Coding For Frequency Hopped Spread Spectrum Satellite Communications

Annual Report for
The Period December 1, 1986 to April 15, 1987

Department of
Electrical Engineering

THE UNIVERSITY OF VICTORIA
P.O. BOX 1700, VICTORIA, B.C. CANADA V8W 2Y2

CRC-DP-CR-87-001

Coding For Frequency Hopped Spread Spectrum Satellite Communications

Annual Report for
The Period December 1, 1986 to April 15, 1987

Prepared for
The Department of Communications
under DSS Contract No. 27ST. 36001-6-3539

by

Q. Wang, T. A. Gulliver, V. K. Bhargava and W. D. Little
Department of Electrical Engineering
University of Victoria
P.O. Box 1700
Victoria, B.C.
Canada V8W 2Y2

Technical Report ECE-87-2

April 15, 1987

Abstract

Performance of various types of error correcting codes is examined under partial band noise jamming and multitone jamming using the fast frequency hopping, noncoherent M-ary frequency-shift-keying technique. Some results are compared to those previously published to ensure the reliability of the software package developed. Several errors in previously published results, some of which are not trivial, are identified and corrected.

As a prelude to implementing more complex codes, we report on the hardware implementation of the well known (24,12) extended Golay code.

Contents

1 Introduction

In defence communication systems, spread-spectrum techniques such as frequency-hopping (FH) have been utilized to provide some protection against jamming. However, an intelligent jammer can drastically reduce the effectiveness of such a system. This effectiveness can be regained through the use of error correcting codes. In this report we present the results of a comprehensive study of the performance of various error correcting codes when used in a frequency-hopping system.

1.1 Project Background and Objective

The system we are considering employs the fast frequency-hopping (FFH) noncoherent M-ary frequency-shift-keying (NCFSK) technique. Our first objective is to investigate the performance of various known error correcting codes in such a system under different kinds of jamming. Slow frequency-hopped systems with differentially coherent modulation techniques will be examined in the future.

1.1.1 System Model

The system model shown in Figure 1 is similar to that under consideration and very typical. System assumptions are as follows.

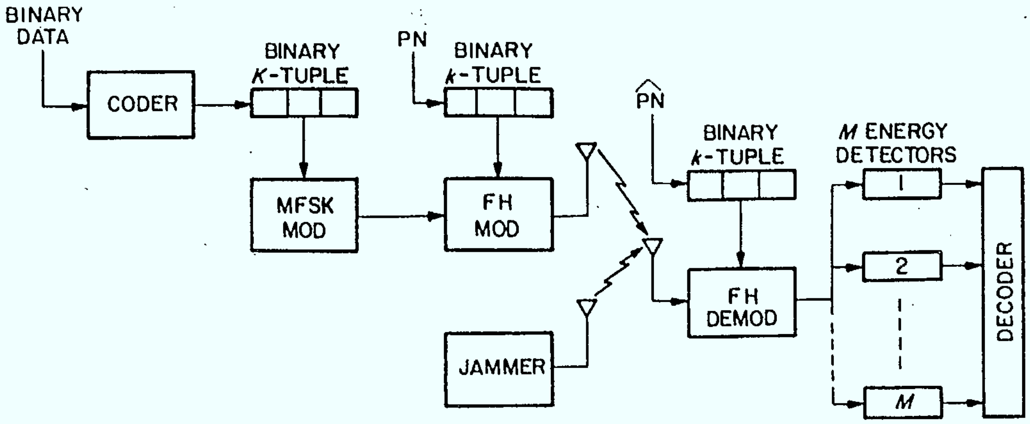

Figure 1: Block diagram of a FH/MFSK system under jamming. Transmit one of $M = 2^K$ tones; carrier is hopped to one of 2^k frequencies determined by k-chip segments of PN code; dehopping requires derived PN reference ($\widehat{\text{PN}}$); non-coherent detection.

Signalling and Detection

Transmitted signals are MFSK orthogonal signals which hop over total spread spectrum bandwith W_{ss}. Noncoherent soft energy detection (square-law reception) of each hop is assumed without quantization. In practice, this can be approximated with finite level quantization. Note that this soft decision is for energy detection. While the soft energy decision may be passed to a soft decision decoder such as that for a convolutional code, the decision made after diversity combination can be a hard decision such as that for hard decision decoding of a block code. The quantization effect of the soft decision is currently undergoing further reseach.

Diversity, Combination and Side Information

By diversity we mean transmit one coded M-ary symbol in L hops.

For a given M and an error correcting (EC) code, when the energy per symbol E_s is fixed, the energy per bit E_b is fixed. In this case, there is usually an optimum L, denoted as L_{opt}, at which the final bit error rate (BER) can be minimized for a given signal to noise ratio. This may not be true when the hop rate R_h is fixed and the information bit rate R_b is varied. However, since the objective of this study is to evaluate the effectiveness of various EC codes, we assume E_b is fixed. This will help identify effective EC codes. Of course, the actual choice of L should be determined by R_h, R_b, etc. as will be discussed shortly. In analysis, L_{opt} provides an indication of how efficient a specific code is. A smaller L_{opt} implies that the code is more efficient against jamming.

In a jamming environment, the channel is nonstationary, and side information is valuable for efficient data reception. However, a system heavily dependent on side information may not be robust, because it may not always be obtainable or its quality may vary greatly. One method used in practice to derive the side information is to implement automatic gain control (AGC) in the receiver, which may be monitored to determine whether jamming power is corrupting a given hop[1]. Based on this implementation, we may assume that the receiver knows with certainty whether each hop of an M-ary symbol is jammed or not. If any of the L hops is not jammed, an error free M-ary decision can be made (the thermal noise is neglected, this will be discussed shortly); otherwise select the largest of the linear combinations (direct sums) of the energy of L hops. Note that the assumed perfect side information is for the diversity combination.

Since the side information comes directly from measurements on the observables rather than from an external source, its reliability aspect is currently undergoing further research.

Fixed Hop Rate

Due to technology and system constraints, the hop rate R_h is usually considered to be fixed in the coding design. For FFH M-ary FSK, where $M = 2^K$, this implies

$$\frac{L}{r \times K} = \frac{R_h}{R_b} \tag{1}$$

where r is the overall error correcting code rate (dimensionless) and R_b is the information bit rate. For instance, when $R_b = 2.4kb/s$, $R_h = 20khop/s$, Equation 1 becomes

$$\frac{L}{r \times K} = 8.33. \tag{2}$$

Candidate codes should be checked against Equation 1 .

1.1.2 Types of Jamming

To reflect realistic jamming scenarios, we neglect the received thermal or non-hostile background noise in deference to the typically dominant jamming power. We consider two types of worst case (WC) intelligent but non-repeat-back jamming, namely, partial band noise and multitone interference. Assume the total jamming power J (referenced to the receiver input) is fixed. Then the effective jamming power spectral density is given by

$$J_O = J/W_{ss}.$$

Partial Band Noise Jamming

Partial band noise (PBN) jamming occurs when the total jamming power is restricted to a fraction ρ $(0 < \rho \leq 1)$ of the full spread spectrum bandwidth. It is equivalent to pulse jamming for frequency hopping systems, and in this case ρ is the fraction of time that the jamming is on.

Multitone Jamming

Multitone jamming (MT) includes band multitone jamming and independent multitone jamming. It has been shown that the worst case multitone jamming is band multitone jamming with a single jamming tone per jammed band[2]. We consider only this worst case multitone jamming and denote it as WC MT. In this case the jammer has one parameter to optimize, namely the ratio of signal power of one hop to the power of the jamming tone, denoted as α.

1.2 Fading and Uniformity

We do not consider fading of the signal due to propagation, but in worst case jamming the signal already suffers from a kind of fading. Thus results without considering propagation fading may be indicative for the case of propagation fading. This point has been verified in previous work. For instance, the broadband jammer is the worst noise jammer in a Rayleigh fading channel[3].

A satellite communication link over frequency bands presently in use can usually be viewed as a uniform channel over W_{ss}.

1.3 A Comment on Previous Work

Although performance of error correcting codes in FH systems has been widely studied, there is no single reference in the literature providing complete information on the BER performance (rather than other criteria, such as the cutoff rate) of various codes for jammed M-ary NCFSK, and hence a convincing comparison of them. Ma and Poole's paper[4] and the book by Simon et al.[3] may be the most comprehensive. Only partial band noise-jamming was considered in [4] and only Reed-Solomon codes and several convolutional codes were considered in [3]. In fact, with so many error correcting codes developed, it is impossible for anyone to give the BER performance of all these codes. Thus a software package was developed to evaluate any candidate codes. Through this work mistakes were found in some previously published results [4,3], some of which are not trivial. These are identified and corrected. The results obtained will serve as a benchmark and a guide for future research.

1.4 Evaluation Methods

For systems such as the one described above, we can consider three methods to evaluate the BER performance of a code.

