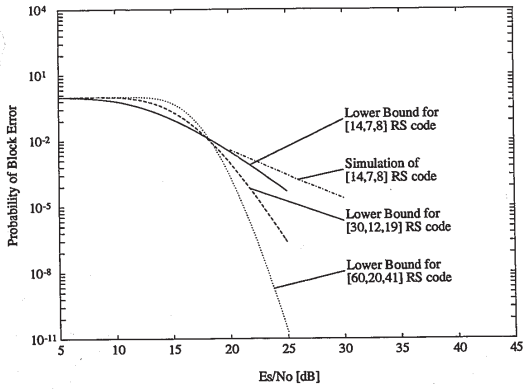

Figure 4.14: Bound on performance of Reed-Solomon Signal Space codes in the Multiplicative Rayleigh Fading Channel

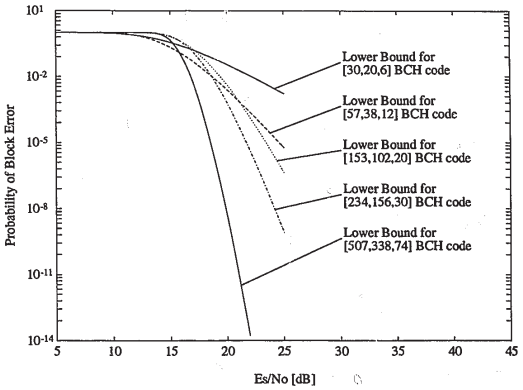

Figure 4.15: Bound on performance of Bose-Chauduri-Hocquenghem Signal Space codes in the Multiplicative Rayleigh Fading Channel

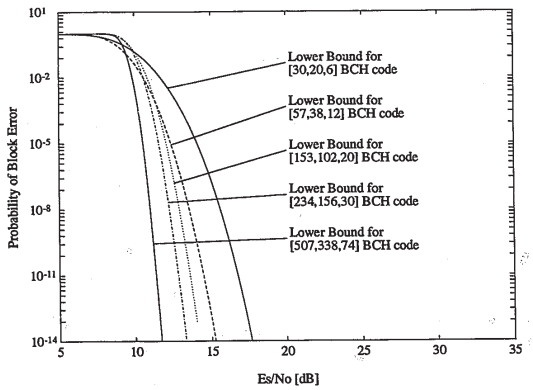

Figure 4.16: Bound on performance of Bose-Chauduri-Hocquenghem Signal Space codes in the Additive White Gaussian Noise Channel

decoder limits its search to. For a complete description of the soft decision decoding algorithm see section 4.3. This probability can be determined by examining the decoding algorithm. The decoder uses signal points that are "close" to the received points only in the positions that are associated with the largest fading parameters in the block. The number of positions that it uses for this purpose is identical to the number of symbols needed so that the entire block can be uniquely determined. Again, this set will be denoted as the regeneration set. For each member of the regeneration set, we wish to find the probability that the transmitted symbol is one of the M most likely transmitted points in the channel signal set, given the value of the channel fading and the received symbol. If we can find these probabilities, then we can calculate the probability that the transmitted codeword is in the search set. In a Reed-Solomon signal space code with parameters [N,K,d], the number of elements in the regeneration set is K, the number of information symbols in the block. Let R_j denote the element in the regeneration set that is associated with the j'th largest fading value. If $P(R_j)$ is the probability that R_j contains, in its list of possibilities, the transmitted symbol for that position in the codeword, then the probability that the transmitted codeword is in the search is

$$P[\text{Transmitted codeword in Search}] = \prod_{j=1}^{K} P(R_j) \tag{4.9}$$

and hence the probability of block error will be greater than

$$P[Block\ Error] = 1 - \prod_{j=1}^{K} P(R_j) \tag{4.10}$$

We must now determine the values of the individual $P(R_j)$'s. Their values depend on the signal to noise ratio, the channel signal set used, the channel model, the decoding depth of the decoder, and the value of j. A general expression for these probabilities is not possible, but we are able to estimate them for some specific cases of interest. By examination of the signal set, we can determine which elements of the signal set will be included in the decoder search given the received signal set. Figure 4.17 shows the regions where the received point must lie for a specific element to be included in the decoder search. This figure is specific to a code which uses the

16-QAM channel signal set and where the decoder depth is 4. The other elements in the signal set will have similar regions in which they will be included in the decoder search due to symmetry. Now consider R_j, the j'th element in the regeneration set. Regardless of which element was transmitted in position R_j, that element will be considered one of the 4 possibilities for R_j, if the magnitude of the noise is less than the distance between the signal points in the signal set.

The distance between the signal points at the transmitter is known, however it is the distance between these points at the receiver, prior to the addition of noise, that we are interested in in this case. This distance is again a random variable because the distribution of fading is random. Each symbol in the block is independently multiplied by a complex random variable whose envelope is Rayleigh distributed. In a Reed-Solomon signal space code derived from an algebraic code with parameters, $[N, K, d]$, the regeneration set includes the K largest fading parameters in a block of length N. The determination of the distribution of a set of sorted random variables is also referred to as the determination of order statistics [22, 1].

Let $X_1, X_2, \ldots, X_n$ be independent identically distributed random variables with common cumulative distribution $F_X(x)$. Denote the i'th smallest of the X_i's by $X_{i:n}$. With this notation $X_{1:n}$ is the smallest and $X_{n:n}$ is the largest in the set. The distribution of $X_{i:n}$ will then be

$$F_{X_{i:n}}(x) = \sum_{j=i}^{n} \binom{n}{j} [F_X(x)]^j [1 - F_X(x)]^{n-j} \tag{4.11}$$

The derivative of equation 4.11 with respect to the variable x will give the probability density function for the order statistics. The probability distribution of the fading has a Rayleigh distributed magnitude. The probability density function for a Rayleigh distribution is

$$P_X(x) = 2x \exp(-x^2) \tag{4.12}$$

and the cumulative distribution is

$$F_X(x) = 1 - \exp(-x^2) \tag{4.13}$$

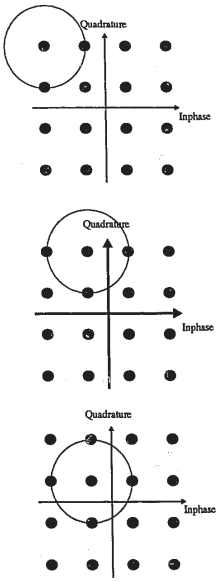

Figure 4.17: 16-QAM Signal Set and Regions in which signal elements are necessarily candidates in the decoder

Substituting the cumulative distribution function for the Rayleigh distribution into 4.11 gives the cumulative distribution of the order statistics of a set of n independent Rayleigh distributed random variables.

The regeneration set includes the K largest in magnitude multiplicative fading parameters taken from a block of length N. The cumulative distribution of the k'th largest will be

$$F_{X_{N-k+1:N}}(x) = \sum_{j=N-k}^{N} \binom{n}{j} \left[1-\exp(-x^2)\right]^j \left[\exp(-x^2)\right]^{N-j} \tag{4.14}$$

and the probability density function for the magnitude of the fading for the k'th element of the regeneration set is

$$\begin{aligned} P_{X_{N-k+1:N}}(x) &= \sum_{j=N-k}^{N} \binom{n}{j} j \left[1-\exp(-x^2)\right]^{j-1} \left[\exp(-x^2)\right]^{N-j} 2x\exp(-x^2) \\ &- \sum_{j=N-k}^{N} \binom{n}{j} \left[1-\exp(-x^2)\right]^{j} (N-j) \left[\exp(-x^2)\right]^{N-j-1} 2x\exp(-x^2) \end{aligned} \tag{4.15}$$

Figures 4.18 and 4.19 show the probability distributions of the largest fading parameters that result from a block length of 14 and 15 respectively. The 7 curves in figure 4.18 correspond to the distribution of the fading parameters in the regeneration set of the Reed-Solomon signal space code on 16-QAM that was derived from the [14,7,8] algebraic code. In figure 4.19, the distributions shown are those of the regeneration set fading magnitudes of the [15,6,10] algebraic Reed-Solomon code mapped to the 32-AMPM signal set. Note that all the distributions shown in figures 4.18 and 4.19 have a small probability of being close to zero in magnitude.

