Coding for Frequency Hopped Spread Spectrum Channel with Jamming and Fading

Binh Dac Nguyen

A Thesis

in

The Department

of

Electrical Engineering

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering at
Concordia University
Montréal, Québec, Canada

February 1985

ABSTRACT

Coding for Frequency Hopped Spread Spectrum Channel with Fading and Jamming

Binh Dac Nguyen

This thesis deals with reliable communications over channels for which the primary additive noise is the partial band jamming . In addition to the noise, the transmitted signal may be subjected to non-selective Rician or Rayleigh fading. The communication system considered utilizes frequency hopping with orthogonal signalling and non-coherent detection.

Smart partial band jammer can cause severe deterioration to the frequency hopping channel. Coding reduces the bit error rate in antijam communication systems. Previous works on the use of coding in the channel considered are summarized. The performance evaluations are based on the cut off rate of the channel.

This thesis provides performance analysis of quasi-cyclic codes and convolutional codes under the worst case partial band jamming and fading. The bounds on the bit error rate are general enough to be applied to any other linear block codes or convolutional codes with known minimum or free distances. The performance curves demonstrate the advantages of coding for spread spectrum systems operating either with hard or soft decision decoding.

ACKNOWLEDGEMENTS

I would like to thank Professor Vijay K. Bhargava, my thesis supervisor, for his advice and encouragement throughout the course of this work.

I would also like to thank:

Mr. A. Benyamin-Seeyar and Mr. M. Khan for some helpful discussion;

Mrs. Madeleine Klein and my brothers Hoa Nguyen and Hung Nguyen for typing parts of my thesis;

All my friends for sharing the pressure, the frustration, the fun and for being there when needed.

Finally, I must thank my family for their understanding and support.

To my parents

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1. GENERAL OVERVIEW

In many communication systems the transmitted signal encounters not only the thermal noise but also noise from other sources. For reliable communication these systems must be designed to function acceptably even in the presence of interferences. The interference is either intentional (hostile) or unintentional. If the noise source is an intentional one it is called a jammer. The only purpose of a jammer is to make the system function as unreliable as possible. This is where spread spectrum modulation applies. This type of modulation uses much more bandwidth than is neccessary for reliable communication in the presence of thermal noise only. If a jammer has only a finite jam power then it cannot cover the entire spread bandwidth, thus the effect on the output of the receiver is less severe.

There are many different types of spread spectrum modulation but the two commonly used are the direct sequence (DS) and the frequency hopped (FH) spread spectrum. The idea behind these forms of modulation is to continuously change the carrier phase of the DS form or to continuously change the carrier frequency of the FH form. Different

forms of spread spectrum give different characteristics. One form might be good for a certain type of jamming but it could be vulnerable to another type of jamming. Beside the intentional jammer a signal can be corrupted by its own faded component. The use of spread spectrum might avoid this type of fading.

Originally spread spectrum was developed for military use but eventually became a hot topic in commercial communications because of its antijam characteristic. Mobile radio telephone services to a large number of customers is an ultimate goal to telephone companies nowadays. Many standard modulation techniques have been proposed for land mobile communication systems but none have achieved the privacy of the conversation. Privacy is an inherent characteristic of spread spectrum modulation technique. In addition, with vehicles moving in a city there is a fading phenomena resulting from shadowing due to buildings and terrain features. Also with all users accessing the same bandwidth, one link might receive partial band burst noise from the other links. All these features hightlight the use of spread spectrum in commercial markets.

Frequency hopping and frequency shift keying with non coherent detection is a primary choice for the mobile radio telephone system. Phase shift keying and coherent detection is not favorable due to the slowness of phase locking process. In a hostile environment the signal is also

subject to a jammer. A smart jammer never tries to jam the whole bandwidh unless this choice gives the maximum error rate. Instead it concentrates all its power only on a fraction of the available band. Then in a jammed band the noise power density is larger than the noise level in the rest of the band. As a result the signal-to-noise ratio (SNR) is reduced by a factor corresponding the jammed band. The rest of the bandwidth is assumed to be noise free thus the SNR is very large. With smart jammer spread spectrum is insufficient to provide acdequate performance. The loss due to smart jamming may be restored if a suitable coding technique is used in addition to spectrum spreading.

1.2. SCOPE OF THE THESIS

In this thesis we will consider the case of M-ary orthogonal signalling with noncoherent detection with frequency hopped modulation. If the phase shift keying is applied there is no gain in using higher signal alphabet with coherent detection [4]. In Chapter 2 we start with concepts of spread spectrum techniques. Direct sequence is summarized as well as the frequency hopped modulation. The optimal strategy of jammer is elaborated. We will also show that if we use direct sequence modulation with partial time jammer then the performance is the same as that of frequency hopped modulation with partial band jamming.

In Chapter 3 we consider a channel with a particular

form of modulation. That is frequency hopping in a Rician fading channel with noncoherent detection with Rayleigh fading channel a special case. The bounds on the bit error rate of these types of channel are determined. The channel analyzed is considered a worst case because the signal fades while the jammer signal unfades. In Chapter 4 we summarize previous works on the performance of coded spread spectrum systems. No specific codes are proposed but low code rates are seen to be superior to higher rates. Chapter 5 concentrates on our work showing how some selected cyclic codes and convolutional codes function in fading and jamming channel. Chapter 6 summarizes the thesis and suggest ideas for further work.

1.3. MAIN CONTRIBUTION OF THE WORK

Previous work on the performance of coded spread spectrum systems were based on the cut off rate of the channel. This approach, however, does not reflect the effectiveness of a particular code on a channel. In this thesis, we propose the use of quasi-cyclic codes and convolutional codes in jamming and fading channel. The union bounds on the bit error rate are formulated for both hard and soft decision decoding. The performance curves of some selected codes are plotted. For a required bit error rate and a degree of hardware complexity one can refer to the performance curves and choose an appropriate code for the system.

CHAPTER 2

SPREAD SPECTRUM TECHNIQUES FOR DIGITAL COMMUNICATIONS

2.1 INTRODUCTION

Spread spectrum communication systems were first developed for military uses but eventually became important in civillian applications as well. A rough definition of spread spectrum is as follow [1,2]:

"Spread spectrum is a means of transmission in which a random auxiliary modulation waveform is employed in order to spread the signal energy over a bandwidth much greater than the minimum necessary information bandwidth."

The randomness of the auxiliary modulation waveform is an important factor in this technique because it causes the original signal appear similar to the random noise. Thus spread spectrum makes the signal insusceptible to the unintended receivers. There are many reasons for spreading the spectrum of the signal, the most important reason is to reject the intentional interference signals. Other reasons would be to reject self-interference and multi-user interference [1,2]. In our work we concentrate mainly on the protection against in-band interference, especially the intentional jammer and self-interference due to fading.

There are many types of spread spectrum techniques but we can categorize them into three distinct classes. The first is called direct sequence (DS) or pseudo-noise (PN) modulation in which the spreading is achieved by changing the phase in the carrier containing data according to a pseudo randomly generated sequence. The second class is frequency hopping in which the the carrier is caused to shift frequency in a pseudo random way. The last class is the time hopping technique wherein burst of signals are initiated at pseudo random time.

In this thesis we will briefly introduce both the direct sequence and frequency hop modulation techniques. However, in our analysis we emphasize on the frequency hop technique. The analysis of FH in noise interference provides analogous results for DS system.

2.2 BASIC CONCEPTS

The block diagram shown in Figure 2.1 illustrates the basic elements of a spread spectrum (SS) system. Multiplication to unrelated signal produces a signal whose spectrum is the convolution of the spectra of the component signals. The transmitter multiplies the data bit d(t) by a binary ±1 "chipping" sequence p(t). Thus if the data d(t) is narrow-band compared to the spreading signal p(t) then their product d(t)p(t) will have nearly the spectrum of the

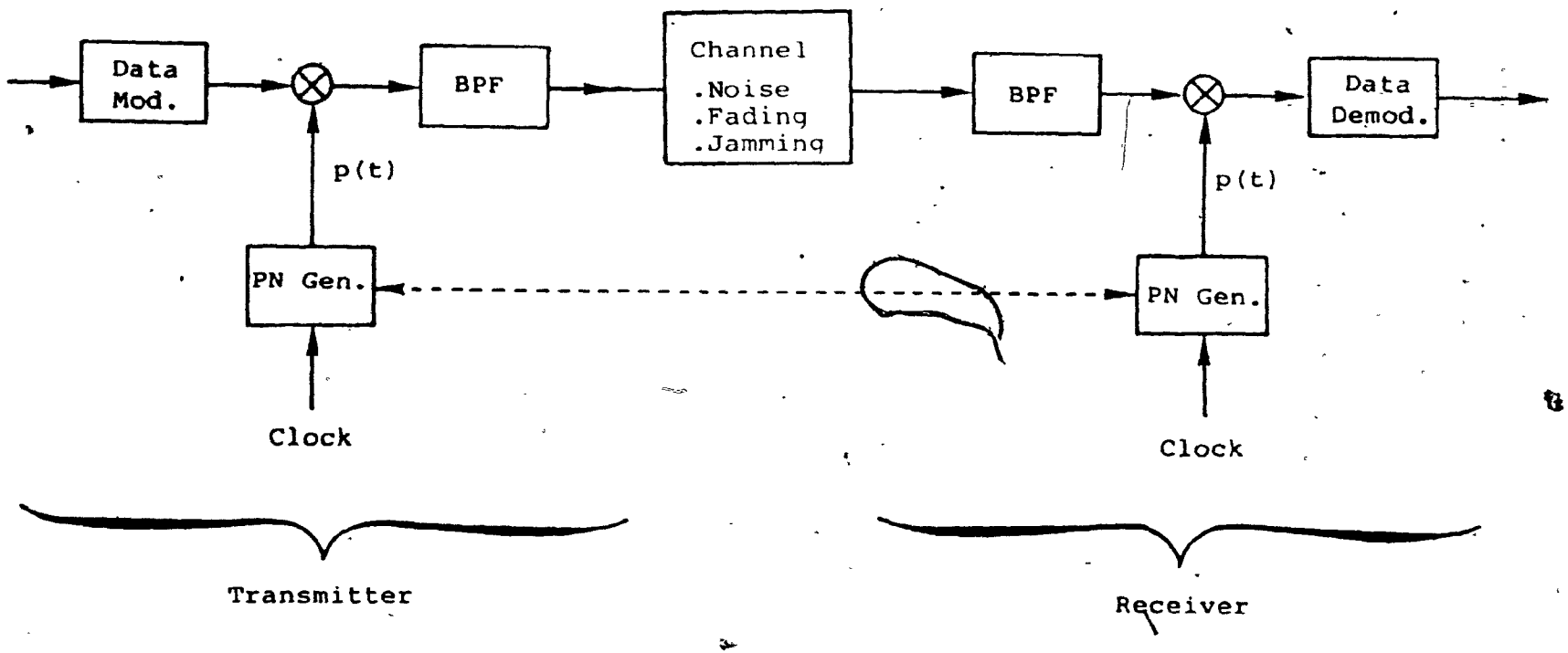


Figure 4.1: Model of spread spectrum communication system

wider signal, i.e. p(t). Suppose that the data bit duration T_b is much larger than the duration T_c of a random bit. The bandwidth expansion can be expressed as [1,3]

$$B_e = \frac{T_b}{T_c} \tag{2.1}$$

The quantity B_e determines the number of chips per information bit. The power spectra of the data signal d(t) and its spread version p(t).d(t) are depicted in Figure 2.2

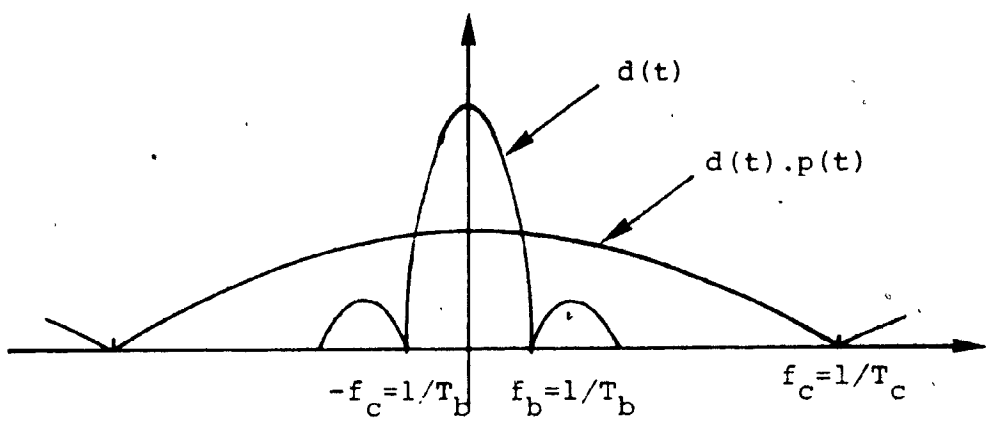


Figure 2.2: Power spectrum of data and of spread signal

The received signal is

$$r(t) = d(t).p(t) + J(t) + n_w(t) \qquad (0<t<T_b) \tag{2.2}$$

and the input to the data demodulator is

$$\begin{aligned} r(t).p(t) &= d(t).p^2(t) + J(t).p(t) + n_w(t).p(t) \\ &= d(t) + J(t).p(t) + n_w(t).p(t) \end{aligned} \tag{2.3}$$

In (2.2) and (2.3) J(t) and $n_w(t)$ represent the jamming signal and the additive white Gaussian noise,

respectively. The first term of (2.3) may be extracted virtually intact with a filter of bandwidth $1/T_b$. The second term will be spread over at least f_c Hz as shown in Figure 2.2. The third term is white noise so the multiplication with p(t) still gives white noise. The rule is then followed: multiplication ONCE by the spread signal spreads the bandwidth, multiplication TWICE followed by filtering recovers the signal bandwidth [4]. Thus the random signal must have very good correlation property to make the desired signal peak up during the demodulation process.

The channel or the propagating medium of Figure 2.1 can be characterized as additive white Gaussian noise (AWGN) with or without Rician or Rayleigh fading. In our analysis we consider the AWGN and Rician fading with Rayleigh fading as a special case. This type of interference is introduced in detail in Chapter 3.

2.2.1 PROCESSING GAIN, JAMMING MARGIN [1,3,6]

A fundamental issue of spread spectrum is how this technique can protect against interfering signals of finite power. The principle is to force the jammer with a fixed amount of total power to either spread its power over the entire bandwidth or place all its power into a small fraction of the band hence leaving the remainder interference free [1]. In the former case jammer induces just a

little interference in each sub-band of the bandwidth. While in the later case only a fraction of the band is highly corrupted and the rest is error free. It is worth mentioning that against white noise which has "infinite" power [1] and constant energy the use of spreading offers no help at all. However, with a fixed finite power jammer spreading bandwidth will make the jammer uncertain as to where the signal would exist in the large space. If the jammer transmits noise signal at frequency f_J, the relationship between signal spectrum and jammer spectrum is shown in Figure 2.3.

To measure the amount of interference rejection we introduce the term processing gain G_p. This quantity represents the advantage gained over the jammer. This gain is obtained by expanding the bandwidth of the transmitted signal. If we define $R_b=1/T_b$ as the information rate and $R_c=1/T_c=f_c$ is the chip rate then the processing gain is determined as

$$G_p = \frac{R_c}{R_b} = f_c T_b \qquad (2.4)$$

Actually G_p was mentioned before as the number of chips per information bit B_e. Typical processing gain for spread spectrum systems run from 20dB to 60dB [7]. In the design of practical system the processing gain is not, by itself, a measure of how well the system is capable of performing in a jamming environment [7]. Therefore we

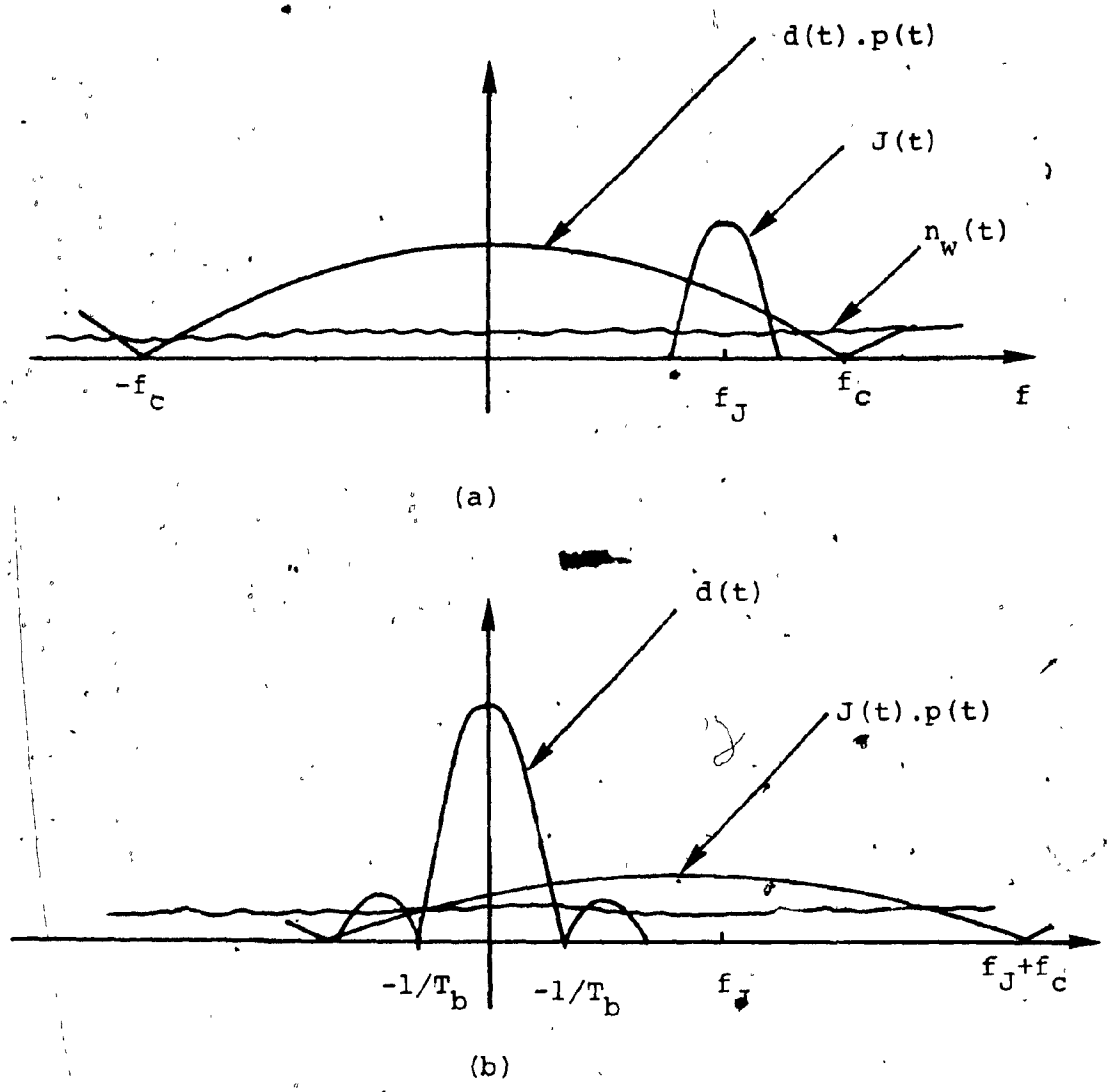


Figure 2.3: Relationship of data and interfering signal power spectra (a) before despreading (b) after despreading.

usually introduce another quantity called jamming margin M_J. Jamming margin is defined as the degree of interference which a spread spectrum (SS) system can withstand while receiving a desired signal and delivering a minimum signal-to-noise ratio (SNR) at its output [3,5,7]. Jamming margin is defined in deciBels as

$$M_J = G_p - \left(\frac{E_b}{N_{0J}}\right) - L \qquad (2.5)$$

where E_b/N_{0J} represents the SNR with E_b the energy of the information bit, N_{0J} is the power spectral density of the AWGN and L is the system loss due to other causes. Typical system losses are in the range of 1dB to 3dB [7]. The jamming margin can be increased by reducing the SNR through the use of coding. The use of coding in SS system will be discussed in Chapter 4.

2.2.2. PSEUDO RANDOM SEQUENCE GENERATOR [1,2,7]

From the definition of the technique an auxiliary random sequence is required in order to spread the bandwidth of the data signal. Unfortunately, to despread the received signal the demodulator must have the replica of the spread sequence in time synchronism. Usually, in practice we use pseudo random or pseudo noise (PN) sequences which satisfy the following properties [1]

1) easy to operate

2) randomness properties

3) long period

4) difficult to regenerate from a short segment

The linear feedback shift register (LFSR) shows properties (1), (3) and most of (2) but not (4). Figure 2.4 shows a LFSR generator, the sequence is formed by taking the binary output from some stages of the shift registers, modulo-2 adding the output in a connection vector $(h_0, h_1, \ldots, h_m)$ and feeding the result back to the input of the register. The sequence of bit flowing out of the LFSR depends on the connection vector $\underline{h}$ and the initial state $(x_0, x_1, \ldots, x_{m-1})$ of the registers. The sequence satisfies the recurrence relation

$$x_i = \sum_{j=1}^{m} h_j x_{i-j} \qquad (i>m) \qquad (2.6)$$

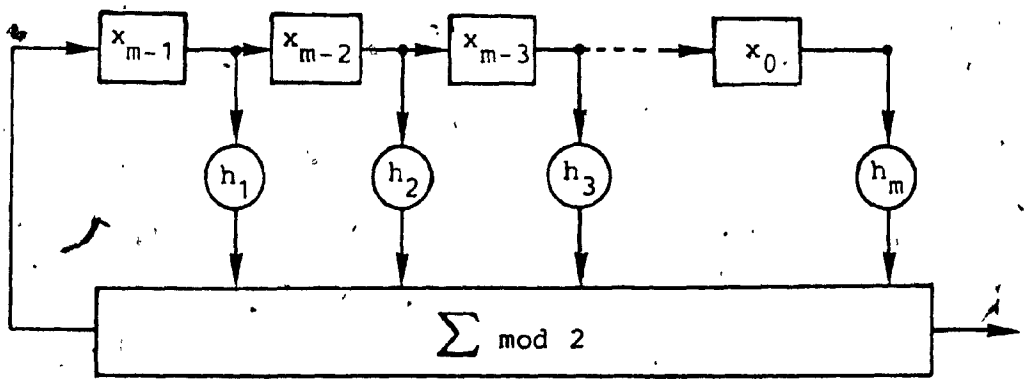


Figure 2.4: Linear feedback shift register generator

The period N of the sequence is at most 2^m-1. For spread spectrum, it is desirable to have maximum period (all binary m-tuples except the all-zero). To achieve the maximum period the generator depends on the connection vector $\underline{h}$. Let the connection polynomial coressponding to $\underline{h}$ be given by

$$h(x) = h_0 + h_1x + h_2x^2 + \ldots + h_mx^m \qquad (2.7)$$

If h(x) is a primitive polynomial of degree m then the sequences generated by h(x) will have maximum period. These sequences are called maximal length LFSR (MLLFSR) and have the following properties:

1) Balance property: there are exactly $2^{m-1}-1$ zeros and 2^{m-1} ones in one period of a maximum length sequence

2) Randomness property: maximum length sequence has a well defined satistical distribution for the runs of ones and zeros. In any period, half of the run of consecutive zeros or ones are of length one, one-fourth of length two, one-eighth of length three, etc.

3) Shift and add property: the modulo-2 adding of an m-sequence and any of its shifted versions yields another shifted vervion of the original sequence. The property is best illustrated by Figure 2.5.

If we define the +1 sequence $x'_i = 1-2x_i$, $x_i = 0,1$ then the autocorrelation function of x'_i is given by [1]

$$R_{x'}(\tau) = \sum_{k=1}^{N} \frac{1}{N} x'_k \, x'_{k+\tau}$$

$$R_{x'}(\tau) = \begin{cases} 1 & \tau = 0, N, 2N, \ldots \\ -\frac{1}{N} & \text{otherwise} \end{cases} \tag{2.8}$$

If we associate sequence $x'(t)$ to our spreading sequence $p(t)$ and if we define

$$q(\tau) = \begin{cases} 1-|\tau| f_c & |\tau| \leq \frac{1}{f_c} \\ 0 & \text{otherwise} \end{cases} \tag{2.9}$$

with $N \gg 1$, then

$$R_p(\tau) \simeq \sum_i q\left(\tau - \frac{iN}{f_c}\right) \tag{2.10}$$

Because of the mapping of (0,1) to (1,-1) we have the isomorphism

$$[(0,1),+] \longleftrightarrow [(1,-1),x]$$

therefore $$C_k + C_{k+\tau} \longleftrightarrow C'_k \cdot C'_{k+\tau} \tag{2.11}$$

By the shift and add property if C_k is a maximal length LFSR sequence so is $C_k + C_{k+\tau}$. Thus by (2.11) sequence $C'_k \cdot C'_{k+\tau}$ is also a maximal length sequence.

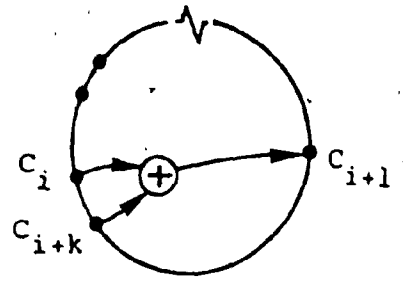
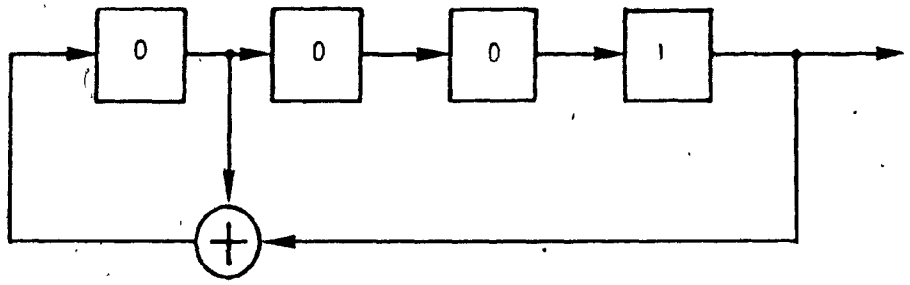


Figure 2.5: Shift and add property of an m sequence. c_i is the original sequence, c_{i+k} is a k-th shifted version of c_i.



(a)

0	0	0	1	flow out of the generator
1	0	0	0	
1	1	0	0	
1	1	1	0	
1	1	1	1	
0	1	1	1	
1	0	1	1	
0	1	0	1	
1	0	1	0	
1	1	0	1	
0	1	1	0	
0	0	1	1	
1	0	0	1	
0	1	0	0	
0	0	1	0	

(b)

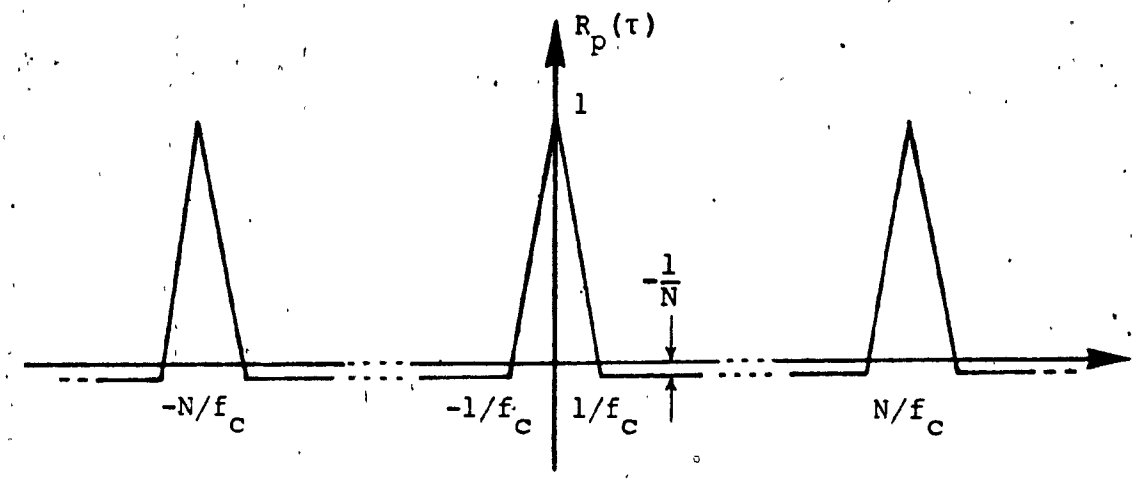
Figure 2.6: (a) Example of a four-stage MLLFSR generator, (b) and its state cycle

Let us take a simple example of a four-stage LFSR with the connection vector $\underline{h}$ = (10011). The initial states of the registers are (1000) as shown in Figure 2.6a. The sequence output is 1000111101... as depicted in Figure 2.6b. After doing the mapping to generate the pseudo noise (PN) sequence p(t) and applying (2.10), the autocorrelation function is shown graphically in Figure 2.7a. We observe that $R_p(\tau)$ is periodic with period $(2^m-1)/f_c$. The power spectrum of p(t) is [1]

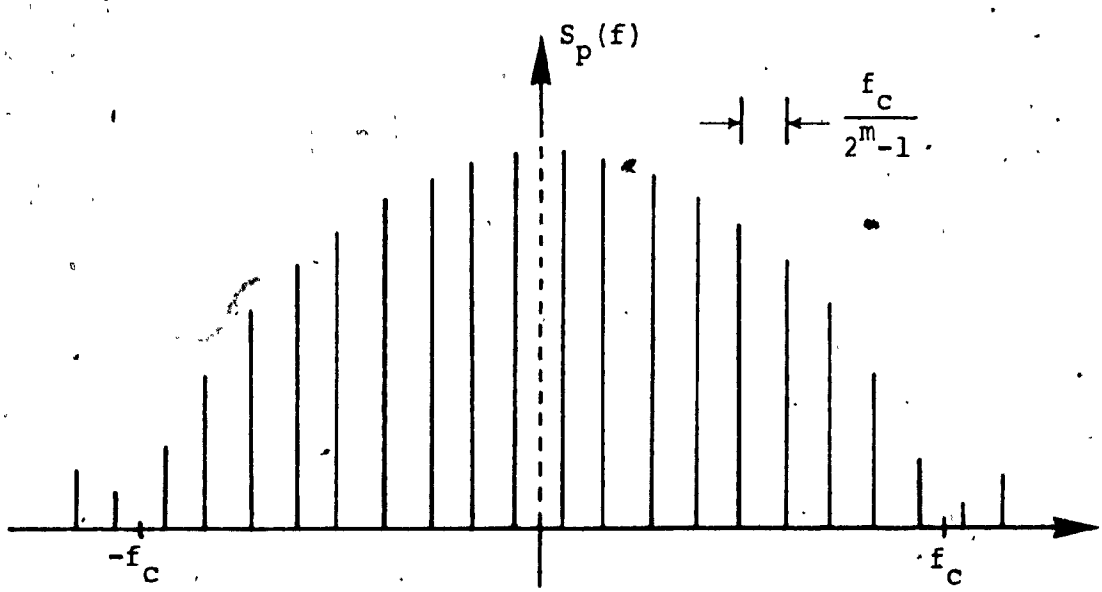
$$S_p(f) = \left\{ \sum_{\substack{m=-\alpha \\ m\neq 0}}^{\alpha} \delta(f-mf_o) \right\} \frac{N+1}{N^2} \left\{ \frac{\sin \pi f/f_c}{\pi f/f_c} \right\}^2 + \frac{1}{N^2}\delta(f) \qquad (2.12)$$

where $f_0 = f_c/(2^m-1)$. This line spectrum is shown in Figure 2.7b.

If N is large the spectral lines get close together and it can be viewed as being continuous and similar to that of a random binary waveform. Unfortunately, intended jammer can observe only 2m-1 consecutive bits in a sequence to be able to solve for the (m-1) middle coefficients of $\underline{h}$ and the initial bits of the registers using Berlekamp-Massey algorithm [1,7]. To further enhance security, the output sequence from the maximum length (ML) LFSR is not used directly. Instead, the output of two sequences can be modulo-2 added to give a new sequence. The new sequences, however, are not maximal. There exists other pseudorandom



(a)



(b)

Figure 2.7: (a) Auto-correlation of p(t)
(b) Power spectral density of (pt)

codes such as nonlinear shift register sequences, composite sequences and JPL (Jet Propulsion Lab) sequences. For the sake of simplicity we assume that the pseudorandom sequences are generated by maximal length LFSR or pseudonoise (PN) generator.

2.2.3. DIRECT SEQUENCE (DS) OR PSEUDONOISE (PN) MODULATION

A block diagram of a DS spread sprectrum system is depicted in Figure 2.8. The data modulator could be any one of a number of standard techniques such as PSK, FSK, DPSK etc.. One of the advantages of DS spread spectrum system is that coherent demodulation can be applied, thus PSK (phase shift keying) is preferable.

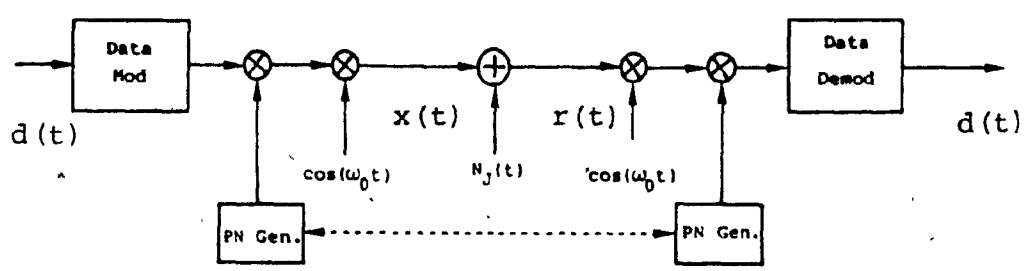


Figure 2.8: Conceptual block diagram of a DS spread spectrum system

If binary PSK is used the modulated biphase waveform

can be expressed as

$$x(t) = \sqrt{2P}\, d(t)\, p(t) \cos(\omega_0 t+\theta) \qquad (2.13)$$

where

P is the signal power

d(t) is the data sequence (+1,-1)

p(t) is the PN code signal (+1,-1)

ω_0 is the carrier frequency (rad/sec)

θ is the carrier phase (rad)

Normally the chip time $T_c=1/f_c$ is small compared to the data bit duration T_b and this difference produces the sprectral spreading. The optimum receiver may be implemented either as a filter matched to the waveform x(t) or as a correlator as illustrated in Figure 2.9 [3]

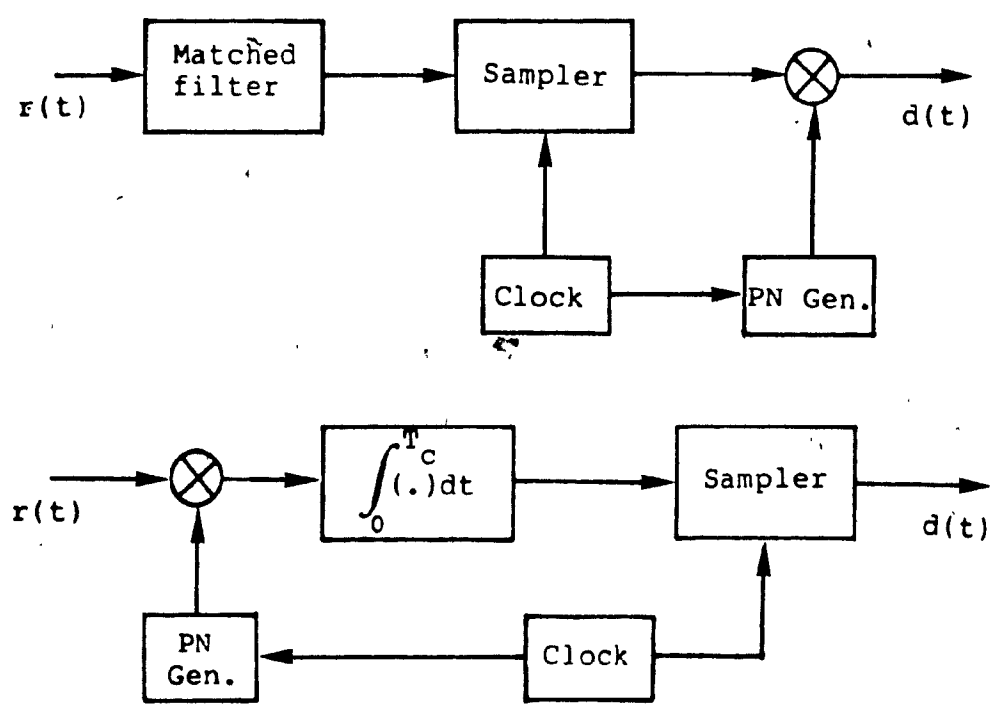


Figure 2.9: Possible demodulator structures for DS spread spectrum signal

Usually each symbol is received in the presence of an intentional jamming J(t) signal plus additive white Gaussian noise $n_w(t)$ of two sided spectral density $N_0/2$. The received signal can be represented as

$$r(t) = \sqrt{2P}\, d(t)\, p(t) \cos(\omega_0 t+\theta) + J(t) + n_w(t) \qquad (2.14)$$

Assume the jammer has an average power J_{av} in the signal bandwidth $W=f_c$. The effect of despreading is to obtain the original signal and to multiply the jamming signal by the PN code. If the average power of the jammer is J_{av} then the equivalent broadband noise spectral density is

$$N_{0J} = \frac{J_{av}}{W} \qquad (2.15)$$

If the signal has the average power P then the energy per bit will be $E_b = P.T_b$. The effective SNR is

$$\frac{E_b}{N_{oJ}} = \frac{P}{R_b}\,\frac{W}{J_{av}}$$

$$= \frac{W/R_b}{J_{av}/P} \qquad (2.16)$$

In (2.16) W/R_b is the processing gain and J_{av}/P is the jamming margin. In fact the jammer can transmit pulses of flat noise for a fraction of the time. This tactic can deteriorate the DS link because it reduces the processing gain. The jammer strategy will be discussed in Section 2.3.

If the processing gain is large we can make an optimistic assumption that the noise is Gaussian [3,5].

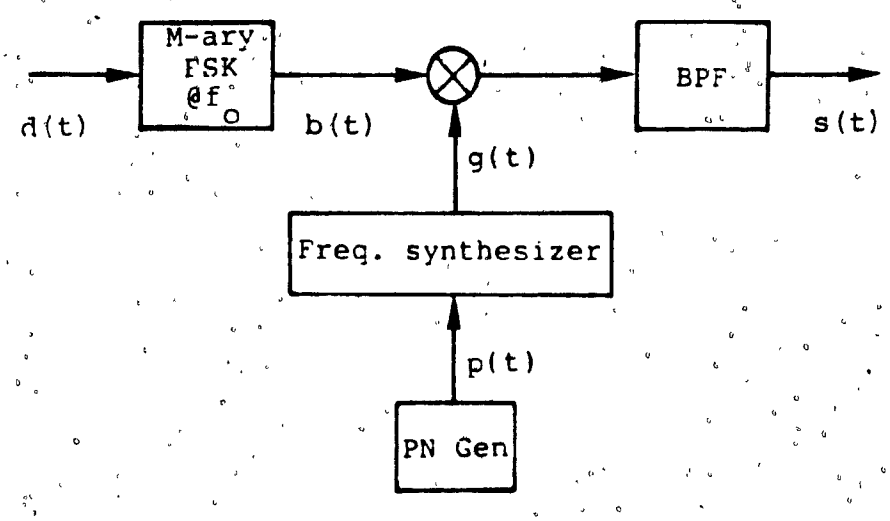
2.2.4 FREQUENCY HOPPED SPREAD SPECTRUM SYSTEM

Another important spread spectrum modulation technique is frequency hopping. In this system the available channel bandwidth is subdivided in to a large number of contiguous frequency slots. The selection of frequency of a synthesizer is made according to the output from a PN generator. The hopping operation may occur several times per symbol (fast hop) or at the symbol rate (slow hop). A block diagram of an uncoded frequency hopped system and its particular hop pattern in the time-frequency plane are shown in Figure 2.10. The data modulation format may be any of a number of standard techniques but it is usually either binary or M-ary FSK.