1.4.1 Computer Simulation

Monte Carlo simulation is the most universal but most time consuming method to evaluate the BER. For the computing power available presently, simulation for a BER $= 10^{-5}$ is near the limit. Therefore, this brute force method is not suitable for a comprehensive preliminary investigation of codes. It may be considered to evaluate the BER performance when a code has been adopted. Since this method has the highest credibility, it is worth examining possible ways to reduce computation time.

1.4.2 Exact Computation

It is generally difficult and cumbersome to compute the exact performance of systems like that above. This is because exact performance computation is a complicated statistical process of combinatorial feature. Since these results are usually very complex, in most cases they do not yield insights as readily as the closed form expressions such as those derived from the Chernoff union bounds.

1.4.3 Chernoff Union Bound

The Chernoff union bound gives an upper bound for the BER. The computation involved in this method is usually much simpler than the other two methods. Though the general credibility of the method remains controversial, for the system of concern here it has been shown to provide useful and reliable information[3]. Due to its relative simplicity it is especially suitable for a comprehensive study of various codes, and thus has been chosen as the method to evaluate BER performance for this report. It will be seen that, for the two types of jamming under consideration, this method provides a kind of unified approach to evaluating the BER performance. This makes programming easier and provides a clear relationship between the system parameters and BER.

2 Performance Evaluation of Error Correcting Codes

In this section the formulas used to evaluate the BER performance are presented. They are based on the work reported in [3]. All of the BER performance are given under the worst case jamming. Some of the results are compared with those previously published to show the reliability of the software developed. BER performance is given vs E_b/J_O, where E_b is the energy per information bit. The signal to noise power ratio is related to E_b/J_O by

$$(S/J)_{dB} = (E_b/J_O)_{dB} - PG$$

where $PG = 10\log_{10}(W_{ss}/R_b)$ is the processing gain. For example, if $W_{ss} = 100MHz$ and $R_b = 2.4kb/s$, $PG = 46.2dB$. Note that the term processing gain has been given several conflicting definitions in the literature[3]. The definition we use is universally valid for all spread spectrum systems.

We give selected results to illustrate the BER performance of some codes. The codes chosen are those with the best performance for the most effective type of jamming, WC MT jamming or WC PBN jamming, at low BER. We only consider M-ary signalling for K up to 5.

2.1 Basic Formulas

Using the Chernoff union bound, the binary error rate P_{be} is upper-bounded by [3]

$$P_{be} \leq \begin{cases} 0.5 \times G(D^L) & \text{PBN jamming;} \\ G(D^L) & \text{MT jamming} \end{cases} \tag{3}$$

where

$$D^L = \begin{cases} e^{-L_{opt}} & L_{opt} > 1; \\ \frac{4e^{-1}}{R'E_b/J_O} & L_{opt} = 1, \quad \text{PBN;} \\ \frac{1}{R'E_b/J_O} & L_{opt} = 1, \quad \text{MT}, \quad K = 1, \quad \frac{E_b}{J_O} \geq \frac{2}{R'}; \\ \frac{1}{2} & L_{opt} = 1, \quad \text{MT}, \quad K = 1, \quad \frac{E_b}{J_O} < \frac{2}{R'}; \\ \frac{\beta K}{R' \frac{E_b}{J_O}} & L_{opt} = 1, \quad \text{MT}, \quad K \geq 2, \quad \frac{E_b}{J_O} \geq \frac{\alpha_0 M}{R'}; \\ \frac{1}{R' \frac{E_b}{J_O}} \left[\frac{\alpha_{wc}(M-2)}{1-\alpha_{wc}} \right]^{1-\alpha_{wc}} & L_{opt} = 1, \quad \text{MT}, \quad K \geq 2, \quad \frac{E_b}{J_O} > \frac{\alpha_0 M}{R'} \end{cases} \tag{4}$$

where R' is the overall code rate including M-ary signalling but excluding diversity and α_{wc} is the worst case α in MT jamming given by

$$\alpha_{wc} = \begin{cases} \alpha_0 & E_b/J_O \geq (L_{opt}\alpha_0 M)/R'; \\ \frac{R'E_b/J_O}{ML_{opt}} & E_b/J_O < (L_{opt}\alpha_0 M)/R' \end{cases} \tag{5}$$

with α_0 given in Table 1, where "1_-" means a value less than but infinitely close to 1. The function $G(D^L)$ in Equation 3 varies for different codes and will be given in the following sections. The worst case ρ, denoted as ρ_{wc}, is given by

$$\rho_{wc} = \begin{cases} \frac{3L_{opt}}{R' E_b/J_O} & E_b/J_O \geq 3L_{opt}/R'. \\ 1 & E_b/J_O < 3L_{opt}/R'. \end{cases} \tag{6}$$

L_{opt} is given by

$$L_{opt} = \begin{cases} \frac{R'}{\gamma}\frac{E_b}{J_O} & E_b/J_O \geq \gamma/R'; \\ 1 & E_b/J_O < \gamma/R'; \end{cases} \tag{7}$$

where γ is given by

$$\gamma = \begin{cases} 4 & \text{worst case PBN jamming;} \\ \beta Ke & \text{worst case MT jamming} \end{cases} \tag{8}$$

and β is given in Table 1. L_{opt} in Equation 7 can be a noninteger which is not realizable.For the purpose of analysis, however, L_{opt} is informative in this finer form, and so is used for evaluation of BER performance of all EC codes in this report. Note that we distinguish P_{be} from the final BER, denoted as P_b. The reason for this distinction is that we are trying to take into account different kinds of codes in a unified approach. In some cases P_b is equal to P_{be}, but not always, as will be shown. In the following sections we will use these formulas for three kinds of codes: block codes, convolutional codes and concatenated codes.

Table 1: Value of α_0 and β

K	α_0	β
1	1	1
2	0.683	0.7945
3	0.527	0.8188
4	0.427	0.9583
5	0.356	1.2204

2.2 Convolutional Codes

For convolutional codes,

$$P_b = P_{be}$$

and

$$R' = r \times K$$

where r is the dimensionless error correcting code rate. $G(D)$ is determined by the code used. Soft decision Viterbi decoding is assumed for all convolutional codes.

2.2.1 Odenwalder Binary Codes

Two commonly used binary convolutional codes are the constraint length 7, rate 1/2 and 1/3 codes discovered by Odenwalder[5]. For a binary code, $K = 1$. For $r = 1/2$,

$$\begin{aligned} G(D) &= 36D^{10} + 211D^{12} + 1404D^{14} + 11,633D^{16} \\ &\quad + 77,433D^{18} + 502,690D^{20} + 3,322,763D^{22} \end{aligned}$$

$$+21,292,910D^{24} + 134,365,911D^{26} + \cdots \tag{9}$$

and for $r = 1/3$,

$$G(D) = D^{14} + 20D^{16} + 53D^{18} + 184D^{20} + \cdots. \tag{10}$$

Rate 1/4 and 1/8 codes can be derived from the above rate 1/2 code, having the same constraint length 7 [4]. For $r = 1/4$,

$$\begin{aligned} G(D) &= 36D^{20} + 211D^{24} + 1404D^{28} + 11,633D^{32} \\ &\quad +77,433D^{36} + 502,690D^{40} + 3,322,763D^{44} \\ &\quad +21,292,910D^{48} + 134,365,911D^{52} + \cdots \end{aligned} \tag{11}$$

and for $r = 1/8$,

$$\begin{aligned} G(D) &= 36D^{40} + 211D^{48} + 1404D^{56} + 11,633D^{64} \\ &\quad +77,433D^{72} + 502,690D^{80} + 3,322,763D^{88} \\ &\quad +21,292,910D^{96} + 134,365,911D^{104} + \cdots. \end{aligned} \tag{12}$$

For these codes, the $r = 1/3$ code performs best. The BER performance of this code is shown in Figure 2. The curve for PBN jamming in Figure 2 is different from the corresponding curve in [3,4] for a BER larger than 10^{-2}. The reason being that a more accurate expression for $G(D)$ has been used, thus our result is more accurate.

The BER performance of the rate 1/2, 1/4 and 1/8 codes under

PBN jamming is shown in Figure 3. In [4], these three curves are the same as that for the rate 1/2 code. This is incorrect, since in that case, for rate 1/4 and 1/8 codes, L_{opt} would be smaller than 1 for a BER larger than 10^{-6}, which is not realizable.

The BER performance of rate 1/2 and 1/4 codes under MT jamming is shown in Figure 4. Note that for the rate 1/4 code, the BER is a constant smaller than 10^{-4} for E_b/J_O up to 9 dB. Similarly, for the rate 1/8 code, the BER for E_b/J_O up to 12 dB is 3.4×10^{-11}. This can also be observed in Figure 2 for the WC MT jamming. Corresponding to these constants, the raw bit error rate before decoding is 1/2. This shows the power of low rate codes in tolerating a large raw error probability.