The values of the probabilities $P(R_j)$ can be found by integrating the probability that the noise magnitude is less than the distance between the signal points over the probability distribution of the fading magnitude of each element in the regeneration set. Since we wish to develop a lower bound, we will integrate over the probability that both the in-phase noise and the quadrature noise are less than the distance between elements in the signal set.

$$\mathrm{P}(R_j) = 2\int_0^\infty \mathrm{Q}\left(x d_S \sqrt{\frac{1}{N_o}}\right) P_{X_{N-j+1:N}}(x)\mathrm{d}x \tag{4.16}$$

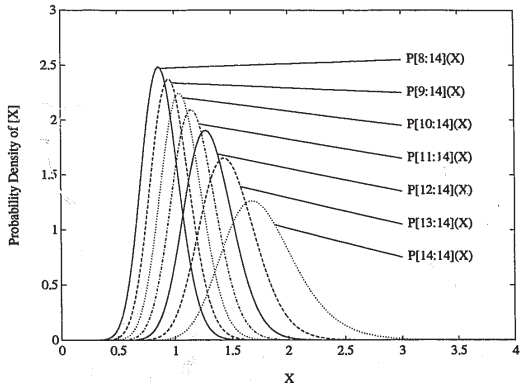

Figure 4.18: Probability distribution of the magnitudes of the Largest 7 Fading Parameters in a code with Block Length 14

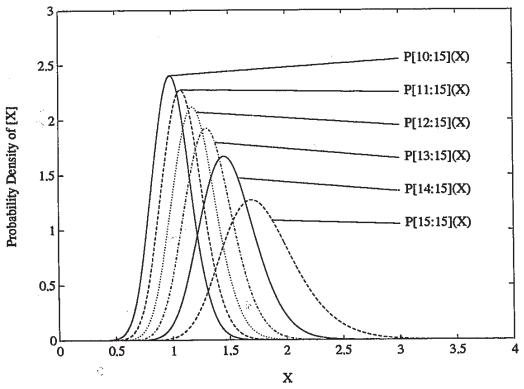

Figure 4.19: Probability distribution of the magnitudes of the Largest 6 Fading Parameters in a code with Block Length 15

The computation of the $P(R_j)$ was performed numerically for the different codes and for different signal to noise ratios and then substituted into equation 4.10 to develop a lower bound on the block probability of error for the decoder. These bounds were computed for the soft decision decoders with a decoding depth of 4 for the block length 14 code on 16-QAM and the block length 15 code on 32-AMPM. The results for the Reed-Solomon signal space code on 16-QAM with 2 bits per channel spectral efficiency is shown in figure 4.20. The error rates shown are block error rates. The code simulated is the [14,7,8] algebraic code on GF(16) mapped to 16-QAM. Figure 4.21 shows results for a Reed-Solomon signal space code that uses the 32-AMPM signal set. In this case, the base code is the [15,6,10] code on GF(32). The results show that the lower bounds on the block error probability of the decoder are quite tight.

4.5 Performance in Correlated Fading

The simulations presented to this point assumed that the fading was independent from symbol to symbol and that the receiver had knowledge of the fading process. In reality, the fading is highly correlated and independence can only be achieved in a system where an interleaver is present to remove the correlations. The presence of the interleaver inherently introduces delays in the system at both the transmitter and receiver. These delays must be kept to a minimum, especially in voice communications systems where excessive delay causes confusion in normal conversation. The simulations of code performance in this section are directed at testing the coding and decoding performance in systems with limited or no interleaving. The long block length codes are unusable for voice communications in a fading environment if they require that each symbol in the block have multiplicative fading values that are independent of one another.

The simulations that were performed in this section use the correlated Rayleigh

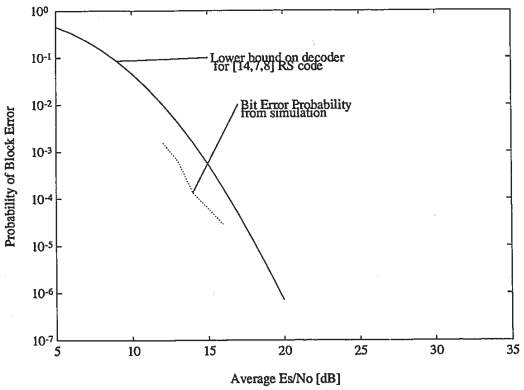

Figure 4.20: Lower Bound on the Probability of Error of the Soft Decision Decoding Algorithm; [14,7,8] Reed-Solomon code on GF(16) Mapped to 16-QAM; Decoding Depth of 4

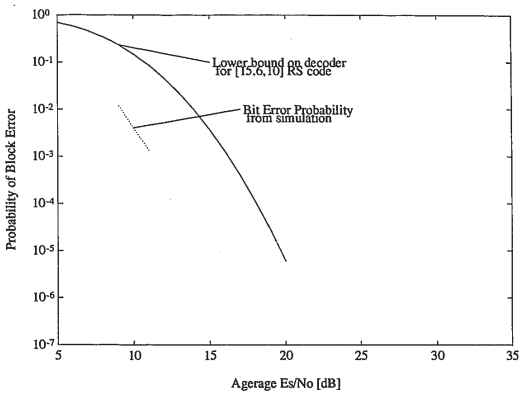

Figure 4.21: Lower Bound on the Probability of Error of the Soft Decision Decoding Algorithm; [15,6,10] Reed-Solomon code on GF(32) Mapped to 32-AMPM; Decoding Depth of 4

channel model. Comparisons are made to simulations in which the fading was independent. This would be the case in which the interleaver depth is infinite. Furthermore, in all simulations the receiver/decoder has perfect knowledge of the fading process. Figure 4.22 shows the performance of the [14,7,8] Reed-Solomon signal space code with a channel signal set, 16-QAM, for different values of interleaving. The channel fading time-bandwidth product used for these simulations is 0.08. The results show that the required value of interleaving to achieve good performance is very small. Without any interleaving the code loses about 5dB as compared to the same code with infinite interleaving. With an interleave depth of only 8, almost all of the loss due to the correlated fading is recovered.

Figure 4.23 show the results of simulations in which the value of the time bandwidth product is varied. In this series of simulations, the interleaver depth was maintained at a constant value of 4. The code used was again the [14,7,8] Reed-Solomon code mapped to the 16-QAM signal set. The results are as expected. A smaller channel time bandwidth product requires a correspondingly larger value of interleaving. A smaller time-bandwidth product produced more correlations in the fading process. These correlations are removed by an interleaver with a larger depth.

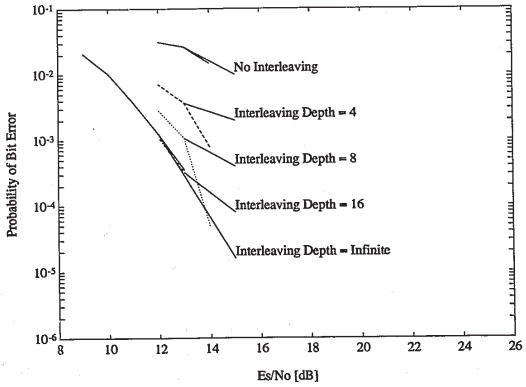

Figure 4.22: Error Performance curves generated by simulation of the Reed-Solomon Signal Space Curves in Correlated Fading; Fading BT product of 0.08; Code is [14,7,8] Reed-Solomon code on a field of 16 elements mapped to 16-QAM

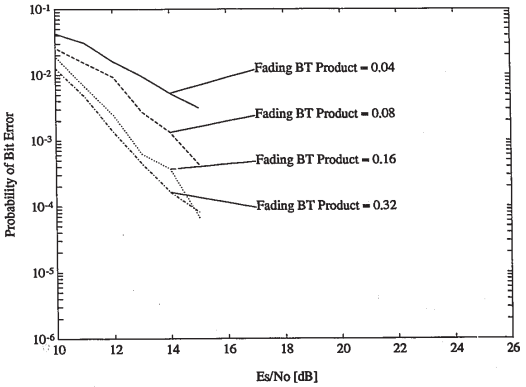

Figure 4.23: Error Performance curves generated by simulation of the Reed-Solomon Signal Space Curves in Correlated Fading; Interleave Depth of 4; Code is [14,7,8] Reed-Solomon code on a field of 16 elements mapped to 16-QAM

Chapter 5

Joint Channel Estimation and Decoding

The simulations and analysis thus far have dealt with a communications channel in which the fading process is known to the receiver. In this chapter, we turn our attention to the problem of estimating the fading process for use in the decoder.