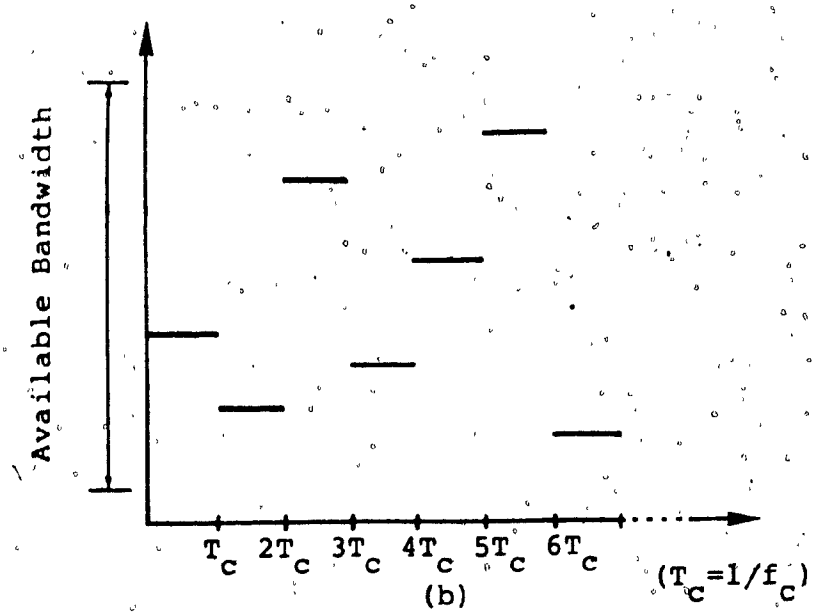
Suppose we have a slow frequency hopped spread spectrum system, the data signal d(t) is a sequence of -1 or +1 rectangular pulses of duration T_b. This data signal is the input to an MFSK modulator and the corresponding output is

$$b(t) = \cos\{2\pi[f_0+d(t)\Delta]t + \phi(t)\} \qquad (2.17)$$

where Δ is one-mth the spacing between the M-ary FSK tones.



(a)



(b)

Figure 2.10: (a) Block diagram of a frequency hopped spread spectrum modulator
(b) An example of a frequency hopped pattern

The phase $\phi(t)$ is introduced to the equation by the FSK modulator. The MFSK is then frequency hopped according to the hopping pattern derived from a frequency synthesizer. The signal from the synthesizer is

$$g(t) = \cos\{2\pi f_c t + \theta_s(t)\} \tag{2.18}$$

θ_s is generated by the synthesizer, the hopping signal is

$$\begin{aligned} s(t) &= g(t).b(t) \\ &= \cos\{2\pi[\, f_o + d(t)\Delta]t + \phi(t)\} \cos\{2\pi f_c t + \theta_s(t)\} \end{aligned} \tag{2.19}$$

The band pass filter (BPF) in Figure 2.10a removes unwanted components present at the output of the multiplier. The signal at the output of the filter is [13]

$$s(t) = \sqrt{2P} \cos\{2\pi f(t)t - \varphi(t)\} \tag{2.20}$$

where

$$f(t) = f_o + d(t)\Delta + f_c$$

$$\varphi(t) = \phi(t) + \theta_s(t)$$

in (2.20) P is the power of the signal at the receiver in the absence of fading. In fact, s(t) represented by (2.20) is an element of the set $\{s_i(t)\}$, $i=1,2,\ldots,M$, of signals used for conveying information to the receiver. We assume that all the signals are narrow band waveforms which are limited in the interval $0 < t < T_c$. The energy of each

signal is

$$E_i = \frac{1}{2}\int_0^{T_c} |s_i(t)|^2 dt \qquad (2.21)$$

thus the power is

$$P_i = \frac{1}{2T_c}\int_0^{T_c} |s_i(t)|^2 dt = \frac{1}{T_c}E_i \qquad (2.22)$$

The cross-correlation coefficient between any two signals is defined as

$$R = \frac{1}{2E_i}\int_0^{T_c} s_i(t)s_j^*(t)dt \qquad (i \neq j) \qquad (2.23)$$

for orthogonal signalling we have R=0.

The effective SNR may be expressed as

$$\frac{E_b}{N_{oJ}} = \frac{PT}{J_{av}/W} = \frac{W/R_b}{J_{av}/P} \qquad (2.24)$$

as in the case of direct sequence system. The processing gain for a frequency hopped system is W/R_b and the jamming margin is J_{av}/P. Again, instead of jamming continuously the jammer can concentrate all its power only in a fraction of the band. This strategy will be further discussed in Section 2.3.

In practice, it is very difficult to maintain phase coherence in the synthesis of the frequencies used in the hopping pattern and also in the propagation of the signal as it hops over a wide bandwidth. Consequently noncoherent

detection is employed in this case. The receiver model for M-ary orthogonal signal is depicted in Figure 2.11. The received signal can be represented as

$$r(t) = s(t)+n_w(t)+J(t)$$
$$=\sqrt{2P}\ A\cos[2\pi f(t)t+\varphi(t)+\Theta(t)]+n_w(t)+J(t) \qquad (2.25)$$

where A is the envelope of the received signal and $\Theta(t)$ is the phase shift due to propagation. These two quantities will be used in the analysis of the fading medium. J(t) and $n_w(t)$ are the jamming and noise signals, respectively.

The first bandpass filter (BPF) of Figure 2.11 has center frequency approximately f_c and the bandwidth approximately W, the bandwidth of the transmitted signal. This is followed by the dehopper which is synchronized in frequency and time to the frequency hopping signal g(t) of (2.18). The second BPF removes unwanted frequencies after dehopping. The unwanted frequencies could be the double-frequency components and the thermal noise that is outside the frequency band occupied by the information signal. The output of the dehopper is demodulated using an ordinary MFSK demodulator.

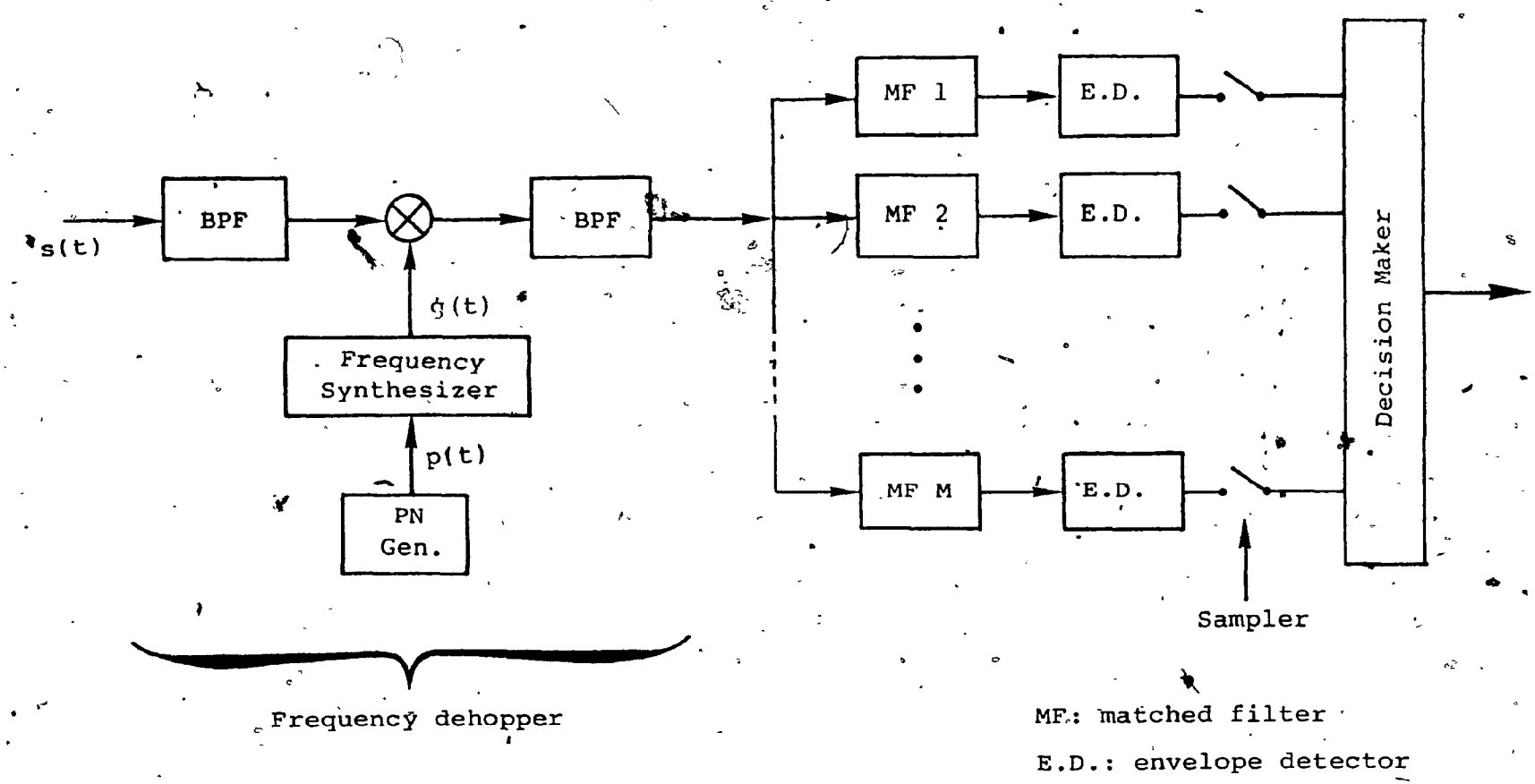


Figure 2.11: Block diagram of FH/MFSK receiver of spread-spectrum system

2.3. JAMMING STRATEGY: PARTIAL JAMMER

The DS technique can produce highly unstructured waveform but still there exists a weak point. The transmitted symbols all have equal length in time and occur with no guard space [5]. A smart jammer can take advantage of this weakness to efficiently use its limited power. Thus, instead of transmitting continously the jammer can transmit pulses at a power J_{av}/λ $(\lambda<1)$, for λ percent of the time, i.e. the probability that the jammer is transmitting at a given instant is λ. Now if the jammer has total average power J_{av} in a signal bandwidth W, the value of the power spectral density for the jamming signal may be expressed as

$$N_{oJ} = \frac{J_{av}}{W} \tag{2.26}$$

For partial time jamming with duty cycle λ, the power spectral density is

$$N_{oJ} = \frac{J_{av}}{\lambda W} \tag{2.27}$$

The effective SNR is

$$\frac{E_b}{N_{oJ}} = \frac{P/R_b}{J_{av}/\lambda W} = \frac{\lambda W/R_b}{J_{av}/P} \tag{2.28}$$

From (2.28) we observe that the processing gain in

partial time jamming equal λ percent of the in case of continous jamming. The bit error probability can be written as [26]

$$P_b = \lambda P\left(\frac{E_b}{N_{oJ}+N_o}\right) + (1-\lambda)\, P\left(\frac{E_b}{N_o}\right) \qquad (2.29)$$

where N_w is the power spectral density of the white Gaussian noise. Assuming that when the jammer is active, the contribution of N_w is negligible, we have

$$P_b = \lambda P\left(\frac{E_b}{N_{oJ}}\right) = \lambda P\left(\frac{\lambda W/R_b}{J_{av}/P}\right) \qquad (2.30)$$

We assume that when the jammer is on, the demodulation output statistic is Gaussian, the error probability is given by [3,5]

$$P\left(\frac{W/R_b}{J_{av}/P}\right) = Q\left[\left(2\,\frac{W/R_b}{J_{av}/P}\right)^{\frac{1}{2}}\right]$$

Thus

$$P_b = \lambda Q\left[\left(2\,\frac{\lambda W/R_b}{J_{av}/P}\right)^{\frac{1}{2}}\right] \qquad (2.31)$$

P_b of (2.31) is shown graphically in Figure 2.12 for several values of λ. We observe that smaller the fraction becomes the more signal energy we have to put in to get a desired bit error rate. In fact, the jammer can select λ to maximize P_b in (2.31). This is found to be [5]

$$P_{b,wc} = \frac{0.0083 J_{av}}{W/R_b} \qquad (2.32)$$

The worst case (wc) is shown in dotted line of Figure 2.12.

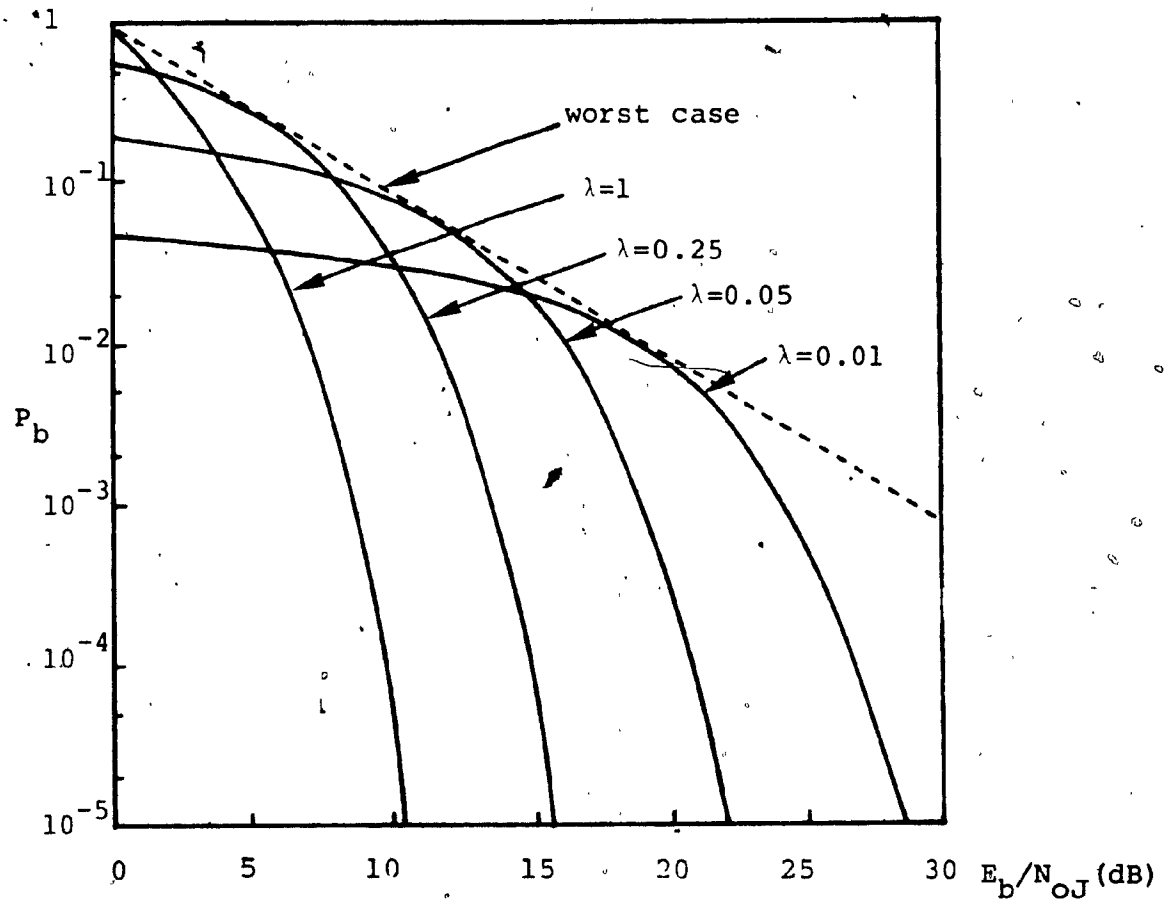


Figure 2.12: Bit error rate for BFSK in DS-SS channel

In case of frequency hopping technique the weak point lies in term of frequency. So instead of jamming the whole band the jammer gathers all its energy within the fraction λ of the available bandwidth as illustrated in Figure 2.13. Thus the signal will be jammed with probabilty λ and will be free of error with probability $(1-\lambda)$. If the modulation is binary FSK with noncoherent detection and under the same condition as in the DS case, the average bit error rate is

$$P_b = \frac{1}{2} \exp\left(- \frac{E_b}{N_{oJ}} \right) \tag{2.33}$$

where

$$\frac{E_b}{N_{oJ}} = \frac{P}{R_b} \cdot \frac{W}{J_{av}}$$

$$= \frac{W/R_b}{J_{av}/P}$$

Under partial band jammer we have $N_{oJ} = J_{av}/\lambda W$, therefore

$$P_b = \frac{\lambda}{2} \exp[-(\lambda W/R_b)/(J_{av}/P)] \tag{2.34}$$

The curves of P_b with different values of λ are shown in Figure 2.14. The dotted line indicates the worst case when the jammer is able to find a value of λ that maximizes P_b of (2.34). The average bit error rate of the worst case is found as [3,5]

$$P_{b,wc} = \frac{J_{av}/P}{(W/R_b)e} \tag{2.35}$$

As indicated before, for each type of spread spectrum techniques there is a type of jammer that can severely

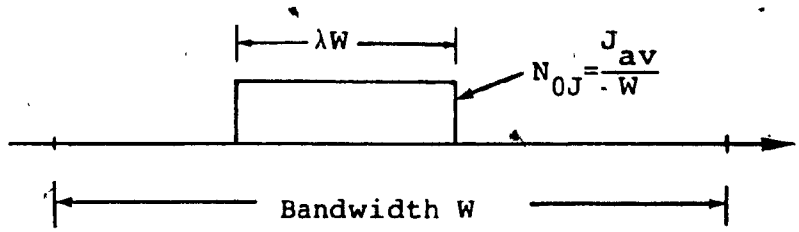


Figure 2.13: Partial band noise jammer

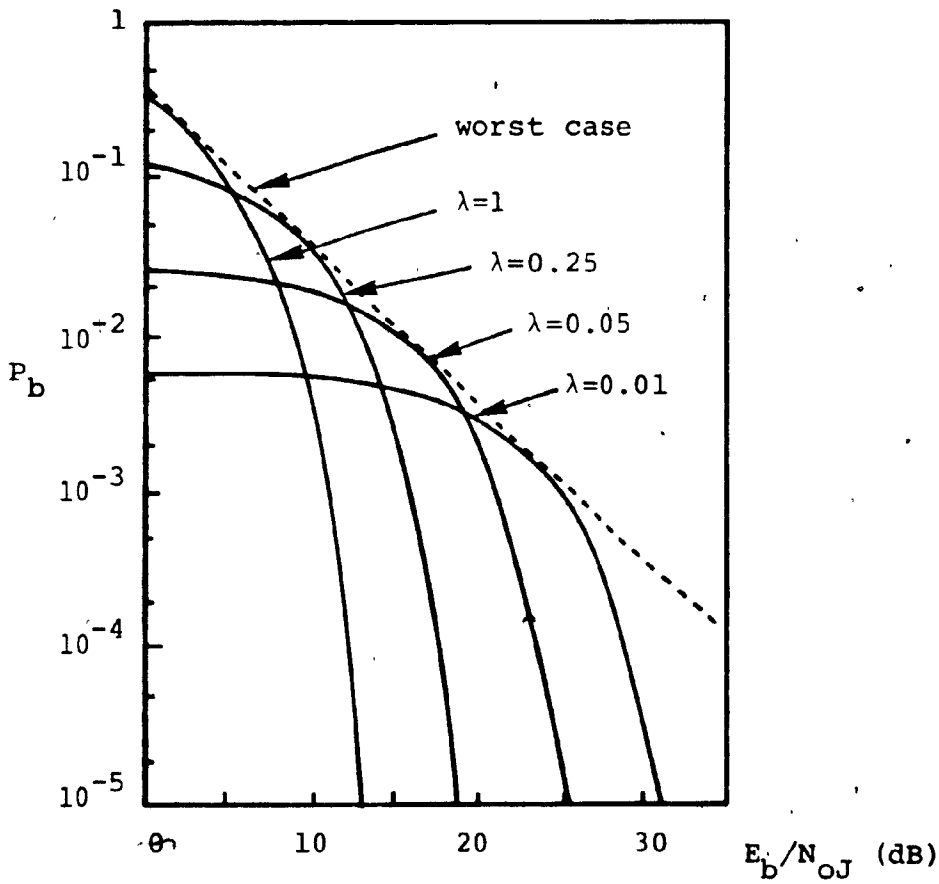


Figure 2.14: Performance of FH/BFSK in partial band jammed channel

damage the detection performance. The performance can be restored if error correcting codes are employed. This will be shown in Chapter 4. The analysis can be carried out for each type separately. Fortunately, the analysis is based on the SNR and from (2.28) and (2.34) we observe that the effective SNR of a DS system is the same as that of a FH system. However the coherent detection used in a DS-PSK will give at least 3dB advantage over a FH-FSK noncoherent system [4]. So we can do the analysis for either type of modulation and the results can be applied as well to the other type [4]. As aforementioned, we will concentrate on the frequency hopped FSK technique with noncoherent detection.

2.4. COMPARISION BETWEEN DS AND FH SPREAD SPECTRUM SYSTEMS

Both techniques have advantage over the jammer because of the processing gain which depends directly on the spread bandwidth. With respect to the processing gain the advantage is in favor of the frequency hop approach. For the DS sytem the spread bandwidth is limited to the rate of the PN sequence. This in turn, is limited by the coherent bandwidth, as determined by the particular mode of transmission and system components. On the other hand, FH system has no such restrictions [10].

Partial band jammer for FH/SS is analogous to partial

time jammer for DS/SS. The pulse jammer trades off peak power versus duty cycle in an analogous way to a partial band jammer. However, the design of a pulse jammer encounters more restrictions than a partial band jammer does. Therefore, a partial band jammer corrupting the FH system represents a greater vulnerability because of the relative ease with which it can be implemented [5,10].

Another basis for comparing the two techniques is the SNR necessary to maintain a given bit error rate. Typically, PSK/coherent is used in DS system while FSK/noncoherent detection is used in FH system. The performance of coherent PSK is known to be better than the noncoherent FSK, about 3dB at a 10^{-4} error rate [4,10]. The loss in FH/MFSK is due to combining loss. Therefore, with respect to the SNR performance, DS has an advantage over FH system.

CHAPTER 3

ERROR PROBABILITIES FOR SLOW FREQUENCY HOPPED SPREAD-SPECTRUM COMMUNICATIONS OVER NON-SELECTIVE FADING CHANNEL

3.1. INTRODUCTION

The use of natural medium for communications implies unavoidable involvement with the random changeability which often accompanies the natural phenomena. Because of this natural phenomena for some channels neither the amplitude nor the phase can be assumed to remain constant over a significant number of bit transmissions. In our analysis we assume that the transmitted signal passes through a linear medium which fades in a frequency-nonselective way. That is, the whole band of frequencies occupied by the signals is acted on uniformly by the medium. There is no probability of simultaneous contructive interference at one frequency and destructive interference at another. In other words, if there is more than one transmission path , the difference of delays of any pair of paths must be less than the reciprocal of the bandwidth of the signal [1,2,6,11,12].

In this chapter we will determine the system performance based on the evaluation of the system error probability. The modulation is frequency hopped M-ary frequency shift keying (FH-MFSK). The channel considered is

modelled as Rician fading channel consisting of a direct path and a random path. The jammer is partial band additive white Gaussian noise jammer. The graphical results presented in Section 3.4 show a serious penalty in signal-to-noise ratio as a consequence of fading and jamming.

3.2. CHANNEL CHARACTERISTIC

The characteristic of a fading channel can be best described by indicating what happens to a signal that passes through it. From Chapter 2 the transmitted signal given by (2.19) is

$$s(t) = \sqrt{2P}\cos\{2\pi f(t)t - \varphi(t)\}$$

which can be rewritten in exponential form as

$$s(t) = \mathrm{Re}\left[\sqrt{2P}\exp\{j[2\pi f(t)t - \varphi(t)]\}\right] \qquad (3.1)$$

and the received signal can be represented as

$$\tilde{s}(t) = \mathrm{Re}\left[\sqrt{2P}\,A\exp\{j[2\pi f(t)t - \varphi(t) - \Theta(t)]\}\right] \qquad (3.2)$$

which is the exponential form of (2.23). Quantity A in (3.2) is the envelope and Θ is the phase shift due to fading. Thus the non-selective fading medium is characterized by two quantities: A, the strength and Θ, the

phase shift. These quantities are random and consequently must be described by the probability density functions. If we assume that the amount of fading does not change appreciably for the duration of the transmitted signal, we can describe it by the joint distribution $f(A,\Theta)$ [11,12,14]

Let Ω be the result of the addition modulo-2π of $\Theta(t)$ and φ. If $\Theta(t)$ and φ are uniformly distributed over $[0,2\pi]$ then under a general condition Ω is also uniformly distributed over the interval $[0,2\pi]$. We assume that the propagation modes are mutually and statistically independent to the additive white Gaussian noise $n_w(t)$. The output of the fading channel may be broken up into two components: a fixed component and a random component. That is

$$s(t) = \sqrt{2P}\,[\alpha \exp(-j\delta) + \beta \exp(-j\varepsilon)] \cdot \exp(j2\pi f(t)t) \qquad (3.3)$$

α and δ are strength and phase shift of the fixed component respectively while β and ε are the same quantities for the random components. Figure 3.1 depicts vectorially the relationship among the quantities $A, \Omega, \alpha, \delta, \beta$ and ε [11].

We postulate

$$f(\beta,\varepsilon) = \begin{cases} \dfrac{\beta}{2\pi\sigma^2} \exp\left[\dfrac{-\beta^2}{2\sigma^2}\right] & \begin{Bmatrix} 0 < \beta < \infty \\ 0 < \varepsilon < 2\pi \end{Bmatrix} \\ 0 & \text{otherwise} \end{cases} \qquad (3.4)$$

β and ε are independent random variables, the first obeys

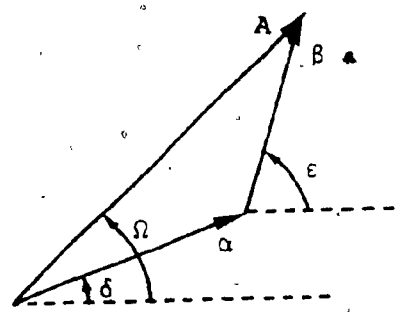


Figure 3.1: Relationship among strengths and phase shifts of a fading channel

the Rayleigh density distribution with zero mean and variance $2\sigma^2$. The second obeys the uniform distribution over the interval $[0,2\pi]$. The joint distribution of the strength and phase of the sum of the fixed component (α,δ) and the random component (β,ε) is [11,13,14, Appendix A]

$$f(A,\Omega) = \begin{cases} \dfrac{A}{2\pi\sigma^2} \exp\left[-\dfrac{A^2+\alpha^2-2A\alpha\cos(\Omega-\delta)}{2\sigma^2}\right] & \begin{Bmatrix} 0 \leq A \leq \infty \\ 0 \leq \Omega-\delta \leq 2\pi \end{Bmatrix} \\ 0 & \text{otherwise} \end{cases} \quad (3.5)$$

The marginal distribution of strength A is

$$f(A) = \int_0^{2\pi} p(A,\Omega)d\Omega$$

$$= \begin{cases} \dfrac{A}{\sigma^2} \exp\left(-\dfrac{A^2+\alpha^2}{2\sigma^2}\right) I_o\left(\dfrac{\alpha A}{\sigma^2}\right) & (0<A<\infty) \\ 0 & \text{otherwise} \end{cases} \quad (3.6)$$

where I_0 is the Bessel function of the first kind of order zero.

In summary, A is the strength of the fixed or specular component and $2\sigma^2$ is the r.m.s. strength of the random or scatter component. If the average power P is transmitted then the average power received is $(\alpha^2 + 2\sigma^2)P$ [14]. For convenience we define $\gamma^2 = \alpha^2/2\sigma^2$ as the ratio of the average power received via the fixed component to the average power received via the random component. As special cases, we obtain a nonfading channel when $\sigma^2 = 0$ or γ^2 approaches infinity or a Rayleigh fading channel when $\alpha^2 = 0$ or γ^2 approaches zero (see Appendix B).

3.3. ERROR PROBABILITY FOR FH/MFSK IN THE PRESENCE OF PARTIAL BAND JAMMER AND FADING

First we will determine the probability of error in a conventional MFSK system and based on this knowledge we will find the probability of error for FH/MFSK in the presence of partial band jammer and fading.

Recall the block diagram of the conventional MFSK shown in the second part of the diagram of Figure 2.11. Matched filters are located at each of the M frequencies. The output of the filters are fed to the envelope detectors and all M envelopes are sampled at the end of the symbol

period. Without loss of generality, let us assume that the symbol is transmitted on frequency f_1. The instantenous SNR at the peak of the filter is denoted as c. The pdf of the normalized envelope sample belonging to frequency f_1 is [15,21]

$$f(a_1) = a_1 \exp\left(-\frac{a_1^2 + 2c}{2}\right) I_o(a_1\sqrt{2c}) \tag{3.7}$$

the output of the other (M-1) filter has the distribution

$$f(a_i) = a_i \exp\left(-\frac{a_i}{2}\right) \qquad \begin{Bmatrix} a_i > 0 \\ i \neq 1 \end{Bmatrix} \tag{3.8}$$

since a_i, $i=2,3,\ldots,M$, are statistically independent and identically distributed, the joint probability conditioned on a_1 is .

$$Pr(a_2<a_1, a_3<a_1, \ldots, a_M<a_1 \mid a_1) = \left[Pr(a_2<a_1 \mid a_1)\right]^{M-1} \tag{3.9}$$

but

$$Pr(a_2<a_1 \mid a_1) = \int_0^{a_1} a \exp\left(-\frac{a^2}{2}\right) da$$

$$= 1 - \exp\left(-\frac{a_1^2}{2}\right) \tag{3.10}$$

Hence the correct signal is selected with the probability

$$P_c = \int_0^\infty \left[1-\exp\left(-\frac{a_1}{2}\right)\right]^{M-1} p(a_1)\, da_1$$

$$= \int_0^\infty \sum_{j=0}^{M-1} (-1)^j \binom{M-1}{j} \exp\left(-\frac{ja_1^2}{2}\right) \cdot a_1 \cdot \exp\left(-\frac{a_1^2+2c}{2}\right) \cdot I_o(a_1\sqrt{2c})\, da_1 \tag{3.11}$$

Using (6.631-4) of [9] we get

$$P_c = \sum_{j=0}^{M-1} (-1)^j \binom{M-1}{j} \frac{\exp(-c)}{j+1} \exp\left(\frac{c}{j+1}\right) \qquad (3.12)$$

The probability of selecting a wrong signal will be

$$P_M = 1 - P_c$$

$$= 1 - \sum_{j=0}^{M-1} (-1)^j \binom{M-1}{j} \frac{1}{j+1} \exp\left[\left(-\frac{j}{j+1}\right)c\right]$$

after some manipulation we get

$$P_M = \frac{1}{M} \sum_{j=2}^{M} (-1)^j \binom{M}{j} \exp\left[-\left(\frac{j}{j+1}\right)c\right] \qquad (3.13)$$

Equation (3.13) represents the probability for M-ary orthogonal signals in an AWGN channel with non coherent detection. In case the signal also experiences fading the frequency hopped signal can be expressed as

$$\tilde{s}(t) = \sqrt{2P}\, A \exp\{j[2\pi f(t)t - \varphi(t) - \theta]\} \qquad (3.14)$$

where A is the envelope of the signal that fades according to the Rice distribution. In addition, the signal is degraded by the noise jammer with average power J_{av}. As mentioned in Chapter 2, the noise jammer concentrates his energy within a fraction λ of the available frequency slots. That is, with probability λ a symbol is received in the

presence of white Gaussian noise of one sided spectral density N_{0J}. With probability $(1-\lambda)$ a symbol is received with AWGN of one sided spectral density N_0. Thus when the jammer is on we get

$$\left.\frac{E_b}{N_o}\right|_{eff} = \frac{E_b}{N_{oJ}+N_o} \tag{3.15}$$

assuming the power of jammer is much higher than N_0 we can rewrite (3.15) as

$$\left.\frac{E_b}{N_o}\right|_{eff} = \frac{E_b}{N_{oJ}} \tag{3.16}$$

Since the detection is noncoherent the phase in the signal of (3.14) can be ignored in the analysis. With A being the sum of the fixed and random components, A^2 is the output of the square-law envelope detector. Let ρ be the normalized bit ernergy to noise density ratio so that $A^2\rho$ is the actual received energy to noise density ratio [13]. We define:

$$\Lambda = E[A^2\rho \mid \text{interference is present}]$$

$$= \frac{E_s}{N_{oJ}} = \lambda\frac{E_s}{J_{av}/W} \tag{3.17}$$

as the ratio of average energy per symbol E_s to the noise density. We have already stated

$$f_A(a) = \frac{a^2}{\sigma^2}\exp\left(-\frac{a^2+\alpha^2}{2\sigma^2}\right) I_o\left(\frac{a\alpha}{\sigma^2}\right)$$

Thus

$$\Lambda = \lambda \frac{E_s}{J_{av}/W} = (\alpha^2+2\sigma^2)\rho \qquad (3.18)$$

for a Rician fading channel.

The conditional probability that A=a given that the interference is present is

$$P_I = \int_0^\infty P_M(a)\ f_A(a)\ da = \int_0^\infty (\sum_{j=1}^{M} P_{I_j}(a))\ da \qquad (3.19)$$

where $f_A(a)$ and $P_M(a)$ are given by (3.6) and (3.13) respectively, with c of (3,13) being replaced by $a^2\rho$.

The integration of (3.19) can be evaluated by using term by term integration with each term being represented by

$$P_{I_j} = \int_0^\infty \exp(-\frac{j-1}{j}\ a^2\rho)\frac{a^2}{\sigma^2}\exp(-\frac{a^2+\alpha^2}{2\sigma^2})\, I_o(\frac{a\alpha}{\sigma^2}) \qquad (3.20)$$

again we use (6.631-4) of [9] and after some manipulation we obtain

$$P_I = \frac{1}{M} \sum_{j=2}^{M} \binom{M}{j}(-1)^j \frac{1}{1+(1-j^{-1})\beta} \exp[-\frac{(1-j^{-1})\delta}{1+(1-j^{-1})\beta}] \qquad (3.21)$$

where

$$\beta = 2\sigma^2\rho$$

$$\delta = \alpha^2\rho$$

Finally, for convenience we define $\gamma^2=\frac{\alpha^2}{2\sigma^2}$ as the ratio of the average energy received via fixed component to the average energy received via random component. The average of a symbol error is $P_s \simeq \lambda P_I$ which can be represented in term of γ^2 and Λ, we get

$$P_s = \frac{\lambda}{M} \sum_{j=2}^{M} (-1)^j \binom{M}{j} \frac{\gamma^2+1}{(\gamma^2+1)+(1-j^{-1})\Lambda} \cdot \exp\left[-\frac{\gamma^2(1-j^{-1})\Lambda}{(\gamma^2+1)+(1-j^{-1})\Lambda}\right] \tag{3.22}$$

For M=2, we get the probability of bit error for BPSK as given in [1], [13] and [14].

Let $\sigma^2=0$, i.e., there is no random component in the received signal. Then $\gamma^2 = \infty$ and $\Lambda=\alpha^2\rho$. The resulting probability of error is

$$P_s = \frac{\lambda}{M} \sum_{j=2}^{M} (-1)^j \binom{M}{j} \exp\left[\left(-\frac{j-1}{j}\right) \alpha^2\rho\right] \tag{3.23}$$

which, in fact, is the expression for an AWGN channel with partial band jamming and no fading. If $\alpha=0$ we get $\Lambda = 2\sigma^2\rho$ and

$$P_s = \frac{\lambda}{M} \sum_{j=2}^{M} (-1)^j \binom{M}{j} \frac{1}{[1+(1-j^{-1})2\sigma^2\rho]} \tag{3.24}$$

which is the probability of error for a channel with partial band noise and Rayleigh fading.

If we wish to show the existence of the spread spectrum parameters in the above expressions, we just have

to replace Λ by

$$\Lambda = \lambda \frac{W/R_b}{J_{av}/P} \frac{1}{\log_2 M} \tag{3.25}$$

since

$$E_b = \text{bit energy} = \frac{E_s}{\log_2 M} = (P\log_2 M)/R_b$$

For binary case, we have $E_b = E_s$.

A smart jammer can select λ such that P_s of (3.22), (3.23) and (3.24) are maximized. In case of Rayleigh fading, the first and second order differentiations show that the optimal value of λ that maximize (3.24) is unity. That is for Rayleigh fading channel uniform jamming (λ=1) is the best strategy. In case of Rician fading, for the sake of simplicity, we let M=2. Doing the mathematical analyses we found that the optimal value of in this case is

$$\lambda = \frac{2(\gamma^2+1)}{(\gamma^2-1)\frac{E_s}{N_{oJ}}} \tag{3.26}$$

provided

$$0 \le \frac{E_s}{N_{oJ}} \le \frac{2(\gamma^2+1)}{(\gamma^2-1)} \tag{3.27}$$

Substituting of (3.26) into (3.22) with M=2 we get

$$P_s = \frac{(\gamma^2+1)e^{-1}}{\gamma^2 \frac{E_s}{N_{oJ}}} \tag{3.28}$$

The mathematical manipulation for higher signal alphabet (M>2) is not always feasible. However, this can be

done graphically as we will demonstrate in the next section. Optimum jamming is also known as worst case jamming in literature.

3.4 GRAPHICAL ANALYSES

In this section we show some curves of the probability of error in both cases of fading. Figures 3.2 to 3.4 show the curves of Rayleigh fading channel for M=2,4,16 respectively. Different curves are obtained in each figure according to different values of λ . We note that as the signal alphabet increases the signal to noise ratio (SNR) required to achieve a given bit error rate decreases as explained by (3.25). However, to get a 10^{-5} bit error rate we must have more than 40dB in SNR if FH/BFSK is used. The situation does not improve very much if the number of the available transmitted frequency is increased. The improvement is in the order of 5dB if 4-ary FSK is used, if 16-ary FSK is employed the improvement is about 10dB. Even though the increasing of the available frequency gives some power gain the use of M-ary FSK with frequency hopping in a Rayleigh fading and partial band jamming channel does not look very attractive. There exists a platform in bit error such that increasing in SNR does not further improve the performance. Furthermore, by looking at the curves, the jammer causes worst performance when λ=1 (uniform jammer). This agrees with the mathematical result shown before. So

with Rayleigh fading jammer does not have to build complicated jamming devices to make the channel performs poorly.

Figures 3.5 to 3.9 show the performance of FH/MFSK in a Rician fading channel with partial band jamming. The advantage of this channel is the parameter γ^2 which is the ratio of the fixed signal component over the random component. As γ^2 increases the performance of FH/MFSK gets better because the fixed signal component becomes a dominant term, making the channel more reliable. In this type of fading, the platform on the bit error rate does exist with low value of λ . For large γ^2 the platform disappears but if the jammer interferes with only a small fraction of the band, the transmitter still has to pay higher cost in SNR to have a reliable link. If the jammer is smart, it can find a value of λ that can maximize the error rate. It is shown by (3.26) that this value is a function of γ^2 and the SNR. The bit error rate for the worst case jamming is given by (3.28) as long as the SNR satisfies the condition of (3.27). If (3.27) no longer hold, uniform interference will cause worst case jamming. The worst case performance for FH/BFSK is depicted in Figure 3.5 by a dotted line. This line is tangential to the other curves of different values of λ . So the worst case performance for higher signal alphabet (M>2) can be found graphically. In chapter 4 and 5, we will show how the use of error control coding can entirely eliminate the loss in SNR in fading and jamming channel.