2.2.2 Trumpis Codes

Trumpis[6] has found two optimum constraint length 7 convolutional codes. Actually these codes are $(K, 1, 7)$ binary convolutional codes, but K bits at the output of the encoder, corresponding to 1 bit at the input, are considered to be one M-ary symbol. One of the two codes is the 4-ary, rate $r = 1/2$ code for which $K = 2$ and

$$G(D) = 7D^7 + 39D^8 + 104D^9 + 352D^{10} + 1187D^{11} + \cdots. \qquad (13)$$

The other is the 8-ary, rate $r = 1/3$ code. In this case we have $K = 3$ and

$$G(D) = D^7 + 4D^8 + 8D^9 + 49D^{10} + 92D^{11} + \cdots. \qquad (14)$$

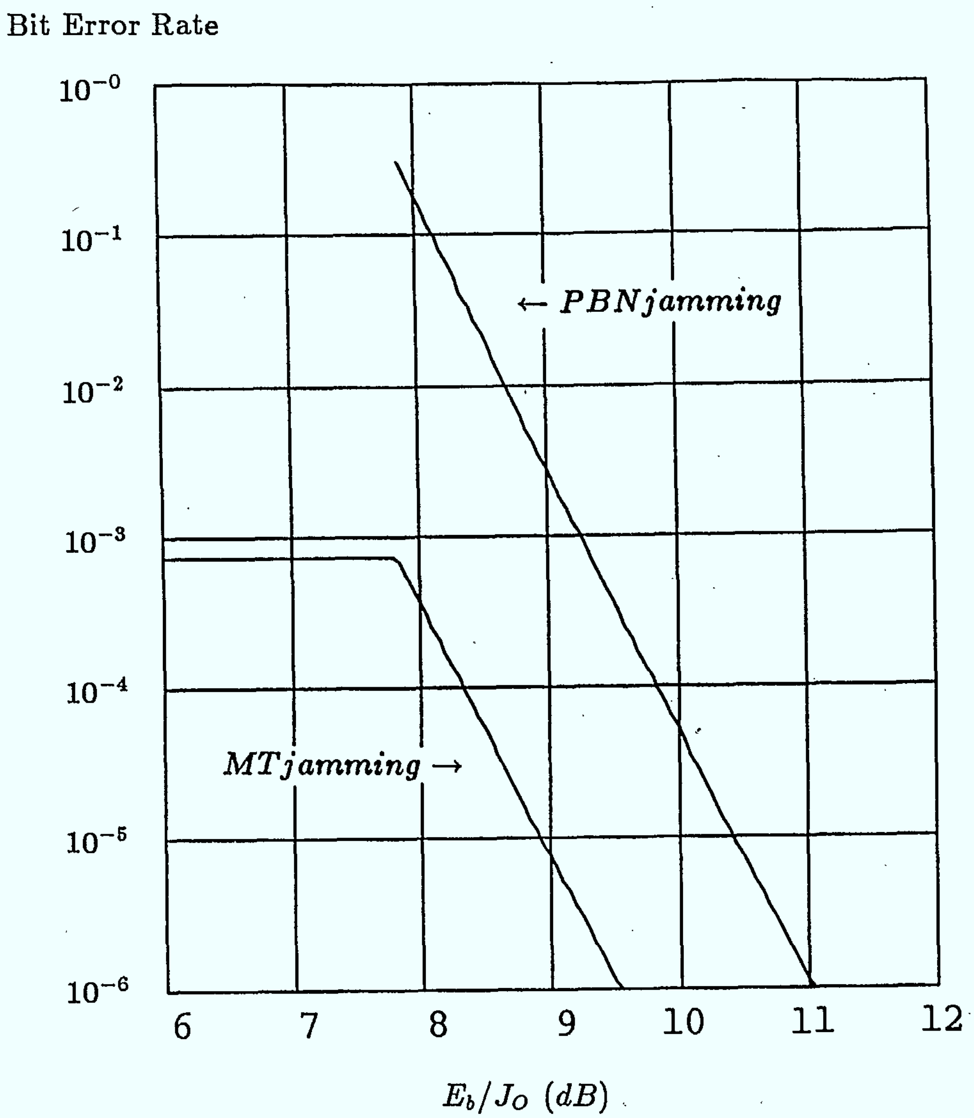

Figure 2: BER performance of the binary Odenwalder convolutional rate 1/3 code, constraint length is 7. At 10^{-5}, $\rho_{wc} = 0.815$ for the WC PBN jamming, and $\alpha_{wc} = 1_{-}$ for the WC MT jamming.

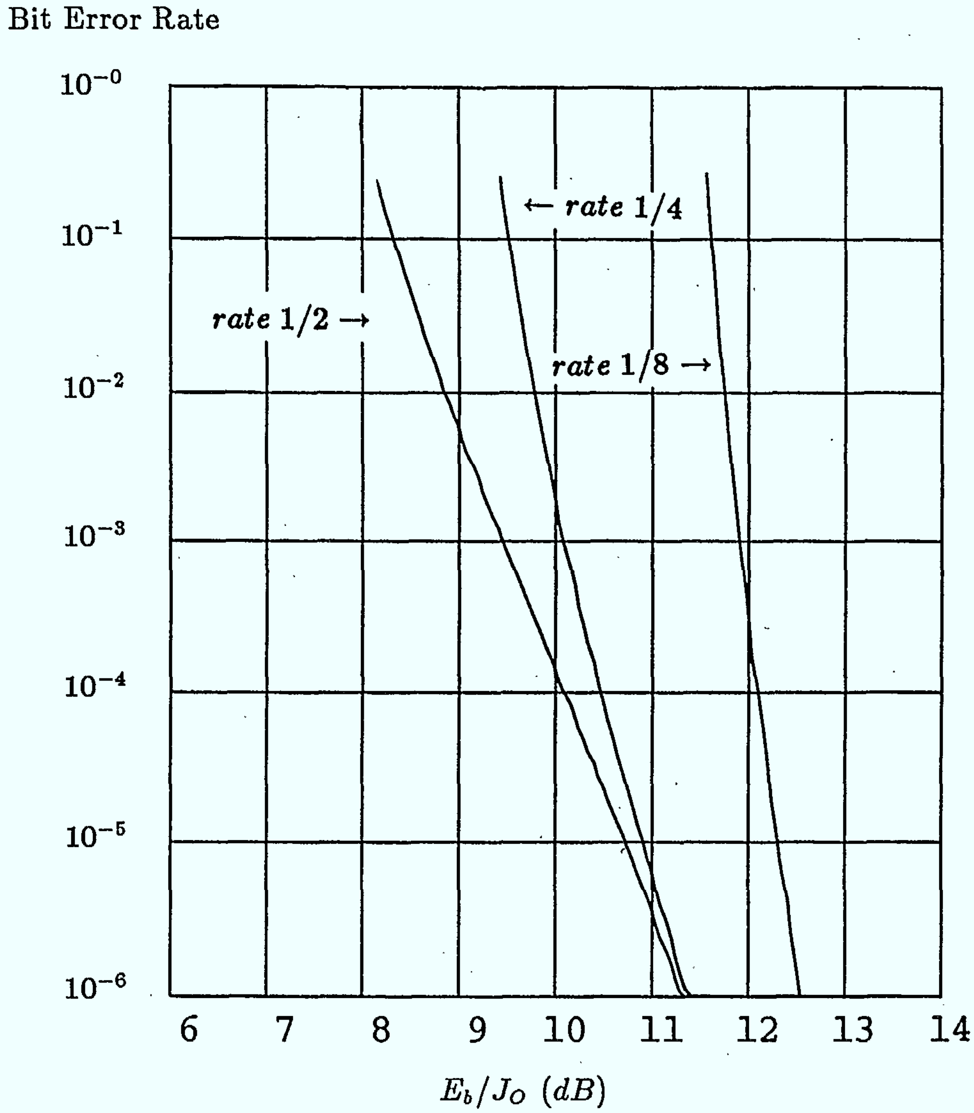

Figure 3: BER performance of the binary Odenwalder convolutional rate 1/2 , 1/4 and 1/8 codes under PBN jamming, constraint length is 7. At 10^{-5}, $\rho_{wc} = 0.75$ for the rate 1/2 code; $\rho_{wc} = 0.975$ for the rate 1/4 code; $\rho_{wc} = 1$ for the rate 1/8 code.