An algorithm for channel estimation is discussed in section 5.1. The process of channel estimation is based on the insertion of periodic known symbols into the transmitted symbol sequence. The performance of the channel estimator will then be discussed in the next section. Finally, in section 5.3 simulation results of joint channel estimation and Reed-Solomon decoding will be presented.

5.1 Channel Estimation

The channel model used throughout this chapter is again the correlated Rayleigh fading channel. However, the receiver does not have access to the fading process. If the receiver uses knowledge of the fading process for purposes of decoding, then it must estimate this from the received information bearing signal. The approach used here is to insert periodic symbols in the transmitted symbol sequence, to be used solely for the purposes of estimating the fading process. These extra symbols in the transmitter sequence bear no additional user information, and therefore, they will

reduce the rate of transmission through the channel. It is desirable then to insert these extra symbols as infrequently as possible to maintain the channel throughput. The channel estimator developed here was not developed by optimizing any design criteria. Channel estimators based on maximum likelihood techniques will likely result in a better channel estimator in terms of mean squared error. The channel estimation technique presented here offers low complexity while generating channel estimates that are useful to the decoder.

The extra symbols in the symbol sequence will be referred to as training symbols. The period at which these symbols are inserted into the symbol sequence will be referred to as the training period. The energy devoted to these symbols is the same as the average energy of information bearing symbols. Therefore, if the transmitter signal constellation is of the PSK type with symbol energy 1, then the energy allocated to the training symbols is also 1. In the case of an AMPM transmitter signal set, the energy allocated to the training symbols is the average signal energy of the signal set being used. For the 8-AMPM or 16-QAM signal set with the in-phase and quadrature levels at the $\pm 1, \pm 3$ values, the energy of the training symbols is 10.

The receiver is assumed to have timing synchronization. That is, both symbol synchronization and block synchronization are known. With knowledge of the transmitter symbols at the training positions and the actual received symbol sequence, the receiver will estimate the fading process values at the training positions. This estimate is calculated as the quotient of the received symbol value divided by the transmitted symbol.

$$\hat{a}_i = \frac{R_i}{T_i} \qquad \text{At training symbols} \tag{5.1}$$

The estimate of the fading process for the remainder of the received symbol sequence is initially estimated by interpolating from the fading estimates at the training symbols. The initial estimates of the fading process are used for performing a hard decision estimate of the transmitted symbol sequence. The initial estimate of the fading process is then updated using the hard decision estimates of the transmitter sequence. Following this, the received symbol sequence and the updated estimate of the fading process is de-interleaved and the training symbols are removed. The updated estimate of the fading process is used in the decoder for performing soft decision decoding of

the Reed-Solomon signal space code.

The interpolation that is used to form the initial estimates of the fading process is a simple quadratic interpolation. Figure 5.1 shows how the initial estimate of a specific symbol is formed. Assume that the symbol in which the initial estimate of the fading is to be estimated is positioned between training symbols at time t and at time $t + T_{Tr}$ where T_{Tr} is the period of the training symbols. If T is the symbol period of the communications system there will be $\frac{T_{Tr}-T}{T}$ channel symbols between the two training symbols. Further, assume that we wish to estimate the fading of the i'th symbol following the training symbol at time t. The initial estimate of the fading at this symbol is formed by averaging two quadratic interpolations. The first interpolation is formed using the training symbols at positions $t-T_{Tr}$, t, and $t+T_{Tr}$. The second quadratic interpolation made using the symbols positioned at times, t, $t+T_{Tr}$ and $t+2T_{Tr}$. A quadratic polynomial is fit to the three estimated fading values at the three training symbols for both the real and imaginary components of the fading process. The interpolated value is this polynomial evaluated at time corresponding to the i'th symbol following the training symbol at time t. This interpolation is performed for each symbol in the received symbol sequence. The sequence of these interpolated fading estimates form the initial estimate of the fading process. We will denote an element of the initial fading estimate as $\hat{a}_{i_1}$, where i is the symbol number and 1 is the first estimate of the fading.

The initial estimate of the fading process is used to obtain a hard decision estimate for each symbol in the received sequence of symbols. The hard decision estimates are made by assuming the initial estimate of the fading process to be the true fading process and then performing a hard decision decoding independently on each of the symbols in the received sequence of symbols. For each symbol in the sequence, the hard decision estimates are the transmitted symbol with the highest probability of being the actual transmitted symbol given the received symbol and the fading estimate for that symbol. This is the closest possible transmitter signal point to the received symbol in the Euclidean distance sense. These estimates are made independently of channel coding.

Finally, the sequence of hard decision estimates is used to form an updated

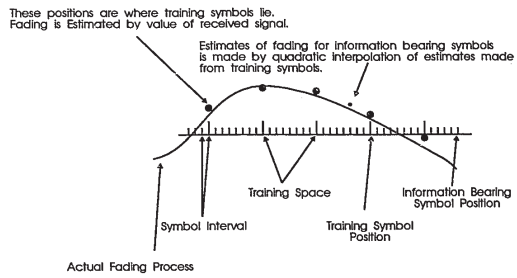

Figure 5.1: Interpolation used to form initial estimate of the fading process from the received symbols at the training symbols

estimate of the fading process. The hard decision estimates will almost certainly contain errors. These errors are in general due to two factors. One is that the initial estimate of the fading process is such that the fade corrected symbol is either scaled or rotated so that the original transmitted symbol is closer to another element than to the transmitted one. The other is that the Gaussian noise causes the symbol error. In both cases, the probability of these events occurring is greater when the magnitude of the fading, $|a_i|$ is small. We will therefore assume that the reliability of the hard decisions is directly proportional to the magnitude of the fading process. The errors that are due to Gaussian noise are independent of one other. Since we wish to improve the estimate of the fading process, and since the fading is highly correlated between symbols, the correction on the fade estimate for a given symbol will be based on the hard decisions of three symbols. The three symbols used to form a correction on symbol i are the symbol itself and the symbols that are immediately before and after symbol i.

The correction to the initial estimate of the fading is made by assuming that

the hard decision estimates for the channel symbols are correct and then estimating the value of fading which would result in the observed received symbol. This calculation is similar to equation 5.1 with the hard decision estimate of the transmitted symbol used instead of the known transmitted symbol.

$$\hat{a}_{i_2} = \frac{R_i}{\hat{T}_i} \qquad \text{At information symbols} \tag{5.2}$$

Denote this estimate of the fading as $\hat{a}_{i_2}$, where the subscript 2 denotes second estimate of the fading. This second estimate of the fading process will be a better estimate of the actual fading process if the hard decisions of the transmitted symbol sequence are correct. Since the hard decisions contain errors, the final estimate of the fading process that will be used in the soft decision decoder is a combination of the initial and the second estimates of the fading process. The correction to the initial estimate is based on the fading estimate of the preceding symbol, the symbol being updated and the following symbol. The final estimate of the fading process is formed by

$$\hat{a}_{i_f} = \hat{a}_{i_1} + \rho_i \left(\frac{\hat{a}_{i-1_2} + \hat{a}_{i_2} + \hat{a}_{i+1_2}}{3} - \hat{a}_{i_1} \right) \tag{5.3}$$

where ρ_i is a scaling factor that reflects the reliability of the hard decisions. If the fading magnitude is large, we wish ρ_i to take a value close to unity, and if the fading magnitude is small, then ρ_i should be close to zero. The value used is based on the magnitude of the initial estimate of the fading process and is calculated as

$$\rho_i = \left[1 - exp(-|\hat{a}_{i_1}|^2) \right]^2 \tag{5.4}$$

The expression inside the square brackets is the cumulative density function of a Rayleigh distributed variable and hence will have a value between 0 and 1. The squaring of the expression emphasizes the correction more when the fading magnitude is large. The inclusion of the channel fading process estimator adds some complexity to the receiver. However this added complexity is marginal compared to the computational effort required in decoding.