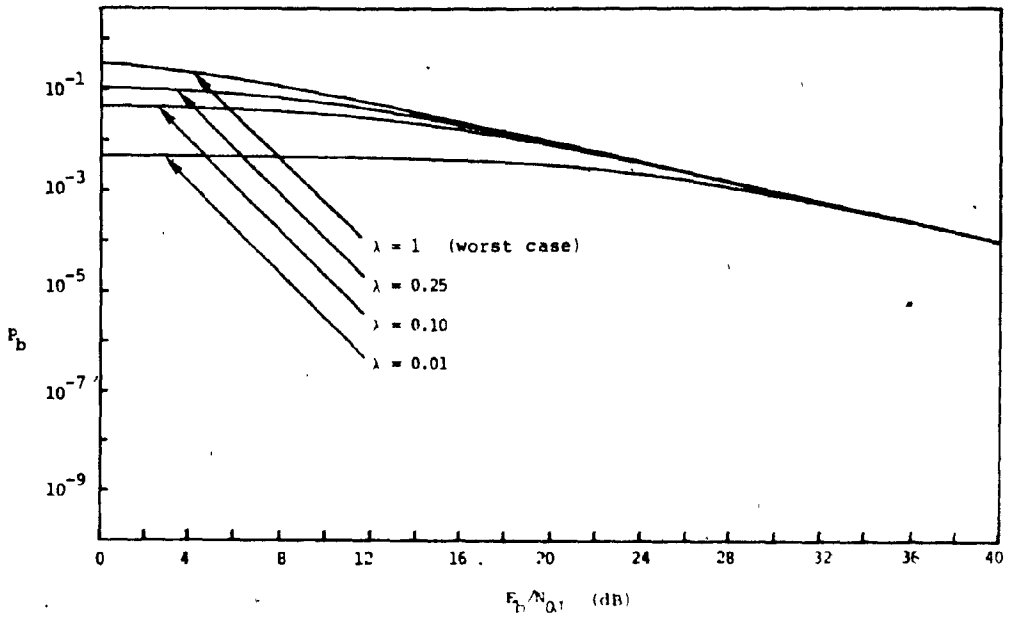


Figure 3.2: Performance of FH/BFSK in partial band jamming and Rayleigh fading

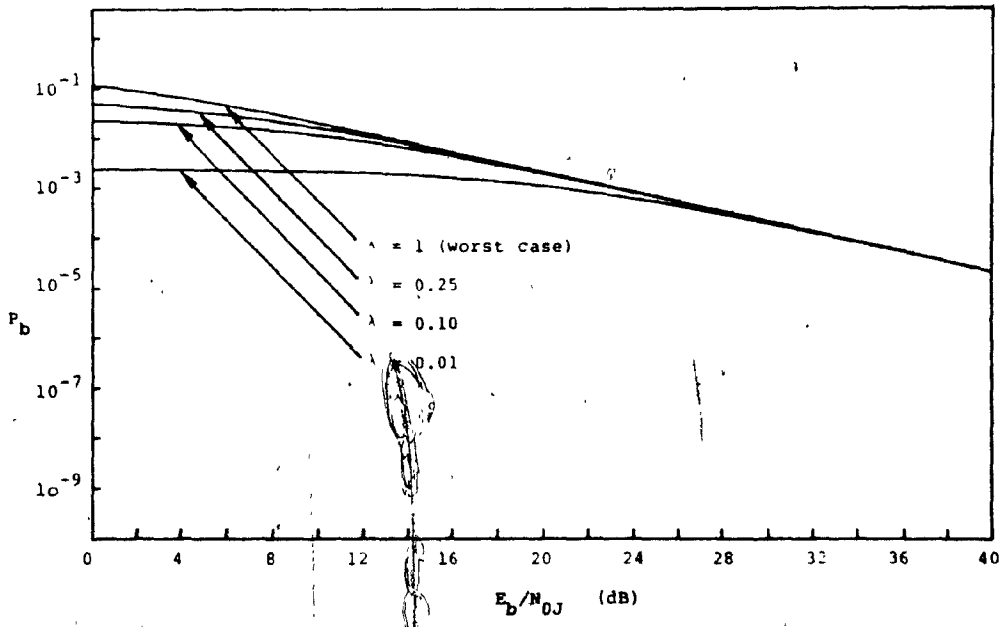


Figure 3.3: Performance of FH/4-ary FSK in partial band jamming and Rayleigh fading

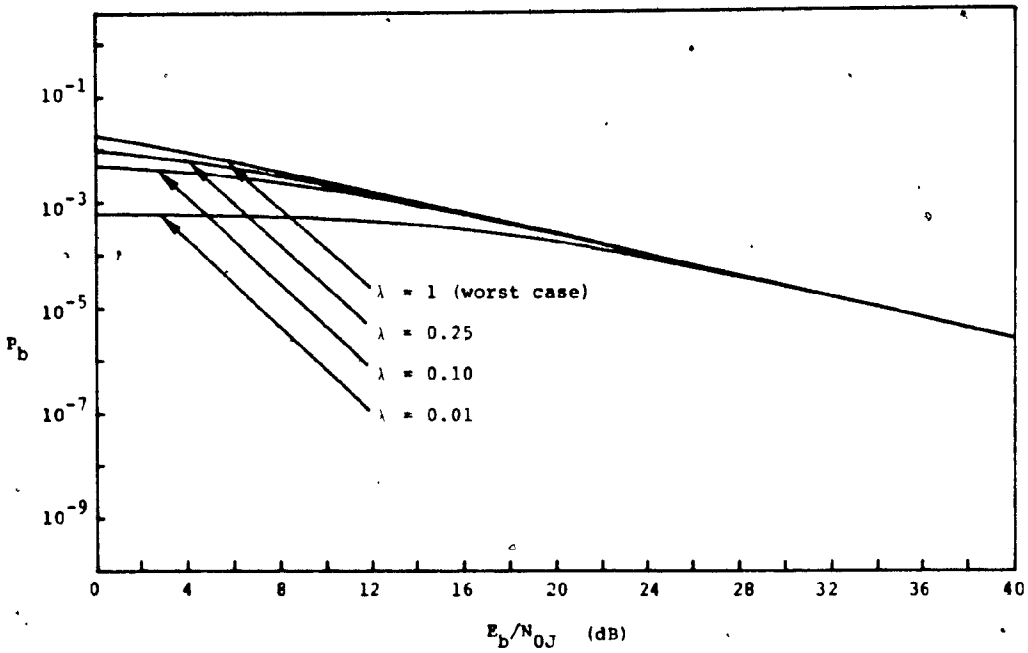


Figure 3.4: Performance of FH/16-ary FSK in partial band jamming and Rayleigh fading

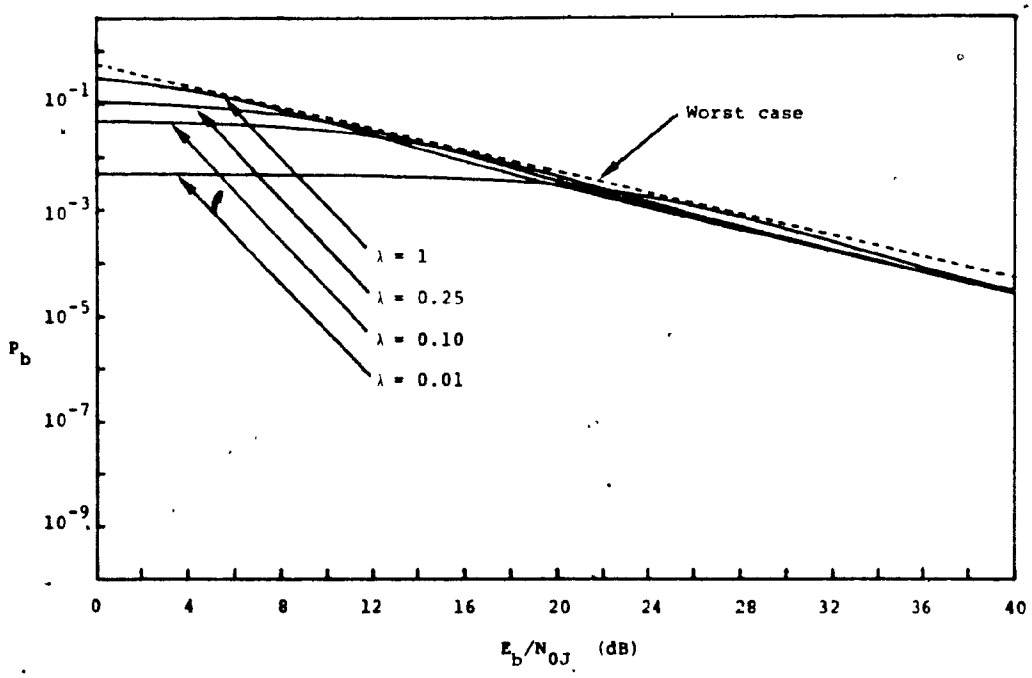


Figure 3.5: Performance of FH/BFSK in partial band jamming and Rician fading, γ^2=2dB

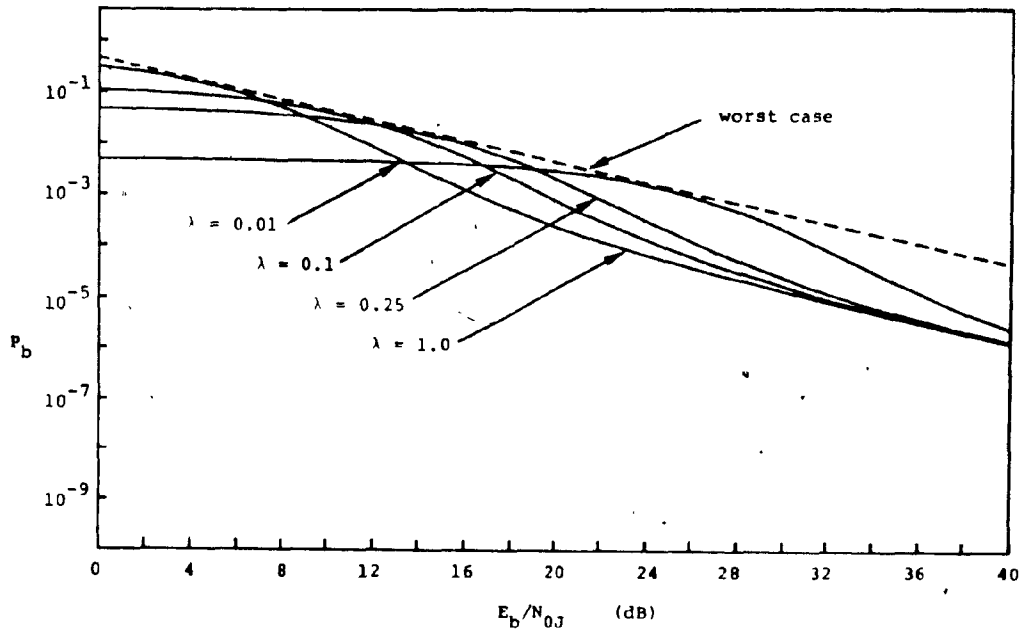


Figure 3.6: Performance of FH/BFSK in partial band jamming and Rician fading, γ^2=4dB

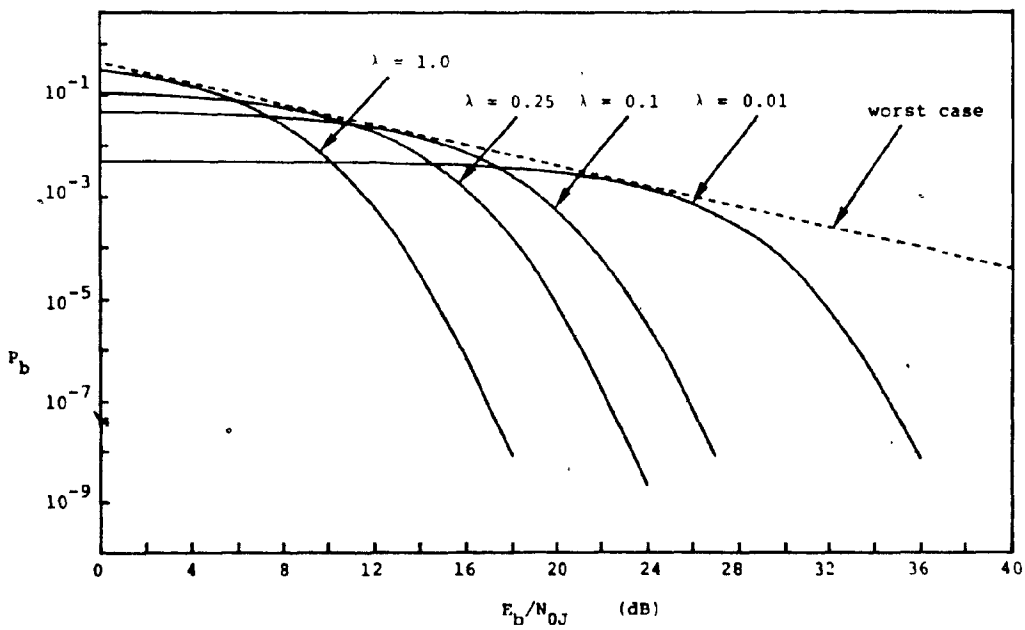


Figure 3.7: Performance of FH/BFSK in partial band jamming and Rician fading, γ^2=8dB

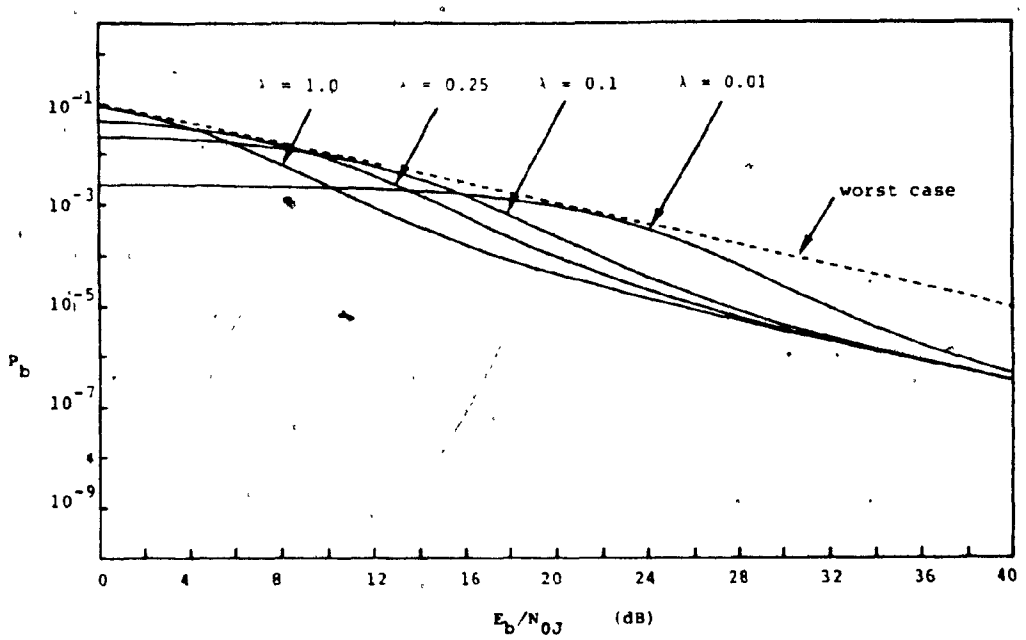


Figure 3.8: Performance of FH/4-ary FSK in partial band jamming and Rician fading, γ^2 =4dB

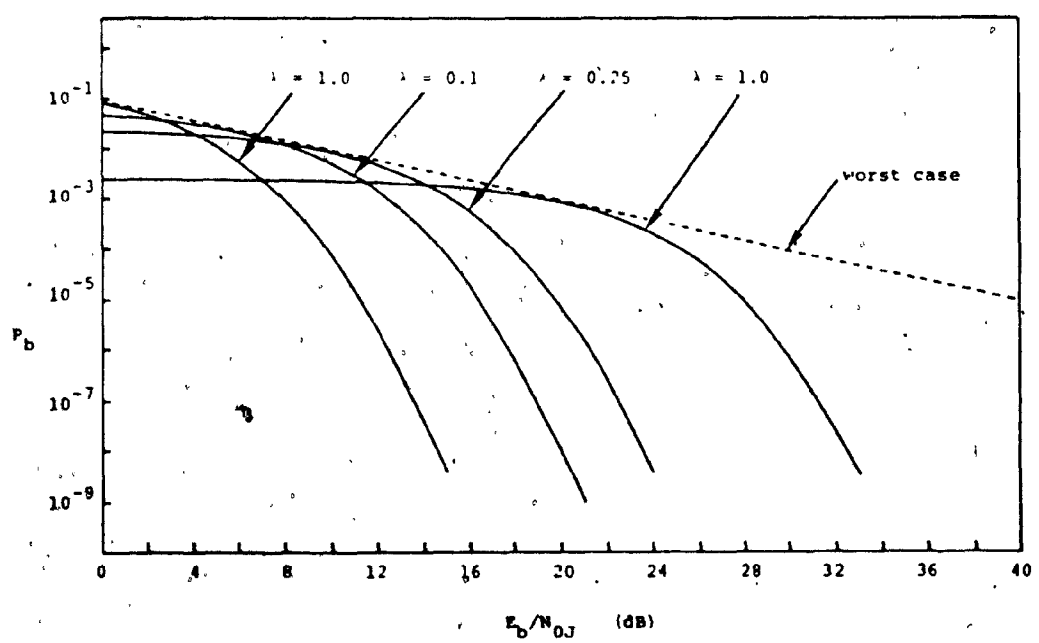


Figure 3.9: Performance of FH/4-ary FSK in partial band jamming and Rician fading, γ^2=8dB

CHAPTER 4

PERFORMANCE OF CODED SPREAD SPECTRUM SYSTEM BASED ON THE CUT OFF RATE R_0

4.1 INTRODUCTION

In 1948 Claude Shannon wrote [45] :

"The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point."

To solve the problem Shannon created a new branch of applied mathematics called information theory and coding. The information theory formulates the basic problem of reliable transmission in statisical terms using probabilistic model for information sources and channels. The source is modelled as a random generator of data or stochastic signal to be transmitted. The source encoder shown in Figure 4.1 converts analog signal into a sequence of binary digits. If the source is digital in nature, there is no need for a source encoder. The second block of Figure 4.1 is the channel encoder and is of interest to us. Shannon proved that in order to reduce errors one must find how to code the information signal rather than increasing the signal-to-noise ratio (SNR). That is one should code long sequences

of bits into a channel, input sequence so that each bit of information is spread thinly over the channel used [45].

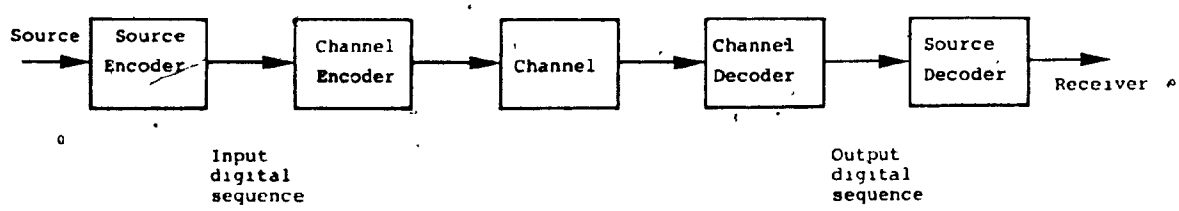


Figure 4.1: Basic model of a digital communication system

The idea was revolutionary at the time the paper was published and not everybody agreed with Shannon. As technology progressed, the idea became obvious and the problem was to find ways to encode information sequences. The encoding scheme would give minimum error rate and should be implementable. There are different ways to encode information signals but we can group them into block codes and convolutional codes. The error performance of specific coded signals can be evaluated using the upper bounds. However, these bounds cannot be calculated easily unless one has a powerful computer. Thus one relies on a so called random coding bound. The basis of this technique is: given that the calculation of the error probabilities for a particular set of 2^k code words of length n is not feasible, consider instead the average error probability over the ensemble of all possible sets of 2^k signals of code rate r. This turns out to be amazingly simple to calculate [46].

In this chapter we will define some fundamental terms used in coding theory. The concepts of block coding and convolutional coding will be introduced next. Finally, the performance of coded FH/MFSK based on the average ensemble performance analysis will presented. Recent research works will also be summarized in this chapter.

4.2 FUNDAMENTAL DEFINITIONS

Let C be an (n,k) code then the Hamming weight of a codeword $\underline{v} \in C$, denoted $w_H(\underline{v})$ defined to be the number of nonzero components of $\underline{v}$. Let A be the number of codewords of weight i in C. The number $A_0, A_1, A_2, \ldots, A_n$ are called weight distribution of C [7,8,18].

The Hamming distance, d_H, between two codewords $\underline{u}$ and $\underline{v}$ is the number of positions in which they differ, clearly

$$d_H(\underline{u},\underline{v}) = w_H(\underline{u}+\underline{v}) \tag{4.1}$$

That is, the Hamming distance between $\underline{u}$ and $\underline{v}$ equals the Hamming weight of the sum of $\underline{u}+\underline{v}$. The minimum distance d_m is defined as

$$d_m = \min\{d_H(\underline{u},\underline{v});\ \underline{u},\underline{v} \in C,\ \underline{u} \neq \underline{v}\}$$

$$d_m = \min\{w_H(\underline{u}+\underline{v});\ \underline{u},\underline{v} \in C, \underline{u} \neq \underline{v}\}$$

$$= \min\{w_H(\underline{x})\ ;\ \underline{x} \in C\ ,\ \underline{x} \neq \underline{0}\} \qquad (4.2)$$

Since $\underline{u}$ and $\underline{v}$ are codewords of a linear code, then the sum $\underline{x}=\underline{u}+\underline{v}$ is also a codeword in the same set. Thus the minimum distance of a linear block code is equal to the minimum weight of its non zero codeword [7,8,18].

Usually after a message sequence is encoded, its binary digits from the encoder are fed into a modulator, which maps each bit into an elementary signal waveform. At the receiving end the modulator may be viewed as a filter matched to the signal waveform corresponding to each transmitted bit. The sampled output of the demodulator may or may not be quantized. If binary quantization is used, we say that a hard decision has been made on each bit [19]. The sequence detected become input to the decoder, which takes the detected bits and attempts to recover the information sequence. Since the decoder operates on the hard decisions made by the demodulator, the decoding process is called hard-decision decoding [3,19].

With coding, it is desirable to keep an indication of how reliable the decision is. A soft-decision decoder takes the analog (unquantized) outputs from the demodulator and computes a "confidence" number [19] which specifies how far from the decision threshold the demodulator is.

However, it is quite complex to operate with the unquantized values. Most commonly the three-bit quantization is employed in a soft-decision decoder.

4.3 CODING TECHNIQUES

4.3.1 LINEAR BLOCK CODES

In block coding scheme, the binary information bit sequence is partioned into block of k bits. Each such block is mapped into an n-bit codeword (n>k). Thus every n-bit transmitted contains only k information bits. The code rate is defined as r=k/n. [7,18].

Let $\underline{u}$, a k-tuple, represent information bit and $\underline{v}$, a n-tuple, represent a codeword. The relationship between $\underline{u}$ and $\underline{v}$ is

$$\underline{v} = \underline{u}.\underset{\sim}{G} \tag{4.3}$$

where $\underset{\sim}{G}$ is the (n x k) generator matrix and is represented as

$$\underset{\sim}{G} = \begin{bmatrix} \underline{g}_1 \\ \underline{g}_2 \\ \underline{g}_3 \\ \vdots \\ \underline{g}_k \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & g_{13} & \cdots & g_{1n} \\ g_{21} & g_{22} & g_{23} & \cdots & g_{2n} \\ g_{31} & g_{32} & g_{33} & \cdots & g_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & g_{k3} & \cdots & g_{kn} \end{bmatrix} \tag{4.4}$$

The number of information bit is k, thus the total number of distinct codewords is 2^k. The requirement to get 2^k codewords is equivalent to the requirement that k rows of $\underset{\sim}{G}$ be linear independent [7,18].

An important subclass of linear codes is the class of cyclic codes. They are attractive because the encoding part can be implemented easily by employing shift registers with feedback connections [33,34]. Secondly, because they have good algebraic structure it is possible to find practical decoding method. An (n,k) linear code C is called a cyclic code if every cyclic shift of a codeword in C is also a codeword in C [7,18].

It is shown elsewhere [7,18] that the generator polynomial g(x) of an (n,k) cyclic code is a polynomial of degree (n-k) and is a factor of (x^n+1). The generator matrix $\underset{\sim}{G}'$ of an (n,k) cyclic code C generated by $g(x)=g_0+g_1x+\ldots+g_{n-k}x^{n-k}$ can be expressed as

$$\underset{\sim}{G}' = \begin{bmatrix} g_0 & g_1 & g_2 & g_3 & \cdots & g_{n-k} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k-1} & g_{n-k} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k-1} & g_{n-k} & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & 0 & 0 & g_0 & \cdots & & & \cdots & & g_{n-k} \end{bmatrix} \quad (4.5)$$

The encoding circuit is shown in Figure 4.2. All register contents are initiated to zero and the gate is a switch which is open (OFF) when parity bits are shifting out from the encoder.

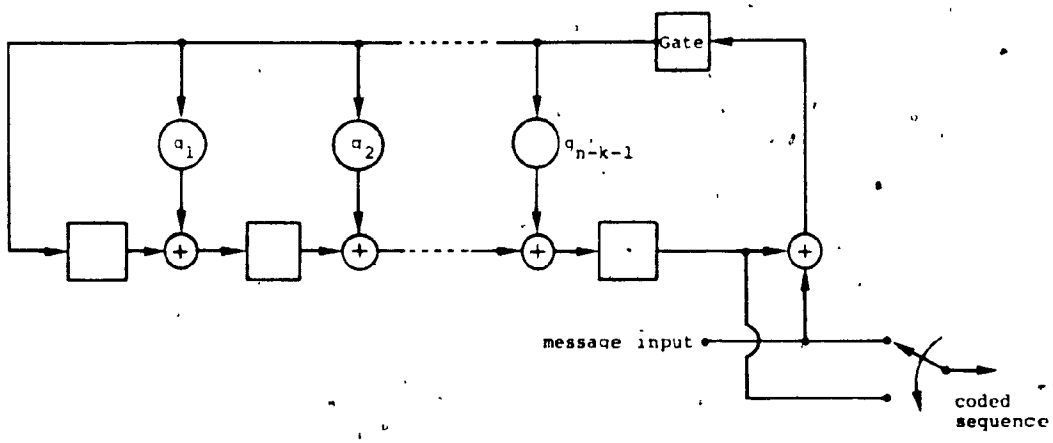


Figure 4.2: Encoder circuit for an (n,k) cyclic code with generator $g(x)=1+g_1x+\ldots+g_{n-k}x^{n-k}$

Let $\underline{a}$ be the codeword sent and $\underline{r}$ be the received word. The received word $\underline{r}$ can be represented in the form of a polynomial of degree (n-1) or less

$$r(x) = r_0 + r_1x + r_2x^2+\ldots+r_{n-1}x^{n-1} \tag{4.6}$$

Dividing r(x) by the generator polynomial g(x), we obtain

$$r(x) = a(x)\ g(x) + s(x) \tag{4.7}$$

Thus s(x) is the remainder of degree (n-k-1) or less. s(x) is identical to zero only if the received polynomial r(x) is the code polynomial or $\underline{r}$ is a codeword.

$s(x)$ is better known as the syndrome polynomial and has an important position in the decoding process.

Let $v(x)$ be the code polynomial and $e(x)$ be the error polynomial of degree $(n-1)$ or less. The received polynomial $r(x)$ is

$$r(x) = v(x) + e(x) \tag{4.8}$$

from (4.7), we have

$$r(x) = v(x) + e(x) = a(x)\, g(x) + s(x)$$

Thus

$$e(x) = [a(x)+b(x)]g(x) + s(x) \tag{4.9}$$

where $b(x)g(x) = v(x)$. This shows that $s(x)$ is the remainder in dividing $e(x)$ by $g(x)$. The syndrome can be calculated from the received word by using (4.7), the error $e(x)$ is unknown to the decoder. Therefore, $e(x)$ must be estimated based on the syndrome. Syndrome computation is well documented in [18].

Some commonly used codes are cyclic codes. They include the Hamming codes, the Bose-Chaudhuri-Hocquenghem (BCH) codes, the Golay codes and the Reed-Solomon (RS) codes [7,18,19]. Their algebraic structures are well defined and can be found in any book on coding theory [7,8,32].

4.3.2 CONVOLUTIONAL CODES

Unlike block codes, the convolutional codes do not break the information into blocks and handle them independently . The convolutional code associates a code sequence with an information sequence [32]. The encoding process is as follows: the given information sequence is broken into k-symbol blocks, the blocks are then used to specify the paths in a tree as shown in Figure 4.3

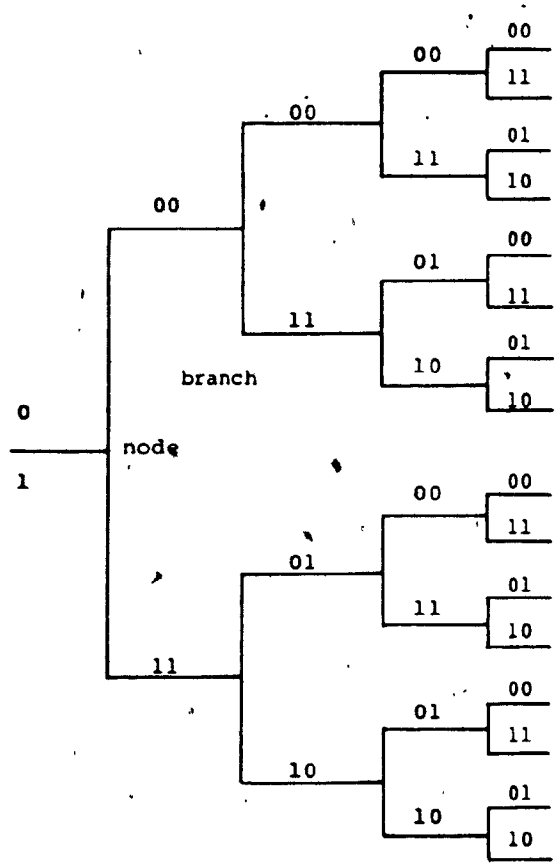


Figure 4.3: A section of a binary tree of a convolutional code

The first block of the information sequence is used to specify one of the branches of the first node according to some prearranged convention. The second block will choose the branch at the second node and so on. In this way a single path is traced through the tree. The n-tuples associated with each branch in the path form the code. As in case of block codes, encoder for convolutional codes can be implemented using shift registers. In general, the shift register consists of L(k-bit) stages and n linear algebraic function generators as shown in Figure 4.4. The binary data is shifted into and along the shift register k bits at a time and the output is a sequence of n bits. The code rate is defined as r=k/n and L is called the constraint length of the code.

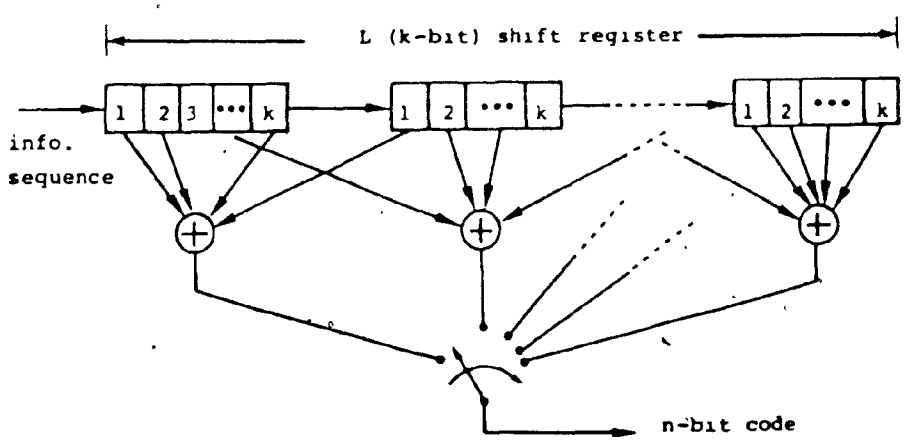


Figure 4.4: A general convolutional encoder

Unlike block codes several distance measures have been proposed for convolutional codes. Let $\underline{u}=(u_1,u_2,\ldots)$ and $\underline{v}=(v_1,v_2,\ldots)$ be two input information sequences, and

let $\underline{x}$ and $\underline{y}$ be the corresponding codewords. The Hamming distance $d^{(u,v)}(n)$ between two codewords of length n, $\underline{x}$ and $\underline{y}$, is equal to the number of positions where $\underline{x}$ and $\underline{y}$ differ [7]. That is

$$d^{(\underline{u},\underline{v})}(n) = d_H(\underline{x}_n,\underline{y}_n) = w_H(\underline{x}_n,\underline{y}_n) \tag{4.10}$$

where d_H and w_H denote the Hamming distance and weight, respectively.

The n-th order column distance function $d_c(n)$ is defined as the minimum Hamming distance between all pairs of codewords of length n branches which differ in their first branch of the code tree [7]. It is given by

$$d_c(n) = \min_{\underline{u}_1 \neq \underline{v}_1} d_H(\underline{x}_n,\underline{y}_n) \qquad \underline{x}_1 \neq \underline{y}_1 \tag{4.11}$$

Two particuliar values of $d_c(n)$ of special interest are the minimum distance d_m and the free distance d_f which are defined as

$$d_m = d_c(L) \qquad \text{L: constraint length} \tag{4.12}$$

$$d_f = \lim_{n \to 0} d_c(n) \tag{4.13}$$

In general, $d_m < d_f$ but for many codes we have $d_f = d_m$. The minimum distance and the free distance are the parameters used in determining the performance of

convolutional codes.

The optimal decoding operation for convolutional codes requires a memory that stores a function of the entire past history of the received bit stream. The performance of a convolutional coding system improves as the memory for the decoder is increased. Several methods of decoding convolutional codes have been developed. The optimal scheme is generally known as the Viterbi algorithm. Other approaches are the sequential decoding and the threshold decoding. In this thesis we consider only Viterbi algorithm because the constraint length of the analyzed codes are reasonably short. Detail description of the above decoding algorithm may be found in [5,7,18,32,46].

4.4 ENSEMBLE AVERAGE ERROR PROBABILITY

4.4.1 SOME BACKGROUND

Usually when choosing a code for a communication link we face the problem of choosing code length, code rate and various different parameters. It would be time consuming if we take every single existing code and then apply to the system to get the minimum bit error rate. Thus it would be a good idea to investigate the minimum achievable probability of decoding error as a function of the code rate r of an ensemble of codes rather than just one

good code. Each code in the ensemble has its own probability of decoding error. Since at least one code in the ensemble must have an error probability as small as the ensemble average, this will give us an upper bound on the probability of error for the best code, i.e., the code with minimum P_e [8,47].

Consider a discrete memoryless channel (DMC) with transition probability $p(\underline{y}|\underline{x})$ and an ensemble of (n,k,d) block codes in which each bit of each codeword is independently selected with probability assignment $Q(\underline{x})$. The ensemble average probability of decoding error is bounded by

$$\bar{P}_e \leq 2^{\{-n[E_0(\rho,Q) - \rho r]\}} \tag{4.14}$$

where

$$E_0(\rho,Q) \doteq -\log_2 \sum_{\underline{y}\in \mathcal{b}} \left\{ \sum_{\underline{x}\in \mathcal{a}} Q(\underline{x})\, p(\underline{y}|\underline{x})^{\frac{1}{1+\rho}} \right\}^{\frac{1}{1+\rho}}$$

ρ is arbitrary and $0<\rho<1$ [47]. $\mathcal{a}$ and $\mathcal{b}$ are input and output alphabets respectively. Since ρ and Q are arbitrary in (4.14) we get the tightest bound by choosing ρ and Q to maximize $E_o(\rho,Q)-\rho r$. This leads us to define the random coding exponent $E_R(r)$ by

$$E_R(r) = \max_{0\leq\rho\leq 1} \max_{Q} [E_o(\rho,Q) - \rho r] \tag{4.15}$$

Of special interest is the cut off rate, R_0, which is defined as

$$R_o = \max_Q [E_o(1,Q)] \tag{4.16}$$

R_0 is the largest rate at which practical coding system can be implemented. Thus the upper bound of the average ensemble probability of error in term of R_0 is

$$\bar{P}_e \leq 2^{-\{n(R_o - r)\}} \tag{4.17}$$

Following the same argument as Gallger's Viterbi [4,46] derived the average ensemble probability of error for convolutional code as

$$\bar{P}_e \leq \frac{2^{-L\frac{R_o}{r}}}{\left\{1-2^{-(\frac{R_o}{r}-1)}\right\}^2} \tag{4.18}$$

The performance of coded systems depend strongly on the value of R_o which is the function of the symbol energy to noise ratio. For the DMC with equally likely inputs the calculation is straight forward. In particular, for the BSC with transition probability p and Q(1)=Q(0)=1/2, (4.16) yields

$$R_o = 1 - \log_2[1 + 2\sqrt{p(1-p)}\,] \tag{4.19}$$

So, in general, cut off rate can be expressed as

$$R_o = \log_2 M - \log_2[1 + (M-1)D] \tag{4.20}$$

where M is the signal alphabet and D is a parameter which is determined by the channel used. In the next section we will show that the performance of a spread spectrum system can be improved by using coding. The performance is based on the cut off rate R_o and from the curves of the cut off rate versus signal-to-noise ratio we can see what code rate we should use to obtain best communication link.

4.4.2 PERFORMANCE OF CODED SPREAD SPECTRUM BASED ON THE CUT OFF RATE R_0

Let x be the transmitted signal and y be the received signal, then

$$y = x + n$$

where n is the Gaussian noise introduced to the channel by an intentional jammer. The jammer interferes for only a fraction λ of the time. During this time the jammer one sided noise density level is N_{oJ}. If the decoder operates on the quantized output from the demodulator and has information on the jamming state, the cut off rate is given as [4]

$$R_o = 1 - \log_2[1 + \exp\{-\lambda E_c/N_o\}] \qquad (4.21)$$

provided DS-BPSK is applied at the transmitted end and

$$\frac{E_c}{N_o} = r\,\frac{E_b}{N_o} = r\,\frac{W/R_b}{J_{av}/P}$$

Rewriting (4.21) in term of E_b/N_{oJ} we have

$$\frac{E_b}{N_o} = -\frac{\alpha}{\lambda R_o} \ln\left[\frac{2^{1-R_o}-1}{\lambda}\right] \tag{4.22}$$

where

$$\alpha = \frac{R_o}{r} < 1$$

The aim of the jammer is to maximize (4.22). Using the differentation method the optimal duty factor λ is found as

$$\lambda = (2^{1-R_o}-1)e \tag{4.23}$$

provided $0<\lambda<1$, hence $R_o > 1-\log_2(1+e^{-1}) = 0.548$. If $R_0 < 0.548$, $\lambda = 1$ is the optimal duty factor. Thus

$$\frac{E_b}{N_0}\max = \begin{cases} \dfrac{\alpha e^{-1}}{R_o(2^{1-R_o}-1)} & R_o > 0.584 \\ -\dfrac{\alpha}{R_o}\ln(2^{1-R_o}-1) & R_o \leq 0.548 \end{cases} \tag{4.24}$$

The quantity $[10\log E_b/N_{oJ} - 10\log\alpha]$ is plotted in Figure 4.5 as a function of $1/R_o$. Thus for a given code rate, r we need to select a value of α to guarantee the required bit error rate according to (4.17) and (4.18). This establishes R_o according to $\alpha = R_o/r$. Finally, we obtain E_b/N_{oJ} by adding $10\log\alpha$ to the ordinate of Figure 4.5 for the given R_o.