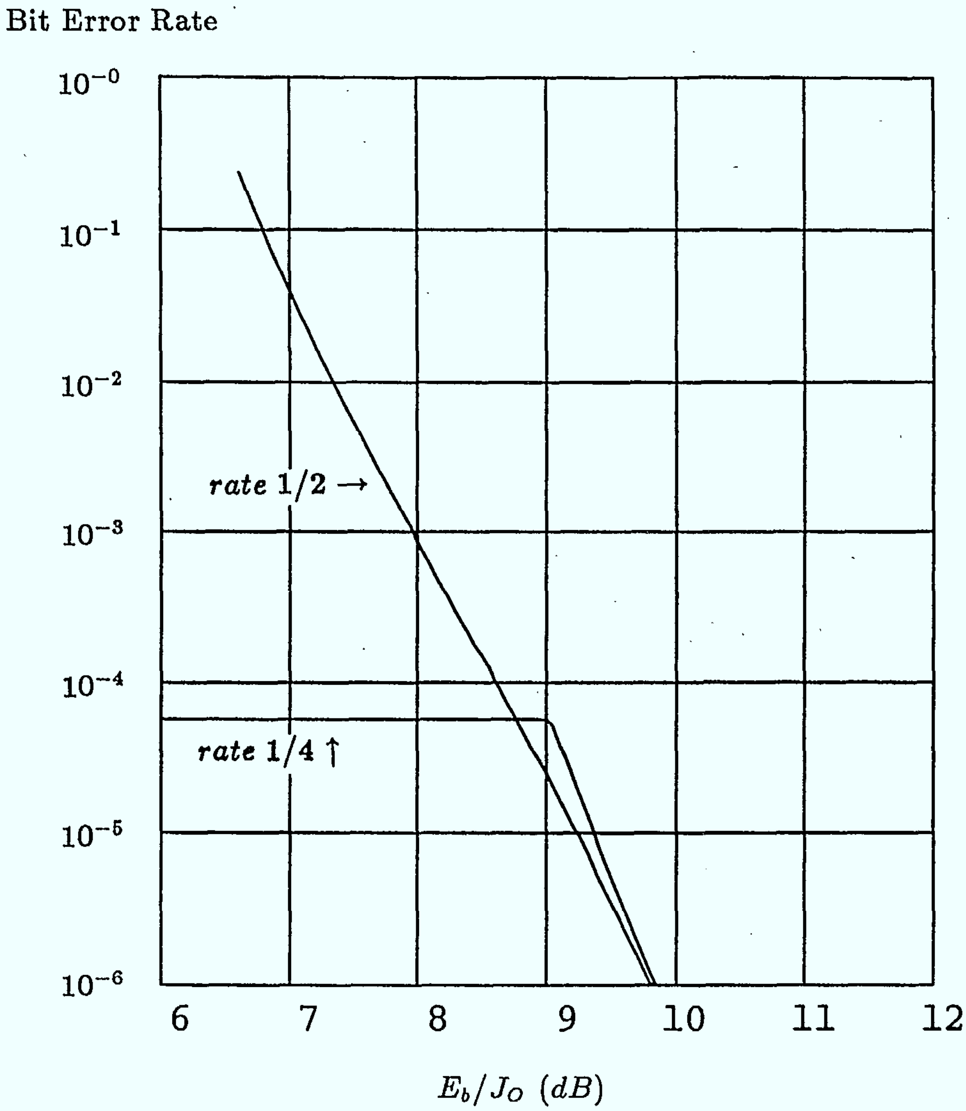

Figure 4: BER performance of the binary Odenwalder convolutional rate 1/2 and 1/4 codes under MT jamming, constraint length is 7. At 10^{-5}, $\alpha_{wc} = 1\_$ for both rate 1/2 and rate 1/4 codes.

Our results for these codes are the same as those in [3].

2.2.3 M-ary Orthogonal Convolutional Codes

M-ary orthogonal convolutional codes are a class of codes of constraint length K, hence $K \geq 2$ [7,1]. In fact, they are $(M, 1, K)$ binary convolutional codes subject to the constraint that each M-bit at the output of the encoder corresponding to 1 bit at the input is one of M orthogonal binary sequences of dimension M. Thus one such M-bit corresponds to one M-ary symbol. In this case, R' is always equal to 1 and we have

$$G(D) = \frac{D^K(1-D)^2}{(1-2D+D^2)^2}. \tag{15}$$

Note that the corresponding formula in [3] is incorrect.

The best code in this class is that for $K = 2$ with BER performance as shown in Figure 5. This class of codes is very weak in matching the M-ary channel by direct use.

2.2.4 Dual-K Convolutional Codes

For all values of K, we have the class of dual-K M-ary convolutional codes with code rate $r = 1/\nu$ over $GF(2^K)$[1,3]. That is, for every M-ary (K-bit) input word, ν M-ary code symbols are generated, where ν is an integer greater than 1. The constraint length is $2K$ which accounts for two

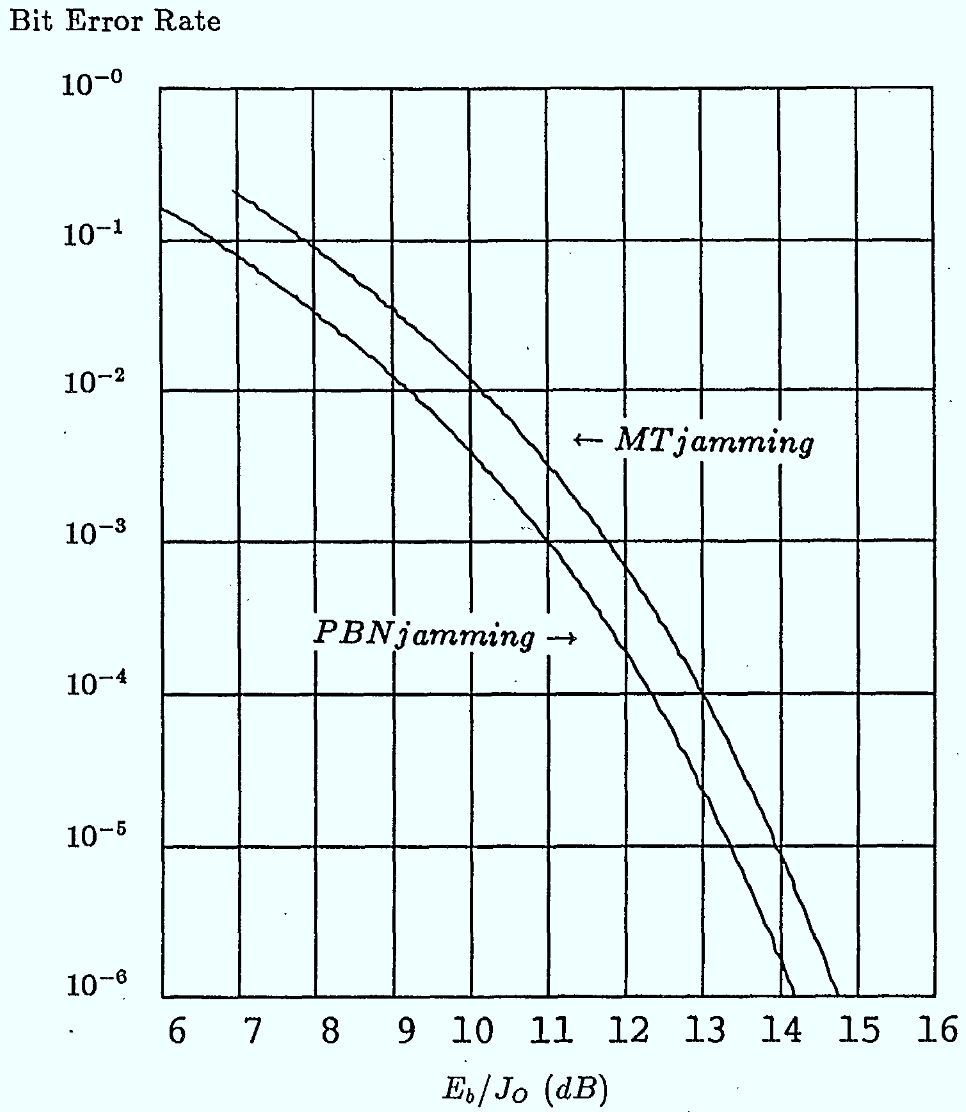

Figure 5: BER performance of 4-ary orthogonal convolutional code. Constraint length is 2. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 0.683$ for the WC MT jamming.

K-stage binary shift registers in the encoder. Now $R' = K/\nu$ and

$$G(D) = \frac{MD^{2\nu}}{2[1 - \nu D^{\nu-1} - (M - \nu - 1)D^{\nu}]^2}. \tag{16}$$

As pointed out in [3], for low BER, the performance of these codes does not depend on ν. The best code is that for $K = 2$. The BER performance of this code is shown in Figure 6 for rate 1/2, which is the same as that shown in [3].

2.2.5 Semi-orthogonal Convolutional Codes

For $K \geq 3$, we have the class of semi-orthogonal M-ary convolutional codes with constraint length $2K + 1$[1,4]. As for the orthogonal convolutional codes, R' is always equal to 1 for the semi-orthogonal convolutional codes. $G(D)$ is give by

$$G(D) \approx D^{2K+1}. \tag{17}$$

The best code in this class is that for $K = 3$. The BER performance of this code is shown in Figure 7.