5.2 Performance of the Channel Estimator

The accuracy of the fading process estimator is extremely important to the overall code performance. This is because any errors in the estimation of the fading will tend to rotate and scale the received signal set with respect to the transmitted signal set, often resulting in an altering of the distance properties of the code. In the presence of large errors in the estimation of the fading process, an error in decoding may result even if the additive Gaussian noise is at a low power level. In this section, we will present some results on the performance of the fading process estimator described in the previous section.

5.2.1 Varying the Training Period

Figure 5.2 shows the typical performance of the fading process estimator when the training period is 4 symbols. The fading is correlated complex Gaussian multiplicative fading with time-bandwidth product of 0.08 and the average receiver signal to noise ratio is set to 15dB. The curves shown are the true fading process and the final estimate to the fading process. Only the inphase component of the fading process is shown. The quadrature component of the fading is similar to that shown in figure 5.2. The results show that the fading process estimator performs well, especially when the magnitude of the fading process is large. Good estimates of the fading process when its magnitude is large are desirable in conjunction with the soft decision decoding algorithm. This is because the decoder chooses the fading parameters with the largest magnitude to construct the regeneration set.

Figure 5.3 shows the mean square estimation error as a function of signal to noise ratio for the fading estimator. The time-bandwidth product of the channel fading process in these simulations was set to 0.08 and the training period was fixed at 4. The simulations show that the estimator generates good estimates for all signal to noise ratios. The mean squared error is larger when the signal to noise ratio is lower because of the randomness of the noise and because the hard decisions of the transmitted sequence have a higher error rate. Simulations that show the effect of increasing the training period are shown in figure 5.4. In these simulations, the channel

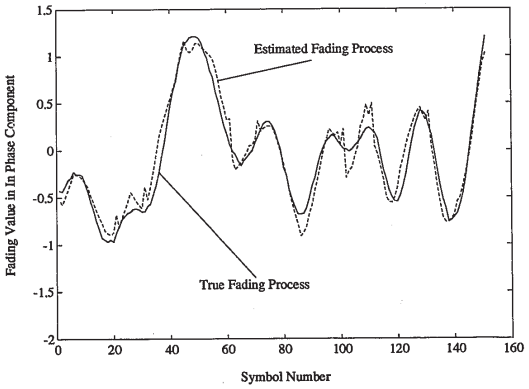

Figure 5.2: Performance of fading process estimator with training period of 4 symbols and estimating a 16-QAM signal set at 15dB average signal to noise ratio with a fading time-bandwidth product of 0.08

Training Period	Average S/N Ratio	Mean Squared Estimation Error
4	10	0.04297
4	15	0.01221
4	20	0.00428
6	10	0.04086
6	15	0.01382
6	20	0.00650
8	10	0.05280
8	15	0.02483
8	20	0.01600
10	10	0.05986
10	15	0.03679
10	20	0.02867

Table 5.1: Mean Squared Estimation Errors of the Fading Process Estimator with Different Training Periods; Fading Time-Bandwidth product is 0.08 and Average Receiver Signal to Noise Ratio is 15dB

fading time bandwidth product were fixed at 0.08 and the receiver signal to noise ratio was set to 15dB. The training period of the estimator was then varied. In all cases the channel signal set used is the 16-QAM signal set. The estimator's performance suffers with increasing training periods. This is because the quadratic interpolator cannot sufficiently generate an initial estimate of the fading process that results in reliable hard decision estimates of the transmitted symbol sequence. The result is that the performance of the estimator with larger training periods does not generate as high a quality estimate as the estimator with lower training periods. Table 5.1 summarizes the means squared estimation errors of the fading process estimator for different signal to noise ratios and for different training periods. All results listed in the table use correlated fading with a time-bandwidth product of 0.08 and a use the 16-QAM channel signal set.

5.2.2 Performance with different Channel signal Sets

Simulations were performed to test whether the channel signal set made a difference on the performance of the estimator. Figure 5.5 shows the mean squared estimation

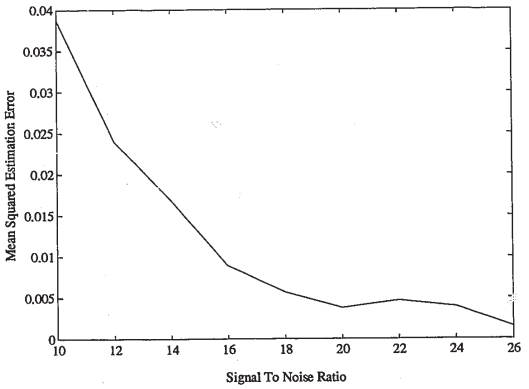

Figure 5.3: Mean Squared Estimation Errors of Fading Process Estimator with Training Period of 4 symbols and Estimating a 16-QAM Signal Set with a fading time-bandwidth product of 0.08

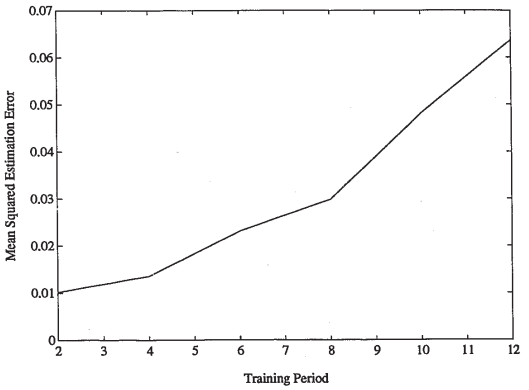

Figure 5.4: Mean Squared Estimation Errors of Fading Process Estimator Estimating a 16-QAM Signal Set at 15dB average signal to noise ratio and a fading time-bandwidth product of 0.08

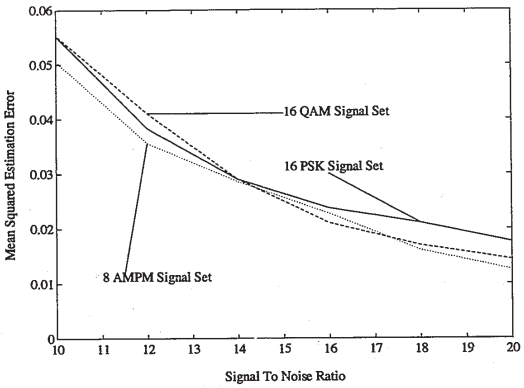

Figure 5.5: Mean Squared Estimation Errors of Fading Process Estimator with Training Period of 4 symbols and a channel fading time-bandwidth product of 0.08

errors of the fading process estimator when the channel signal set is changed. The simulation used correlated fading with a fading time-bandwidth product of 0.08 and an average receiver signal to noise ratio of 15dB. The results show that there is little benefit to using a channel signal set with a smaller number of elements. There is also little difference in the performance of the estimator if the signal set is changed from the popular PSK signal set to the AMPM signal set with the same number of elements.

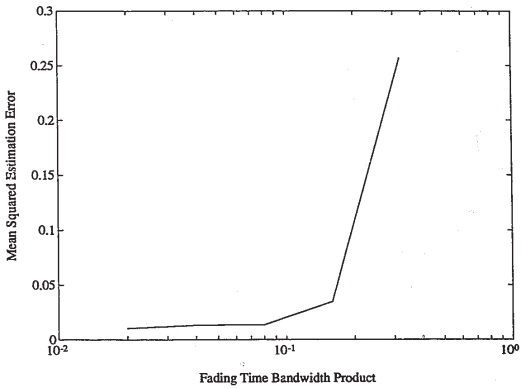

Figure 5.6: Mean Squared Estimation Errors of Fading Process Estimator with Training Period of 8 symbols and Estimating a 16-QAM Signal Set at 15dB average signal to noise ratio

5.2.3 Varying the Fading Time-Bandwidth Product

When the fading time-bandwidth product is smaller, the fading process is slower and we would expect that the problem of channel estimation be easier. This was observed in the simulations. The simulations performed used the 16-QAM channel signal set with a training period of 8 symbols and an average channel signal to noise ratio of 15dB. The fading time-bandwidth product of the fading process was varied and the mean squared estimation errors of the fading process estimator was observed. the results are shown in figure 5.6. The estimator performed better when the correlation of the fading process increased.