It is shown in [5] that for DS/BPSK the loss due to worst case partial time jammer is around 35dB at 10^{-5} BER. As seen in Figure 4.5 coding recovers all the loss and with

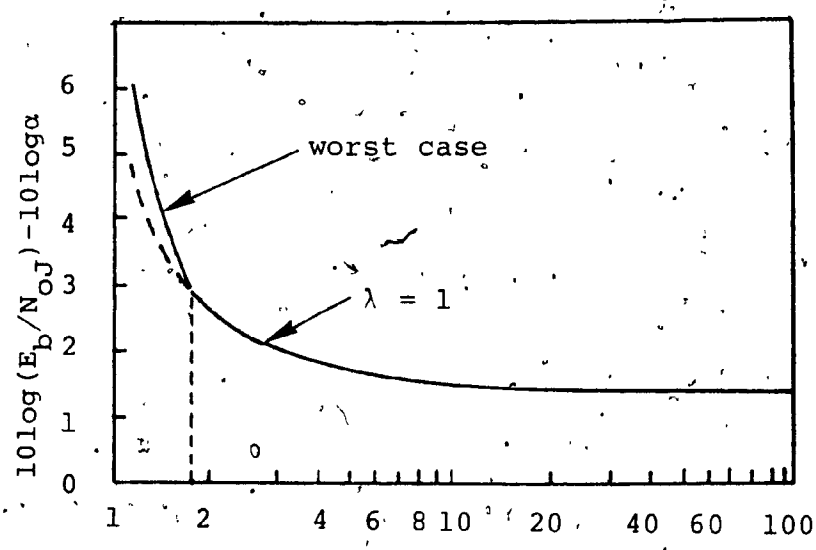


Figure 4.5: E_b/N_{oJ} requirement in worst case partial band jamming

$R_o < 0.548$ coding makes the jammer appears as uniform noise. Now if the channel also experiences fading or specially the signal is faded while the jammer is unfaded. The received signal is

$$y = ax + n \tag{4.25}$$

If both signal and noise are fading and fading is happening independently, then

$$y = ax + bn \tag{4.26}$$

where a and b are independently distributed random variables having a Rayleigh distribution

$$f(\alpha) = \frac{\alpha}{\sigma^2} \exp\{-\frac{\alpha}{2\sigma^2}\} \qquad (\alpha \geq 0) \tag{4.27}$$

The cut off rate R_o for the case of faded signal and unfaded jammer is given as [28]

$$R_o = 1 - \log_2\left(1+\frac{1}{r\bar{\gamma}_b+1/\lambda}\right) \qquad \bar{\gamma}_b \geq 0 \tag{4.28}$$

where $\bar{\gamma}^2=E[\alpha^2 E_b/N_{oJ}]$ is the average signal to noise ratio. From (4.28) the optimum jammer duty factor is $\lambda=1$, i.e., broadband jamming. The operation at cut off rate and optimal jamming yields [28]

$$\bar{\gamma}_b = \frac{1}{R_o}\left[\frac{2-2^{1-R_o}}{2^{1-R_o}-1}\right] \tag{4.29}$$

In case of faded signal and faded jammer the cut off rate is given as [28]

$$R_o = 1 - \log_2[2 + r\bar{\gamma}_b \exp\{r\bar{\gamma}_b\}\, E(-\bar{\gamma}_b)] \qquad (\bar{\gamma}_b > 0) \tag{4.30}$$

where

$$E(x) = \int_{-\infty}^{x} \frac{e^{-t}}{t}\, dt \qquad (x<0)$$

The worst case jamming for this type of channel happens at $\lambda=1$. Figure 4.6 is the plot of the required average received bit energy to noise ratio for operation at the cut off rate R_o and worst case jamming. This plot, in combination with Figure 4.5, shows that fading in jamming signal improves the performance of coded system, with a larger improvement at lower rates. In all cases, the faded signal with unfaded jammer case give worst performance which is as expected. However, at lower rate (less than 0.5 bit/symbol) there is noticeable improvement as seen in Figure 4.6.

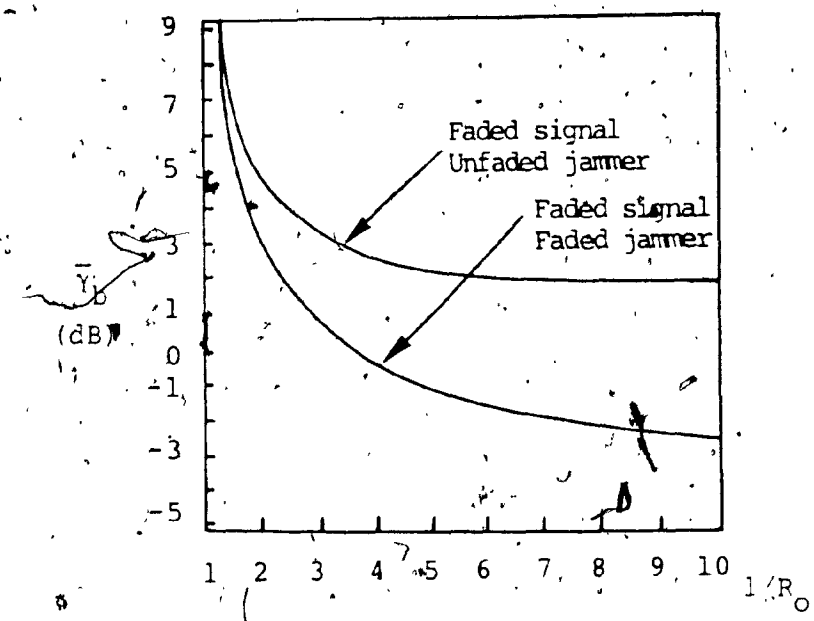


Figure 4.6: SNR requirement for operation at cut off rate for DS/BPSK with partial time jammer[28]

If frequency hopping is used instead of direct sequence spread spectrum then we can use higher signal alphabets. There is nothing to gain by using multiple signal alphabets for coherent, direct sequence system [4]. The cut off rate in general form is as given before

$$R_o = \log_2 M - \log_2[1-(M-1)D]$$

where M is the signal alphabet and D is determined by the channel of interest. Again we consider three types of channel as in the case of DS/BPSK. Parameter D is found for different cases as shown below

a) Unfaded signal and unfaded jammer [4]

$$D = \begin{cases} \frac{1}{1+\rho} \exp\{-\frac{\rho}{1+\rho}(\frac{rE_b}{N_o}) \log_2 M\} & r\frac{E_b}{N_0} < 3dB \\ \frac{4e^{-1}}{(r\frac{E_b}{N_o}) \log_2 M} & r\frac{E_b}{N_o} \geq 3dB \end{cases} \quad (4.31)$$

b) Faded signal with an unfaded jammer [28]

$$D = \int_0^\infty \frac{a\lambda}{\sigma^2(1-\rho^2)} \exp\{-(\frac{\rho}{\rho}\lambda\gamma_c^2+1)\} \frac{a^2}{2\sigma^2} da \qquad (4.32)$$

c) Faded signal with a faded jammer [28]

$$D = \int_0^\infty\int_0^\infty \frac{ab}{\sigma^4(1-\rho^2)} \exp\{-\frac{\rho a^2\bar{\gamma}_c}{(1+\rho^2)b^2} - \frac{a^2}{\sigma^2} - \frac{b^2}{\sigma^2}\} da\, db \qquad (4.33)$$

For all the cases, we have

$$\rho = [-(1+\delta) + \sqrt{(1+\delta)^2+4\delta}]/2 \qquad (4.34)$$

with

$$\delta = \frac{E_c}{N_{oJ}}/2 = \frac{1}{2}\frac{E_b}{N_{oJ}} \log_2 M \qquad (4.35)$$

for case (a). For case (b), we have

$$\delta = \lambda \frac{\alpha^2\bar{\gamma}_c}{\sigma^2} \qquad (4.36)$$

and for case (c) we have

$$\delta = \lambda \frac{a^2}{b^2}\frac{\bar{\gamma}_c}{2} \qquad (4.37)$$

where $\bar{\gamma}_c = r\,\bar{\gamma}_b \log_2 M$ and $\bar{\gamma}_b$ were defined before in case of DS/BPSK.

The worst case partial band jamming is the uniform jamming in the two latter cases. In case there is no fading

the optimal λ is $\lambda=1$ when E_c/N_{oJ} <3dB while if E_c/N_{oJ}>3dB the optimal λ is $\lambda=3/(4E_c/N_{oJ})$. The operation at cut off rate $r=R_o$ of E_b/N_{oJ} versus the cut off rate are plotted in Figures 4.7 to 4.9. From these figures we can see that when both the signal and jammer are faded the performance no longer increases with increasing M. This in fact happens for FH/MFSK over an AWGN channel. As in the case of DS/BPSK a system with faded signal and an unfaded jammer perform very poorly compared to other cases. However at low rates the system is acceptable for cases (b) and (c). If both the signal and jammer are unfaded, the SNR increases at both very low rate and high rate. The increases at high rates is due to the lack of coding redundancy [4]. The increases at low rate is due to higher loss in noncoherent combining [4,28].

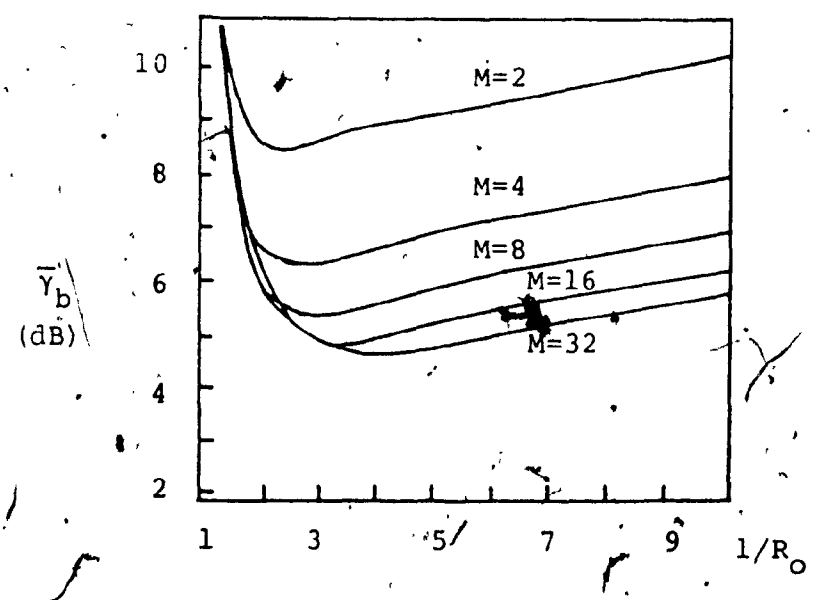


Figure 4.7: SNR requirement for operation at cut off rate. Unfaded FH/MFSK signal and unfaded [28] optimal jammer

We have demonstrated that coding is critical to adequate performance of spread spectrum system. Once the curves of the inverse of R_o versus SNR are established we can find the average ensemble probability of error based on equations (4.17) and (4.18). For MFSK the value 2 in (4.17)

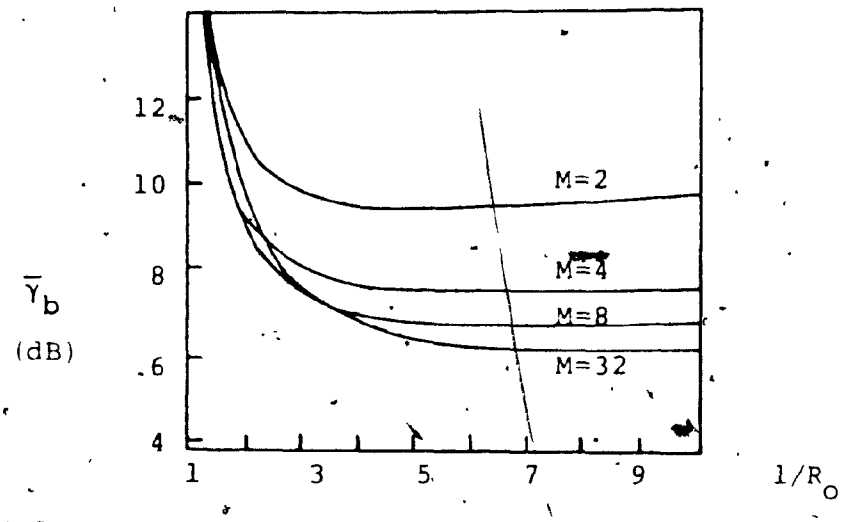


Figure 4.8: SNR requirement for operation at cut off rate Faded FH/MFSK signal and unfaded jammer [28]

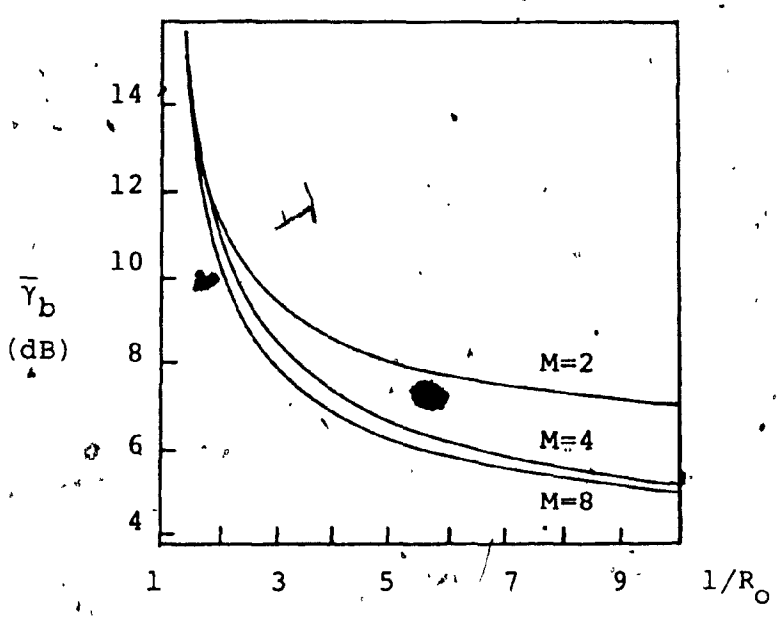


Figure 4.9: SNR requirement for operation at cut off rate. Faded FH/MFSK signal and faded jammer [28]

and (4.18) must be replaced by M. Thus for different values of λ we can find the corresponding E_b/N_{oJ} and then establish the performance curves.

From the average ensemble probability of error we can determine at what code rate we should operate for different channels. If we wish to find the performance of the specific code for the determined rate r, we have to do some transformations as proposed by Omura et al [27]. Instead of considering the whole system as depicted in Figure 4.1 in their analysis Omura et al decouple the system into two parts as shown in Figure 4.10.

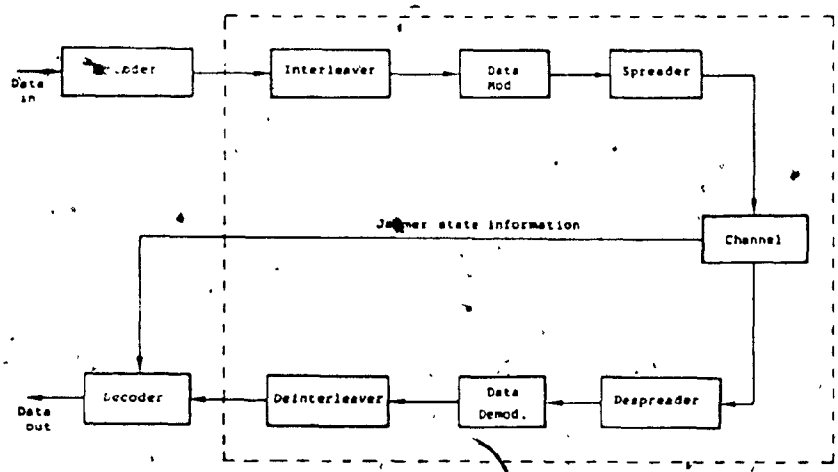


Figure 4.10: Decoupled communication link [27]

If we do not consider the coder and the decoder, we do not have to bother about the bit energy and the code rate. Instead we use coded symbol energy $E_c=rE_b$ in the analysis. For clarity we will take an example to demonstrate the approach, the same steps will be applied to

any other cases.

Let us assume that BPSK is used in an additive white Gaussian noise channel. At the receiving end the output of the demodulator will pass through a quantizer. If the quantizer forces a decision on each transmitted code symbol into either of the two levels then we have a binary symmetric channel (BSC). This results in a hard decision channel. If the decoder operates on the actual demodulated voltage (converted into digital form) we called it a soft decision channel. For the BSC channel the cut off rate is

$$R_o = 1 - \log_2[1 + 2\sqrt{p(1-p)}]$$

where p is the transition error probability.

If soft decision is assumed, the parameter D in the expression for R_0 is given as [27]

$$D = e^{-E_c/N_{oJ}} \tag{4.38}$$

Thus

$$R_o = 1 - \log_2[1 + e^{-E_c/N_{oJ}}] \tag{4.39}$$

Figure 4.11 shows R_0 versus E_c/N_{oJ} for the soft and hard decision detector.

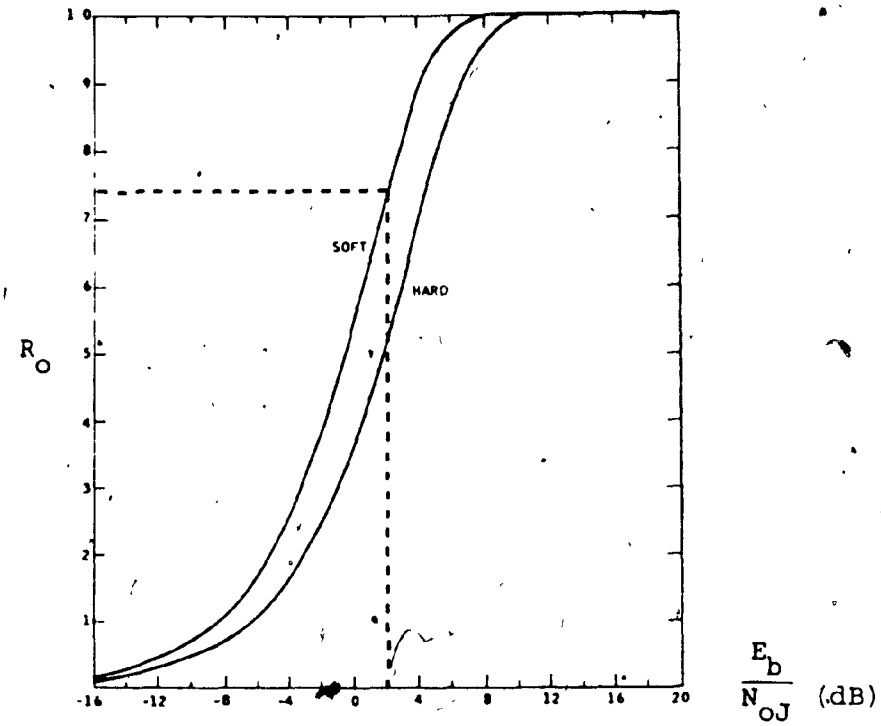


Figure 4.11: R_o for hard and soft decision detections[27]

The cut off rate given by (4.19) and (4.39) are for the channel which has uniform (broadband) white Gaussian noise and modulator does not use spread spectrum. If the transmitter decides to use DS/BPSK, the cut off rate must be recalculated. Also assume that there is a pulse jammer with average power J_{av}/λ for fraction of the time and zero power of $(1-\lambda)$ fraction of time.

If the receiver can detect the jammer signal when it is on we say that the channel has side information. The parameter is found for the channel with side information as

$$D = \lambda \exp\{-\lambda(\frac{E_c}{N_o})\} \qquad (4.40)$$

If the receiver has no side information then D is

given as [48]

$$D = \min_{\rho \geq 0}\{\exp(-2\rho E_c)[\lambda \exp(\rho^2 E_c N_o/\lambda) + 1 - \lambda]\} \quad (4.41)$$

Both (4.40) and (4.41) correspond to soft decision detectors. The cut off rates $R_o=1-\log_2(1+D)$ with D given by (4.40) and (4.41) are shown in Figures 4.12 and 4.13, respectively.

For hard decision channels we have the results [48]

$$D = \lambda\sqrt{4p(1-p)} \quad (4.42)$$

when the receiver has jammer state information and [48]

$$D = \sqrt{4\lambda p(1-\lambda p)} \quad (4.43)$$

when the receiver has no side information. For both cases, we have

$$p = Q\left(\sqrt{\frac{2\lambda E_c}{N_o}}\right) \quad (4.44)$$

Now we are in a position to find the upper bound of the bit error rate for DS/BPSK channel. Suppose we want to use the rate 1/2 convolutional code with constraint length L=7 in a DS/BPSK antijam system where there is a pulse jammer with $\lambda = 0.05$. Before going further, we need the coded bit error bounds for this specific code over the

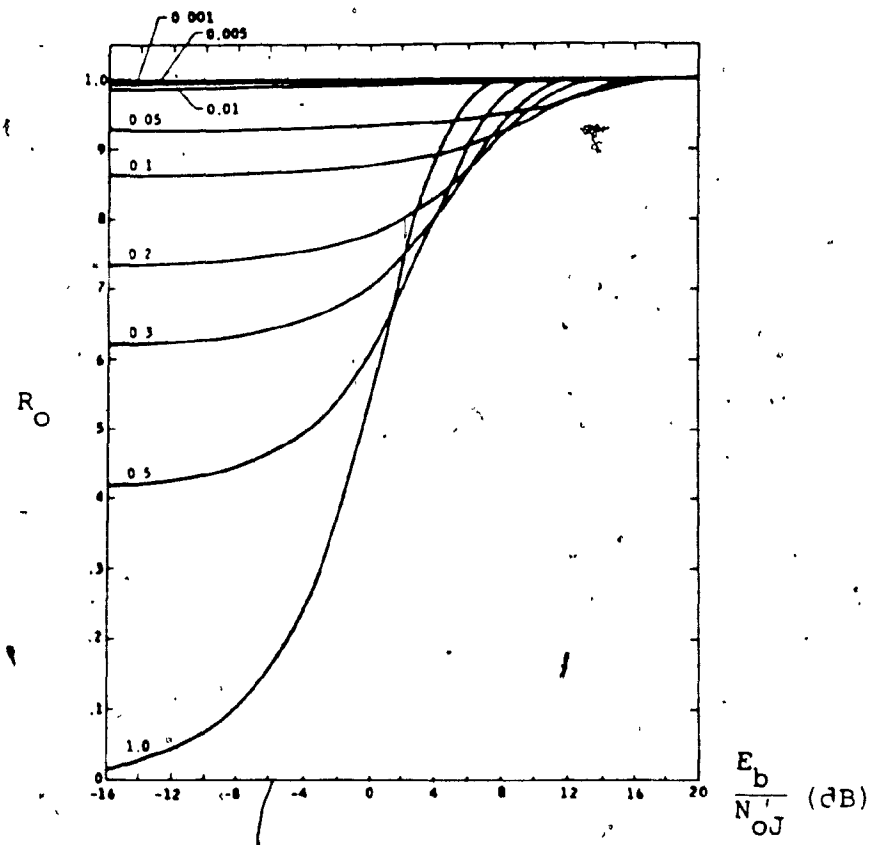


Figure 4.12: Soft decision with side information [27]

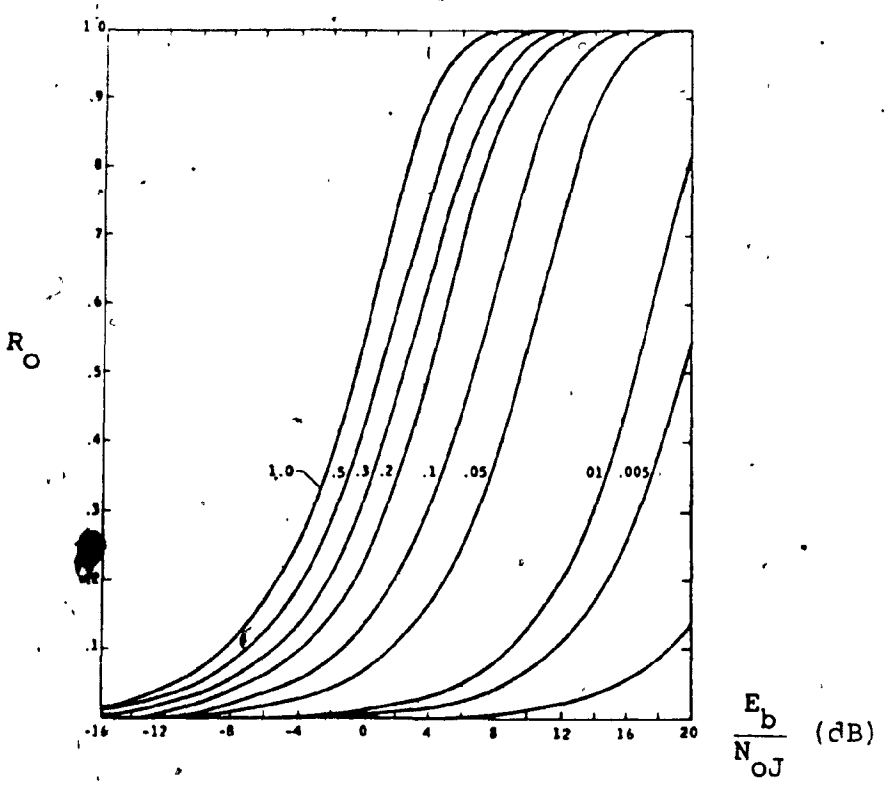


Figure 4.13: Soft decision with no side information[27]

Gaussian noise channel. This curve is available in textbooks and is replotted in Figure 4.14.

Suppose the detector used was a soft decision detector and no side information is available. To obtain 10^{-6} bit error probability the constraint length 7 and rate 1/2 requires 5dB in SNR (obtained from Figure 4.14) thus

$$\left.\frac{E_b}{N_o}\right|_o = 5\text{dB} \tag{4.45}$$

since $E_c = rE_b$, for r=1/2 we get

$$\left.\frac{E_c}{N_o}\right|_o = 2\text{dB} \tag{4.46}$$

For this choice of E_c/N_o from Figure 4.11 the cut off rate required is

$$R_o = 0.74 \qquad \text{bit/symbol} \tag{4.47}$$

For the new coded channel we determine from Figure 4.13 for $R_o = 0.74$ and $\lambda = 0.05$

$$\frac{E_c}{N_{oJ}} = 12\text{dB} \tag{4.48}$$

or

$$\frac{E_b}{N_{oJ}} = 15\text{dB} \tag{4.49}$$

Thus in a partial time jamming we require 15dB of

SNR to achieve 10^{-6} coded bit error probability with a given code. By continuing this process we can obtain the complete curve of P_b for the channel of interest.

Thus if we have another coding channel with the same value of the cut off rate R_o then the bit error bound is also the same [27]. We have shown an example for a DS/BPSK channel with rate 1/2 convolutional coding. The translation of standard coded bit error bounds to obtain corresponding bit error bounds of different coding channel applies to all binary coding channel. The application can also be generalized to FH/MFSK coded channel.

The technique is very attractive but it requires a lot of calculations and also requires the curve of the bit error rate performance in AWGN channel. However the cut off rate R_o tells us at what rate we would minimize the bit error rate. The probability of error can be directly calculated as we will demonstrate in the next chapter.

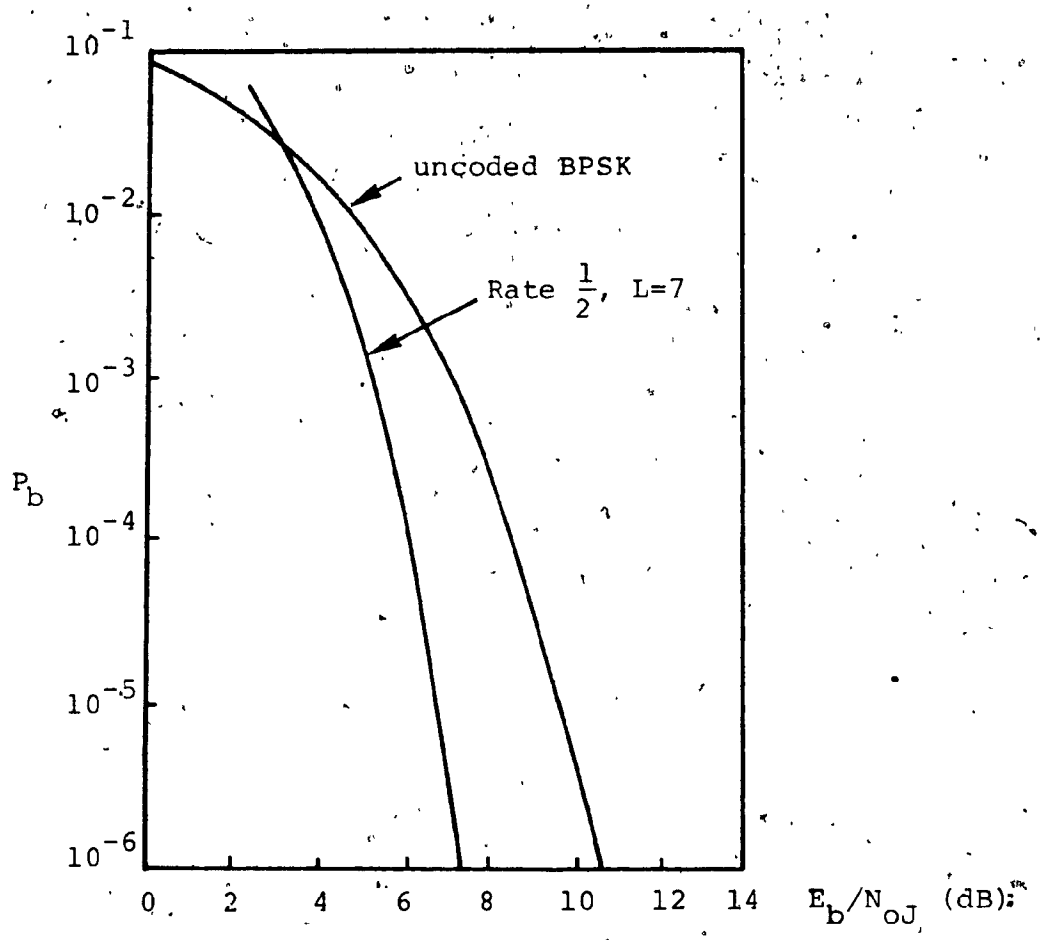


Figure 4.14: The bit error probability performance of rate 1/2, L=7 convolutional code with soft Viterbi decoding

CHAPTER 5

PERFORMANCE OF CODED SPREAD SPECTRUM SYSTEM BASED ON THE UNION BOUND

5.1. INTRODUCTION

In Chapter 4 we have briefly summarized the evaluation of a coded spread spectrum system. These evaluations are based on the cut off rate R_o which is the maximum practically achievable rate of a coded system. The curves of SNR versus the cut off rate do show the improvement of systems using codes. However they do not show how a specific code performs in these systems. Low code rates are required to give good results but how long a code should be, how many errors it can correct. These questions cannot be answered using the average ensemble probability of error. Upper bound on the error rate can be obtained by doing the transformation as in the last part of Chapter 4. However this technique is tedious and requires the knowledge of some existing performance curves. Therefore there is an urge to generate curves on the bounds of the bit error rate for different codes used in faded spread spectrum channel.

The minimum distances of block codes and convolutional codes were already defined in Chapter 4. In case of block codes, it is shown elsewhere [7,18,32] that a

t-error correcting code must have

$$d_m > 2t + 1 \tag{5.1}$$

Thus for a given block code with minimum distance d_m any number of error up to

$$t = \left\lfloor \frac{d_m - 1}{2} \right\rfloor \tag{5.2}$$

are always correctable, $\lfloor x \rfloor$ denotes the largest integer contained in x. So it is desirable to have codes with large minimum distance d_m. In general, we would require (a) long codes to average the effect of noise over a large number of symbols, (b) low code rates to satisfy the conditions we found in Chapter 4, (c) practical method of encoding and decoding, and (d) practical method of making decision at the receiver [27,28,32].

Among different classes of block codes, cyclic codes and its subclass, the Bose-Chaudhuri-Hocquenghem (BCH) codes, stand out because they satisfy most of the requirements. BCH codes of moderate length are rather powerful random-error correcting codes and can be implemented with a modest amount of equipment. However the efficiency of the code, k/n, approaches zero as n approaches infinity. The code rate k/n is bounded by the minimum distance and block length n and the distance is small when n is large. So, long BCH cannot be used in our analysis. [32,33,34]

One alternative is the quasi-cyclic (Q.C.) codes. It has been shown that these codes have a rich mathematical structure, and are easy to encode and to decode [33]. In this thesis we emphsize on the quasi-cyclic codes and use them in our proposed channel. The code rates used are 1/3, 1/2 and 2/3. The convolutional codes of the same code rate and compatible minimum distances are also evaluated. The channel is a Rician or Rayleigh fading channel. The jammer is partial band noise jammer and only the worst case partial band jammer is considered.

Before going to the evaluation of the coded spread spectrum channel it is worth mentioning that coded systems requires more bandwidth than the non coded one. Viterbi has shown that coding does not reduce the effective processing gain in a spread spectrum system [4]. The statement is true if and only if the bandwidth of the coded system is expanded in a coded system. This is depicted in Figure 5.1.

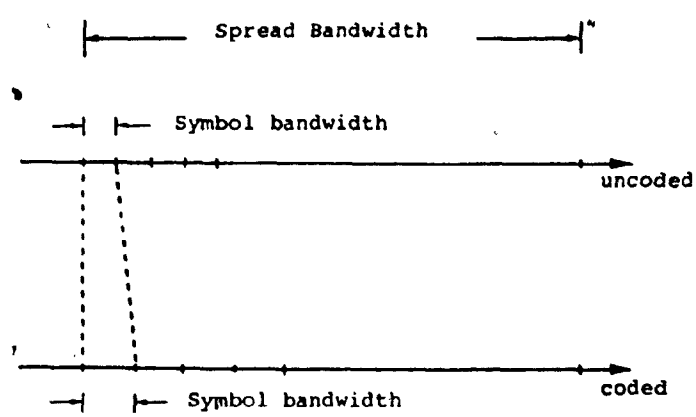


Figure 5.1: Symbol bandwidth in an uncoded and coded system

So if we keep the spread bandwidth the same in both the uncoded and coded systems, the frequency hopper in the coded one will have less slots to hop to. Thus the processing gain is decreased in coded system unless the bandwidth is expanded to give more space. Although coded systems require a larger bandwidth, the impressive saving in the effective SNR at 10^{-5} BER justifies the cost. With present technology the achievable bandspreading with frequency hopping is implementable. The use of coding offers a nonrefusable benefit in combating intelligent jammers.

5.2. QUASI-CYCLIC CODES

An (mn_o, mk_o) linear code is said to be quasicyclic with basic block length n_o if every shift of a codeword by n_o symbols yields another codeword. The generator matrix of quasi-cyclic codes has the form [33].

$$\underset{\sim}{G} = \begin{bmatrix} \underset{\sim}{C}_{11} & \underset{\sim}{C}_{12} & \underset{\sim}{C}_{13} \cdots & \underset{\sim}{C}_{1n_o} \\ \underset{\sim}{C}_{21} & \underset{\sim}{C}_{22} & \underset{\sim}{C}_{23} \cdots & \underset{\sim}{C}_{2n_o} \\ \vdots & \vdots & \vdots & \vdots \\ \underset{\sim}{C}_{k_o 1} & \underset{\sim}{C}_{k_o 2} & \underset{\sim}{C}_{k_o 3} \cdots & \underset{\sim}{C}_{k_o n_o} \end{bmatrix} \tag{5.3}$$

where each $\underset{\sim}{C}_{ij}$ is a circulant matrix of order m of the form

$$\underset{\sim}{C} = \begin{bmatrix} c_o & c_1 & c_2 \cdots & c_{m-1} \\ c_{m-1} & c_o & c_1 \cdots & c_{m-2} \\ \vdots & \vdots & \vdots & \vdots \\ c_1 & c_2 & c_3 \cdots & c_o \end{bmatrix} \tag{5.4}$$

with $c_i \in GF(2)$ (GF(q) is a Galois field of q elements with q a prime power).

Note that each row is the previous row shifted once and the matrix C of (4.4) is completely specified by the elements of the first row which associates with the polynomial

$$C(x) = c_o + c_1 x + c_2 x^2 + \ldots + c_{m-1} x^{m-1} \pmod{x^m - 1} \quad (5.5)$$

Thus the algebra of polynomials modulo x^m-1 over GF(q) is isomophic to algebra of all (mxm) circulant matrices over GF(q). The code generated by (5.3) is not in systematic form, that is, any particular code does not consist of mk_o information bits followed by $(mn_o - mk_o)$ parity bits. We can rearrange (5.3) to obtain the generator matrix

$$\underset{\sim}{G}_s = \left[\underset{\sim}{I} \,\vdots\, \underset{\sim}{C} \right] \quad (5.6)$$

$$\underset{\sim}{G} = \begin{bmatrix} \underset{\sim}{I} & \underset{\sim}{0} & \cdots & \underset{\sim}{0} & \underset{\sim}{C}_{1,k_o+1} & \cdots & \underset{\sim}{C}_{1,n_o} \\ \underset{\sim}{0} & \underset{\sim}{I} & \cdots & \underset{\sim}{0} & \underset{\sim}{C}_{2,k_{o+1}} & \cdots & \underset{\sim}{C}_{2,n_o} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \underset{\sim}{0} & \underset{\sim}{0} & & \underset{\sim}{I} & \underset{\sim}{C}_{k_o k_{o+1}} & \cdots & \underset{\sim}{C}_{k_o n_o} \end{bmatrix} \quad (5.7)$$

where $\underset{\sim}{I}$ and $\underset{\sim}{0}$ refer to the identity and all zero matrices of order m, respectively. The rate $r = k_o/n_o = 1/2$ quasi-cyclic codes have been well studied and in some sense can be regarded as the building blocks for higher rate quasi-cyclic

codes [35]. For rate 1/2 we have $k_o=n_o-k_o=1$, thus

$$\underset{\sim}{G}_s = \left[\underset{\sim}{I} \;\vdots\; \underset{\sim}{C}_{1,2}\right] \tag{5.8}$$

where I and $C_{1,2}$ are mxm matrices. Let $\underline{i}$ be the message to be encoded, then the corresponding codeword is

$$\underline{v} = \underline{i}\,\underset{\sim}{G}_s \tag{5.9}$$

Let $i(x)$ represent the m-tuple of information bits in polynomial form, then the polynomial $v(x)$ associated to $\underline{v}$ is

$$v(x) = [i(x),\ i(x)C(x)] \bmod x^m-1 \tag{5.10}$$

thus parity digits generated by $\underset{\sim}{G}_s$ are $i(x)C(x)$.