2.3 Block Codes

If we use an (n, k) Q-ary block code, the final BER for a Q-ary symbol error rate P_s is given by[8]

$$P_b = \frac{Q}{2(Q-1)} P_s. \tag{18}$$

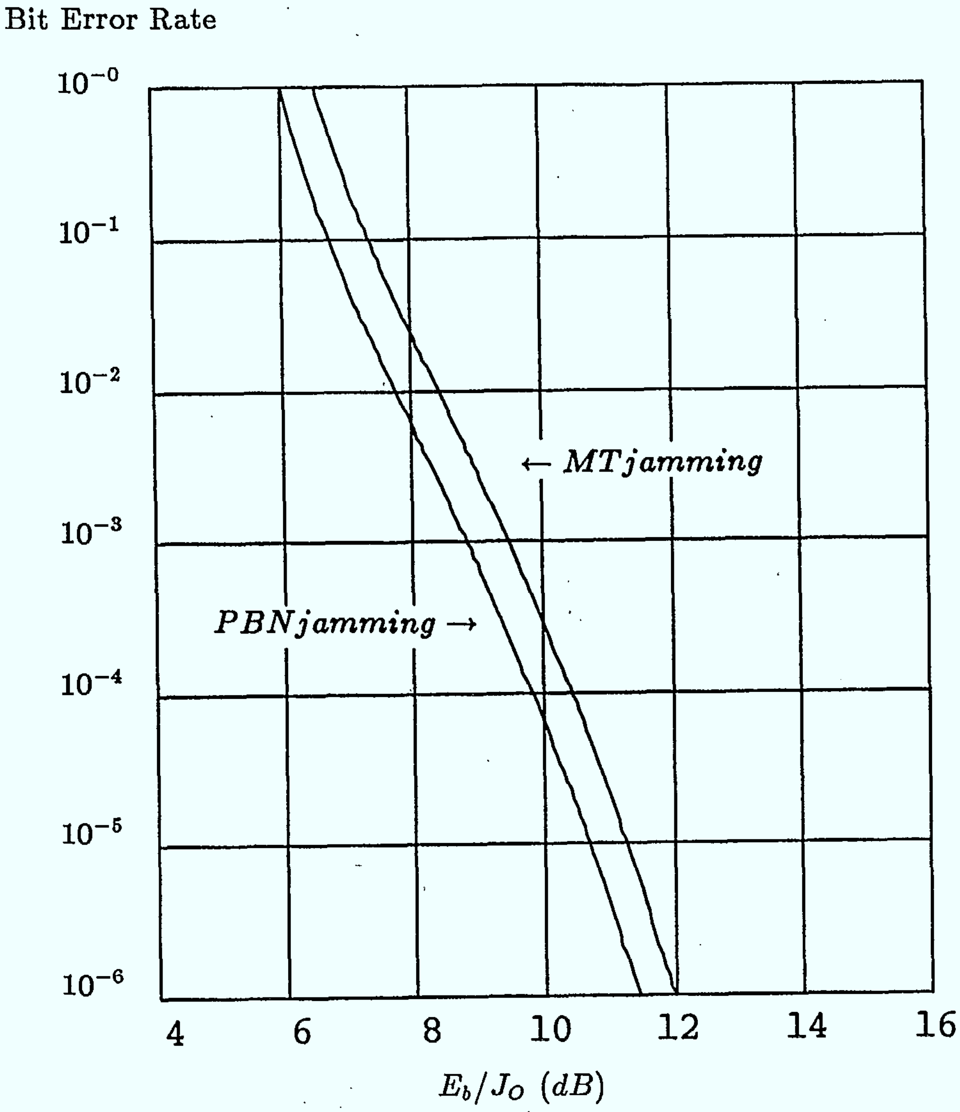

Figure 6: BER performance of the dual-2 rate 1/2 4-ary convolutional code. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 0.683$ for the WC MT jamming.

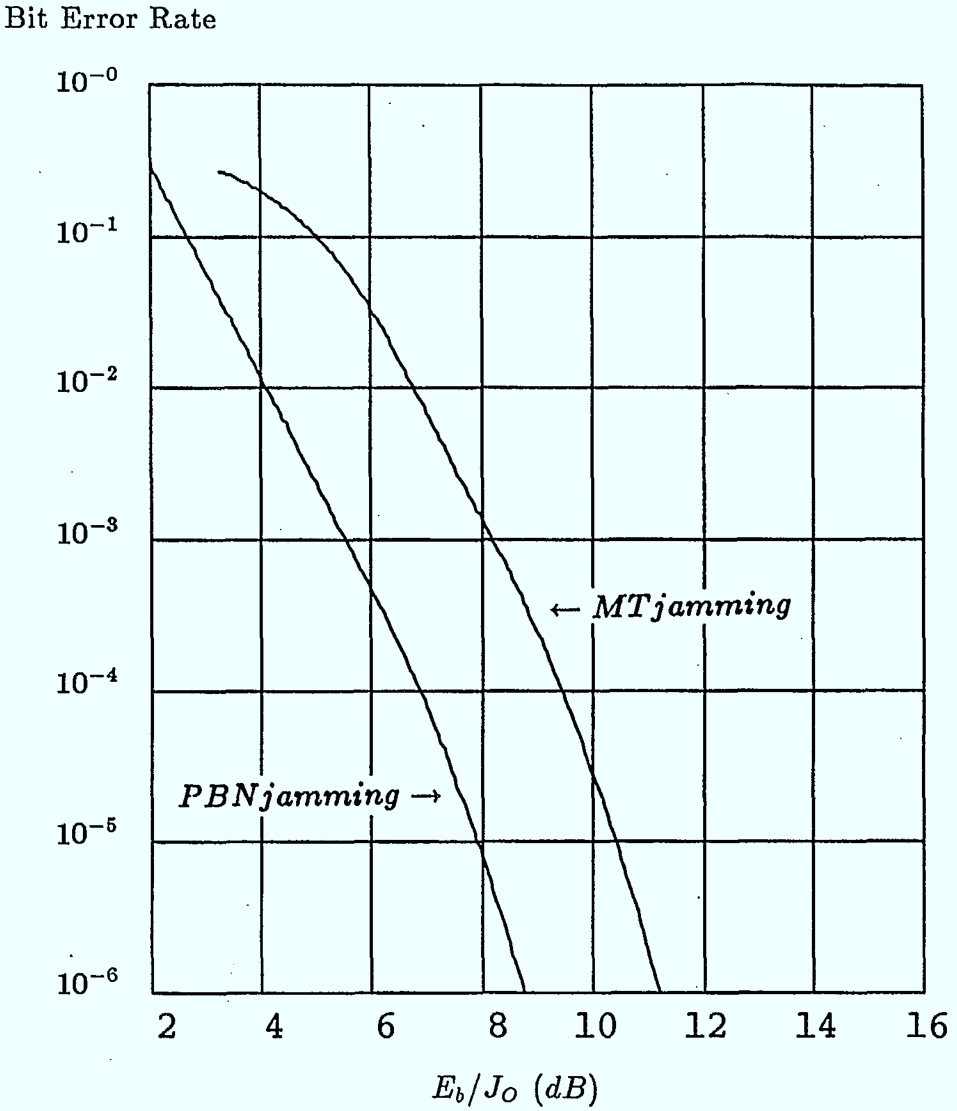

Figure 7: BER performance of the semi-orthogonal 8-ary convolutional code. Constraint length is 7. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 0.527$ for the WC MT jamming.

For an (n,k) Q-ary block code with minimum distance d, let

$$t = [(d-1)/2]$$

where [x] denotes the integer part of x. With bounded-distance (hard decision) decoding, P_s is related to the Q-ary symbol error rate before decoding P_Q by the well known formula (e.g see [4])

$$P_s \approx \frac{1}{n} \sum_{i=t+1}^{n} i \binom{n}{i} P_Q^i (1-P_Q)^{n-i}. \tag{19}$$

For M-ary signalling, let P_K be the K-bit symbol error rate during transmission (referenced to the point after diversity combination). Denote the relation between P_Q and P_K by

$$P_Q = 1 - (1-P_K)^C. \tag{20}$$

where C is a positive integer (the meaning of C will be discussed later). P_K is related to P_{be} in Equation 3 by

$$P_{be} = \frac{M}{2(M-1)} P_K \tag{21}$$

for

$$G(D) = \frac{M}{2} D. \tag{22}$$

2.3.1 Binary Codes

For binary (n,k) block codes, we have $K=1$, $M=Q=2$, $C=1$ and $R' = k/n$.

Hamming Codes

We examined the (7,4) and (31,26) Hamming codes which are single error correcting with minimum distance $d = 3$.

Golay Code

We examined the perfect (23,12) Golay code which is triple error correcting with minimum distance $d = 7$.

BCH Codes

We examined multi-error correcting BCH codes of length $n = 127$ and $n = 255$. For $n = 127$, these are (127,36) with $d = 31$, (127,64) with $d = 21$, (127,92) with $d = 11$, (127,99) with $d = 9$, (127,106) with $d = 7$ and (127,113) with $d = 5$. For $n = 255$, these are (255,71) with $d = 59$, (255,131) with $d = 27$ and (255,179) with $d = 21$.

Summary of Results

The best binary block code up to length 127 of those listed above is the (127,92) BCH code. The BER performance of this code is shown in Figure 8. The best of the length 255 BCH codes listed above is the (255,179) code. The BER performance of this code is shown in Figure 9.