5.3 Simulation Results

The simulations presented in this section perform joint fading process estimation and decoding. The channel model used is the correlated Rayleigh fading channel. The receiver must recover the bit sequence that was put into the transmitter with knowledge of only the received sequence of symbols. The fading process parameters that the decoder requires to perform decoding must be estimated from the information bearing signal. The channel estimation technique is aided by the use of periodic training symbols inserted into the transmitter symbol sequence. A full description of the estimation technique is given in section 5.1. Comparisons are made to simulations in which the fading was independent, and where the receiver has perfect knowledge of the fading process.

5.3.1 Effect on Code Performance with Joint Fading Estimation

Figure 5.7 shows the performance of the [14,7,8] Reed-Solomon signal space code with a channel signal set of 16-QAM for a interleaving depth of 8 symbols. Different error rate curves were generated for different values of training periods. The channel fading time-bandwidth product used for these simulations was set to 0.08. The results show that the additional requirement on the receiver to estimate the fading process does not degrade the performance of the codes significantly.

5.3.2 Degradation in Total System Performance with Training Symbols and Fading Process Estimation

The addition of training symbols into the transmitter symbol sequence reduces the rate of communication on the channel. With the use of Reed-Solomon signal space codes or Bose-Chauduri-Hocquenghem signal space codes, one may easily restore the original rate of communication on the channel by using a higher rate algebraic code in code construction. If the training period of the channel estimator algorithm were X symbols, then the rate of the original code must be increased by a factor of $\frac{X+1}{X}$

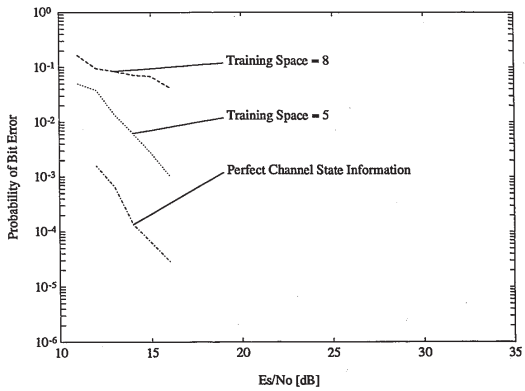

Figure 5.7: Error Performance curves generated by simulation of the Reed-Solomon Signal Space Curves in Correlated Fading with Joint Channel Estimation; [14,7,8] Reed-Solomon code on a field of 16 elements mapped to 16-QAM

to maintain the original channel throughput without training symbols. If there is a desired fixed channel throughput, then there will be a tradeoff between having a more powerful code and having better channel fading estimates. A high value for the training period will allow a very powerful code to be used for the transmission of information, but the imperfect fading estimates will cause the decoder to make more error. When a small value is used for the training period, then the use of a higher rate code is necessary to compensate for the training symbols.

The simulation presented here use Reed-Solomon signal space codes whose code rates have been adjusted to compensate for the insertion of the training symbols. The results for systems where the final throughput of the system is 2 bits per channel symbol are given in figures 5.8. In figure 5.8, the codes are Reed-Solomon signal space codes that exist on a field of 16 elements and have been mapped to the 16-QAM signal set. The algebraic code used to construct the codes and the training periods used are shown in the figure for each code. The fading time-bandwidth product for each simulation is identical and is set to 0.08. Results indicate that with Reed-Solomon codes and the method of fading process estimation discussed in section 5.1, we can expect to achieve an error rate of 10^{-2} at 15dB average channel symbol energy to noise ratio.

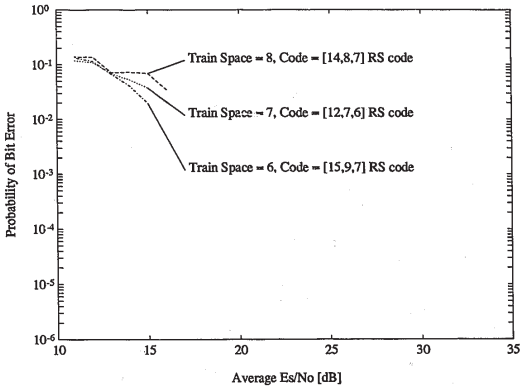

Figure 5.8: Error Performance curves of Systems with Joint Channel estimation and Decoding; 2 Bits per Channel Symbol Spectral Efficiency; Reed-Solomon Codes on GF(16)

Chapter 6

Conclusions

In this chapter, we will review the major results of the thesis. We will also discuss some potential areas of further research and introduce other related research problems.

6.1 Summary of main results

The major results of this thesis are the design and evaluation of a class of block codes that efficiently signal binary information through a fading communications channel and the development of a soft decision decoding technique that decodes these codes. Previous attempts at the design of block codes for the use in the Rayleigh fading channel have resulted in pessimistic results [23, 13]. This work is the first that uses a block coding scheme to signal in a fading channel whose performance in terms of channel bit error rate rivals that of the best trellis codes published. The previous attempts at using block codes for communicating in the Rayleigh fading channel did not investigate soft decision decoding and therefore could not take advantage of the power of block codes as a form of reliable communication.

The soft decision decoding algorithm for the decoding of Reed-Solomon signal space codes operating in a fading environment performs very well as compared to maximum likelihood decoding. Furthermore, the analysis of the decoding procedure and the subsequent bounding of the error probability of the decoding give more insight into the fading channel itself.

This thesis also develops some design criteria for use in the design and analysis of block codes to be used in the Rayleigh fading channel. The analysis leading to the design criteria also provides further insight into the effects of Rayleigh fading on an information bearing signal.

Other contributions of this work are the results on the performance of Reed-Solomon signal space codes in the presence of correlated fading and in the presence of a channel estimator. These studies suggest that the assumptions leading to the design of the Reed-Solomon signal space codes are valid. They also show that the performance of the Reed-Solomon signal space codes is not seriously degraded in the presence of correlated fading or when the estimates of the channel fading process that is required by the decoder are imperfect. Another result from the study on the channel estimator is that the use of a QAM type signal constellation does not prevent the channel estimator from generating useful estimates of the channel fading process. Most code design for use on the Rayleigh channel to date assumes the use of a PSK type channel signal set.

6.2 Suggestions for Further Research

The greatest potential improvement of the Reed-Solomon block coding signalling scheme for use in the Rayleigh fading channel is in the soft decision decoding algorithm. If a decoding algorithm that is extremely efficient at finding the maximum likelihood transmitter codeword could be found, the Reed-Solomon signal space codes could find use in many applications where fast multipath fading is present. The algorithm introduced in this thesis considerably reduces the number of codewords that are candidates as the transmitted codeword. However, when a powerful code is used, the number of codewords that remain in the decoder search is still formidable. It would be desirable to have an algorithm that is capable of decoding the more powerful Reed-Solomon signal space codes so that more of their potential can be realized.

Another area of great interest would be the development of a soft decision decoding algorithm for the Bose-Chauduri-Hoquenghem signal space codes. If a soft decision decoding scheme for these codes were available, these codes could offer tremendous coding gain as compared to all known signalling schemes for signalling through the Rayleigh fading channel. If a general soft decision decoding scheme for BCH codes could be found, then the BCH signal space codes could find use in many other channels, including the additive white Gaussian noise channel.