For rate $r=2/3$ we have $k_o=2$; $n_o=3$, then the generator matrix $\underset{\sim}{G}_s$ will have the form

$$\underset{\sim}{G} = \left[\begin{array}{c|c} \underset{\sim}{I} & \begin{matrix}\underset{\sim}{C}_{1,2}\\ \underset{\sim}{C}_{2,2}\end{matrix}\end{array}\right] \tag{5.11}$$

where $\underset{\sim}{I}$ is the (2mx2m) identity matrix and $\underset{\sim}{C}_1, \underset{\sim}{C}_2$ are (mxm) circulant matrices over GF(2) of the form (5.7). Each codeword generated by $\underset{\sim}{G}_s$ is of the form [36]

$$v(x) = [i_1(x),\ i_2(x),\ p(x)](\bmod x^m-1) \tag{5.12}$$

where $p(x)=i_1(x)C_1(x)+i_2(x)C_2(x)(\bmod x^m-1)$ are the parity digits.

In case of rate 1/3 codes the generator matrix can

be represented in the form

$$\underset{\sim}{G}_s = \left[\underset{\sim}{I} \;\middle|\; \underset{\sim}{C}_{1,2} \;\middle|\; \underset{\sim}{C}_{1,3} \right] \tag{5.13}$$

therefore [36]

$$v(x) = [i(x),\ i(x)C_{1,2}(x),\ i(x)C_{1,3}(x)] \pmod{x^m-1} \tag{5.14}$$

It is possible to encode quasicyclic code with a k-stage shift register in a manner exactly analogous to that for the encoding of cyclic codes explained in Chapter 4 [32,33,34]. The decoding process, however, shows some levels of difficulties. The decoding of rate 1/2 codes has been examined in detail by Karlin and decoding procedure for codes of rate $(n_0-1)/n_0$ has been proposed by Shiva and Tavares, these two algorithms can be found in [33] or [35].

The weight distribution of a code contains useful information about the code such as its minimum distance and the probability of undetected error. The weight distributions of some quasi-cyclic codes of rate 1/3, 1/2 and 2/3 are listed in [35-40]. In the next following two sections we will determine the bounds on the probability of bit error for spread spectrum systems which employ quasi-cyclic codes and hard or soft decision decoding.

5.2.1. HARD DECISION DECODING OF QUASI-CYCLIC CODES

As discussed previously the decoder decodes correctly if the number of errors in a codeword is less than half the minimum distance of the code. That is any number of errors up to

$$t = \left\lfloor \frac{d_m - 1}{2} \right\rfloor .$$

Since the source is binary and the received signal is quantized into two levels, the channel is called the binary symmetric channel (BSC). The BSC is a memoryless channel, so the bit errors occur independently. Hence the probability of i errors in a block of n bits is

$$P(i,n) = \binom{n}{i} p^i (1-p)^{n-i} \tag{5.15}$$

In a t-error correcting code the probability of block error is given by [5,32]

$$P_e = \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i} \tag{5.16}$$

where in (5.15) and (5.16) p reprsents the symbol error rate in the channel of interest. If an all zero codeword is sent, the detector will select a codeword which is different in d_m positions to the all zero code word if and only if (2t+1) errors have occured. If the number of errors is greater than (2t+1) then the decoder will select any code word in the set. In general, if i errors occur (i>t) then

the fraction of (i+t)/n of k information symbols will be decoded errornously [5]. The average bit error rate is

$$P_b \leq \sum_{i=t+1}^{n} \frac{(i+t)}{n} \binom{n}{i} p^i (1-p)^{n-i} \tag{5.17}$$

Equation (5.17), in fact, is the bit error rate for binary codes. For non binary codes, a code symbol represents m information bits. We assume that an incorrectly decoded symbol is equally likely to be any of the remaining symbols in the alphabet. Among 2^m equally likely symbols, a given bit is a one in 2^{m-1} cases and a zero in 2^{m-1} cases. When there are 2^{m-1} equally likely incorrect symbols, we have [31]

$$P_b = \frac{2^{m-1}}{2^m-1} \cdot P_s$$

$$= \frac{2^{m-1}}{2^m-1} \sum_{i=t+1}^{n} \frac{(i+t)}{n} p_s^i (1-p_s)^{n-i} \tag{5.18}$$

where the symbol error is p_s and bounded by

$$p_s \leq (2^m-1)p \tag{5.19}$$

In our analysis all codes are binary codes and the probability of error p is given by (3.22) for Rician fading channel with partial band jamming. In case of Rayleigh fading and partial band jamming p is given by (3.24)

Performance of some selected quasi-cyclic codes of

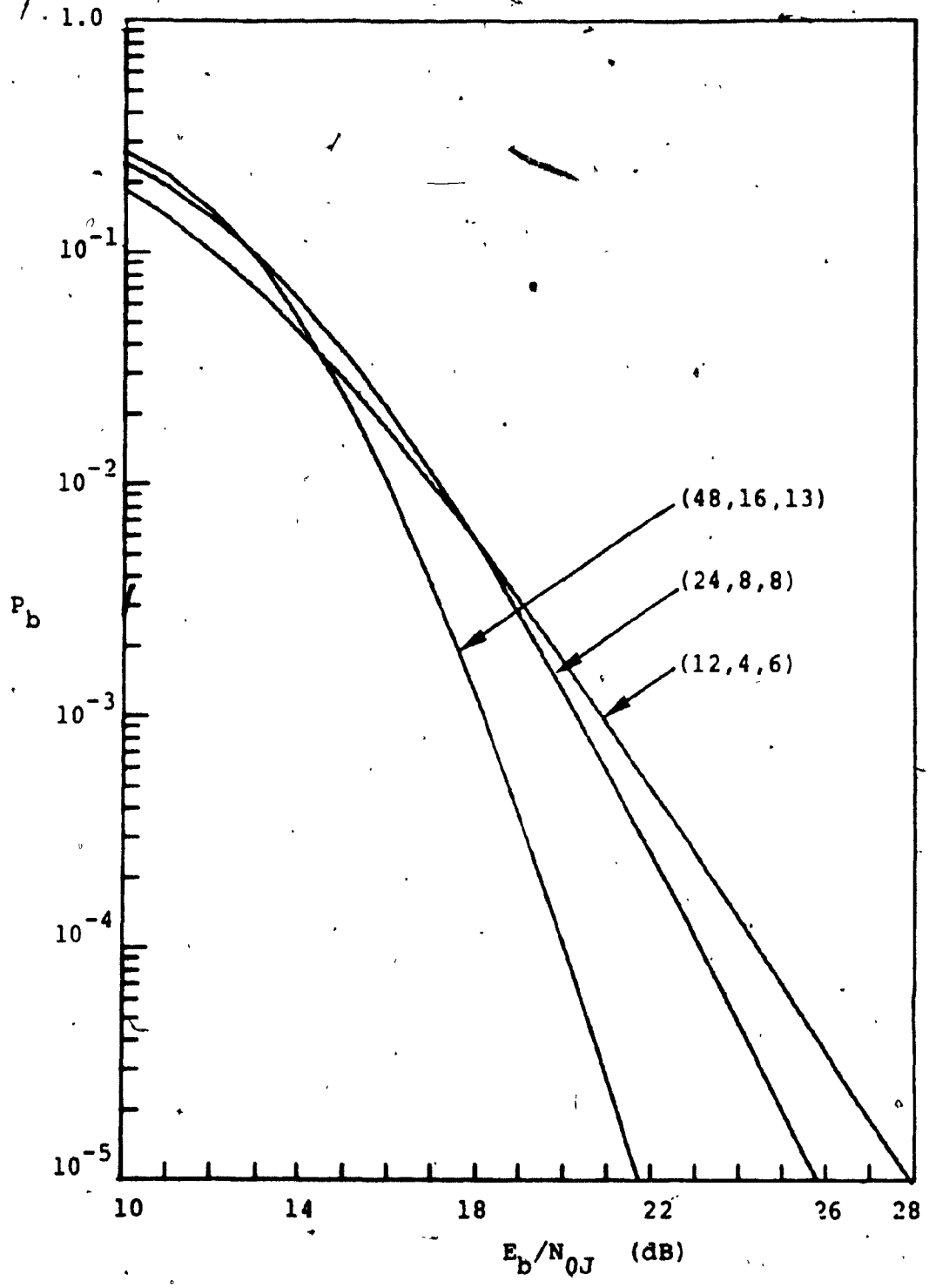


Figure 5.2: Performance of rate $\frac{1}{3}$ Q.C. codes with hard decision decoding in worst case partial band jamming and Rayleigh fading

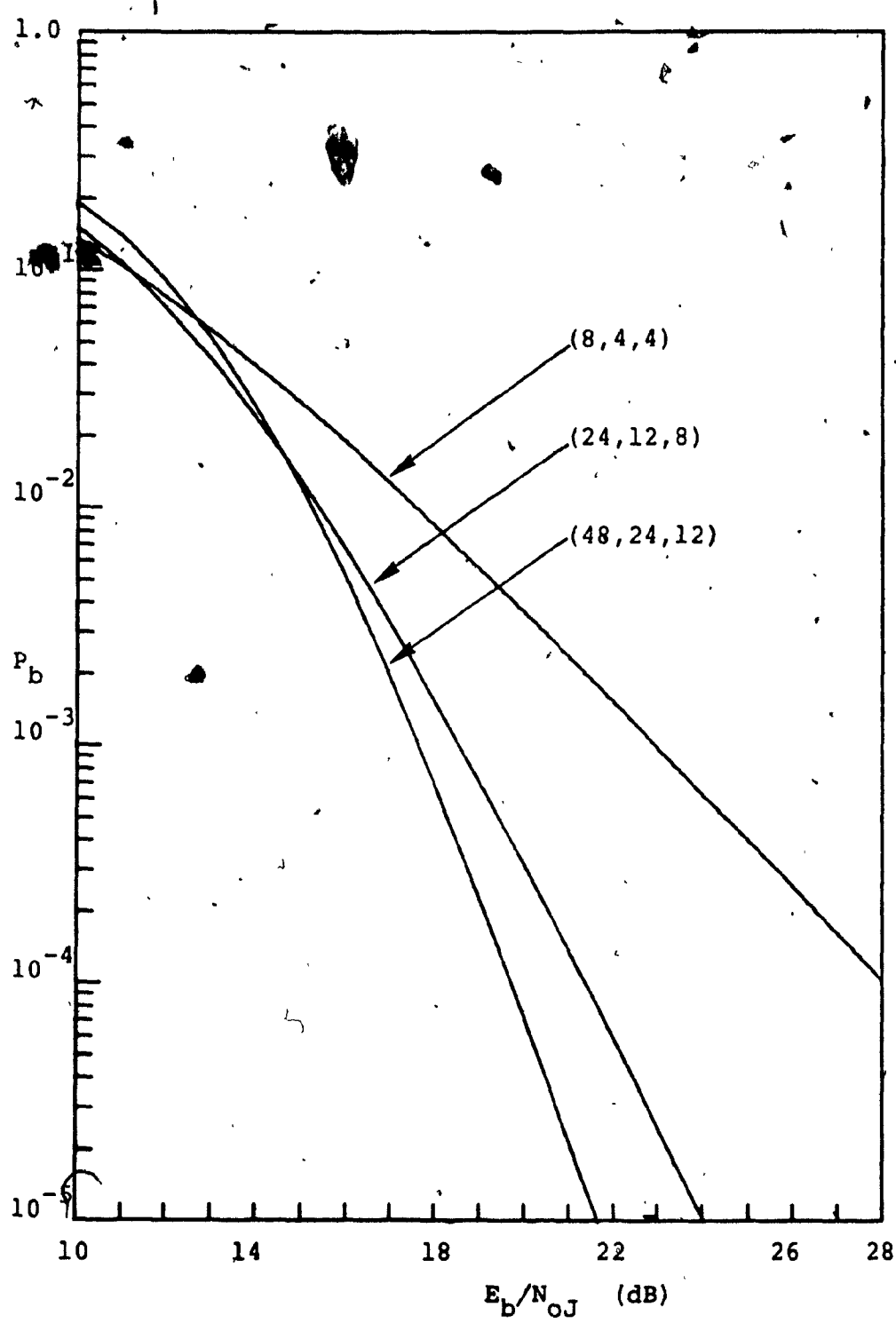


Figure 5.3: Performance of rate $\frac{1}{2}$ Q.C. codes with hard decision decoding in worst case partial band jamming and Rayleigh fading

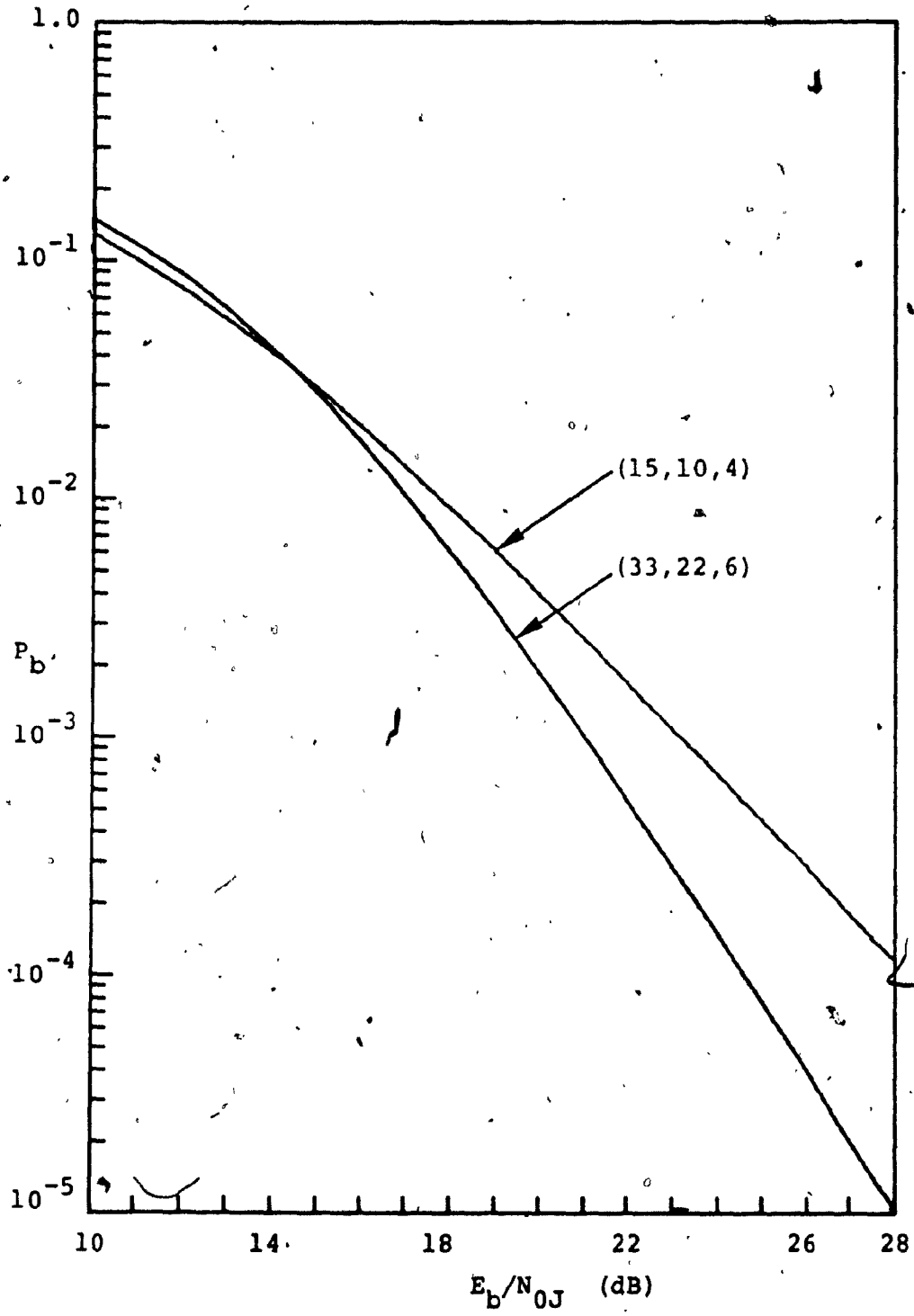


Figure 5.4: Performance of rate $\frac{2}{3}$ Q.C. codes with hard decision decoding in worst case partial band jamming and Rayleigh fading

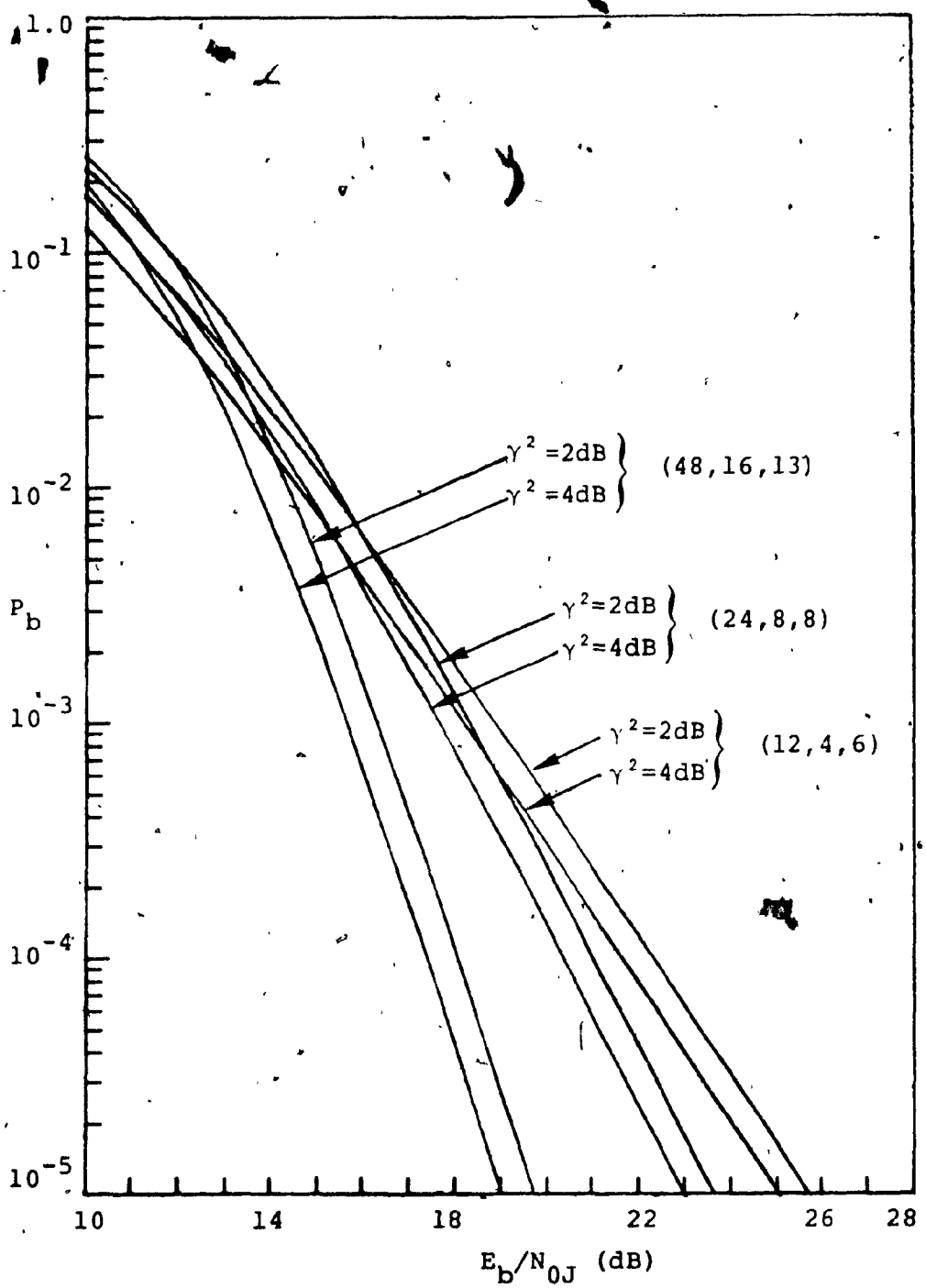


Figure 5.5: Performance of rate $\frac{1}{3}$ Q.C. codes with hard decision decoding in worst case partial band jamming and Rician fading

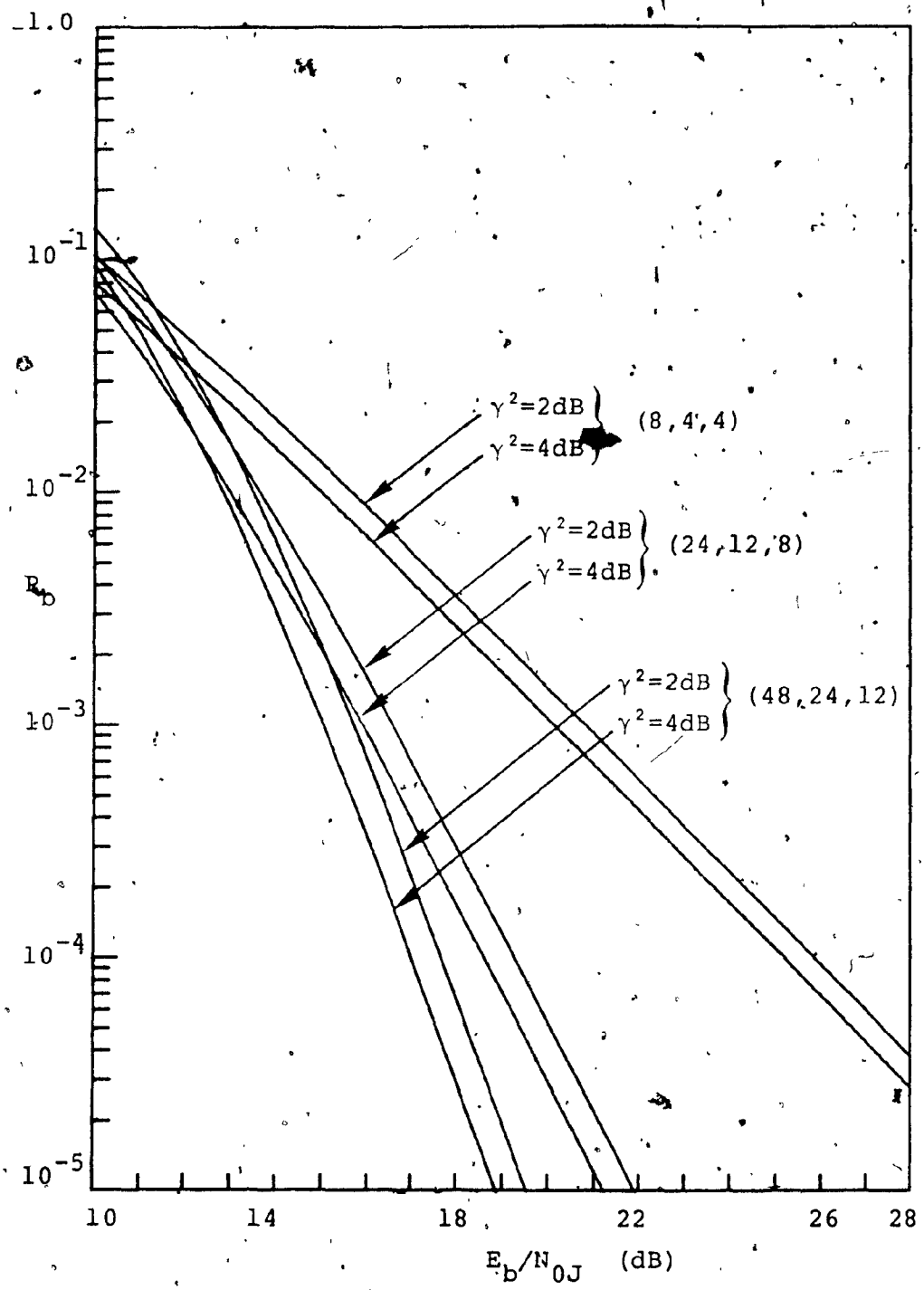


Figure 5.6: Performance of rate $\frac{1}{2}$ Q.C. codes with hard decision decoding in worst case partial band jamming and Rician fading

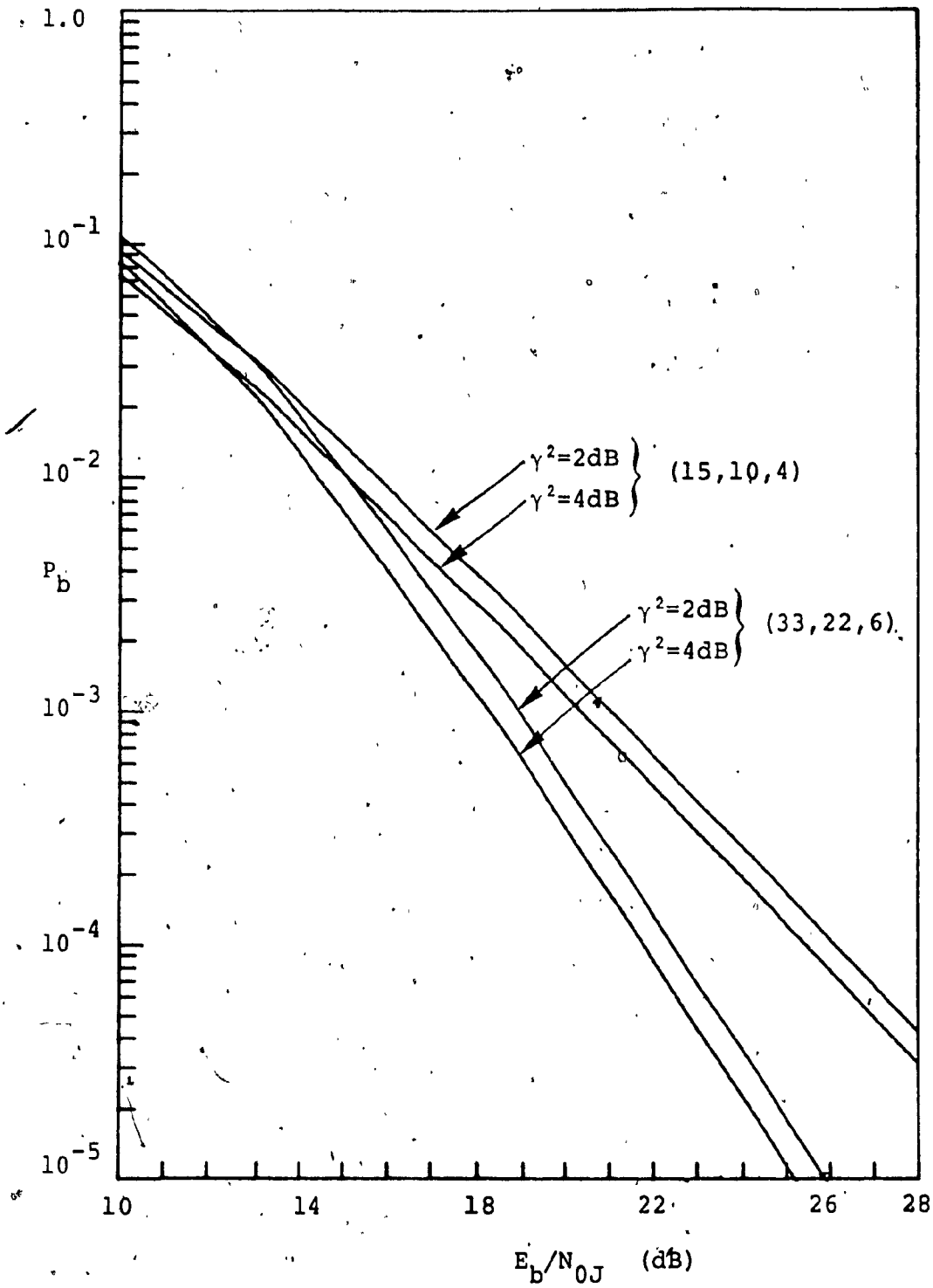


Figure 5.7: Performance of rate $\frac{2}{3}$ Q.C. codes with hard decision decoding in worst case partial band jamming and Rician fading

rate 1/3, 1/2, and 2/3 are plotted in Figures 5.2 to 5.7 respectively. We will analyze their performance in section 5.2.3 after discussing the soft decision decoding for quasi-cyclic codes.

5.2.2 SOFT DECISION DECODING OF QUASI-CYCLIC CODES

In this section, a codeword C_i, $i=1,2,\ldots,2^k$, having bit c_{ij}, $j=1,2,\ldots,n$, is mapped into BFSK signal waveforms in such a way that if $c_{ij}=0$, frequency f_{0j} is transmitted and if $c_{ij}=1$, frequency f_{1j} is transmitted. Actually, f_{0j} and f_{1j} will be further modulated according to a hopping pattern in (2.19). Let y_{rj}, $r=1,2$, $j=1,2,\ldots,n$ represent the square root of n sampled output of the enveloped detector. If the decoder is a soft decision decoder, it will form the 2^k decision variables [3]

$$U_i = \sum_{j=1}^{n} [(1-c_{ij})|y_{oj}|^2 + c_{ij}|y_{1j}|^2]$$

$$= \sum_{j=1}^{n} [|y_{oj}|^2 + c_{ij}(|y_{1j}|^2-|y_{oj}|^2)] \qquad (5.20)$$

Without loss of generality, let us assume that the all zero codeword is transmitted. Thus the decision variable U_1 is given by (4.16) with $c_{1j}=0$ for all j. The decoder will decode incorrectly if one of the other decison variable U_i is larger than U_1; thus the probability of error is the one in choosing the m-th codeword.

$$P = Pr(U_m > U_1) = Pr(U_1 - U_m < 0)$$

$$= Pr\{ \sum_{j=1}^{n} [|y_{oj}|^2 - |y_{1j}|^2 - c_{oj}(|y_{1j}|^2 - |y_{oj}|^2)] < 0\}$$

$$= Pr\{ \sum_{j=1}^{n} c_{ij}(|y_{oj}|^2 - |y_{1j}|^2) < 0\} \qquad (5.21)$$

the sum of all the bits in one codeword yields its weight, hence (4.17) becomes

$$P = Pr\{ \sum_{j=1}^{w_m} (|y_{oj}|^2 - |y_{1j}|^2) < 0\} \qquad (5.22)$$

where w_m represents the weight of the m-th code. The inequality ($\sum |y_{oj}|^2 < \sum |y_{1j}|^2$) represents the deciding factor of the square-law combining method for a diversity channel. The probability is

$$P(w_m) = \left\{\frac{1+\gamma^2}{2(1+\gamma^2)+\Lambda}\right\}^{w_m} \exp\{- \frac{w_m\gamma^2}{2(1+\gamma^2)+\Lambda} \} \cdot$$

$$\sum_{m=0}^{w_m-1} \sum_{\ell=0}^{m} \binom{m+w_m-1}{m-\ell} \left\{\frac{1+\gamma^2+\Lambda}{2(1+\gamma^2)+\Lambda}\right\} \frac{x^\ell}{\ell!} \qquad (5.23)$$

where

$$x = \frac{w_m\gamma^2}{(1+\gamma^2+\Lambda)[2(1+\gamma^2)+\Lambda]}$$

All the parameters in (5.23) are already defined in Chapter 3. The proof of (5.23) in shown in Appendix B. In the case of Rayleigh fading channel (5.23) reduces to

$$P(w_m) = \left(\frac{1}{2+\Lambda}\right)^{w_m-1} \sum_{m=0}^{w_m-1} \binom{w_m-1-m}{m} \left(\frac{1+\Lambda}{2+\Lambda}\right)^m \qquad (5.24)$$

Let n_i be the number of codewords of weight i. The total probability of the all-zero codeword received as a codeword of weight i is

$$P_{total} = n_i P(n_i) \qquad (5.25)$$

Therefore, the average probabilty of error using soft decision decoding in partial band jamming is

$$P_b = \frac{1}{n} \sum_{i=d}^{n} i\, n_i\, \lambda^i\, P(n_i) \qquad (5.26)$$

where $P(n_i)$ is given either by (5.23) or (5.24). A good approximation can be made by considering only the largest n_d terms on the equation (5.26). This approximation is based on using only the largest n_d terms in the union bound which corresponding to the n_d codewords of minimum distance d and neclecting the probability of an error for the other codewords [22]. We get

$$P_b = \frac{d}{n} \lambda^d n_d\, P(\text{d-order of diversity}) \qquad (5.27)$$

Equation (5.27) is of great help if the computation is carried out in a small computer such as the PDP11/45. The worst case jamming, when soft decision detector is employed,is not very easy to derive. However, graphical

analyses shows that the optimal value of λ is $\lambda = 1$. Figure 5.2 to 5.13 show the performance of quasi-cyclic codes used in FH/MFSK with soft decision decoding and worst case jamming.

5.2.3. DISCUSSION ON GRAPHIC RESULTS

We have chosen some rates 1/3, 1/2 and 2/3 quasi-cyclic codes which have known weight distributions [35,36,37,38,39]. The rate 2/3 codes chosen have the largest possible minimum distance and the rate 1/3 codes are their duals [36]. The codes are selected to have compatible length and minimum distance. Among the selected codes, the (8,4) code is equivalent to the Hamming (7,4) code, the (24,12) code is equivalent to the Golay (23,12) code [37]. The modulation is binary frequency shift keying with slow frequency hopping. The channel experiences Rayleigh or Rician fading and worst case partial band jamming.

As an example we tabulate the required effective signal-to-noise ratio at $P_b = 10^{-5}$ and the gain of the energy ratio when coding is applied. The gain is the difference in the effective SNR's at a given bit error rate between coded and non coded systems. From Figures 5.2 to 5.13 and from Tables 5.1 and 5.2, we observe that low rate codes give better results than higher rate codes. This agrees with the prediction using Figure 4.7. Also as predicted, long

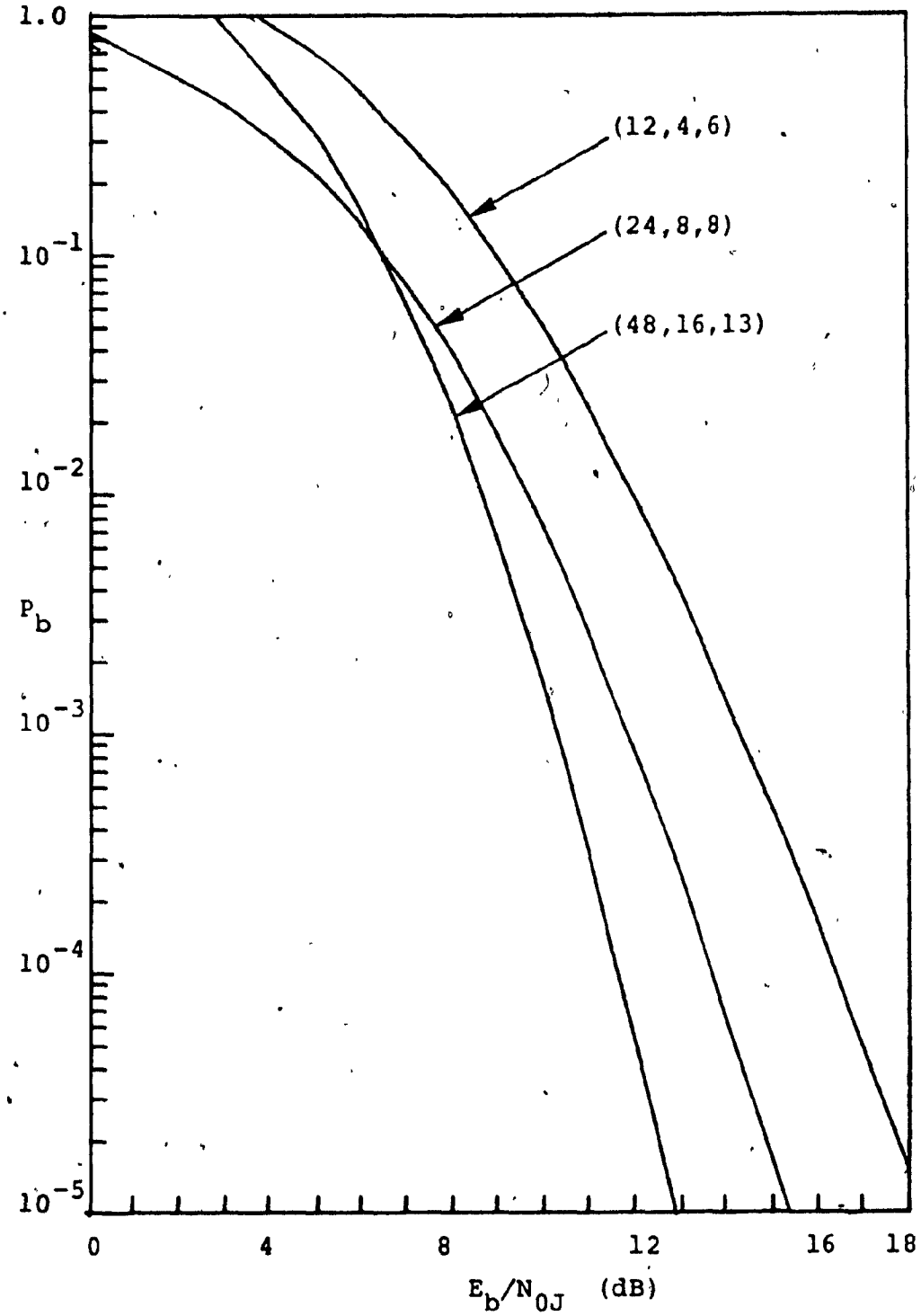


Figure 5.8: Performance of rate $\frac{1}{3}$ Q.C. codes with soft decision decoding in worst case partial band jamming and Rayleigh fading