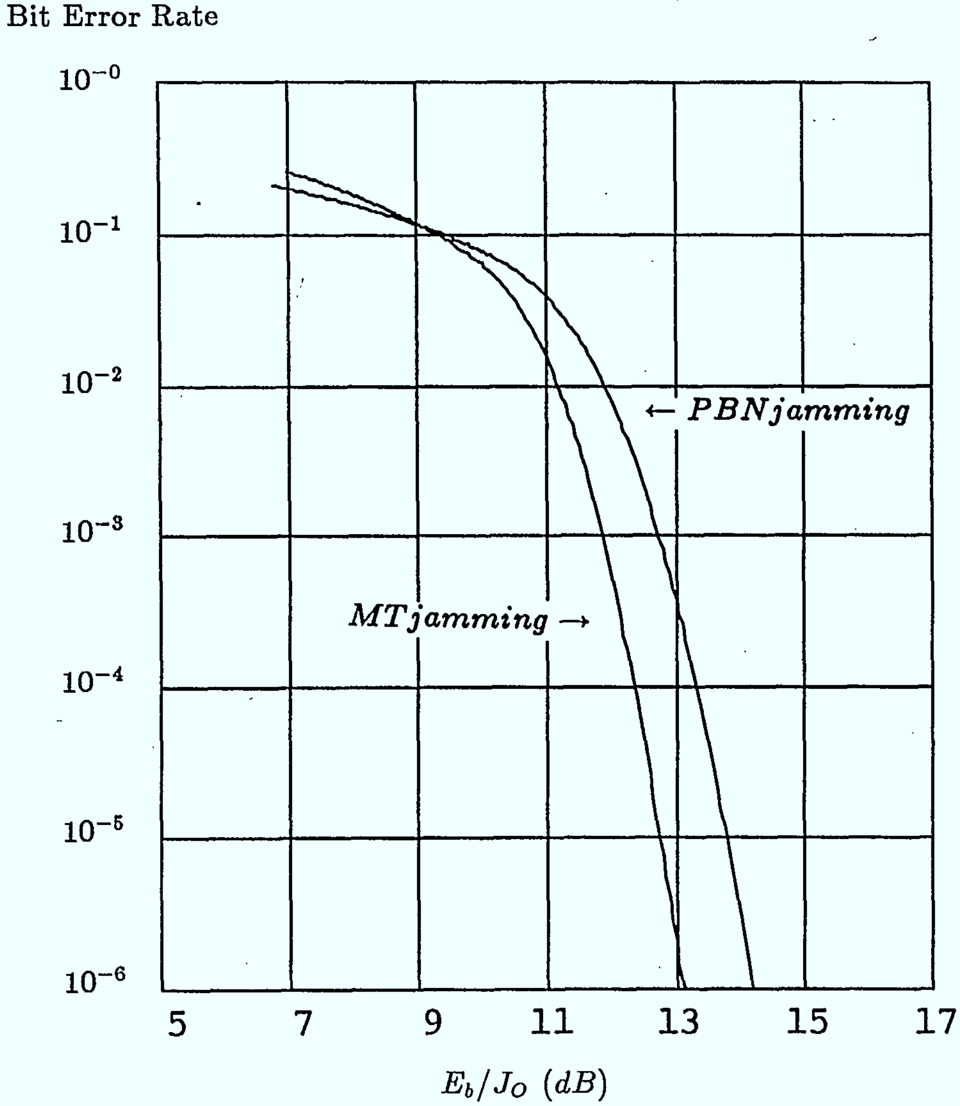

Figure 8: BER performance of the (127,92) BCH code. The minimum distance d is 11. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 1$ for the WC MT jamming.

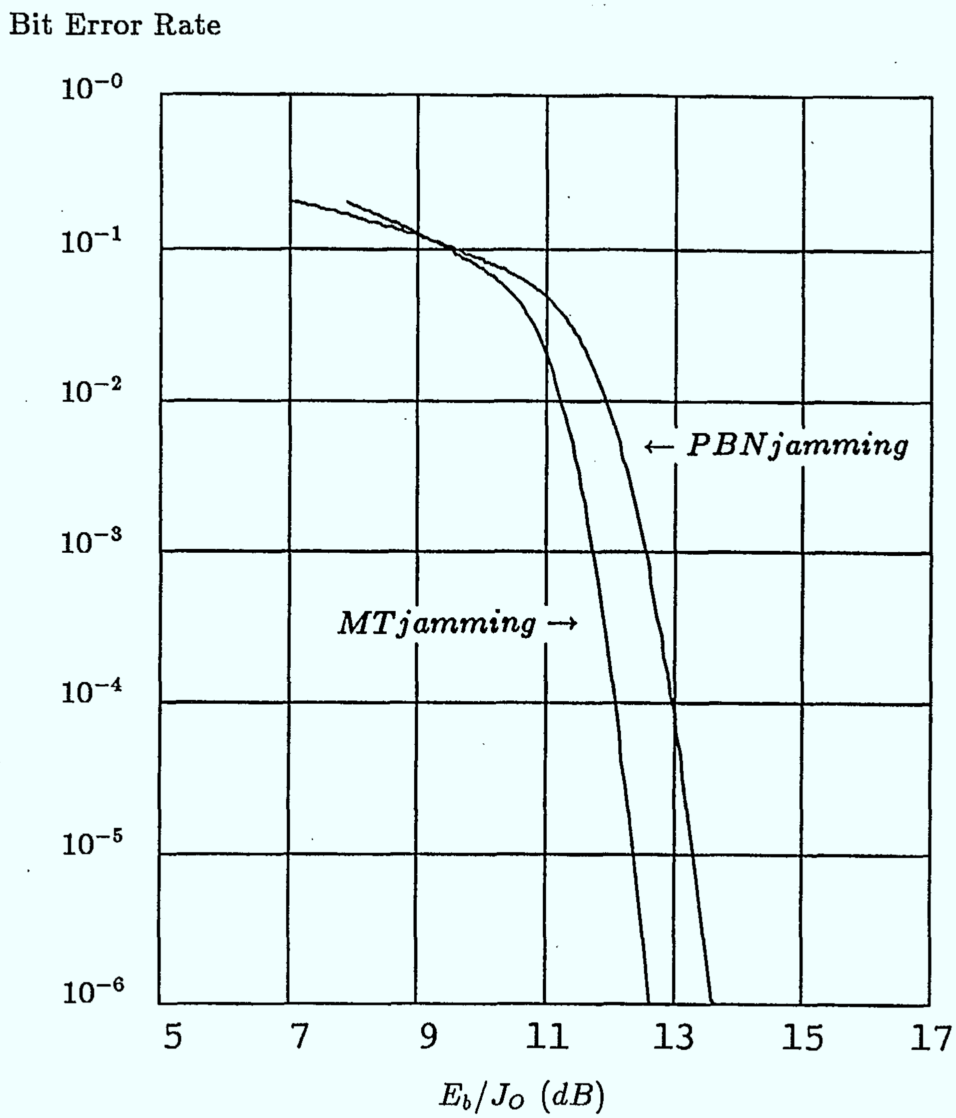

Figure 9: BER performance of the (255,179) BCH code. The minimum distance d is 21. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 1_{-}$ for the WC MT jamming.

2.3.2 Reed-Solomon Codes

Length $n = Q - 1$ Reed-Solomon (RS) codes are Q-ary codes over $GF(Q)$. For (n, k) RS codes, $d = n - k + 1$. Since RS codes meet the Singleton bound, they are called maximum-distance codes[9]. There are two different ways to use these codes in conjunction with M-ary signalling. In both cases, $R' = \frac{k}{n}K$.

Direct Use

By direct use we mean to transmit the symbol of (n,k) RS codes over $GF(Q)$ directly over M-ary channel. In this case, $Q = M$, $K \geq 2$ and $C = 1$. We examined the (7,3) code with $K = 3$, the (15,9) and (15,7) codes with $K = 4$ and the (31,15) code with $K = 5$.

Alphabet Conversion

To get a larger minimum distance for RS codes of a fixed rate, the code length must be increased. In turn the size of the alphabet over which a RS code is defined must be increased too. In this case, $Q > M$. Thus alphabet conversion is required. For practical ease, a Q-ary symbol may be composed of, say C, M-ary symbols, where C is an integer larger than 1. It is clear that no conversion is a special case with C equal to 1. Now we have

$$C = \log_2 Q/K.$$

Note that for small P_K, $P_Q \approx CP_K$. This means that there is a multiplication in the error probability by a factor C during the alphabet conversion.

For $K = 1$, we examined (31,15), (63,31), (127,63), (255,191), (511,447) and (1023,959) codes which correspond to C from 5 to 10. For $K = 2$, we examined (15,7), (63,31), (255,191) and (1023,959) codes which correspond to C from 2 to 5. For $K = 3$, we examined (63,31) and (511,447) codes which correspond to C equal to 2 and 3. For $K = 4$, we examined the (255,191) code which corresponds to C equal to 2. For $K = 5$, we examined the (1023,959) code which corresponds to C equal to 2.

Summary of Results

The best RS code of those investigated is the (255,191), $K = 2$, $C = 2$ code; followed by the (1023,959), $K = 2$, $C = 5$ code; and the (511,447), $K = 3$, $C = 3$ code. Their BER performance is shown in Figures 10 - 12.