A possible area of investigation is the decoding of either the Reed-Solomon codes or the BCH codes on extension fields of the symbol field of the code. This may be especially attractive for BCH codes since the roots of the generator polynomial exist on extension fields of the symbol field. The received signal point for each symbol would be hard quantized to one element of the extension field. For example, in a code where the symbol field contains 8 elements, the received signal for each symbol in the block of the code would be quantized to one of 512 (a possible extension field of the 8 element field) possible values. It is possible to overlay a 512 element signal constellation over a 8 element signal constellation so that the 8 elements of the symbol field correspond to the 8 subfield elements of the 512 element field and the other elements in the 512 point constellation lie in an identical pattern around a subfield element. Algebraic decoding would then be performed to complete decoding. The received symbols in a block would be viewed as a polynomial in the extension field. If there were no errors in transmission, this polynomial would necessarily have roots in the locations of the roots of the generator polynomial. Furthermore, it would also contain roots in the locations of the conjugates of all the roots in the generator polynomial. Therefore, a number of equations involving the received quantized symbols could be written. If a unique solution to this set of equations could be found that results in a codeword with elements in the channel symbol field, then we would have an algebraic decoder that can perform soft decision decoding. This type of decoder would have the advantage that it only performs arithmetic on a Galois field and that it has a finite and fixed number of computations to perform.

Other avenues of interest are the investigation and development of a better method of channel estimation. The estimation investigated in this thesis was only

performed to verify the feasibility of channel estimation for use with decoding and to verify that the QAM signal set format is compatible with correlated channel fading estimation. Detection and estimation theory may be used to develop a good channel estimator that does not require the periodic training symbols that the estimation technique used in this thesis requires. Also, performance limits on channel estimation for the correlated Rayleigh channel need to be evaluated and used as benchmarks in developing channel estimation strategies.

Appendix A

Galois Field Theory

A field is a set of numbers where you can add, subtract, multiply and divide. The most common field is the field of rational numbers. Another example is the field of complex numbers. The set of integers is not a field because under normal division, the result is not in the set of integers. The above examples have an infinite number of elements in the field. Galois fields are fields with a finite number of elements and are often referred to as finite fields.

Formally, a field, F is a set with with two operations, "+" and ".", called addition and multiplication, such that

1. F is an Abelian group under "+", with an identity element 0.
2. The nonzero elements of F are an Abelian group under ".".
3. The distributive law, $a \cdot (b + c) = a \cdot b + a \cdot c$, holds.

The set of integers modulo p will always form a field under normal arithmetic when p is a prime number. We will denote these prime finite fields as

$$GF(p) = \{0, 1, \ldots, p-1\} \qquad \text{arithmetic mod } p \tag{A.1}$$

There are other finite fields however. There also exist finite fields that have p^n elements, where p is a prime and n is an integer. These finite fields will be denoted as $GF(p^n)$. Moreover, these fields will always contain the elements of $GF(p)$ and

are referred to as extension fields of $GF(p)$. There are no other finite fields. Extension fields can be constructed from the prime fields. Before we give the construction technique we must discuss a little about Euclidean domains.

An integral domain is a set D, with two operations, "+" and ".", called addition and multiplication, such that

1. D is an Abelian group under addition with an identity element 0.
2. Multiplication is associative and commutative, and has an identity element called 1.
3. The cancellation law holds. If $ab = ac$ and $a \neq 0$, then $b = c$.
4. The distributive law, $a \cdot (b + c) = a \cdot b + a \cdot c$, holds.

A Euclidean domain is an integral domain that has a concept of size among its components. The size of an element a is denoted $g(a)$, is a non-negative integer such that

$$g(a) \leq g(a \cdot b) \tag{A.2}$$

where a, b are elements of the Euclidean domain, and for all $a, b \neq 0$ there exist a quotient q and a remainder r, such that

$$a = qb + r \qquad \text{with } g(r) < g(b) \tag{A.3}$$

The remainder may be zero. Examples of Euclidean domains are the set of integers where $g(a) = |a|$, or the set of polynomials, $f(x)$ over a field F where $G(f(x)) =$ degree(f).

With any finite number of elements of a Euclidean domain, D, there exists a greatest common divisor. The greatest common divisor, denoted

$$d = \gcd(b_1, b_2, \ldots, b_n) \tag{A.4}$$

is the element which divides into all the elements $(b_1, b_2, \ldots, b_n)$ and which itself can be divided by all the other common divisors of $(b_1, b_2, \ldots, b_n)$. Furthermore this greatest common divisor can be written as a linear sum of the b_i's.

$$d = \sum_{i=1}^{n} \mu_i b_i \qquad \mu_i \in D \tag{A.5}$$

An element in the Euclidean domain can be factored if it can be written as

$$b = a_1 a_2 \cdots a_r \tag{A.6}$$

An element in D is considered to be a unit, u, if it divides into 1. In the set of integers, the units are the elements ± 1. In the set of polynomials over a field, the units are polynomials of degree zero. Two elements a, b are called associates if $a = ub$ for some unit u. The element p in D is considered to be prime if all possible factorizations of p result in

$$p = a_1 a_2 \cdots a_r \tag{A.7}$$

where each of the a_i's is either a unit or an associate of a. The primes of the Euclidean domain of the integers are well known and are simply called the prime numbers. There exists at least one prime polynomial of every degree over the fields $GF(q)$.

Now we are able to introduce the construction for the extension fields. If p is a prime in the Euclidean domain D, then

$$D \bmod p \tag{A.8}$$

is a field. Note that the prime fields can also be constructed with this definition, by choosing $D = Z$, the set of integers, and p being any prime number.

To construct extension fields from the prime finite fields, let the Euclidean domain be,

$$D = F_p(x) \tag{A.9}$$

where x is the indeterminate, and $F_p(x)$ denotes the set of polynomials with coefficients in the prime field $GF(p)$. Furthermore, let and the prime of the Euclidean domain being be a prime polynomial over the field $GF(p)$. With this construction, it is possible to construct every extension field.

It is instructive at this point to give an example of the construction of an extension field. Choose $GF(2)$ as the prime field. Then D is the set of polynomials with coefficients in $GF(2)$. If we choose $p(x) = x^3 + x + 1$ as the irreducible polynomial, then all polynomials modulo $p(x)$ will result in the set of polynomials of the form $a_2x^2 + a_1x + a_0$, with coefficients in the field $GF(2)$. These polynomials

+	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

Table A.1: Addition table for $GF(2^3)$.

are representatives of the 8 field elements of this field which is denoted $GF(2^3)$. A simpler representation is to use the coefficients $a_2a_1a_0$ as a representation of the field elements. The addition table for this field can then be filled. The addition table is given in table A.1.

The multiplication of the 8 field elements is found by multiplying the coefficients of the polynomials representing the field elements.

$$\begin{aligned}(a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0) &= a_2b_2x^4 + (a_2b_1 + a_1b_2)x^3 \\ &+ (a_2b_0 + a_1b_1 + a_0b_2)x^2 \\ &+ (a_1b_0 + a_0b_1)x + a_0b_0 \end{aligned} \tag{A.10}$$

This polynomial must be reduced modulo $p(x)$. We can eliminate the third and fourth degree terms by substituting

$$x^3 \equiv x + 1 \pmod{x^3 + x + 1} \tag{A.11}$$

$$x^4 \equiv x^2 + x \pmod{x^3 + x + 1} \tag{A.12}$$

Substituting and simplifying results in a polynomial $c_2x^2 + c_1x + c_0$ whose coefficients are

$$c_2 = a_2b_2 + a_2b_0 + a_0b_2 \tag{A.13}$$

$$c_1 = a_2b_2 + a_2b_1 + a_1b_2 + a_1b_0 + a_0b_1 \tag{A.14}$$

$$c_0 = a_2b_1 + a_1b_2 + a_0b_0 \tag{A.15}$$

·	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	010	101	110	111	000	001
011	000	011	101	110	111	000	001	010
100	000	100	110	111	000	001	010	011
101	000	101	111	000	001	010	011	100
110	000	110	000	001	010	011	100	101
111	000	111	001	010	011	100	101	110

Table A.2: Multiplication table for $GF(2^3)$.

The multiplication table for $GF(2^3)$ is shown in table A.2.