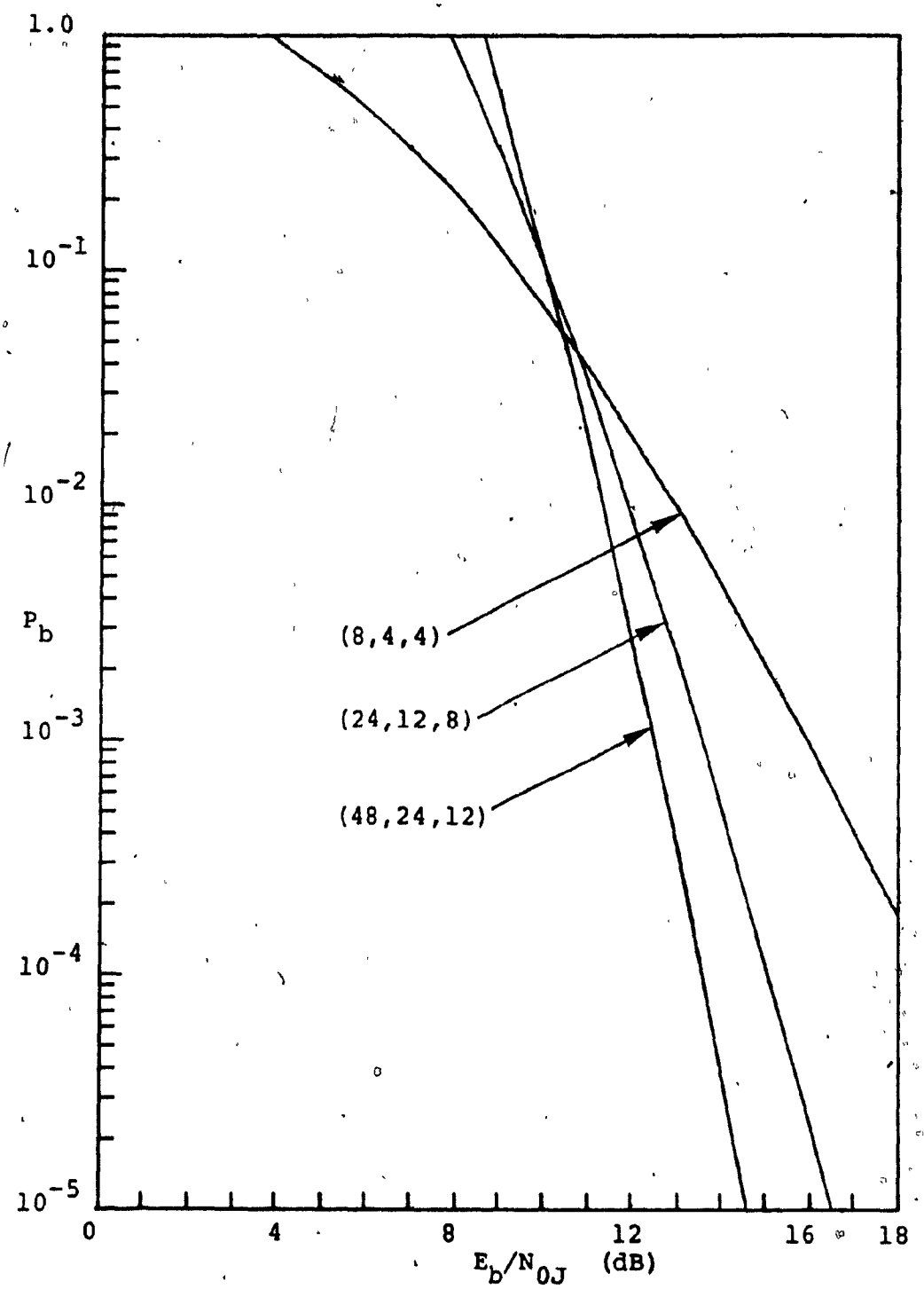


Figure 5.9: Performance of rate $\frac{1}{2}$ Q.C. codes with soft decision decoding in worst case partial band jamming and Rayleigh fading

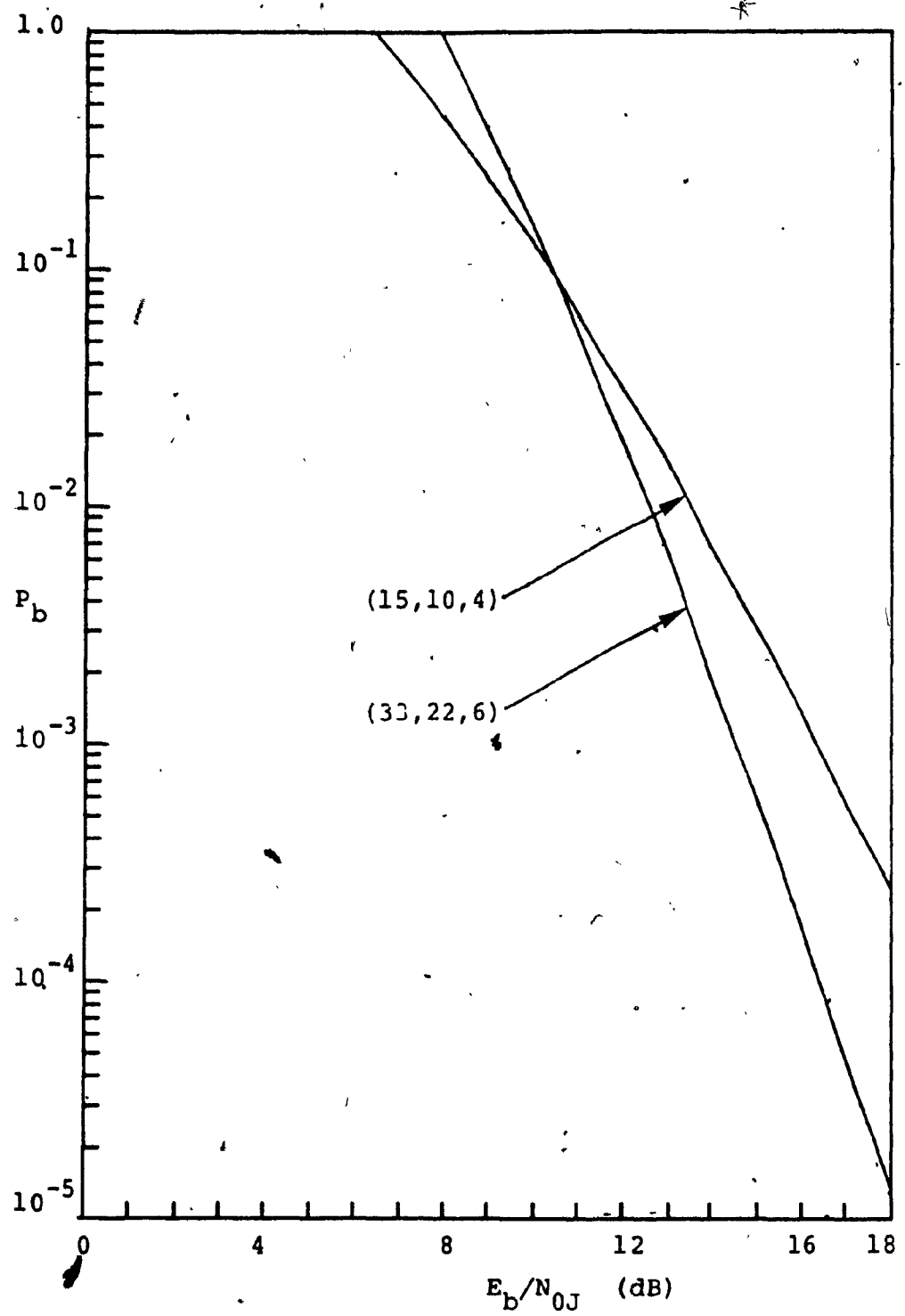


Figure 5.10: Performance of rate $\frac{2}{3}$ Q.C. codes with soft decision decoding in worst case partial band jamming and Rayleigh fading

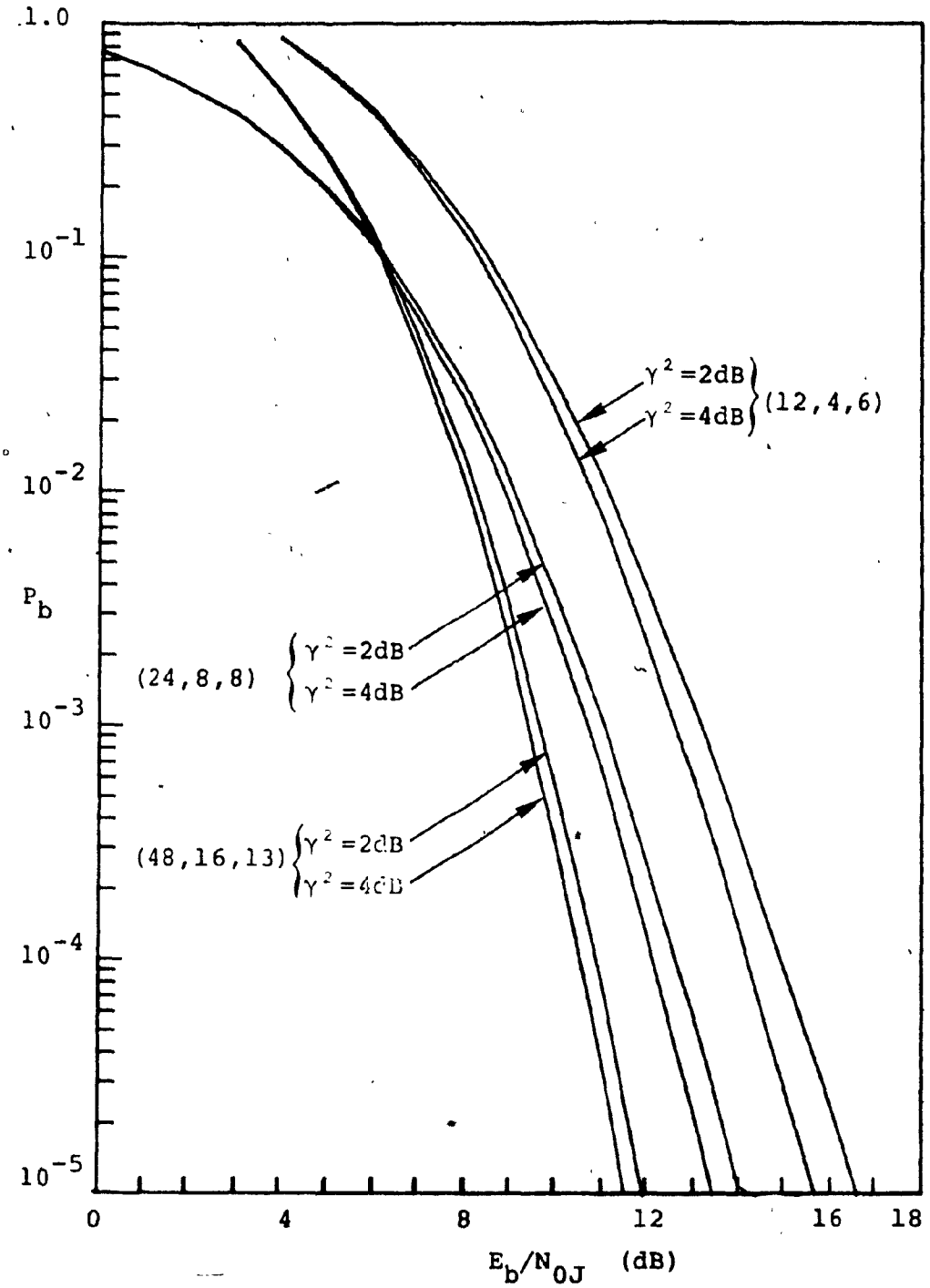


Figure 5.11: Performance of rate $\frac{1}{3}$ Q.C. codes with soft decision decoding in worst case partial band jamming and Rician fading

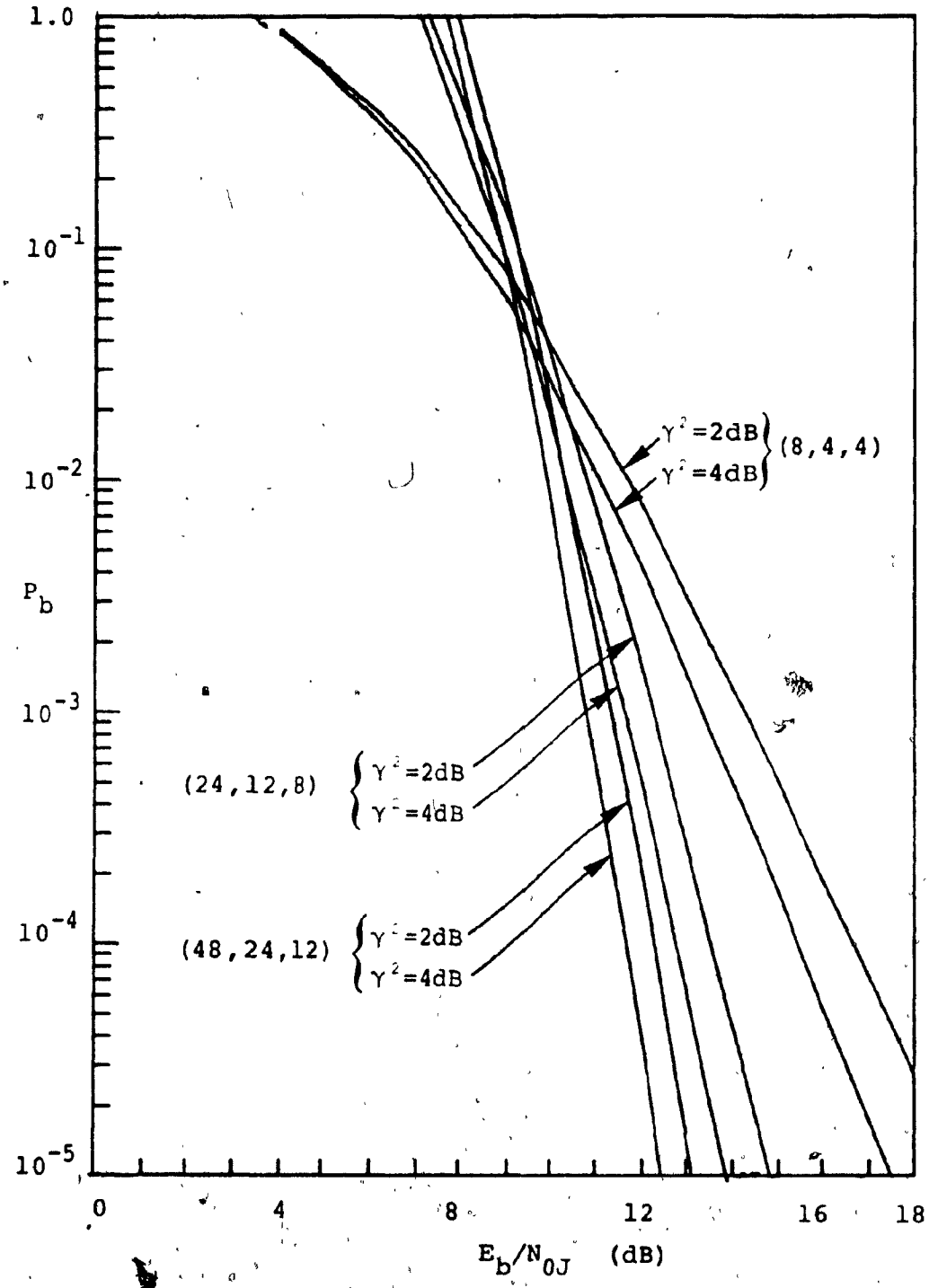


Figure 5.12: Performance of rate $\frac{1}{2}$ Q.C. codes with soft decision decoding in worst case partial band jamming and Rician fading

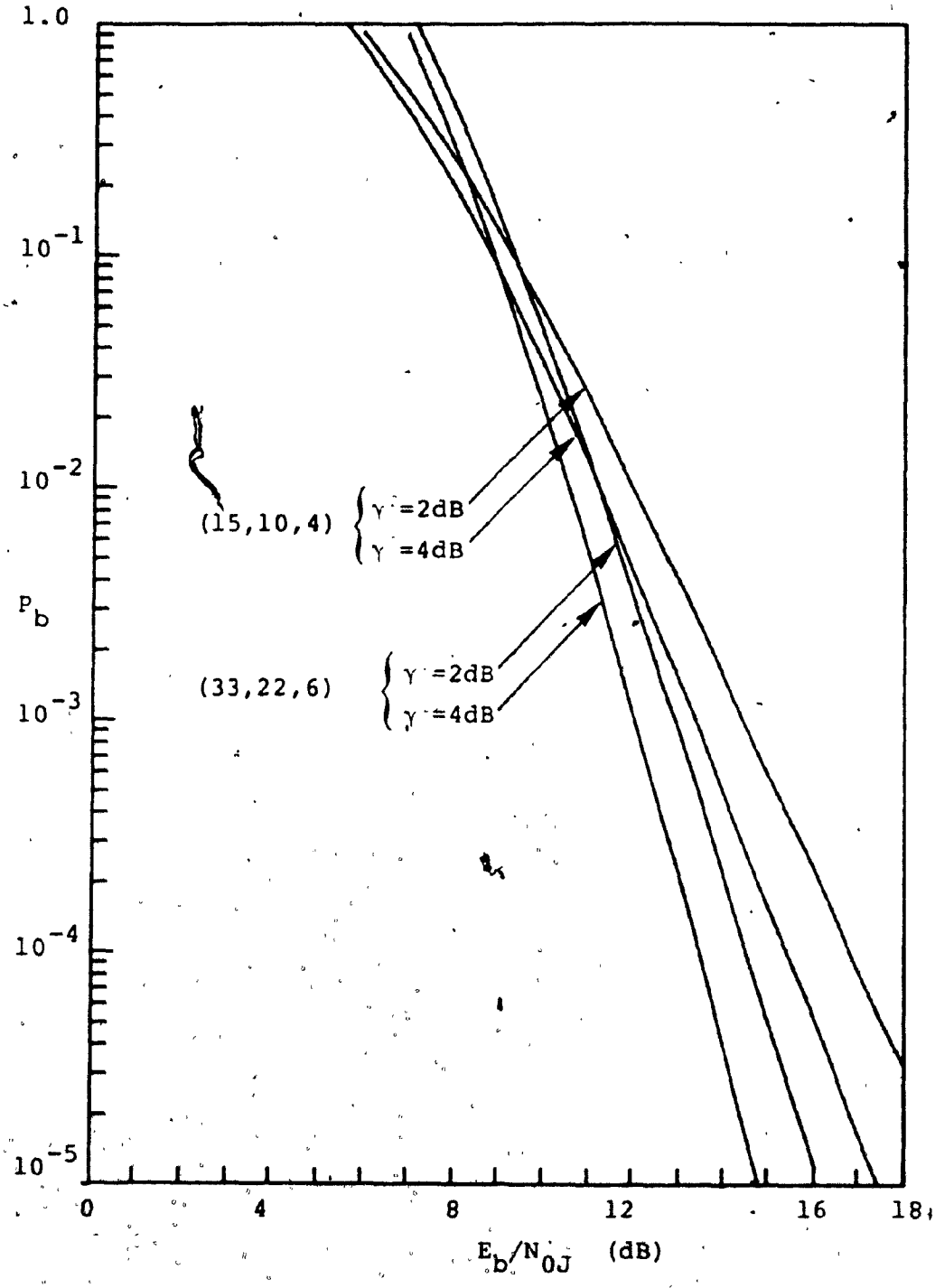


Figure 5.13: Performance of rate $\frac{2}{3}$ Q.C. codes with soft decision decoding in worst case partial band jamming and Rician fading

codes perform better than shorter codes due to the reduction of noise over a large number of symbols. The coding gain between hard and soft decision decoding is from 10dB to 12dB. This is a significant difference compared to the 3dB difference in a nonfading AWGN channel.

In Table 5.2 we compare the performance of hard and soft decision decoding in a Rician fading channel with partial band jamming. The ratio γ^2 is selected to be 2dB. This ratio varies for different propagation medium, but it acts in favor to users of a Rician fading channel. The larger the value of γ^2 the more reliable link we can establish. However, this gain is not very profound in worst case partial band jamming because, from the graphs, the increase of 2dB in results in only in 1dB gain in SNR. If γ^2 is very small, we can estimate the performance of the system using Rayleigh fading model.

The soft decision decoding for quasi-cyclic has not been implemented yet due to its complexity. However, the performance of soft decision is evaluated using the diversity combining technique. Hence it would be easier to build a diversity channel than a soft decision decoder.

Table 5.1: Performance of some quasi-cyclic codes with worst case partial band jamming and Rayleigh fading at $P_b = 10^{-5}$

		Hard decision decoding		Soft decision decoding	
code	rate	SNR (dB)	Gain (dB)	SNR (dB)	Gain (dB)
(n ,k,d)					
(12,4,6)	1/3	28	20	18.5	29.5
(24.8,8)	1/3	25.8	22.2	15.3	32.7
(48,16,13)	1/3	21.8	26.2	12.9	35.1
(8,4,4)	1/2	33	15	21.5	26.5
(24,12,8)	1/2	24	24	16.5	31.5
(48,24,12)	1/2	21.6	26.4	14.6	33.4
(15,10,4)	2/3	33	15	22	26
(33,22,6)	2/3	28	20	18.2	29.8

Table 5.2: Performance of some quasi-cyclic codes with worst case partial band jamming and Rician fading at $P_b = 10^{-5}$, $\gamma^2 = 2$dB

		Hard decision decoding		Soft decision decoding	
code	rate	SNR (dB)	Gain (dB)	SNR (dB)	Gain (dB)
(n ,k,d)					
(12,4,6)	1/3	25.8	16.2	16.5	25.5
(24.8,8)	1/3	23.6	18.4	14	28
(48,16,13)	1/3	19.7	22.3	12	30
(8,4,4)	1/2	31	11	20	12
(24,12,8)	1/2	22	20	14.8	27.2
(48,24,12)	1/2	19.5	22.5	13.1	28.9
(15,10,4)	2/3	30	12	20	22
(33,22,6)	2/3	25.9	16.1	16.1	25.9

5.3 CONVOLUTIONAL CODES

5.3.1 HARD DECISION DECODING OF CONVOLUTIONAL CODES

We observe that the tree of Figure 4.3 repeats itself after the third stage. There are two nodes with state "00", two nodes with state "11", two nodes with state "10", and two state with state "01". In other words, the code tree contain redundant information which can be eliminated by merging branches of the same state. The resulting structure has been called a trellis by Forney [19] and the trellis for the tree of Figure 4.3 is illustrated in Figure 5.14

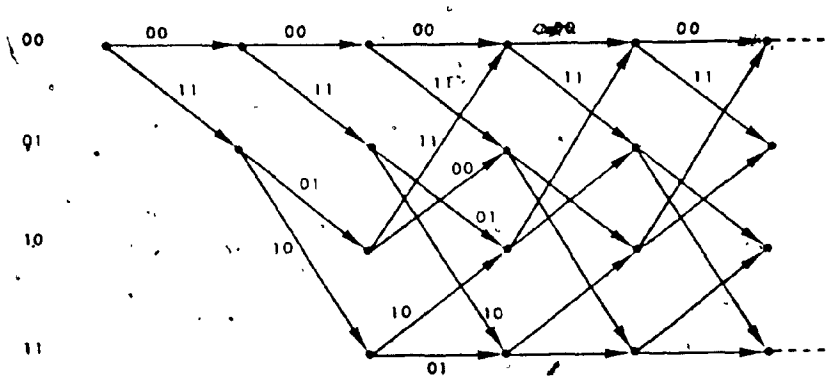


Figure 5.14: Trellis for a constraint length 3 convolutional code

The convention is that an input 0 corresponds to the selection of the upper branch and an input 1 corresponds to the selection of the lower branch. It is well known that the convolutional codes are group code, thus we may assume that the all zero path was transmitted without loss of generality [41]. Then a first event error is made at the j-th step if the all zero path is eliminated at this point by

another path merging with it. Suppose that the path being compared with the all-zero path at some node A has distance d from the all-zero path. If d is odd, the all-zero path will be correctly selected if the number of errors in the received sequence is less than $(d+1)/2$. The probability of error in selecting an incorrect path is

$$P_j(d) = \sum_{k=\frac{d+1}{2}}^{d} \binom{d}{k} p^k (1-p)^{d-k} \qquad \text{(d odd)} \qquad (5.28)$$

where p is the channel bit error rate [5]. If the distance is even, the correct path is selected when the number of errors is less than d/2. If the number of errors equals d/2 then there is a tie which, if resolved by coin flipping, will result in an error only half the time [41]. The error probability is

$$P_j(d) = \frac{1}{2}\binom{d}{\frac{d}{2}} p^{\frac{d}{2}} (1-p)^{\frac{d}{2}} + \sum_{e=\frac{d}{2}+1}^{d} \binom{d}{e} p^e (1-p)^{d-e} \qquad \text{(d even)} \qquad (5.29)$$

The probability, $P_j(d)$, of the all-zero path being eliminated by a path of weight j merging with it is dependent only on the weight of that path. Therefore, a union bound on the first event error, P_e, can be calculated by summing the error probabilities $P_j(d)$ over all the possible paths which merge to the all-zero path at a given node [3,5,7,41]. Thus

$$P_e < \sum_{d=d_f}^{\infty} n_d P_j(d) \qquad (5.30)$$

where n_d is the number of possible paths of weight d merging with the all zero path. Let the total information weight of these paths be w_j, then the union bound on the probability of bit error, P_b, may be obtained from (5.30) by weighting each term by corresponding number of bit errors (the information weight of each path)

$$P_b < \frac{1}{k} \sum_{d=d_f}^{\infty} w_d \, \lambda^d \, P_j(d) \qquad (5.31)$$

Figures 5.15 to 5.20 plot the performance curves of some of the rate 1/3, 1/2 and 2/3 convolutional codes. Again we will analyze these curves after discussing the soft decision decoding.

5.3.2 SOFT DECISION DECODING OF CONVOLUTIONAL CODES

Assume that an information sequence $\underline{u}$ is encoded into a codeword $\underline{v}$ and that the receiver receives a codeword $\underline{r}$. Then the Viterbi decoder has to compute a parameter called the metric associated with the path $\underline{v}$. The metric can be coarsely defined as the distance from the received sequence. The metric is defined as [3,18]

$$\mu_j^r = \log_2 P(\underline{y}_j | \underline{v}_j^r) \qquad (5.22)$$

where $P(\underline{y} \mid \underline{v})$ is the joint probability of the output sequence of the demodulator conditioned on the transmitted

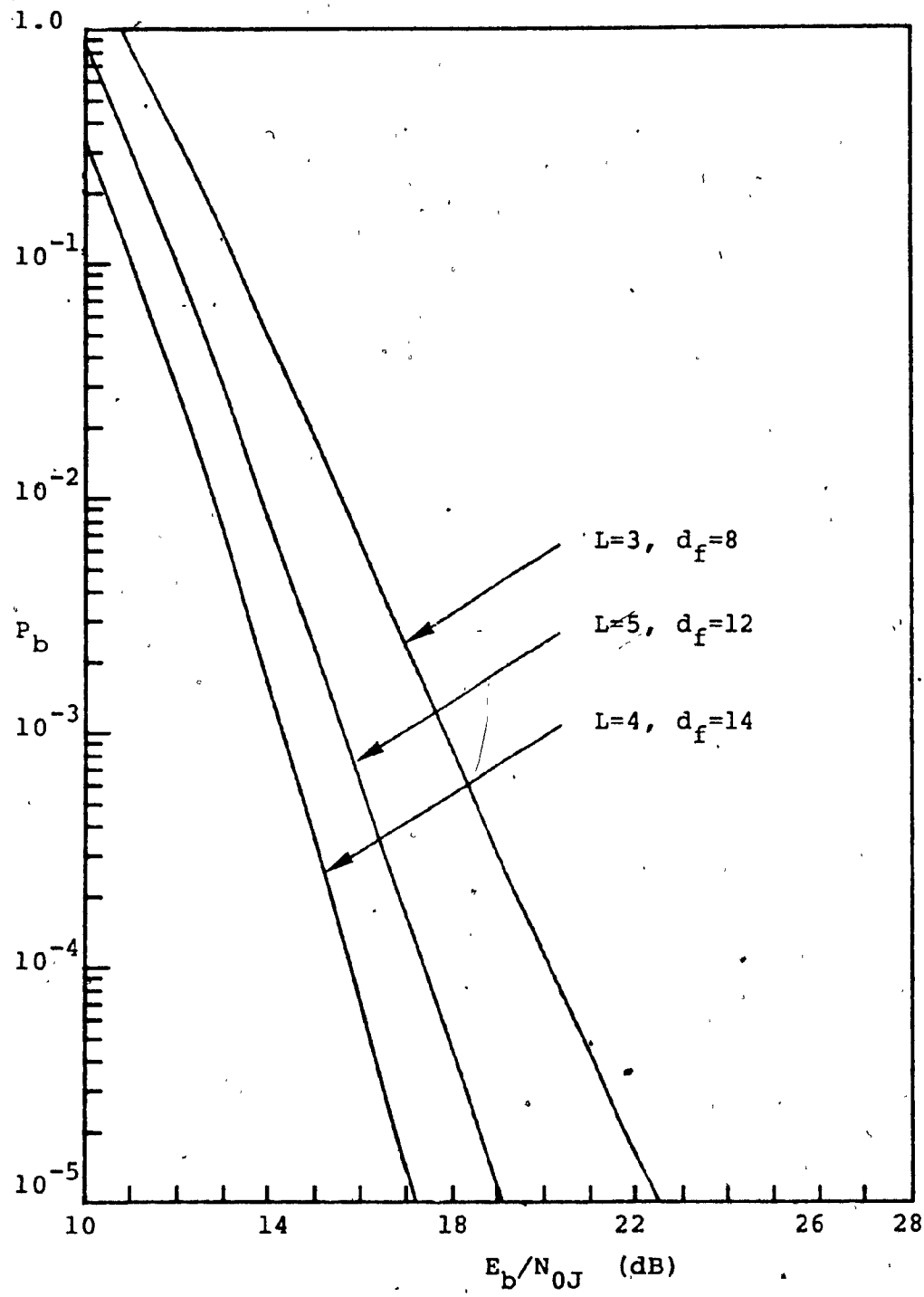


Figure 5.15: Performance of rate $\frac{1}{3}$ convolutional codes with hard decision decoding in worst case partial band jamming and Rayleigh fading

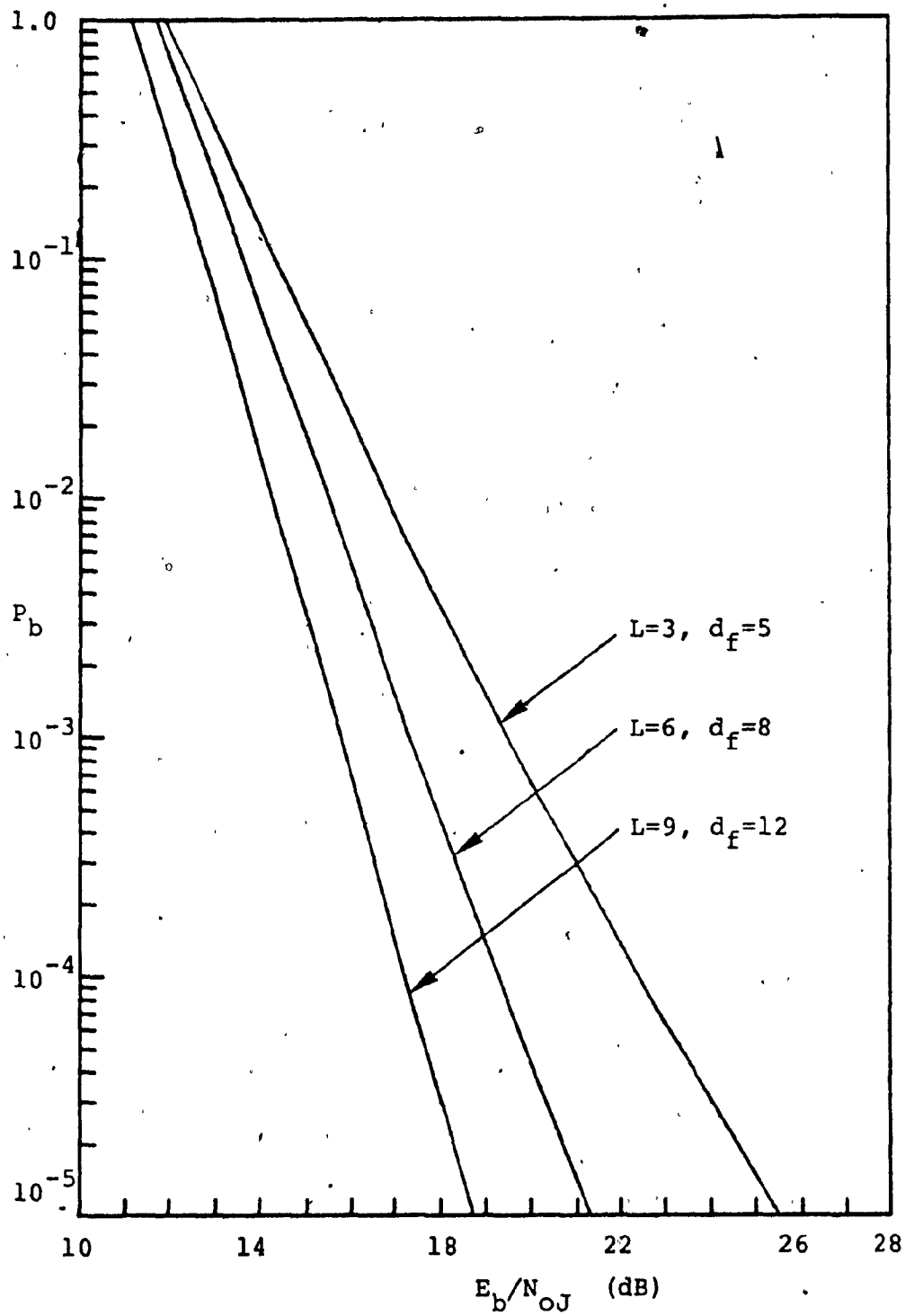


Figure 5.16: Performance of rate $\frac{1}{2}$ convolutional codes with hard decision decoding in worst case partial band jamming and Rayleigh fading

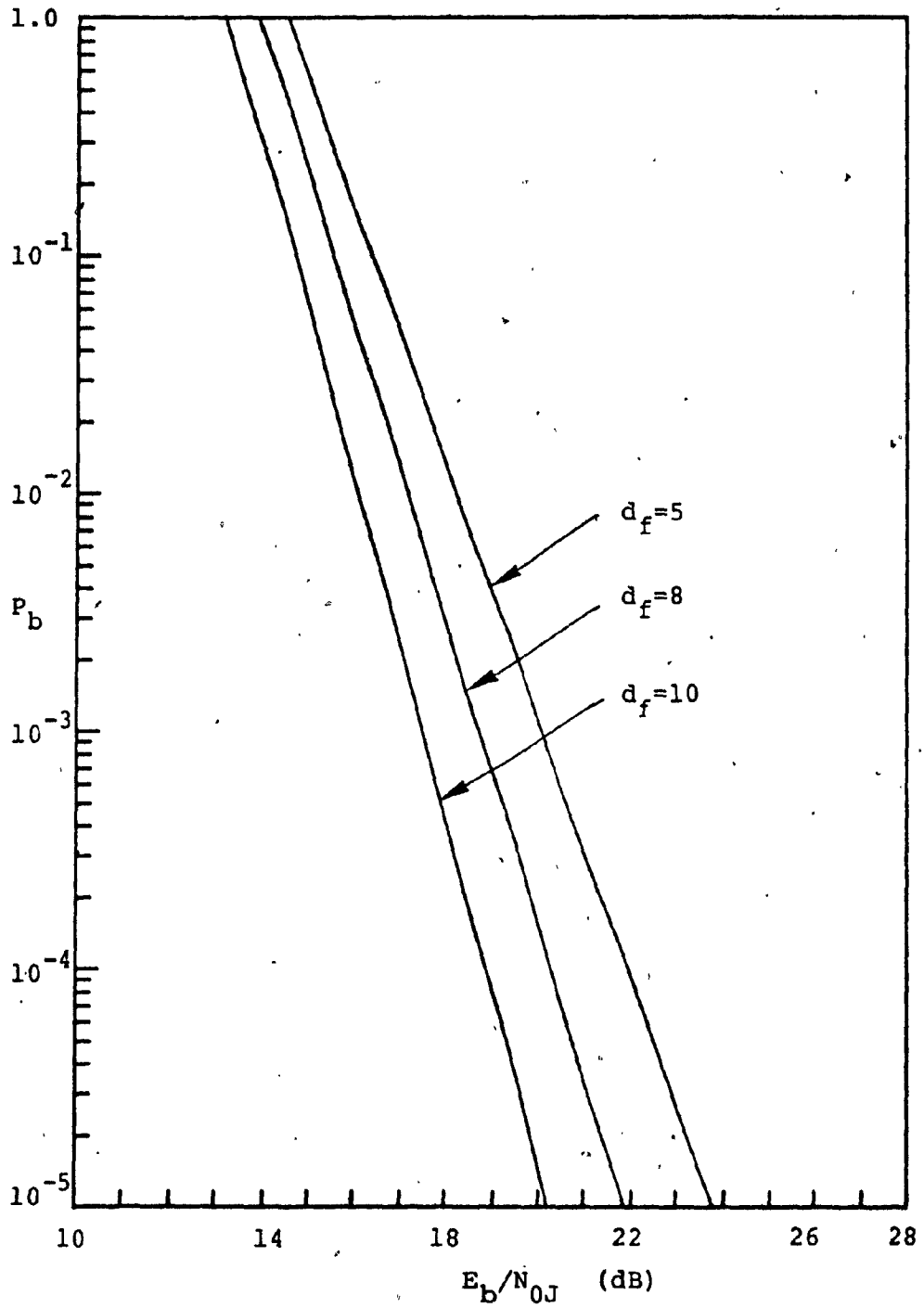


Figure 5.17: Performance of rate $\frac{2}{3}$ convolutional codes with hard decision decoding in worst case partial band jamming and Rayleigh fading

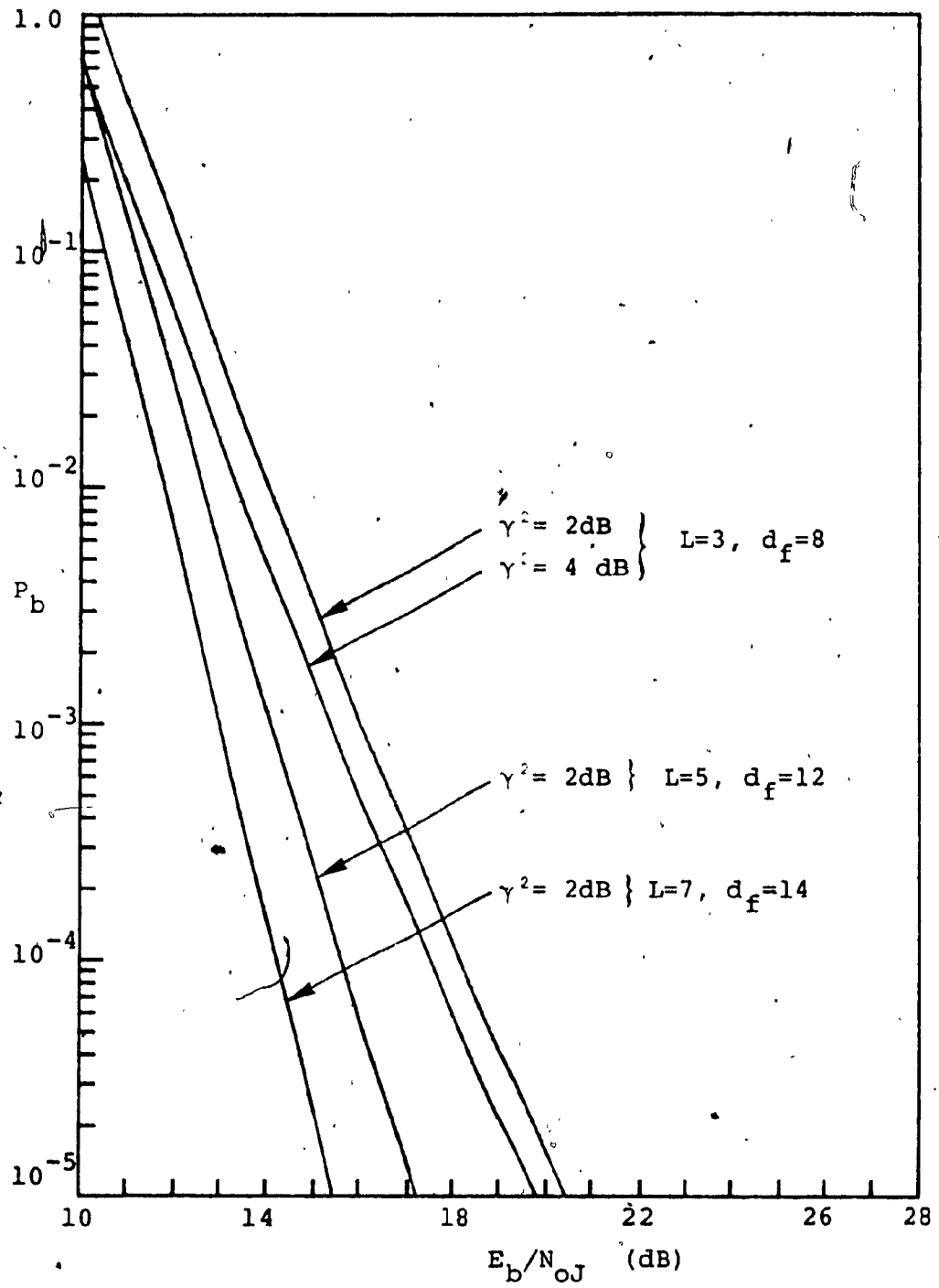


Figure 5.18: Performance of rate $\frac{1}{3}$ convolutional codes with hard decision decoding in worst case partial band jamming and Rician fading