2.4 Concatenated Codes

It is well known that concatenation of a RS outer code with some inner code can form a very powerful error correcting code. We suppose that an (n,k) Q-ary RS code is used as the outer code and a convolutional code or a block code is used as the inner code. Whenever necessary, interleaving is assumed between the inner code and the outer code so that the input

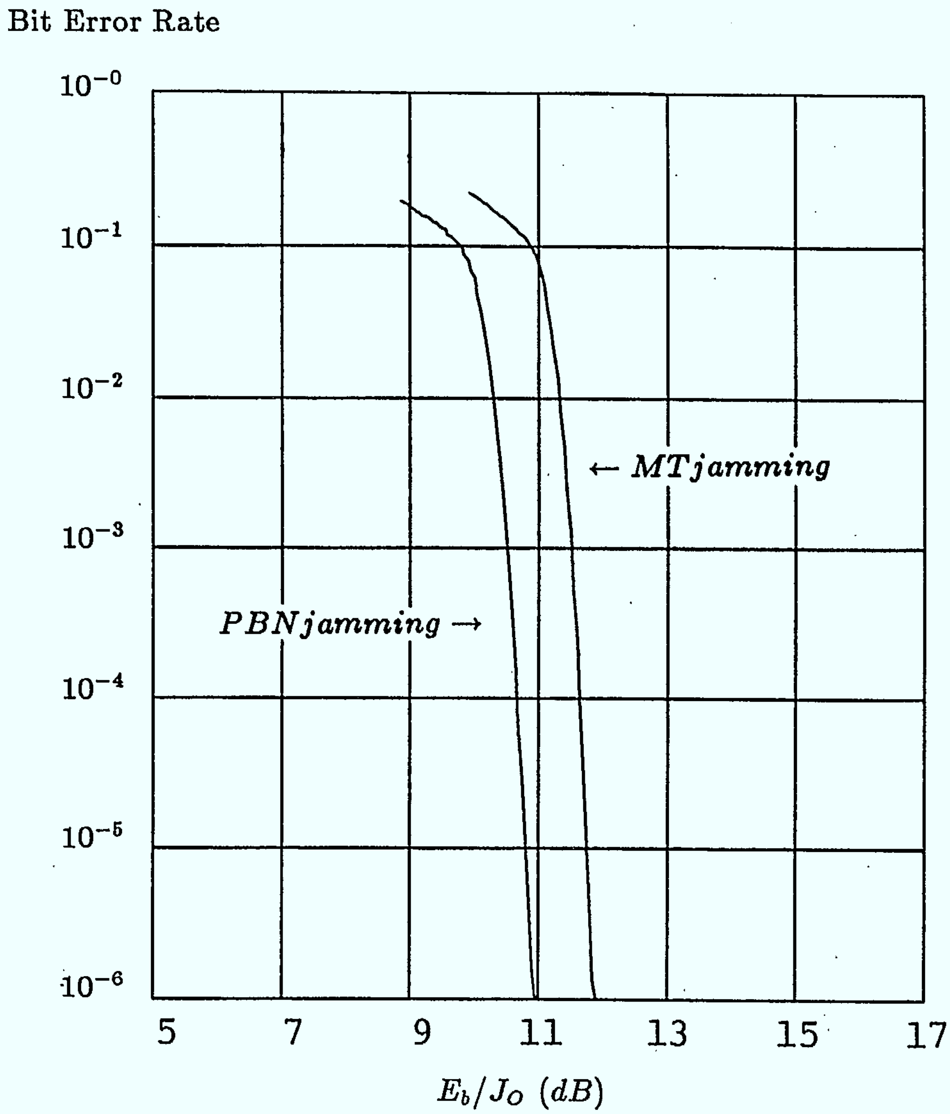

Figure 10: BER performance of the (255,191) RS code when $K = 2$ and $C = 4$. The minimum distance d is 65. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 0.683$ for the WC MT jamming.

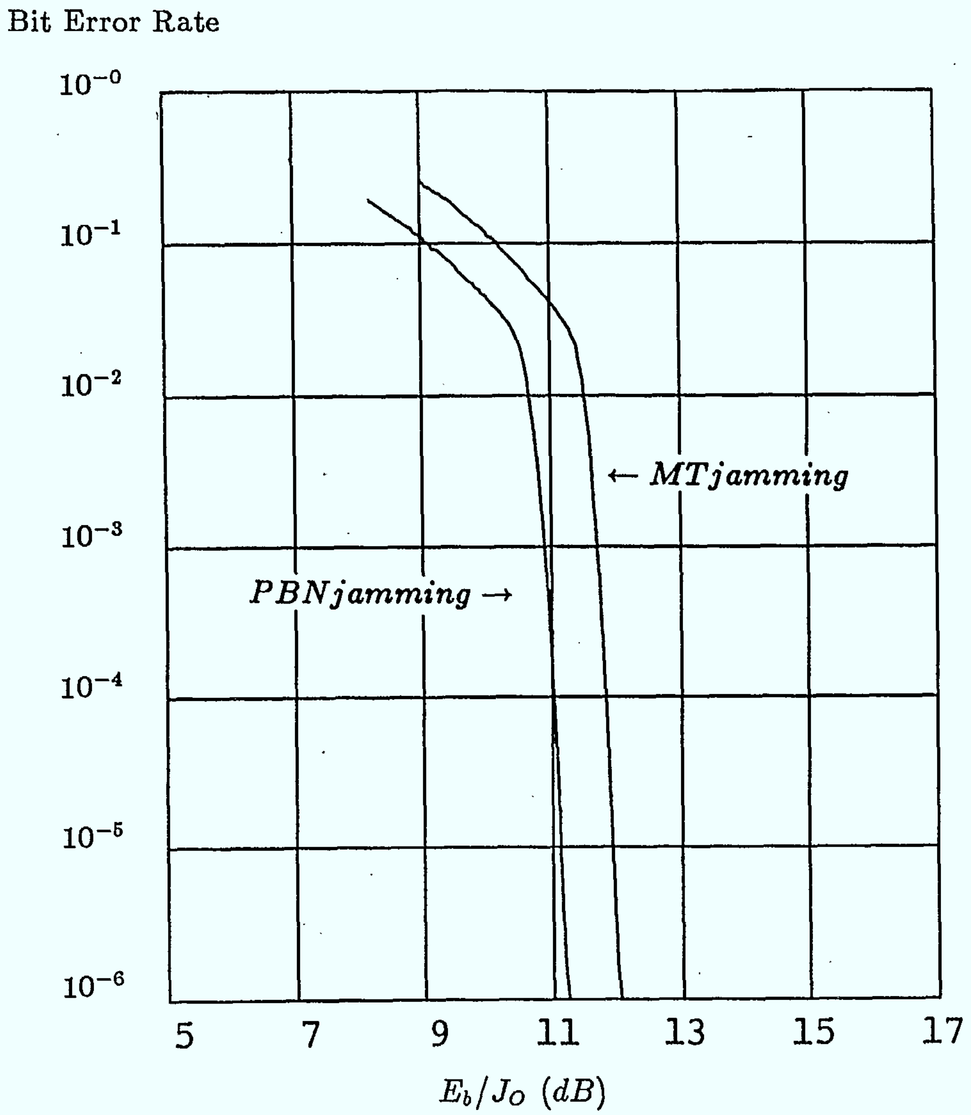

Figure 11: BER performance of the (1023,959) RS code when $K = 2$ and $C = 5$. The minimum distance d is 65. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 0.683$ for the WC MT jamming.