There is another way to represent the components of a finite field that simplifies multiplication. If we calculate the first several powers of the element, α, corresponding to the polynomial x, we get

$$\alpha^0 = 1 \tag{A.16}$$

$$\alpha^1 = \alpha \tag{A.17}$$

$$\alpha^2 = \alpha^2 \tag{A.18}$$

$$\alpha^3 = \alpha + 1 \tag{A.19}$$

$$\alpha^4 = \alpha^2 + \alpha \tag{A.20}$$

$$\alpha^5 = \alpha^2 + \alpha + 1 \tag{A.21}$$

$$\alpha^6 = \alpha^2 + 1 \tag{A.22}$$

$$\alpha^7 = 1 \tag{A.23}$$

The first seven powers of α are all distinct. However, there are only seven nonzero elements in this field. Therefore, every nonzero element in the field is a power of the element, α. This element, called a primitive element can be used as a base for a log type function with the convention

$$\log_\alpha(\beta) = k \qquad \text{means } \alpha^k = \beta. \tag{A.24}$$

Every extension field contains at least one primitive element [12]. Then if we wish to

β	$\log_\alpha(\beta)$	k	α^k
000			000
001	0	0	000
010	1	1	010
011	3	2	100
100	2	3	011
101	6	4	110
110	4	5	111
111	5	6	101

Table A.3: Logarithm and Anti-logarithm for $GF(2^3)$.

multiply two nonzero elements

$$c = a \cdot b \tag{A.25}$$

$$\log_\alpha(c) = [\log_\alpha(a) + \log_\alpha(b)] \bmod q - 1 \tag{A.26}$$

where q is the number of elements in the field. Note that exponents can be reduced mod $q - 1$ because for every primitive element $\alpha^{q-1} = 1$. Continuing again with the example on $GF(2^3)$, we can generate a table of logarithms and anti-logarithms for performing arithmetic on this field. This is given in table A.3

Such a table can be generated for every finite field. Addition and multiplication can then be computed easily on that field. We have already stated that there exists a finite field with $q = p^n$ elements for every prime p and any integer. In fact, there exists only one field for each p and n. The only difference may be in the way the elements are labeled.

Appendix B

Decoding of Reed-Solomon Codes

The decoding of Reed-Solomon algebraic codes is performed in the same way as decoding for BCH codes. The decoder for decoding BCH codes presented here was developed for binary codes by Peterson [19]. Gorenstien and Zierler generalized his results [9]. The decoding algorithm presented here is often called the Peterson-Gorenstien-Zierler decoder. It should be noted that by developing a decoder for BCH codes, an explicit proof of their distance properties follows.

Let $\mathcal{C}$ be a BCH code on a field $GF(q)$, designed to correct up to t errors. Suppose the code was constructed with the primitive element α. The error polynomial of the code is

$$e(x) = e_{n-1}x^{n-1} + e_{n-2}x^{n-2} + \cdots + e_1 x + e_0 \tag{B.1}$$

where at most t coefficients are non-zero. If there were actually v errors, where $0 \le v \le t$, in locations $i_1, i_2, \ldots, i_v$, then the error polynomial can be written as

$$e(x) = e_{i_1}x^{i_1} + e_{i_2}x^{i_2} + \cdots + e_{i_v}x^{i_v} \tag{B.2}$$

The syndromes are calculated by evaluating the received polynomial at the zeros of the generator polynomial or at the first t powers of α.

$$\begin{aligned} S_j &= v(\alpha^j) && \text{(B.3)}\\ &= c(\alpha^j) + e(\alpha^j) && \text{(B.4)}\\ &= e(\alpha^j) && \text{(B.5)}\\ &= e_{i_1}\alpha^{ji_1} + e_{i_2}\alpha^{ji_2} + \cdots + e_{i_v}\alpha^{ji_v} && \text{(B.6)} \end{aligned}$$

For the purpose of simplifying the notation, let Y_l be the magnitude of the error in the l'th location and let $X_l = \alpha^{i_l}$ be the field element that we will associate with the error position, i_l. Y_l is called the error magnitude and X_l is called the error location number. The error location numbers will all be distinct since α is a primitive element and hence has order n. With these definitions, the syndrome equations can be written as

$$\begin{aligned} S_1 &= Y_1X_1 + Y_2X_2 + \cdots + Y_vX_v\\ S_2 &= Y_1X_1^2 + Y_2X_2^2 + \cdots + Y_vX_v^2\\ S_3 &= Y_1X_1^3 + Y_2X_2^3 + \cdots + Y_vX_v^3\\ &\vdots \quad \vdots\\ S_{2t} &= Y_1X_1^{2t} + Y_2X_2^{2t} + \cdots + Y_vX_v^{2t} \end{aligned} \tag{B.7}$$

which in matrix form is

$$\begin{bmatrix} X_1 & X_2 & X_3 & \cdots & X_{v-1} & X_v\\ X_1^2 & X_2^2 & X_3^2 & \cdots & X_{v-1}^2 & X_v^2\\ X_1^3 & X_2^3 & X_3^3 & \cdots & X_{v-1}^3 & X_v^3\\ \vdots & & & & \vdots & \\ X_1^{2t} & X_2^{2t} & X_3^{2t} & \cdots & X_{v-1}^{2t} & X_v^{2t} \end{bmatrix} \begin{bmatrix} Y_1\\ Y_2\\ Y_3\\ \vdots\\ Y_v \end{bmatrix} = \begin{bmatrix} S_1\\ S_2\\ S_3\\ \vdots\\ S_{2t} \end{bmatrix} \tag{B.8}$$

The decoder must solve for the $2v$ unknowns with these $2t$ simultaneous equations.

In order to solve for these equations, it is instructive to introduce an error locator polynomial, $\Lambda(x)$, whose zeros are the at the inverse locations of the error location numbers.

$$\begin{aligned} \Lambda(x) &= (1 - xX_1)(1 - xX_2)\cdots(1 - xX_v) && \text{(B.9)}\\ &= \Lambda_v x^v + \Lambda_{v-1}x^{v-1} + \cdots + \Lambda_1 x + 1 && \text{(B.10)} \end{aligned}$$

If we evaluate this error locator polynomial at the inverse locations of the errors we get

$$\Lambda(X_l^{-1}) = \Lambda_v X_l^{-v} + \Lambda_{v-1}X_l^{-(v-1)} + \cdots + \Lambda_1 X_l^{-1} + 1 \tag{B.11}$$

The left side of equation B.11 is equal to zero because of the way the polynomial is defined. If we multiply the left side of the equation by $Y_lX_l^{j+v}$, this results in

$$0 = Y_l\left(\Lambda_v X_l^j + \Lambda_{v-1}X_l^{j-1} + \cdots + \Lambda_1 X_l^{j+v-1} + X_l^{j+v}\right) \tag{B.12}$$

Now, this holds for all l and all v. If we sum up equation B.12 from $l = 1$ to $l = v$ we get

$$0 = \sum_{l=1}^{v} Y_l\left(\Lambda_v X_l^j + \Lambda_{v-1}X_l^{j-1} + \cdots + \Lambda_1 X_l^{j+v-1} + X_l^{j+v}\right) \tag{B.13}$$

which can be rewritten as

$$\begin{aligned} 0 &= \sum_{l=1}^{v} Y_l\Lambda_v X_l^j + \sum_{l=1}^{v} Y_l\Lambda_{v-1}X_l^{j-1} + \cdots + \sum_{l=1}^{v} Y_l\Lambda_1 X_l^{j+v-1} + \sum_{l=1}^{v} Y_l X_l^{j+v}\\ &= \Lambda_v S_j + \Lambda_{v-1}S_{j-1} + \cdots + \Lambda_1 S_{j+v-1} + S_{j+v} \end{aligned} \tag{B.14}$$

because the summations are just the syndromes defined in equation B.7. B.14 is valid for $1 \le j \le v$ because there are $2t$ syndromes and we are assuming that $v \le t$. Therefore we have a set of equations, which can be written in matrix form as

$$\begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_{v-1} & S_v\\ S_2 & S_3 & S_4 & \cdots & S_v & S_{v+1}\\ S_3 & S_4 & S_5 & \cdots & S_{v+1} & S_{v+2}\\ \vdots & & & & & \vdots\\ S_v & S_{v+1} & S_{v+2} & \cdots & S_{2v-2} & S_{2v-1} \end{bmatrix} \begin{bmatrix} \Lambda_v\\ \Lambda_{v-1}\\ \Lambda_{v-2}\\ \vdots\\ \Lambda_v \end{bmatrix} = \begin{bmatrix} -S_{v+1}\\ -S_{v+2}\\ -S_{v+3}\\ \vdots\\ -S_{2v} \end{bmatrix} \tag{B.15}$$