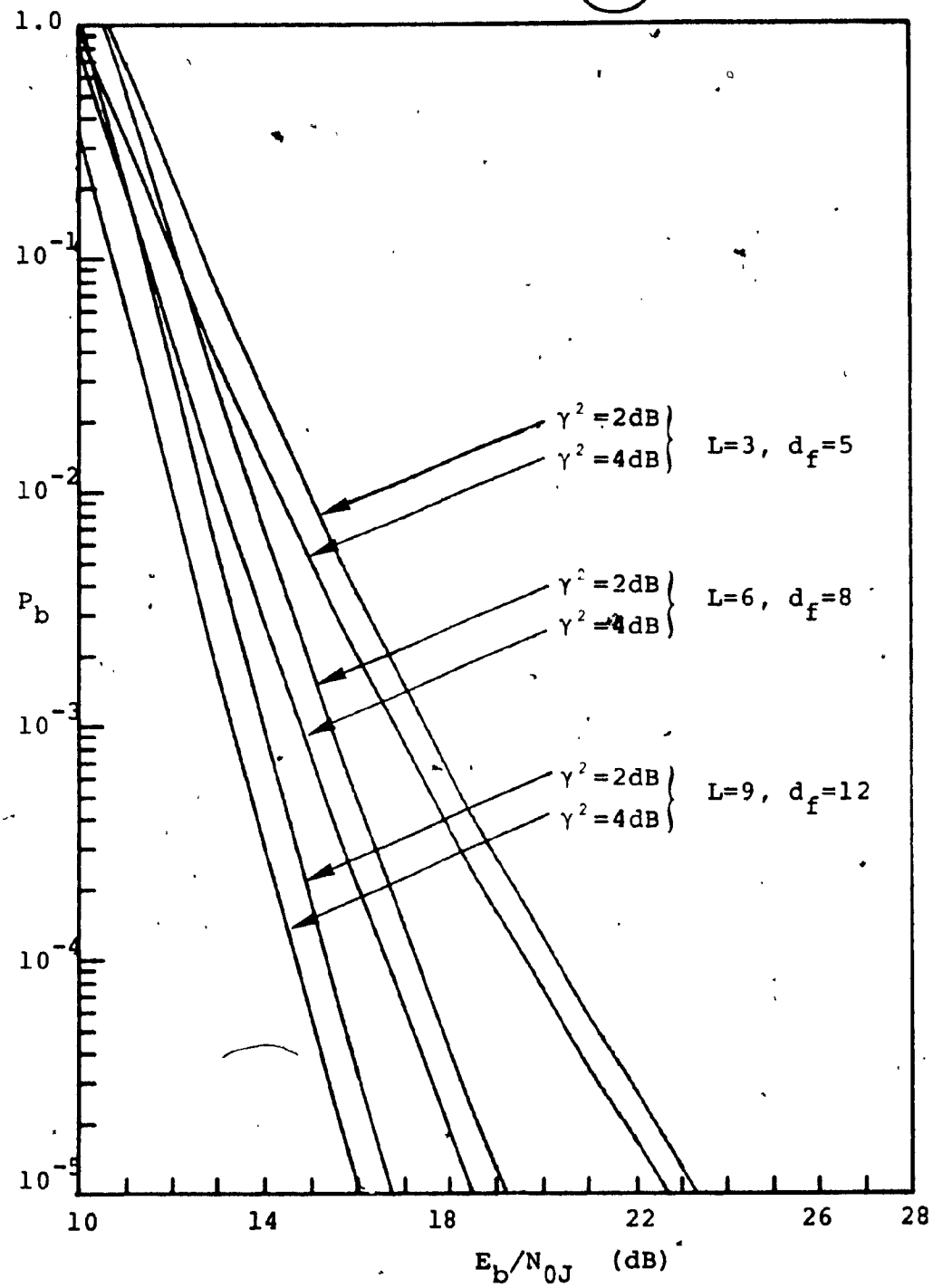


Figure 5.19: Performance of rate $\frac{1}{2}$ convolutional codes with hard decision decoding in worst case partial band jamming and Rician fading

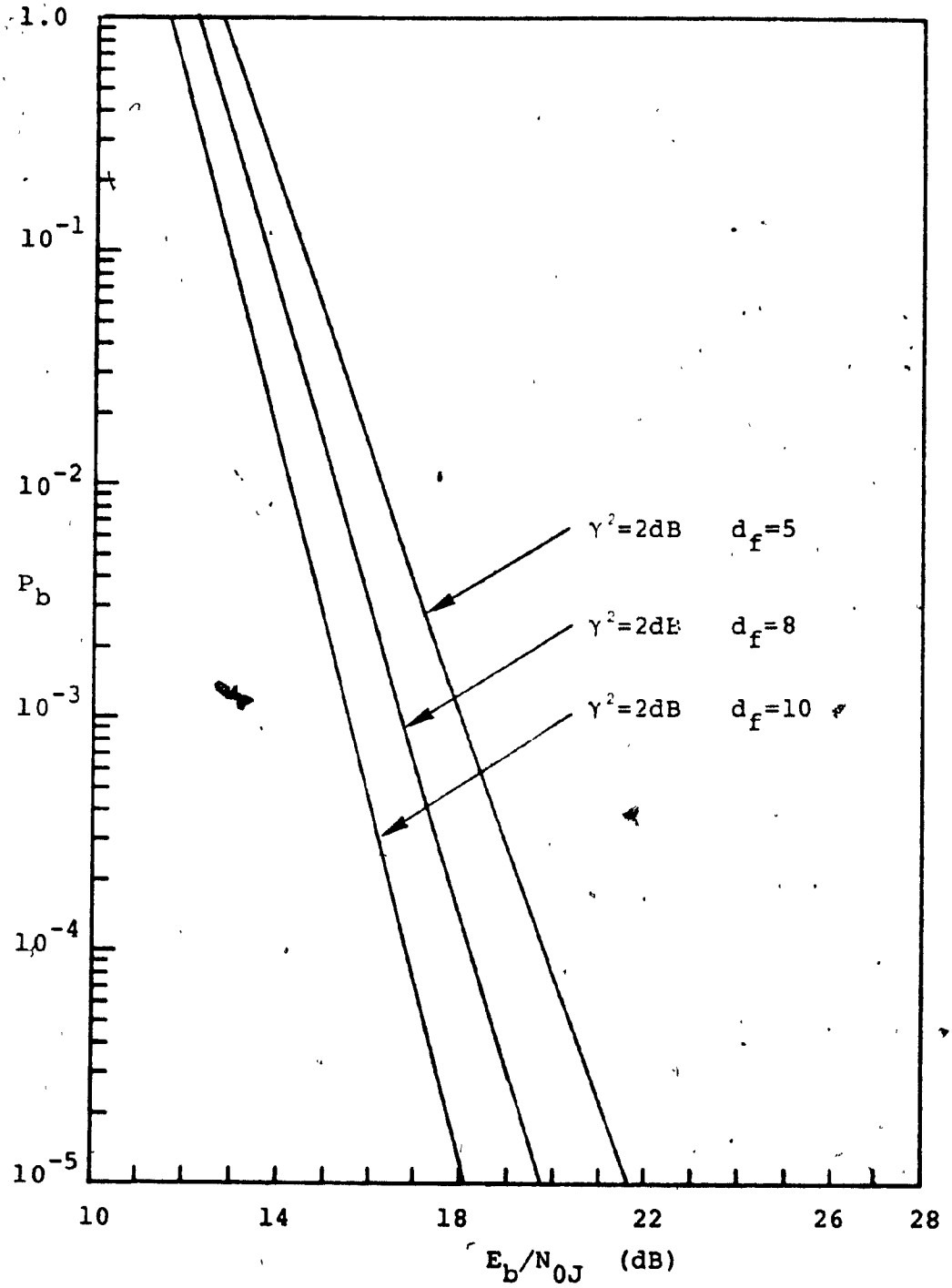


Figure 5.20: Performance of rate $\frac{2}{3}$ convolutional codes with hard decision decoding in worst case partial band jamming and Rician fading

codeword. The index j indicates the j-th branch and the index r indicates the r-th path through the trellis. A metric for the r-th path consisting of B branches through the trellis is

$$U^r = \sum_{j=1}^{B} \mu_j^r \tag{5.33}$$

If soft decision decoding is used with Viterbi algorithm, we define the metric for the j-th branch as

$$\mu_j^r = \sum_{m=1}^{n} |y_{1jm}|^2 \, v_{jm}^2 + (1-v_{jm}^2)\,|y_{0jm}|^2 \tag{5.34}$$

where n is the number of bits transmitted for every k input bits. $|y_{ijm}|^2$ denotes the square-law detected output from the demodulator, $i=0,1$ denotes the transmitted frequency and jm denotes the m-th bit of the j-th branch.

Again we assume that the all zero code is transmitted. The path metric for the all-zero path at node B is

$$U^0 = \sum_{j=1}^{B}\sum_{m=1}^{n} |y_{0jm}|^2 \tag{5.35}$$

A first-event error occurs when the decoder excludes the all zero path and takes another path at distance d from the all zero path. Hence [3]

$$P_j(d) = Pr(U^r \geq U^0) = Pr(U^r - U^0 \geq 0)$$

$$= \Pr\left(\sum_{j=1}^{B}\sum_{m=1}^{n} |y_{1jm}|^2 \cdot v_{jm}^r - |y_{0jm}|^2 \, v_{jm}^r\right) \qquad (5.36)$$

Since the code bits in the two paths differ only in d positions, (5.36) can be written in a simpler form [3]

$$P_j(d) = \Pr\left(\sum_{i=1}^{d} |y_{1i}|^2 > |y_{0i}|^2\right) \qquad (5.37)$$

where the index runs over the set of d bits in which the two path differ and the set $|y_{ji}|^2$ represents the output of the square-law detector for these d bits [3]. $P_j(d)$ is, in fact, the probability of error for BFSK with square-law detection and d-th order diversity. Thus $P_j(d)$ has the form of (5.23) for block codes. The bound on the bit error rate has the form of (5.31) but $P_j(d)$ is replaced by (5.23).

5.3.3 DISCUSSION ON GRAPHICAL RESULTS

As in the case of block coding we select some rate 1/3, 1/2 and 2/3 convolutional codes to show that coding can exceptionally improve the performance of a spread spectrum system. The rate 1/3 and 1/2 convolutional codes and their distance parameters are taken from [31]. For these codes the constraint length is known for each codes. However, for rate 2/3 convolutional codes, their parameters were calculated using "brute force technique" [42].

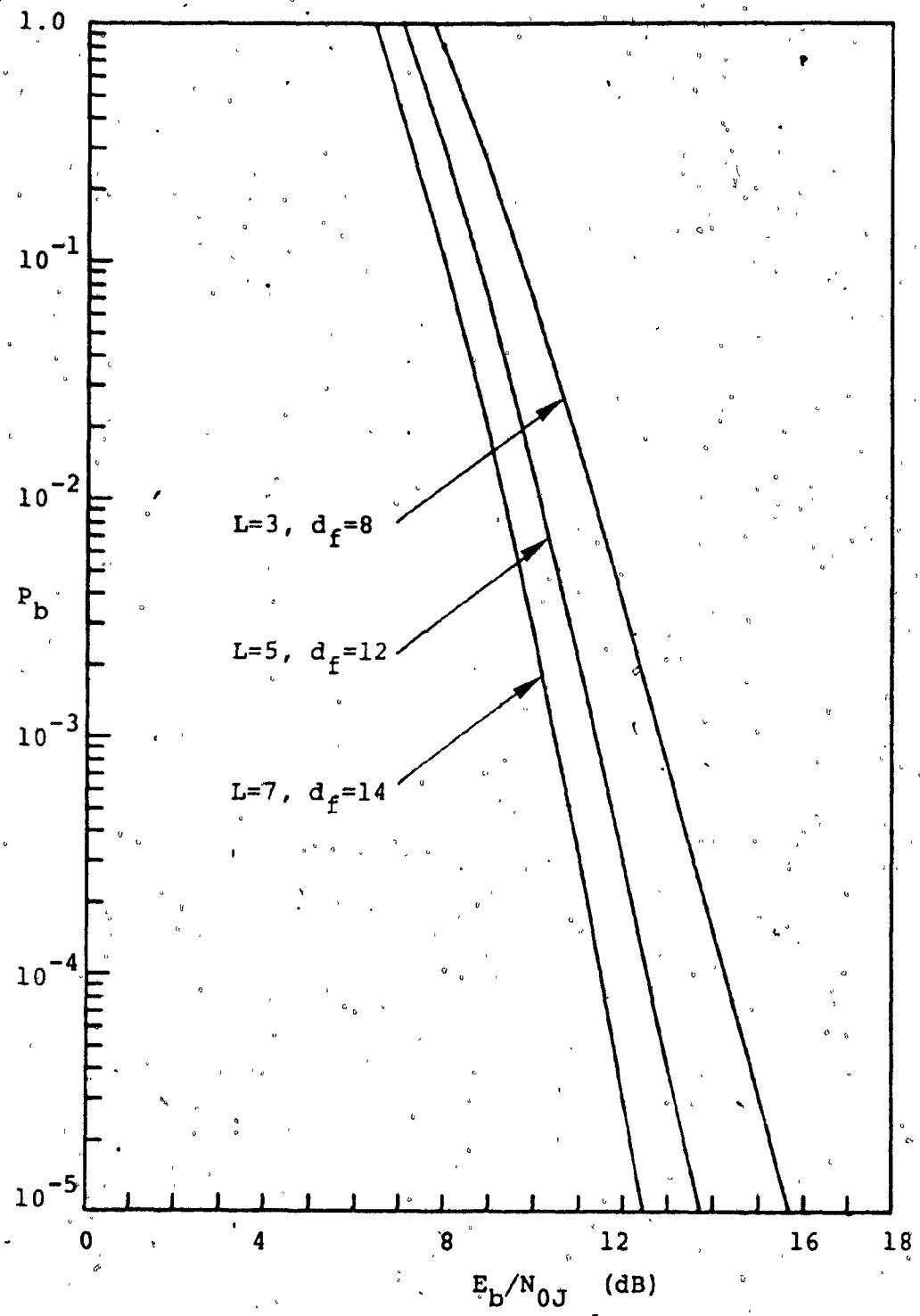


Figure 5.21: Performance of rate $\frac{1}{3}$ convolutional codes with soft decision decoding in worst case partial band jamming and Rayleigh fading

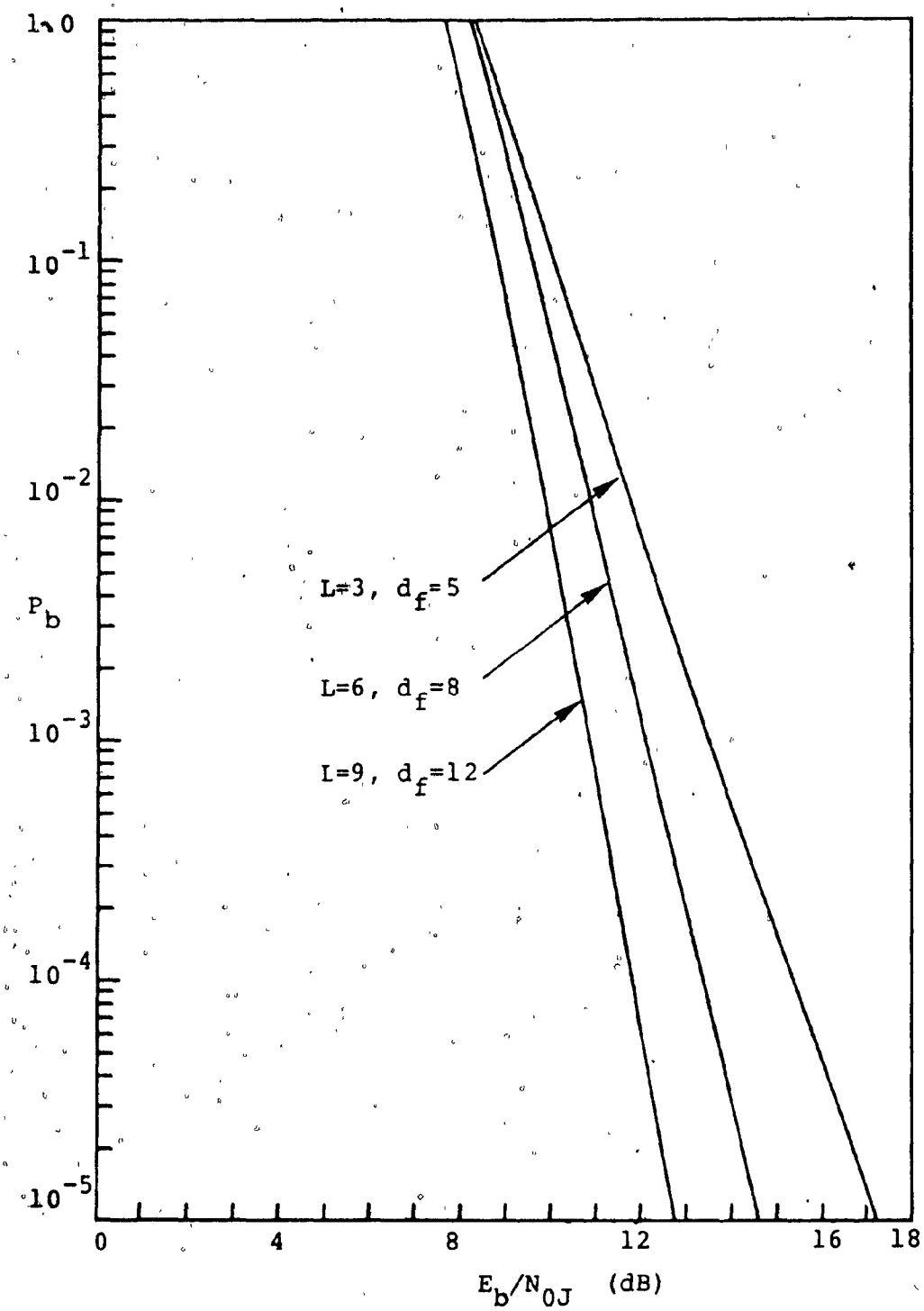


Figure 5.22: Performance of rate $\frac{1}{2}$ convolutional codes with soft decision decoding in worst case partial band jamming and Rayleigh fading

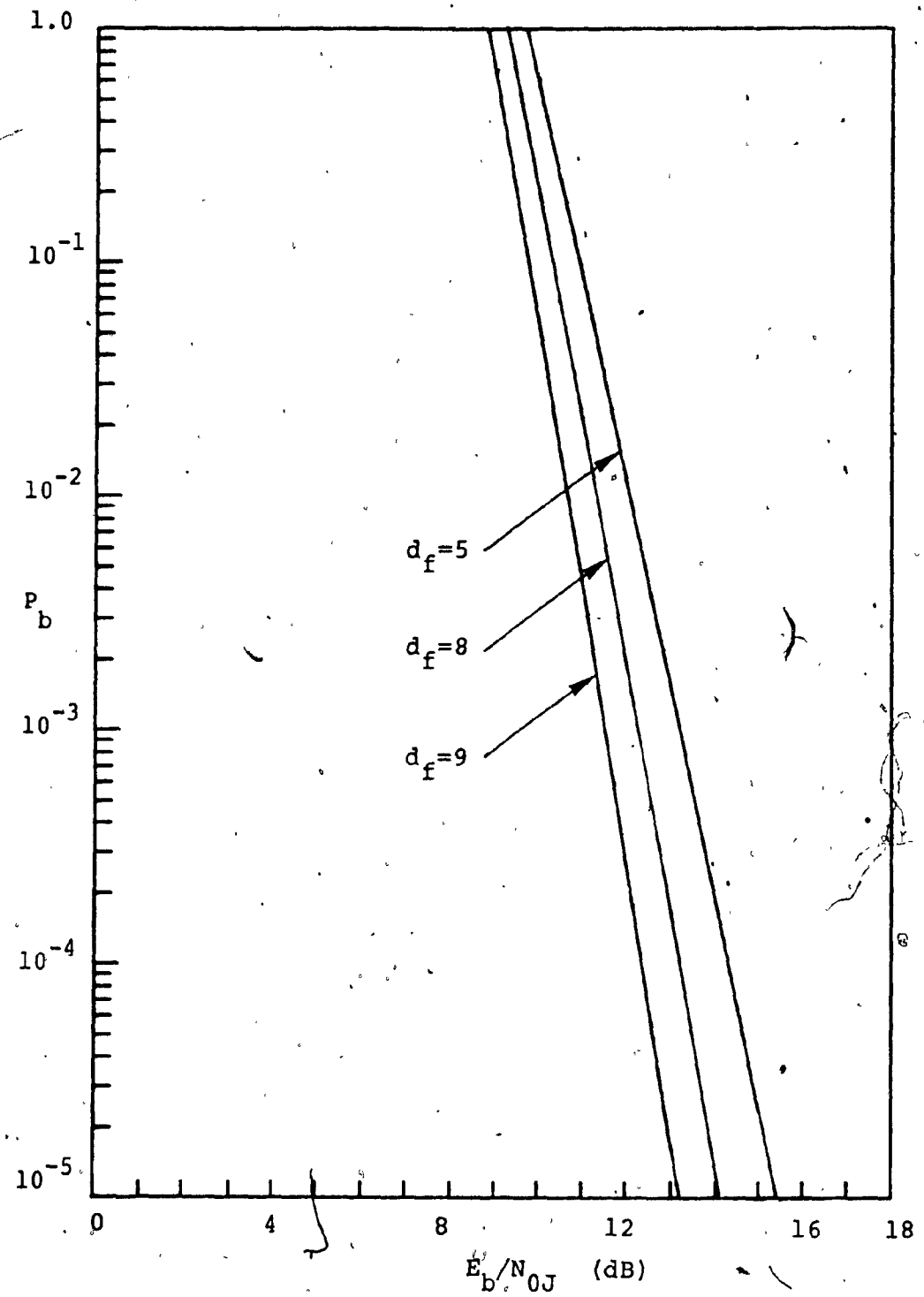


Figure 5.23: Performance of rate $\frac{2}{3}$ convolutional codes with soft decision decoding in worst case partial band jamming and Rayleigh fading

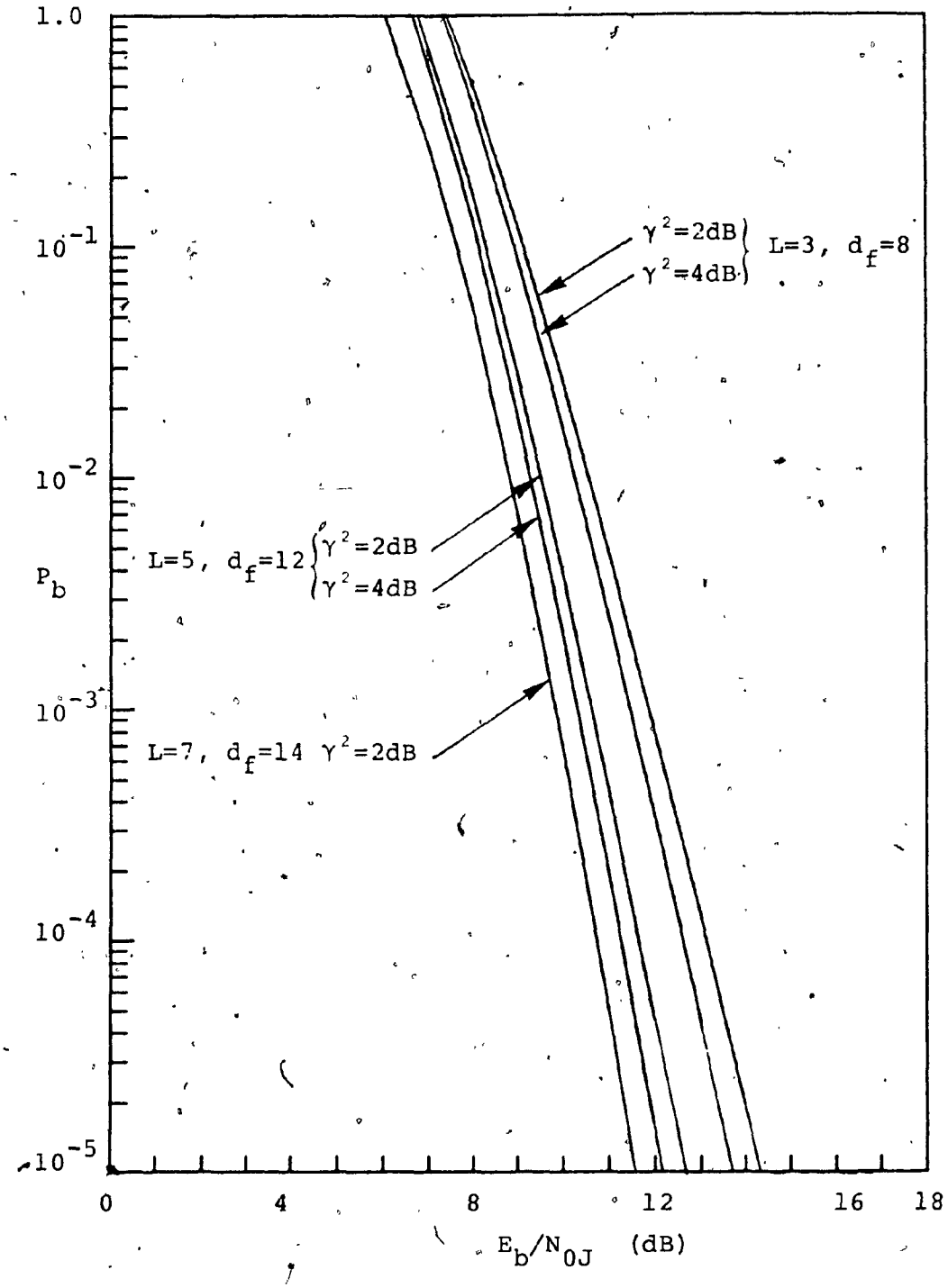


Figure 5.24: Performance of rate $\frac{1}{3}$ convolutional codes with soft decision decoding in worst case partial band jamming and Rician fading

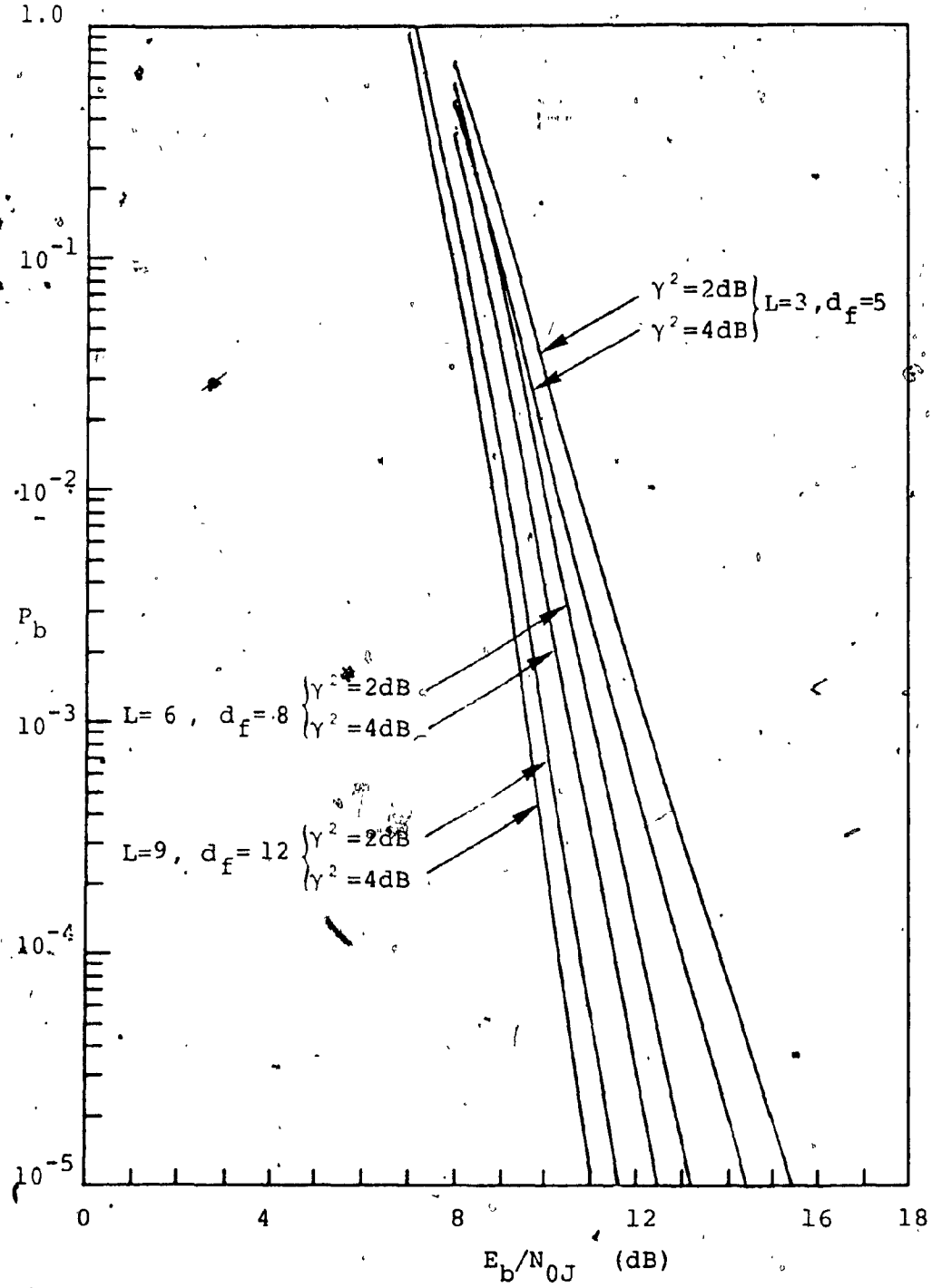


Figure 5.25: Performance of rate $\frac{1}{2}$ convolutional codes with soft decision decoding in worst case partial band jamming and Rician fading

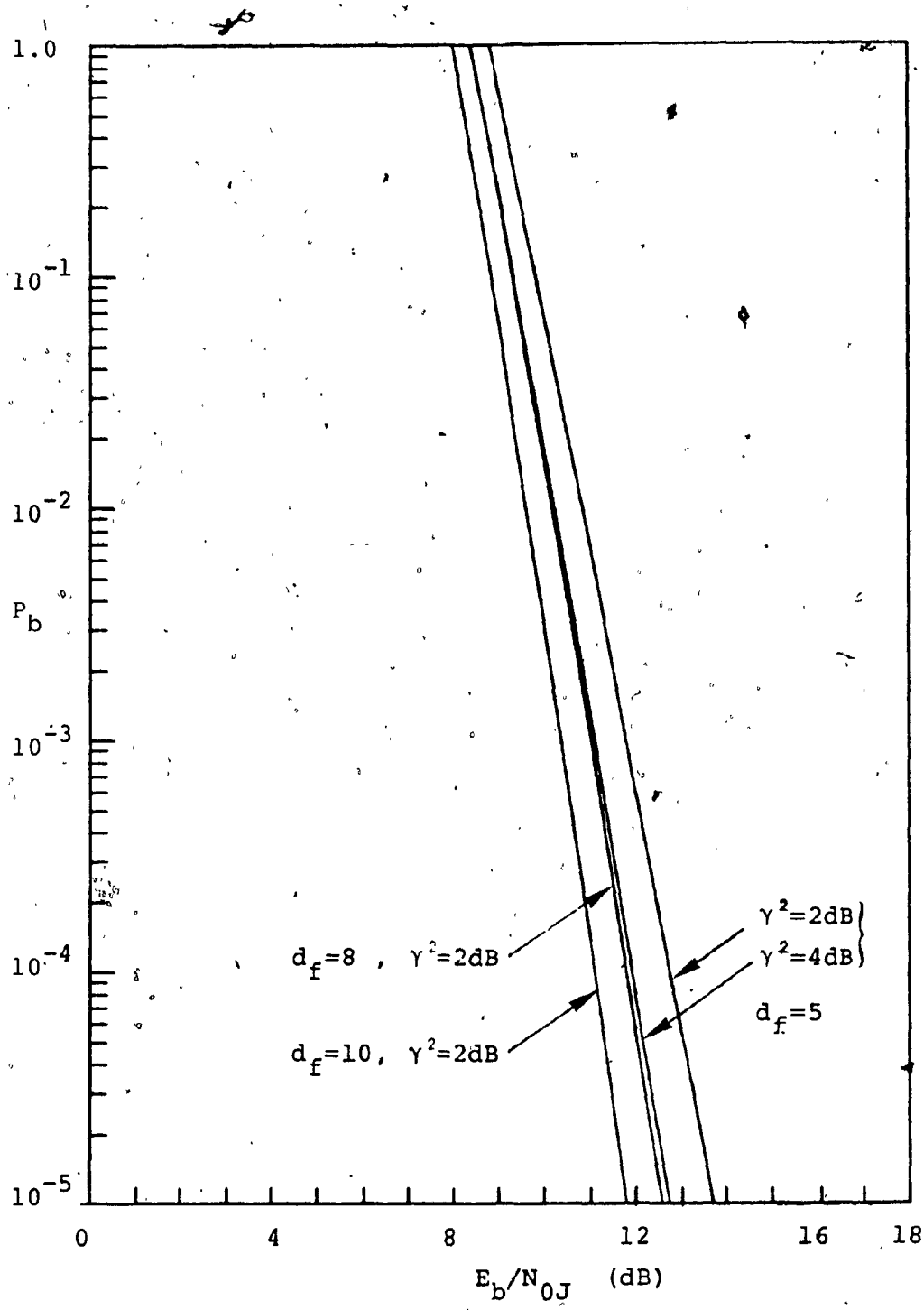


Figure 5.26: Performance of rate $\frac{2}{3}$ convolutional codes with soft decision decoding in worst case partial band jamming and Rician fading

Again we tabulate the performance of a coded system at $P_b=10^{-5}$ for Rayleigh and Rician fading channel under worst case partial band jamming. From Tables 5.3 and 5.4 we note that convolutional codes give comparable results to those of quasi-cyclic codes of compatible distance. Convolutional codes give and average of 28-30dB gain in SNR over a noncoded system. In case of Rician fading, as we can expect from the results of quasicyclic codes, the quantity γ^2 does not give much improvement to the performance of a coded system under worst case jamming. We also note that rate 1/3 codes perform better than rate 1/2 and 2/3 codes. But rate 1/2 codes do not give superior result compared to those of rate 2/3. This is due to the free distances of these selected codes.

Thus we have shown that coding completely recovers the loss due to fading and worst case jamming. In fact, coding almost eliminates the effects of fading in the channel. In the next section, we will summarize some previous works on the exact or bound on probability of errors in FH/MFSK on additive white Gaussian channel and worst case partial band jamming.

5.4 DISCUSSION ON PREVIOUS RESEARCH WORKS

Error-correcting coding is an antijam technique in spread spectrum systems in AWGN channel and partial band

Table 5.3: Performance of some convolutional codes with worst case partial band jamming and Rayleigh fading at $P_b = 10^{-5}$.

		Hard decision decoding		Soft decision decoding	
code	rate	SNR (dB)	Gain (dB)	SNR (dB)	Gain (dB)
$(L=3, d_f=8)$	1/3	22.5	25.5	15.6	32.4
(5,12)	1/3	19.1	28.9	13.8	34.2
(7,14)	1/3	17.2	30.8	12.5	35.5
(3,5)	1/2	25.5	22.5	17.2	30.8
(6,8)	1/2	21.2	26.8	14.5	33.5
(9,12)	1/2	18.8	29.2	12.7	35.3
(-,5)	2/3	23.8	24.2	15.4	32.6
(-,8)	2/3	21.8	26.2	14.1	33.9
(-,9)	2/3	20.2	27.8	13.2	34.8

Table 5.4: Performance of some convolutional codes with worst case partial band jamming and Rician fading at $P_b = 10^{-5}$, $\gamma^2 = 2$dB.

		Hard decision decoding		Soft decision decoding	
code	rate	SNR (dB)	Gain (dB)	SNR (dB)	Gain (dB)
$(L=3, d_f=8)$	1/3	20.4	21.6	14.3	27.7
(5,12)	1/3	17.2	24.8	12.6	29.4
(7,14)	1/3	15.4	26.6	11.5	30.5
(3,5)	1/2	21.3	20.7	15.4	26.6
(6,8)	1/2	19.2	22.8	13.2	28.8
(9,12)	1/2	16.7	25.3	11.6	30.4
(-,5)	2/3	21.6	20.4	13.6	28.4
(-,8)	2/3	19.8	22.2	12.5	29.5
(-,9)	2/3	18.1	23.9	11.8	30.2

jamming. But only a few analysis have treated fading channel with partial band jamming. Thus this section is included to show that coding almost neutralize the effect of fading on the spread spectrum system in addition to antijamming. Most of the previous papers considered the complete knowledge of jamming state in soft decision decoding. In realistic communication network application, the geographically dispersed signal sources, jammer and channel fading, and variations in the received signal energy complicate the jamming state determination [48]. So it is reasonable not to consider side information in a fading channel.

In fact, the additive white Gaussian noise channel is a special case of the channel considered in Chapter 3. It is known from [26],[30] and [48] that the bit error rate for FH/MFSK in partial band jamming is given as

$$P_{b,u}(\lambda) = \frac{\lambda}{2(M-1)} \sum_{i=2}^{M} (-1)^i \binom{M}{i} \exp\{-k\frac{E_b}{N_o}(1-\frac{1}{i})\} \tag{5.38}$$

Thus a symbol error P_s is found by multiplying (5.38) with $(2^k-1)/(2^{k-1}-1)$

$$P_s(\lambda) = \frac{\lambda}{M} \sum_{i=2}^{M} (-1)^i \binom{M}{i} \exp\{-k \frac{E_b}{N_o}(1-\frac{1}{i})\} \tag{5.39}$$

Equation (5.39) is exactly (3.23) with $\alpha^2\rho$ being replaced by

$$\alpha^2\rho = \log_2 M \frac{E_b}{N_{oJ}} = \frac{KE_b}{N_{oJ}} \tag{5.40}$$

If an (n,k) block code is used, then $\alpha^2\rho$ will be replaced by KrE_b/N_{oJ}. For the worst case; we obtain [30]

$$P_s = \begin{cases} \dfrac{\alpha(2^k-1)}{(2^k-1)E_b/N_o} & (r\dfrac{E_b}{N_o} \geq \varepsilon) \\ \\ \dfrac{1}{M}\displaystyle\sum_{i=2}^{M}(-1)^i \binom{M}{i} \exp\{-kr\dfrac{E_b}{N_o}(1-\dfrac{1}{i})\} & (r\dfrac{E_b}{N_o} < \varepsilon) \end{cases} \tag{5.40}$$

and are enumerated in Table 5.5 [30,48]

Table 5.5: Performance parameters of codes FH/MFSK in worst case partial band jamming

$M=2^k$	α	ε
2	$e^{-1}=0.3679$	2
4	0.2329	1.192
8	0.1954	0.927
16	0.1813	0.798
32	0.1764	0.723

The coded bit error rate is approximated by

$$P_b \leq \frac{1}{n}\sum_{i=t+1}^{n} i \binom{n}{i} p_s^i (1-p_s)^{n-i} \tag{5.41}$$

which is different from (5.17) because (5.41) considers only errors that cause the decoder to incorrectly select a codeword which is different from a particular transmitted codeword. However, in (5.17) all possible transmitted codewords

are accounted.