If the matrix of syndromes on the left hand side of equation B.15 has a non-zero determinant, then the matrix of syndromes can be inverted. This is in fact the case and therefore the error locator polynomial can be determined by solving for the system of equations defined by equation B.15. The actual location of the errors can be found by finding the zeros of the error locator polynomials. One simple method for doing this is to evaluate the error locator polynomial at different field elements until the v error locations are found. This is usually not a computational problem because the number of elements in the field is finite. With knowledge of the location of the errors equation B.8 can then be solved because the first v rows of the matrix forms a system of linear equations. The only problem remaining is to determine the actual number

of errors that occurred. This information can also be determined by examination of the matrix of syndromes. The matrix

$$M = \begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_{\mu-1} & S_\mu\\ S_2 & S_3 & S_4 & \cdots & S_\mu & S_{\mu+1}\\ S_3 & S_4 & S_5 & \cdots & S_{\mu+1} & S_{\mu+2}\\ \vdots & & & & & \vdots\\ S_\mu & S_{\mu+1} & S_{\mu+2} & \cdots & S_{2\mu-2} & S_{2\mu-1} \end{bmatrix} \tag{B.16}$$

will have a zero determinant when $\mu > v$ [3]. Therefore, the number of errors can be determined by letting $\mu = t$ and evaluating the determinant of the matrix of syndromes, M. If the determinant is zero, reduce the value of μ by 1 and recalculate M. This process can be repeated until the matrix M has a non-zero determinant and the number of errors is determined as $v = \mu$. The decoding algorithm can be summarized as follows:

1. Enter $v(x)$, the received polynomial
2. Compute the syndromes
   $S_j = v(\alpha^j)$ for $j = 0, \ldots, 2t-1$
3. Let $v = t$
4. Generate the syndrome matrix
   $\mathbf{M} = \begin{bmatrix} S_1 & \cdots & S_v\\ \vdots & & \vdots\\ S_v & \cdots & S_{2v-1} \end{bmatrix}$
5. Calculate the determinant of $\mathbf{M}$
6. If $\det(\mathbf{M}) = 0$ then let $v = v - 1$ and goto step 4

7. Calculate the error locator polynomial as
$$\begin{bmatrix} \Lambda_v \\ \Lambda_{v-1} \\ \vdots \\ \Lambda_1 \end{bmatrix} = \mathbf{M}^{-1} \begin{bmatrix} -S_{v+1} \\ -S_{v+2} \\ \vdots \\ -S_{2v} \end{bmatrix}$$

8. Find the locations of the errors, $X_1, \cdots X_v$, by finding the zeros of $\Lambda(x)$

9. Calculate the error values by
$$\begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_v \end{bmatrix} = \begin{bmatrix} X_1 & X_2 & \cdots & X_v \\ X_1^2 & X_2^2 & \cdots & X_v^2 \\ \vdots & & \vdots & \\ X_1^v & X_2^v & \cdots & X_v^v \end{bmatrix}^{-1} \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ -S_{2v} \end{bmatrix}$$

There are other algorithms for the decoding of BCH or Reed-Solomon codes. However, the Peterson-Gorenstien-Zierler decoder is perhaps the easiest to understand and the most instructive. Other methods usually offer more computationally efficient methods of computing the errors. The Berlekamp-Massey algorithm is an alternative method for finding the error locator polynomial that doesn't require a matrix inversion [3]. The Forney algorithm is an alternative method for evaluating the error magnitudes. This too eliminates the need for matrix inversion. These algorithms are especially attractive when used with powerful (i.e. long block length) codes.

Bibliography

[1] Barry C. Arnold and N. Balakrishnan. *Relations, Bounds and Approximations for Order Statistics.* Springer-Verlag, New York, 1989.

[2] E. Arthurs and H. Dym. On the optimum detection of digital signals in the presence of white Gaussian noise – A geometric interpretation and a study of three basic data transmission systems. *IRE Transactions on Communication Systems*, pages 386–372, December 1962.

[3] Richard E. Blahut. *Theory and Practice of Error Control Codes.* Addison-Wesley Publishing Company, Don Mills, Ontario, 1983.

[4] R. C. Bose and D. K. Ray-Chaudhuri. On a class of error-correcting binary group codes. *Information and Control*, 3:68–79, 1960.

[5] Wayne C. Dam. An adaptive maximun likelihood recever for Rayleigh fading channels. Master's thesis, McMaster University, Hamilton, Ontario, November 1990.

[6] Robert Charles Dingman. A new upper bound on trellis code error performance on Rayleigh flat-fading channels. Master's thesis, McMaster University, Hamilton, Ontario, 1992.

[7] Dariush Divsalar and Marvin K. Simon. The design of trellis coded MPSK for fading channels. *IEEE Transactions on Communications*, 36(9):1004–1012, 1988.

[8] G. David Forney, Jr. The Viterbi algorithm. *Proceedings of the IEEE*, 61(3):268–278, March 1973.

[9] D. C. Gorenstien and N. Zierler. A class of error-correcting codes in p^m symbols. *Journal of the Society of Industrial and Applied Mathematics*, 9:207–214, 1961.

[10] R. W. Hamming. Error detecting and correcting codes. *Bell System Technical Journal*, 29:147–160, 1950.

[11] A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffres*, 2:147–156, 1959.

[12] McEliece Robert J. *Finite Fields for Computer Scientists and Engineers.* Kluwer Academic Publishers, Boston, Massachusetts, 1987.

[13] S. Hamidreza Jamali and Tho Le-Ngoc. Bandwidth efficient communication via a Rayleigh channel using RS coded multiphase signaling. *IEEE Transactions on Communications*, 41(11):1594–1597, 1993.

[14] T. Kailath. Correlation detection of signals perturbed by a random channel. *IRE Transactions on Information Theory*, IT-6(3):361–366, June 1960.

[15] R. S. Kennedy. *Fading Dispersive Communication Channels.* John Wiley and Sons, New York, 1969.

[16] W. C. Y. Lee. *Mobile Communication Engineering.* McGraw-Hill, New York, 1982.

[17] William C. Y. Lee. Estimate of channel capacity in Rayleigh fading environment. *IEEE Transactions on Vehicular Technology*, VT-39(3):187–189, August 1990.

[18] William C. Lindsey and Simon Marvin K. *Telecommunication System Engineering.* Prentice-Hall, Englewood Cliffs, New Jersey, 1973.

[19] W. W. Peterson. Encoding and error-correction proceedures for Bose-Chaudhuri codes. *IEEE Transaction on Information Theory*, IT-16:359–360, 1960.

[20] W. Wesley Peterson and E. J. Weldon, Jr. *Error Correcting Codes.* MIT Press, Cambridge, Massachusetts, 2nd edition, 1972.

[21] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society of Industrial and Applied Mathematics*, 8:300–304, 1960.

[22] Richard L. Scheaffer. *Introduction to Probability and its Applications.* Kent Publishing, Boston, Massachusetts, 1990.

[23] Christian Schlegel and Daniel J. Costello. Bandwidth efficient coding for fading channels: Code construction and performance analysis. *IEEE Journla on Selected Areas in Communications*, 7(9):1356–1368, 1989.

[24] Claude E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, XXVII(3):379–423, July 1948.

[25] Claude E. Shannon. Communication in the presence of noise. *Proceedings of the IRE*, pages 10–21, January 1949.

[26] Gottfried Ungerboeck. Channel coding with multilevel/phase signals. *IEEE Transactions on Information Theory*, IT-28(1):55–67, January 1982.

[27] Andrew J. Viterbi. Convolutional codes and their performance in communication systems. *IEEE Transactions on Communications*, COM-19(5):751–772, October 1971.

[28] W. F. Walker. The error performance of a class of binary communications systems in fading and noise. *IEEE Transactions on Communications Systems*, CS-12(3):28–45, March 1964.

[29] John M. Wozencraft and Irwin Mark Jacobs. *Principles of Communication Engineering.* John Wiley and Sons, New York, 1965.