The performance of some binary codes such as Hamming code, Golay code and BCH codes are depicted in Figure 5.27. Codes which are equivalent to quasi-cyclic codes give same curve shapes of quasi-cyclic codes used in fading channel but a 5dB penalty is paid due to fading. However, the gain compared to uncoded system is more on fading channel which proves that coding functions better as an antifading, antijamming technique. If the code used is not in binary form then M-ary signalling is preferred. For Reed Solomon codes, k-bits are sent as a symbol. In this case, the bit error rate is given by (5.18) and symbol error rate is given by (5.40).

For rate 1/2, constraint length 7 binary convolutional, code used on the binary channel (M=2), it is known that [30,27]

$$P_b \leq 0.5(36D^{10} + 211D^{12} + 1404D^{14} + \ldots) \qquad (5.42)$$

for rate 1/3, constraint length 5, we get

$$P_b \leq 0.5(D^{14} + 20D^{16} + 53D^{18} + \ldots) \qquad (5.43)$$

where D is the same parameter used in the computational cut off rate R_o in Chapter 4. For BSC, AWGN with hard quantization, we get $D= 2\sqrt{p(1-p)}$ as in (4.19) but p is

given by (5.40). Equations (5.42) and (5.43) are derived from the transfer functions of convolutional codes. Plots of the above mentioned convolutional codes are also shown in Figure 5.27.

It is well known that diversity alone can provide a large improvement in performance by adding redundancy analogous to the redundancy in a codeword. It is of interest to see how diversity can be applied in FH/MFSK. With diversity, each M-ary symbol is divided into m equal subsymbol each of which is sent on a different frequency hop with energy KE_b'/m. This give us m independent chances, each with probability $(1-\lambda)$ of receiving error free M-ary data. Diversity can be achieved in hop rate equals to the symbol rate but this approach is not always feasible because of hardware limitation [48]. Interleaving provides an alternative way to produce redundancy.

Assuming perfect knowledge of jamming state, an error can occur if all the diversity chips are jammed, the M-ary symbol is determined by the largest of the metric [48].

$$\Lambda_i = \sum_{j=1}^{m} X_{ij} \qquad (5.44)$$

where X_{ij} is the output of the i-th energy detector $(1<i<M)$ on the j-th diversity transmission. If the metric of (5.44) is used then the bit error rate is bounded as [27]

$$P_b \leq 2^{k-2} \min_{\leq\rho\leq} [\frac{\lambda}{(1-\rho^2)} \exp\{-(\frac{\rho}{1+\rho})(\frac{\lambda KE_b}{mN_o})\}^m] \tag{5.45}$$

where ρ is the Chernoff parameter.

For optimum jamming, the duty cycle is [27]

$$\lambda = \frac{3m}{KE_b/N_o} \tag{5.46}$$

for which

$$P_b \leq 2^{K-2} \left(\frac{4me^{-1}}{KE_b/N_o} \right)^m \tag{5.47}$$

provided $\lambda < 1$. For $E_b/N_{oJ} < 3m/k$, broad band jamming is optimum. The optimum diversity occurs at

$$m_{opt} = \frac{KE_b}{4N_o} \tag{5.48}$$

which gives

$$P_b \leq 2^{K-2} \exp\{-\frac{KE_b}{4N_o}\} \tag{5.49}$$

and

$$\lambda = \frac{3}{4} \tag{5.50}$$

So optimum diversity restores the exponential relationship between P_b and E_b/N_{oJ}. The upper bound on E_b/N_{oJ} required to achieve $P_b=10^{-5}$ is depicted in Figure 5.28. So diversity alone can restore the loss due to worst case partial band jamming. The analysis above may be extended to convolutional codes. The only difference is

that diversity is specified in terms of diversity per ℓ bit instead of the diversity per M-ary symbol m. For the metric defined in (5.44) we have [27]

$$\ell_{opt} = \frac{E_b}{4N_o} \tag{5.51}$$

$$\lambda = \frac{3}{4}$$

for all cases. The amount of interleaving would be

$$d = \frac{\ell R_b}{R_c} \tag{5.52}$$

where R_b and R_c are data rate and hop rate, respectively. Without showing the mathematics involved, the upper bound of the constraint length 7, rate 1/2 code is

$$P_b \leq 18 \exp\{-5E_b/4N_o\} \tag{5.53}$$

Equation (5.52) shows that the performance of this code in BFSK is exponentionally equivalent to the uncoded 32-ary FSK system. In general, more the partial band jamming protection provided by the coded redundancy lesser the diversity that is required. Usually, the soft decision decoding metric with perfect jamming state is not feasible in most of the system. A hard decision metric without side information can perform acceptably in worst case partial band jamming [27].

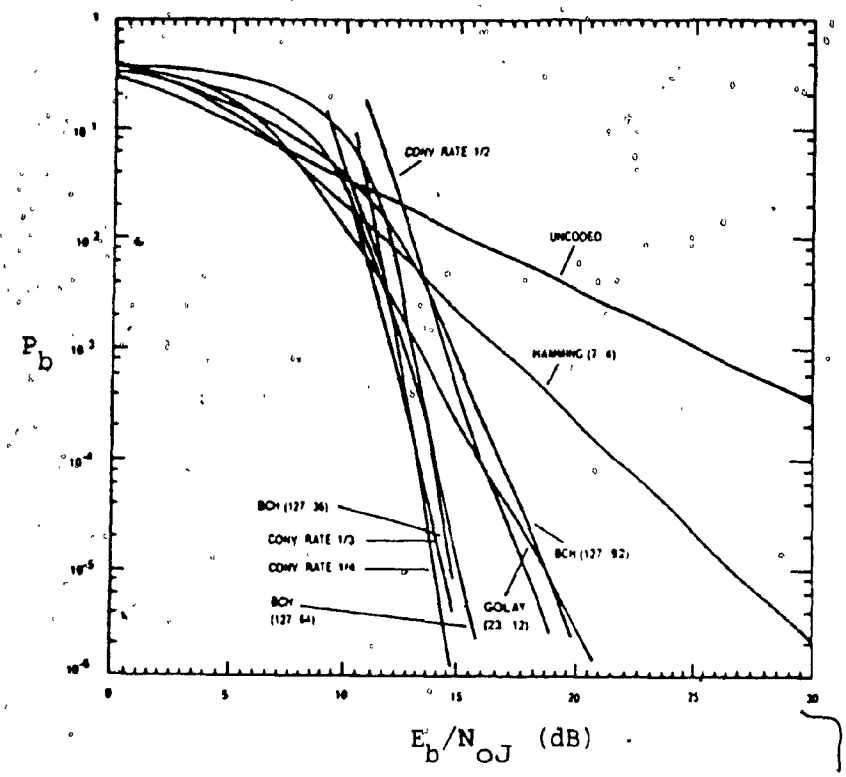


Figure 5.27: Performance of some binary block codes and convolutional codes in worst case partial band jamming and hard decision decoding [30]

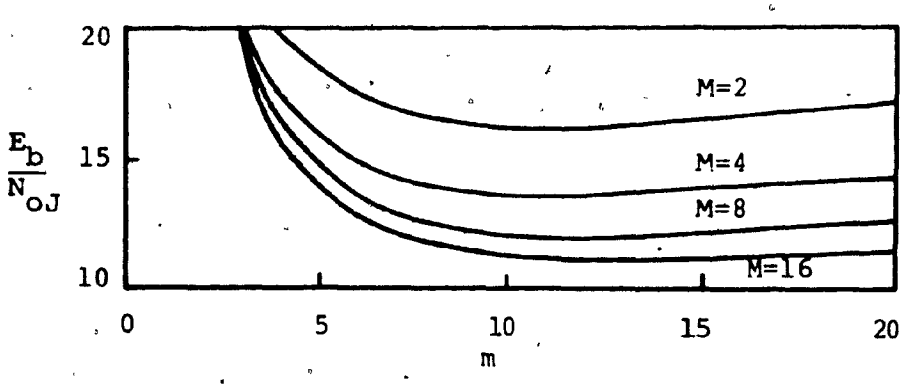


Figure 5.28: E_b/N_{oJ} required to achieve $P_b=10^{-5}$ for uncoded FH/MFSK with optimum diversity in worst case partial band noise

CHAPTER 6

SUMMARY AND CONCLUSION

6.1. SUMMARY AND CONCLUSION

In this thesis we have examined the performance of codes on spread spectrum channel with jamming and fading. The basic concepts of spread spectrum techniques were presented in Chapter 2. Two types of spread spectrum modulation are briefly stated. Partial jammer, i.e. a jammer which feeds noise into the channel for only a fraction of the time or only a fraction of the bandwidth, can cause severe damages to the channel. The performances of DS and FH in partial jammer environment are analogous in term of the effective signal to noise ratio.

In Chapter 3, bounds on the raw bit error of frequency hopping, multiple frequency-shift-keying system were presented. The received signal experiences either Rayleigh fading or Rician fading in addition with non fading partial band noise. The detection is carried out noncoherently. We made an assumption that there was no background noise in the channel. Since the amplitude of the received signal fades according to Rayleigh or Rice distributions, we derived the expressions of bit error rates based on the received amplitudes and their distributions. Performance of FH under partial band jamming were plotted for binary, 4-ary and 16-ary FSK. The increase in the signal alphabet does

curves showed that the system is much improved by the use of coding. The codes in the analyses were selected rate 1/3, 2/3, and 1/2 codes. Rate 1/3 and 1/2 gave similiar values of SNR at $P_b=10^5$ when hard decoding is employed. If soft decision decoder was used, rate 1/3 codes with compatible code length and minimum distance showed better curves than the other two code rates. Similar results were obtained when convolutional codes were used.

In the case of Rician fading channel the ratio γ^2 plays an important role in the decoding performance. Since $\gamma^2=\frac{\alpha^2}{2\sigma^2}$ denotes the received energy via fixed component over the received energy via random component. Larger γ^2 results in the fixed component becoming a dominant term. Thus with large γ^2 we can approximate the bit error rate using the results of a AWGN channel. This is true if the jammer is not an optimal one. If the jammer is a worst case jammer increasing in γ^2 gave little improvement in the SNR.

We also showed that in order to maitain the processing gain as in the case of non coding system we must expand the bandwidth according to the code and its rate. We conclude that good coding schemes exist for channels with partial band interference and fading and are essential for reliable communications. However, all the curves shown in Chapter 4 and Chapter 5 represent a relative performance of how well the proposed coding /decoding system will function against a variable level of average channel noise. More

not offer much improvement in the performances.

Linear block codes and convolutional codes have been studied for possible application in spread spectrum channel. But at what code rate one should use or how long a code is required? Those questions were answered in Chapter 4. Instead of finding one good code which is a long process, we considered the ensemble of codes of rate, say, 1/2 and evaluated the average ensemble probability of error on a particular channel. This average error depends on the cut off rate R_o which is a function of the SNR and channel parameters. Curves of the cut off rate R_o versus E_b/N_{oJ} provide guidelines in choosing code rates for different channels. A transformation process was proposed to convert the bit error rate of any specific code in the AWGN channel to the bit error rate for any type of channels provided the performance curves of the AWGN channel are available.

In Chapter 5 we tried to find the bounds on the bit error rate for specific codes. A bound was derived for any code with unknown or known weight distributions. Also the bounds depend on the minimum distance, so larger the minimum distance the better the code will perform. BCH codes are among the common codes used but a low code rate (r=k/n) BCH codes tend to deteriorate quickly. So we proposed the use of quasi-cyclic codes in the fading channel. Quasi-cyclic codes represent linear block codes and their performance

compulational work is required for a complete study because the channel varies from time to time depending on various factors such as weather or temporary obstacles that can defect the communication link.

6.2. SUGGESTION FOR FUTURE WORK

As we mentioned in Chapter 4 the information in the presence of the jammer can be acquired by monitoring the frequency slots. If this side information is available, it can be used to help the soft decision decoder make more reliable decisions. It is of interest to find the bounds or error probability for the channel that we have considered. Also, it would be helful to determine the sensitivity of a system to the accuracy of the side information.

REFERENCES

1. Pickholtz, R.; Schilling, D.; Milstein, L., "Theory of Spread Spectrum Communication: A Tutorial", IEEE Trans. on. Comm. vol COM-30, pp.855-884, May 1982.

2. Natali, F. , A Tutorial in Spread Spectrum Technique, National Telesystem Conference, San Francisco, Nov. 1983.

3. Proakis, J. , Digital Communication, New York: McGraw-Hill, 1982.

4. Viterbi, A. , "Spread-Spectrum Communication - Myth and Realities", IEEE Communication Magazine, vol.17, pp. 11-18, May 1979.

5. Clark, G.C. and Cain, J.B. ; Error-Correction Coding for Digital Communications, New York: Plenum Press, 1981.

6. Wozencraft, J.M. ; Jacobs, I.M., Principles of Communication Egineering, New York: Wiley, 1965.

7. Bhargava, V.K.; Haccoun, D.; Matyas, R. and Nuspl, P., Digital Communications by Satellite, New York: Wiley, 1981.

8. Séguin, G., Lecture Notes of ELEC N613 "Introduction to Error Control Coding", Concordia University, Montréal, 1983.

9. Huth, G.K., "Optimization of Coded Spread-Spectrum System Performance", IEEE Trans. on Comm., vol. COM-25, pp.763-770, Aug. 1977.

10. Spellman, M. , "Comparision Between Frequency Hopping and Direct Spead PN as Antijam Techniques", Proc. of the 1982 Military Commun. Conf. (MILCOM82), pp. 14.4-1, 6, 1982.

11. Turin, G.L., "Error Probabilities for Binary Symmetric Ideal Reception Through Nonselective Slow Fading and Noise.", Procceding of the IRE, vol 46, pp. 1603-1619, Sept. 1958.

12. Schwartz, M. ; Bennett, W.R. and Stein, S. , Communication System and Techniques, New York: McGraw Hill, 1966.

13. Geraniotis, E.A. and Pursley, M.B. , "Error Probabilities for Slow-Frequency-Hopped Spread Spectrum Multiple-Access Communications over Fading Channels", IEEE Trans. on Comm., vol.COM-30, pp.996-1009, May 1982.

14. Lindsey, W.C. , "Error Probabilities for Rician Fading Multichannel Reception of Binary and N-ary Signals.", IEEE Trans. on Info. Theo. , vol IT-10, pp.339-350, Oct.1964

15. Reiger, S. , "Error-rate in Data Transmission.", Proc. of IRE, vol 46, pp . 919-920, May 1958.

16. Pursley, M.B., "Coding and Diversity for Channels with Fading and Pulsed Interference", Proceedings of the 1982 Conference on Information Sciences and Systems, Princeton University, March 1982.

17. Gradshteyn, I.S. and Ryzhik, I.K. , Table of Integrals

Series and Products, Academic Press, 1965.

18. Lin, S. and Costello, D., Error-Control Coding: Fundamentals and Applications, New Jersey: Prentice Hall, 1983.

19. Bhargava, V.K. , " Forward Error-Control Schemes for Digital Communications", IEEE Communications Magazine, vol. 21, pp.11-19, Jan. 1983.

20. McElice, R. , The Theory of Information and Coding, Massachusetts: Addison-Wesley, 1977.

21. Hahn, P.M. , "Multichannel FSK and DPSK Reception in Multiple Frequency, Shift Keying", IRE Trans. on Comm. Systems, vol. CS-10, pp. 177-184, June 1962.

22. Chase, D. , "Digital Signal Design Concept for a Time Varying Rician Channel", IEEE Trans. on Comm. Tech., vol. COM-24, pp.164-172, Feb. 1976.

23. Chase, D., "A Class of Algorithms for Decoding Block Codes with Channel Measurement Information", IEEE Trans. on Info. Theory, vol. IT-18, pp. 170-182, Jan. 1972.

24. Berlekamp, E.R. , "The Technology of Error Correcting Codes", Proc. of the IEEE, vol. 68, pp. 564-592, May 1980.

25. Pursley, M.B. and Stark, W.E. , "Antijam Capabilities of Frequency-Hop Spread-Spectrum with Reed-Solomon Codes", Proc. of the 1983 IEEE Military Comm. Conference (MILCOM83), pp. 7-11, Oct.1983.

26. Houston, S.W. , "Modulation Techniques for Communication Part 1: Tone and Noise Jamming Performance of Spread Spectrum M-ary FSK and 2,4-ary DPSK Waveform", Record of the NAECON, pp.51-58, June 1975.

27. Omura, J.K. and Levitt, B.K. ,"Coded Error Probability Evaluation for Antijam Communication System", IEEE Trans. on Comm., vol COM-30, pp.896-903, May 1982.

28. Stuber, G.L. ; Blake, I.F. and Mark, J.W., "Performance of Coded Spread Spectrum Systems over Fading Jamming Channels", Proc. of the Twelfth Biennial Symposium on Communications, Queen's University, Kingston, Canada, pp.B4.1-4, June 1984.

29. Blake, I.F. and Mark, J.W, "Fast FH-MFSK with Partial Band and Tone Jamming", Proc. on the Twelfth Biennial Symposium on Communications, Queen's University, Kingston, Canada, pp. B4.5-8, June 1984.

30. Ma, H.H. and Poole, M.A. , "Error Correcting Codes Against The Worst-Case Partial Band Jammer", IEEE Trans. on Comm., vol COM-32, pp.124-133, Feb. 1984.

31. Torrieri, D.J. , "Frequency Hopping with Multiple Frequency Shift Keying and Hard Decisions", IEEE Trans. on Comm. vol COM-32, pp. 574-582, May 1984.

32. Peterson, W.W. and Weldon, E.J. , Error-Correcting Codes, Cambridge: The MIT Press, 1972.

33. Bhargava, V.K. , "Construction and Weight Structure of Some Binary Quasi-Cyclic Codes", Master's Thesis, Queen's University, Kingston, Nov. 1971.

34. Chen, C.L. ; Peterson, W.W. and Weldon, E.J., "Some Results on Quasi-Cyclic Codes", Inform. Comtrol, vol 15, pp.407-423, Nov. 1969.

35. Tavares, S.E.; Bhargava, V.K. and S.G.S Shiva, "Some Rate p/(p+1) Quasi-Cyclic Codes", IEEE Trans. on Inform. Theo., vol. IT-20, pp. 133-135, Jan. 1974.

36. Stein, J.M.; Bhargava, V.K. and Tavares, S.E. , "Weight Distribution of Some 'Best' (3m,2m) Binary Quasi-Cyclic Codes", IEEE Trans. on Inform. Theo., pp.708-711, Nov. 1975.

37. Bhargava, V.K. and Avni, M. ,"Net Coding Gain of Some Rate 1/2 Block Codes", Proc. of the IEE, vol. 130, part F, pp. 325-330, June 1983.

38. Bhargava, V.K. ; Seguin, G.E. and Stein, J.M., "Some (mk,k) Cyclic Codes in Quasi-Cyclic Form", IEEE Trans. on Inform. Theory, vol IT-24, pp. 630-632, Sept. 1978.

39. Bhargava, V.K., "(54,18) Code With Weights Divisible by Four", Proc. of the IEEE, vol. 65, pp. 1080-1081, July 1977.

40. Bhargava, V.K. , "Odd Weight Symmetry in Some Binary Codes", IEEE Trans. on Inform. Theo., vol. IT-23, pp. 518-520, July 1977.

41. Viterbi, A.J., "Convolutional Codes and Their

Performance in Communication Systems", IEEE Trans. on Commun. Theo., vol COM-19, no.5, pp. 751-771, Oct. 1971.

42. Conan, J. ,"On the Distance Properties of Paaske's Class of Rates 2/3 and 3/4 Convolutional Codes", IEEE Trans. on Inform. Theo., vol. IT-30, no.1, pp. , Jan. 1984.

43. Papoulis, A. , Probability, Random Variables and Stochastic Processes, New York:McGraw Hill, 1965.

44. Rice, O.S., "Mathematical Analysis of Random Noise", Bell Sys. Tech. Journal, vol. 24, pp.46-157, Jan. 1945.

45. Massey, J.L.,"Information Theory: The Copernican System of Communications", IEEE Communication Magazine, vol.22, pp.26-28, Dec.1984.

46. Viterbi, A.J. and Omura, J.K., Principle of Digital Communication and Coding, New York: McGraw Hill, 1979.

47. Gallager, R.G., Information Theory and Reliable Communication, New York: John Wiley and Sons, 1968.

48. Levitt, B.K. and Omura, J.K., "Coding Trade Off for Improved Performance of FH/MFSK Systems in Partial Band Noise", Nat. Telecommun. Conf. Record, pp. 9.11-9.15, Nov.1981.

APPENDIX A

RICE AND RAYLEIGH DISTRIBUTIONS

In this appendix we derive the Rice and Rayleigh distributions used in Chapter 3. First we will show that the pdf of a random variable has a Rayleigh density if it equals the square root of the sum of two squared normal, independent random variables. Then we use this result to prove Equation (3.5).

Let X and Y be two random variables and $g(x,y)$ be the function of the real variables x and y. We define

$$Z = g(X,Y) \tag{A.1}$$

The distribution $F_Z(z)$ is determined as

$$F_Z(z) = \Pr\{Z \leqslant z\} \tag{A.2}$$

and the pdf is

$$f_Z(z) = \frac{d}{dz}F_Z(z) \tag{A.3}$$

Thus we must find the probability of event $\{Z \leq z\}$. Let D_z be a region in the xy plane such that

$$g(x,y) \leqslant z \tag{A.4}$$

then

$$\{Z \leq z\} = \{(X,Y) \in D_z\}$$

and

$$F_Z(z) = Pr\{Z \leq z\} = Pr\{(X,Y) \in D_z\}$$

$$= \iint_{D_z} f_{XY}(x,y)\,dxdy \qquad (A.5)$$

where $f_{XY}(x,y)$ is the joint density of X and Y.

The pdf can be found by using (A.3) or by determining the region ΔD_z such that

$$z < g(x,y) \leq z\ dz$$

From Figure A.1 we have [43]

$$\{z < Z < z+d_z\} = \{(X,Y) \in \Delta D_z\}$$

thus

$$f_Z(z)dz = Pr\{z < Z < z\ dz\}$$

$$= \iint_{\Delta D_z} f_{XY}(x,y)\,dxdy \qquad (A.6)$$

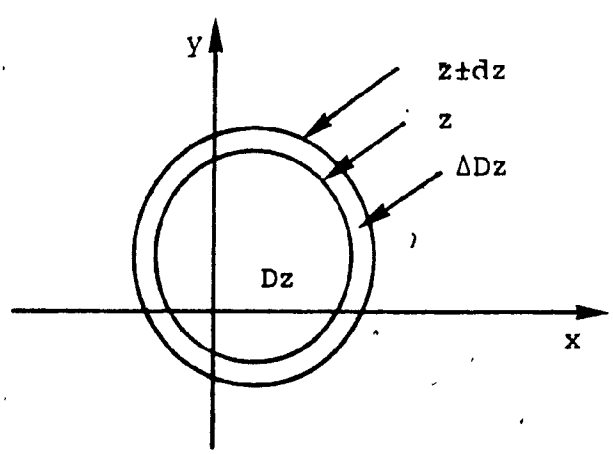


Figure A.1: Regions in xy plane used to determine $F_Z(z)$ and $f_Z(z)$

Now let x and y be two normal, independent random variables with zero mean and equal variance. Thus their joint density is

$$f_{XY}(x,y) = \frac{1}{2\pi\sigma^2} \exp\{ -(x^2+ y^2)/2\sigma^2 \} \qquad (A.7)$$

and define

$$z = g(x,y) = \sqrt{x^2 + y^2} \qquad (z>0)$$

Using (A.5) we get

$$F_Z(z) = \iint_{\Delta D_z} \frac{1}{2\pi\sigma^2} \exp\{-(x^2+y^2)/2\sigma^2\} \, dxdy \qquad (A.8)$$

which is equal the mass in the circle $z > \sqrt{x^2+y^2}$

Let $x = r\cos\theta$ and $y = r\sin\theta$ then

$$x^2 + y^2 = r^2$$

and

$$dxdy = rdrd\theta$$

(A.8) becomes

$$F_Z(z) = \frac{1}{2\pi\sigma^2}\int_0^{2\pi}\int_0^{z}\exp\{- r^2/2\sigma^2\}rdrd\theta$$

$$= 1 - \exp\{-z^2/2\sigma^2\}$$

and $$f_Z(z) = \frac{d}{dz} F_Z(z) = \frac{z}{\sigma^2} \exp\{-z^2/2\sigma^2\} \qquad (z>0) \tag{A.9}$$

Equation (A.9) is also known as Rayleigh density [43].

Now if (A.7) is replaced by

$$f_{XY}(x,y) = \frac{1}{2\pi\sigma^2} \exp\{-[(x-\alpha)^2 + y^2]/2\sigma^2\} \tag{A.10}$$

then $f_z(z)$ can be determined using (A.6). The region ΔD_z, shown in Figure A.2, is

$$z < \sqrt{x^2 + y^2} < z+dz \qquad (z>0)$$

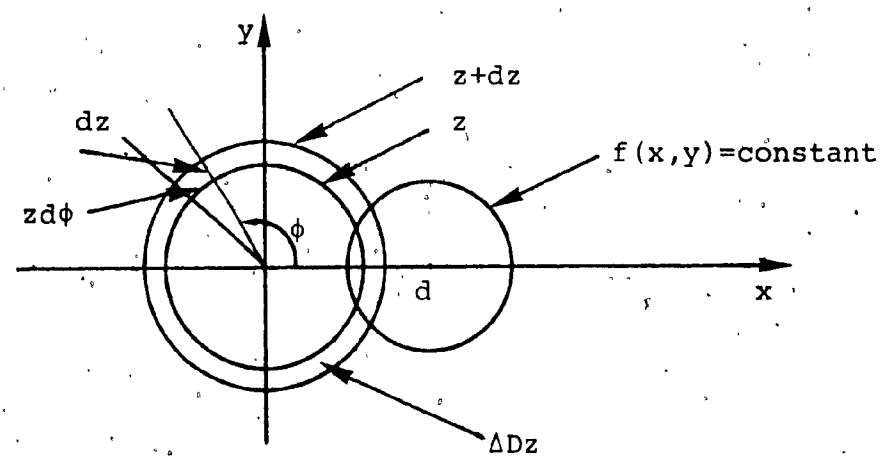


Figure A.2

By letting $x = z\cos\theta$, $y = z\sin\theta$ we have $dxdy = zdzd\theta$.

Then applying (A.6) gives [43,44]

$$f_Z(z)\,dz = \iint_{\Delta Dz} f_{XY}(x,y)\,dxdy$$

$$= \frac{1}{2\pi\sigma^2}\int_0^{2\pi} \exp\{-[(z\cos\theta-\alpha)^2+(z\sin\theta)]/2\sigma^2\}\,zdzd\theta$$

Thus

$$f_Z(z) = \frac{z}{2\pi\sigma^2}\exp\{-(z^2+\alpha^2)/2\sigma^2\}\int_0^{2\pi}\exp\{z\alpha\cos\theta/\sigma^2\}\,d\theta$$

but

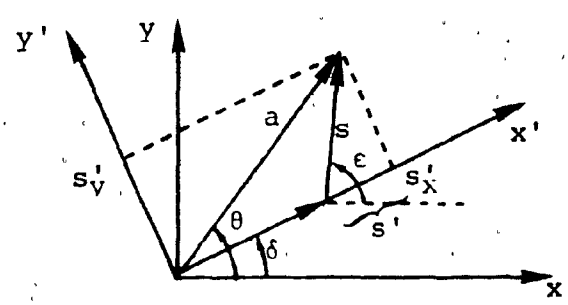
$$I_0(x) = \frac{1}{2\pi}\int_0^{2\pi}\exp\{x\cos\theta\}d\theta = \sum_{n=0}^{\infty}\frac{x^{2n}}{2^{2n}(n!)^2}$$

Hence

$$f_Z(z) = \frac{z}{\sigma^2}\exp\{-(z^2+\alpha^2)/2\sigma^2\}I_0\left(\frac{z\alpha}{\sigma^2}\right) \qquad (z>0) \qquad (A.11)$$

Equation (A.11) was first derived by S.O. Rice [44] so it is also known as Rice distribution. The Rayleigh distribution (A.9) is a special case of (A.11) with $\alpha = 0$

Now recall Figure 3.1



We rotate xy plane by an angle δ to have the new coordinate x'y' with x' coinciding with the fixed vector α. The pdf of vector S is postulated as Rayleigh distribution. Thus by (A.9) S' and S'_y are normally distributed with zero mean and equal variance σ^2. Since S' is normally distributed so is $S'^{\circ}_x = (\alpha+S')$. In this case we return to the distribution of (A.10) and the distribution of vector a is given by (A.11).

APPENDIX B

DIVERSITY COMBINING IN MULTIPLE FREQUENCY SHIFT KEYING

B.1 INTRODUCTION

In this section we determine the performance of M-ary orthogonal signals transmitted over a Rician fading channel. The MFSK signal on the several diversity channels are presumed to be perturbed independently by Rician fading and additive white Gaussian noise. The diversity combining method is chosen so that the receiver performs a maximum likelihood test to decide which one of the M frequencies was actually transmitted. The optimum combining method is to square and add the detected outputs of the corresponding filters from each diversity channel and then make a decision as to which one of the frequencies was sent.

B.2. ERROR PROBABILITY FOR THE M-ary NON-COHERENT DETECTION

Without loss of generality we assume that signal one was transmitted. Let x_1 be the normalized aquared envelope detected by the detector. The pdf of x_1 is

$$p_1(x_1) = \frac{1}{1+\beta} \exp\{(x_1+\delta_1)/1+\beta\}\ I_0\{\sqrt{4\delta_1 x_1/(1+\beta)^2}\} \quad \text{for } x>0 \qquad (B.1)$$

$$= 0 \qquad \text{elsewhere}$$

where $\delta_1 = \alpha_1^2\rho$ and $\beta = 2\sigma^2\rho$ as defined in Chapter 3. If the order of diversity is L then the other L(M-1) channel outputs are noise samples y_i, $i=1,2,3,\ldots,L$, with the pdf given as

$$p_k(y_i) = \exp(-y_i) \qquad (y_i>0)$$
$$= 0 \qquad \text{otherwise} \tag{B.2}$$

where $k \neq i$. Equation (B.1) and (B.2) can be obtained by transforming (3.22) and (3.15) respectively to a squared variable. Since the order is L, the decision variales are

$$X = \sum_{j=1}^{L} x_j$$

and

$$Y = \sum_{j=1}^{L} y_j \tag{B.3}$$

and their pdf's are

$$p_1(X) = (1+\beta)^{-1}(X/S\beta)^{\frac{L-1}{2}} \exp\{-\frac{X+S\beta}{1+\beta}\} \; I_{L-1}\{\sqrt{\frac{4S\beta X}{(1+\beta)^2}}\}$$

$$p_k(Y) = \frac{Y^{L-1}}{\Gamma(L)} \exp(-Y) \tag{B.4}$$

where $$S = \{\sum_{i=1}^{L} \alpha_i^2\}/2\sigma^2 = \sum_{i=1}^{L} \gamma_i^2$$

$$\gamma_i^2 = \alpha^2/2\sigma^2 = \text{signal-to-scatter ratio}$$

$$S\beta = \{\sum_{i=1}^{L} \gamma_i^2\} 2\sigma^2 E_b/N_{oJ}$$

$$= \sum_{i=1}^{L} \delta_i$$

and k=1,2,...,M and $\Gamma(L)$ is the Gamma function. The probability of correct detection is [14].

$$P_c(M,L) = \int_0^\infty p_1(X)\left\{\int_0^\infty p_k(Y)dY\right\}^{M-1}dX \qquad (B.5)$$

Substitution of (B.4) into (B.5) gives

$$P_c(M,L) = \int_0^\infty p_1(X)\left\{\int_0^\infty Y^{L-1}/\Gamma(L)\exp(-Y)dY\right\}^{M-1}dX$$

which becomes

$$P_c(M,L) = \int_0^\infty p_1(X)\left\{1-\sum_{\ell=0}^{L}(X^\ell/\ell!)\exp(-X)\right\}^{M-1}dX$$

$$= \sum_{m=0}^{M}(-1)^m \binom{M-1}{m}\int_0^\infty p_1(X)\left\{\sum_{\ell=0}^{L-1}(X^\ell/\ell!)\exp(-X)\right\}dX \qquad (B.6)$$

but,

$$\{\sum_{\ell=0}^{L-1}(\frac{X^\ell}{\ell!})\exp(-X)\}^m = \exp(mX)\sum_{k=1}^{m(L-1)} c_k X_k \qquad (B.7)$$

by using multinomial theorem to expand the integrand. c_k is the k-th coefficient in the expansion of the summation in the LHS[14,21].

Thus

$$P_c(M,L) = \sum_{m=0}^{M-1} (-1)^m \binom{M-1}{m} \sum_{k=0}^{m(L-1)} c_k \int_0^\infty X^k \exp\{-mX\} p_1(X)\,dX \qquad (B.8)$$

Substitution of (B.4) into (B.7) gives (after rearranging)

$$P_c(M,L) = \left\{(S\beta)^{1-L/2}/(1+\beta)\right\} \exp\left\{-S\beta/1+\beta\right\} \sum^{M-1} (-1)^m \binom{M-1}{m} \cdot$$

$$c^k \int_0^\infty X^{L/2+k} \exp\{-(X(1+m+m\beta)/(1+\beta)\} I_{L-1}\{(\frac{4S\beta X}{(1+\beta)^2})^{1/2}\}dX$$

$$(B.9)$$

Let $X = Z^2$, (B.9) becomes

$$P_c(M,L) = A \sum_{m=0}^{M-1} (-1)^m \binom{M-1}{m} \sum_{k=0}^{m(L-1)} 2c_k \int_0^\infty Z^{L+2k} \cdot$$

$$\exp\{-Z^2(1+m+m\beta)/(1+\beta)\} I_{L-1}\{(\frac{4S\beta X}{(1+\beta)^2})^{1/2}\}dZ \qquad (B.10)$$

where

$$A = \frac{(S\beta)^{1-L/2}}{(1+\beta)} \exp\left\{-S\beta/(1+\beta)\right\}$$

If we use the following result

$$\int_0^\infty \exp(-a^2x^2)x^{\mu-1} I_\nu(bx)dx = \frac{b^\nu \Gamma(\frac{\mu+\nu}{2})}{2^{\nu+1} a^{\nu+\mu} \Gamma(\nu+1)} \cdot$$

$$\exp(b^2/4a^2) F(\nu+\mu/2+1, \nu+1; -b^2/4a^2)$$

where $$F(a,c;z) = \sum_{n=0}^{\infty} \frac{(a)_n}{(c)_n} \cdot \frac{z^n}{n!}$$

$$b_n = \frac{\Gamma(b+n)}{\Gamma(b)}$$

If we use (B.11) in (B.10) and let

$$a^2 = \frac{1+m(1+\beta)}{1+\beta}$$

$$b = \frac{4S\beta}{(1+\beta)^2}$$

and

$$\mu+1 = L+2k$$

$$\nu = L-1$$

then the integration becomes

$$\int_0^{\infty} z^{\mu-1} \exp(-a^2z^2) I_{\nu}(bz)\,dz = \frac{\left\{\frac{4S\beta}{(1+\beta)^2}\right\}^{L-1} \Gamma\left(\frac{L+2k+1+L-1}{2}\right)}{2^{L-1+1}\, a^{L+2k+1+L-1}\, \Gamma(L-1+1)} \cdot$$

$$\exp\left\{\frac{\frac{4S\beta}{(1+\beta)^2}}{4\left(\frac{1+m+m\beta}{1+\beta}\right)}\right\} F\left\{\frac{L-1-L+2k-1}{2}+1, L; \frac{\frac{4S\beta}{(1+\beta)^2}}{4\left(\frac{1+m+m\beta}{1+\beta}\right)}\right\} \tag{B.11}$$

After simplifying and substituting (B.12) into (B.11) we get

$$\sum_{m=0}^{M-1}(-1)^m \binom{M-1}{m} \sum_{k=0}^{m(L-1)} c_k \frac{(S\beta)^{1-L/2}}{1+\beta} \exp\left(-\frac{S\beta}{1+\beta}\right) \frac{\Gamma(L+k)}{\Gamma(L)} \cdot$$

$$\left\{\frac{\left\{\frac{4S\beta}{(1+\beta)^2}\right\}^{L-1}}{2^{L-1}\left(\frac{1+m+m\beta}{1+\beta}\right)^{2(L+k)}}\right\} \cdot \exp\left\{\frac{-S\beta}{(1+\beta)(1+m+m\beta)}\right\} F\left(-k, L; \frac{-S\beta}{(1+\beta)(1+m+m\beta)}\right)$$

$$= \sum_{m=0}^{M-1}(-1)^m \binom{M-1}{m} \sum_{k=0}^{m(L-1)} c_k \cdot \frac{\Gamma(L+k)}{\Gamma(L)} \cdot \exp\left\{-\frac{mS\beta}{(1+\beta)(1+m+m\beta)}\right\} \cdot$$

$$\left\{\frac{(1+\beta)^k}{(1+m+m\beta)^{L+k}}\right\} F\left(-k, L; -\frac{S\beta}{(1+\beta)(1+m+m\beta)}\right) \tag{B.12}$$

Now the probability of error is obtained as

$$P_e(M-L) = 1 - P_c(M-L)$$

by letting m=0 in (B.8) we have

$$P_c(M,L)\big|_{m=0} = \int_0^\infty p_1(x)\,dx = 1$$

Thus

$$P_e(M,L) = \sum_{m=1}^{M-1}(-1)^m \binom{M-1}{m} \cdot \left\{\frac{1}{1+m+m\beta}\right\}^L \cdot \exp\left\{-\frac{mS\beta}{1+m+m\beta}\right\} \cdot$$

$$\sum_{k=0}^{m(L-1)} \frac{\Gamma(L+k)}{\Gamma(L)} \cdot \left\{\frac{1+\beta}{1+m+m\beta}\right\}^L \cdot F\left(-k, L; \frac{-S\beta}{(1+\beta)(1+m+m\beta)}\right) \tag{B.13}$$

Special cases

Let L=1, i.e. no diversity, (B.13) gives

$$P_e(M) = \sum_{m=0}^{M-1} (-1)^m \frac{\binom{M-1}{m}}{1+m+m\beta} \cdot \exp\left\{-\frac{m\gamma^2\beta}{1+m+m\beta}\right\} \qquad (B.14)$$

If we wish to represent (B.14) in term of the average SNR, we have to rewrite

$$\frac{\overline{E}_b}{N_{oJ}} = \frac{(\alpha^2+2\sigma^2)}{N_{oJ}} E_b = (1+\gamma^2)\beta$$

$$\beta = \frac{1}{1+\gamma^2} \frac{\overline{E}_b}{N_{oJ}} \qquad (B.15)$$

Substituting (B.15) into (A.14) gives back (3.31) and (3.32) with $\lambda=1$.