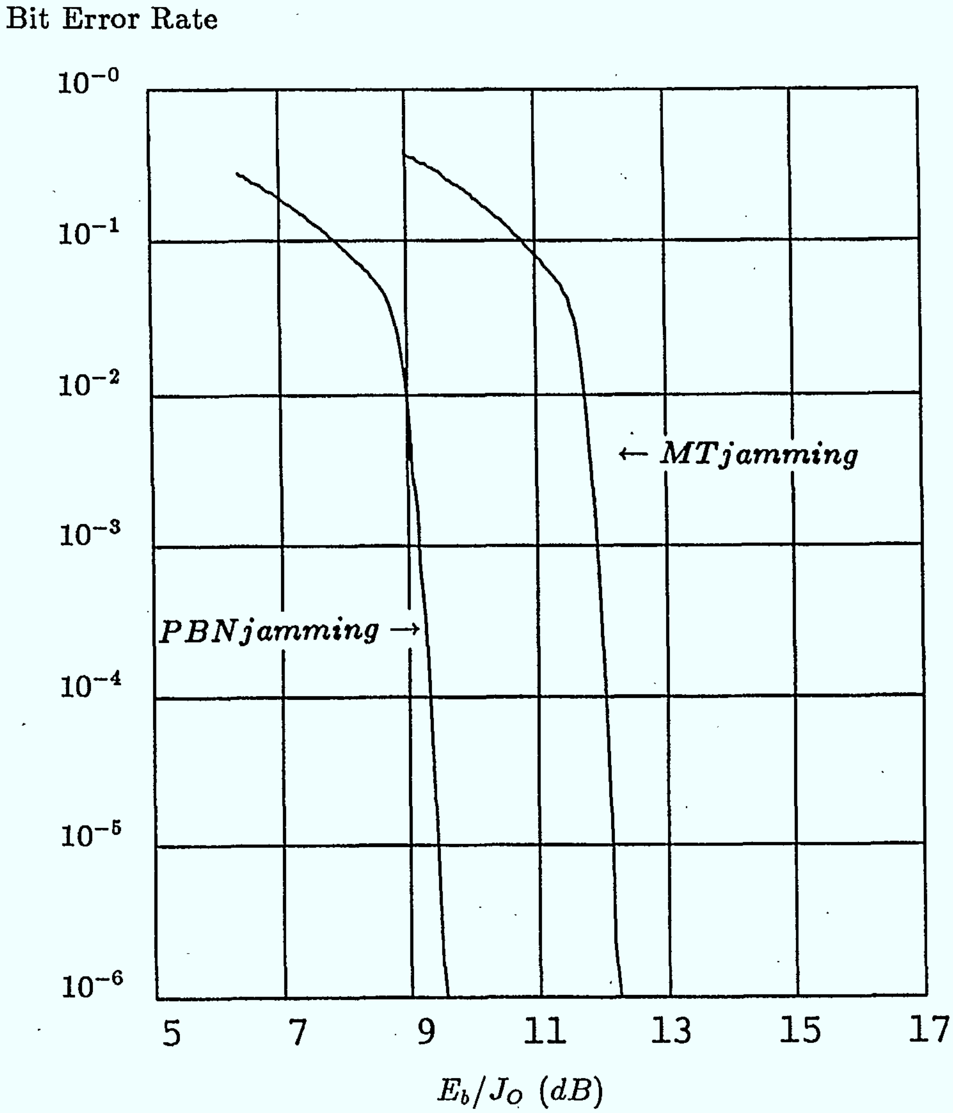

Figure 12: BER performance of the (511,447) RS code when $K = 3$ and $C = 3$. The minimum distance d is 65. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 0.527$ for the WC MT jamming.

to the outer RS decoder appears to have memoryless Q-ary symbol errors. Now $R' = \frac{k}{n} r_i K$, where r_i is the inner code rate (dimensionless). We observe that there is a threshold effect in the BER performance of all concatenated codes, that is, when E_b/J_O approaches the threshold from above, the BER increases rapidly and when E_b/J_O approaches the threshold from below, the BER decreases rapidly. This sensitivity should be taken into account in the design of a system. Based on the concept of the " super channel ", this threshold should exist even when the system thermal noise is considered.

2.4.1 Convolutional Inner Codes

We can evaluate the final BER performance of a RS code concatenated with a convolutional inner code by evaluating the BER performance of the outer RS code using formulas developed above for block codes, with the exception that $G(D)$ in Equation 22 is replaced by $G(D)$ of the inner convolutional code given in Section 2.2, where C is explained as follows. Due to the assumption of soft decision decoding of convolutional codes, we only consider convolutional codes in direct use with M-ary signalling, thus there is no alphabet conversion between them. For the same reason discussed in Section 2.3.2, there may be an alphabet conversion between the outer and inner codes, that is C inner code symbols form an outer code symbol.

Dual-K Convolutional Inner Codes

We considered dual-K rate 1/2 convolutional codes as inner codes. For $K = 1$, we examined the (255,191), (511,447) and (1023,959) RS codes as outer codes which correspond to C from 8 to 10. For $K = 2$, we examined the (15,7), (63,31), (255,191) and (1023,959) RS codes as outer codes which correspond to C from 2 to 5. For $K = 3$, we examined the (7,3), (63,31) and (511,447) RS codes as outer codes which correspond to C from 1 to 3. For $K = 4$, we examined the (15,7) and (255,191) RS codes as outer codes which correspond to C equal to 1 and 2. For $K = 5$, we examined the (31,15) and (1023,959) RS codes as outer codes which correspond to C equal to 1 and 2.

For these codes, the code with the (1023,959) RS outer code and dual-2 inner code for $C = 5$ has the best performance. The BER performance of the code is shown in Figure 13.

Odenwalder Binary Convolutional Inner Codes

We considered the rate 1/2 Odenwalder binary convolutional code as the inner code, so that $K = 1$. We examined the (31,15), (63,31), (127,63), (255,191), (511,447) and (1023,959) RS codes as outer codes which correspond to C from 5 to 10.

For these codes, the code with (1023,959) RS outer code for $C = 10$ and the code with (511,447) RS outer code for $C = 9$ showed the best

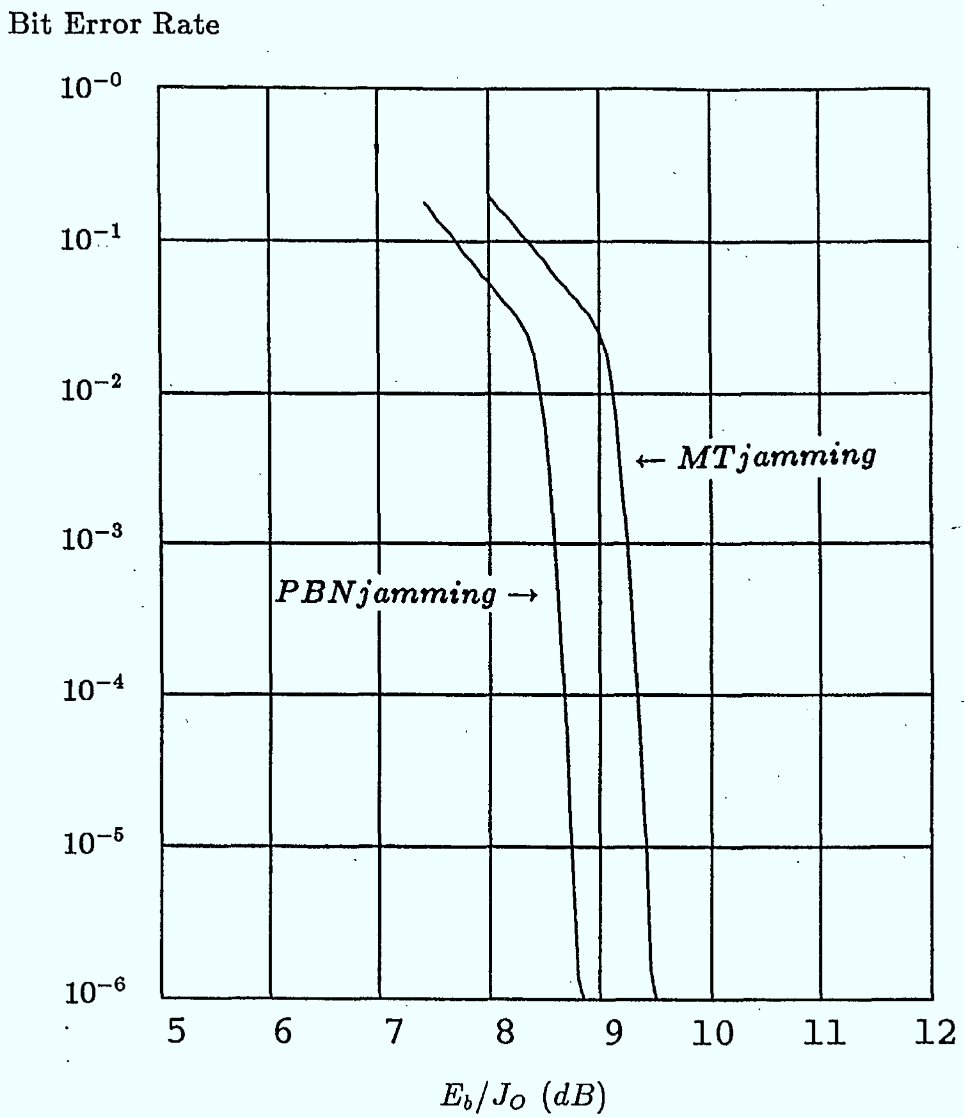

Figure 13: BER performance of the concatenated code with (1023,959) RS outer code and dual-2 rate 1/2 convolutional inner code. $C = 5$. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 0.683$ for the WC MT jamming.

performance. The BER performance of these codes is shown in Figures 14 and 15.

Trumpis Convolutional Inner Codes

We considered Trumpis 4-ary and 8-ary convolutional codes as inner codes. For $K = 2$, we examined the (15,7), (63,31), (255,191) and (1023,959) RS codes as outer codes which correspond to C from 2 to 5. For $K = 3$, we examined the (7,3), (63,31) and (511,447) RS codes as outer codes which correspond to C from 1 to 3.

For these codes, the code with (1023,959) RS outer code for $C = 5$ performed best. In fact, this code outperforms all codes considered thus far, with respect to BER. Note that this code performs 0.1 dB better than that reported in [3] for $P_b = 10^{-5}$. The reason is that a more correct alphabet conversion is used. The BER performance of this code is shown in Figure 16.

2.4.2 Block Inner Codes

As for convolutional inner codes, assume there is no alphabet conversion between the inner block code and the M-ary signalling. Let the inner block code be an (n_i, k_i) block code with minimum distance d_i, and

$$t_i = [(d_i - 1)/2].$$

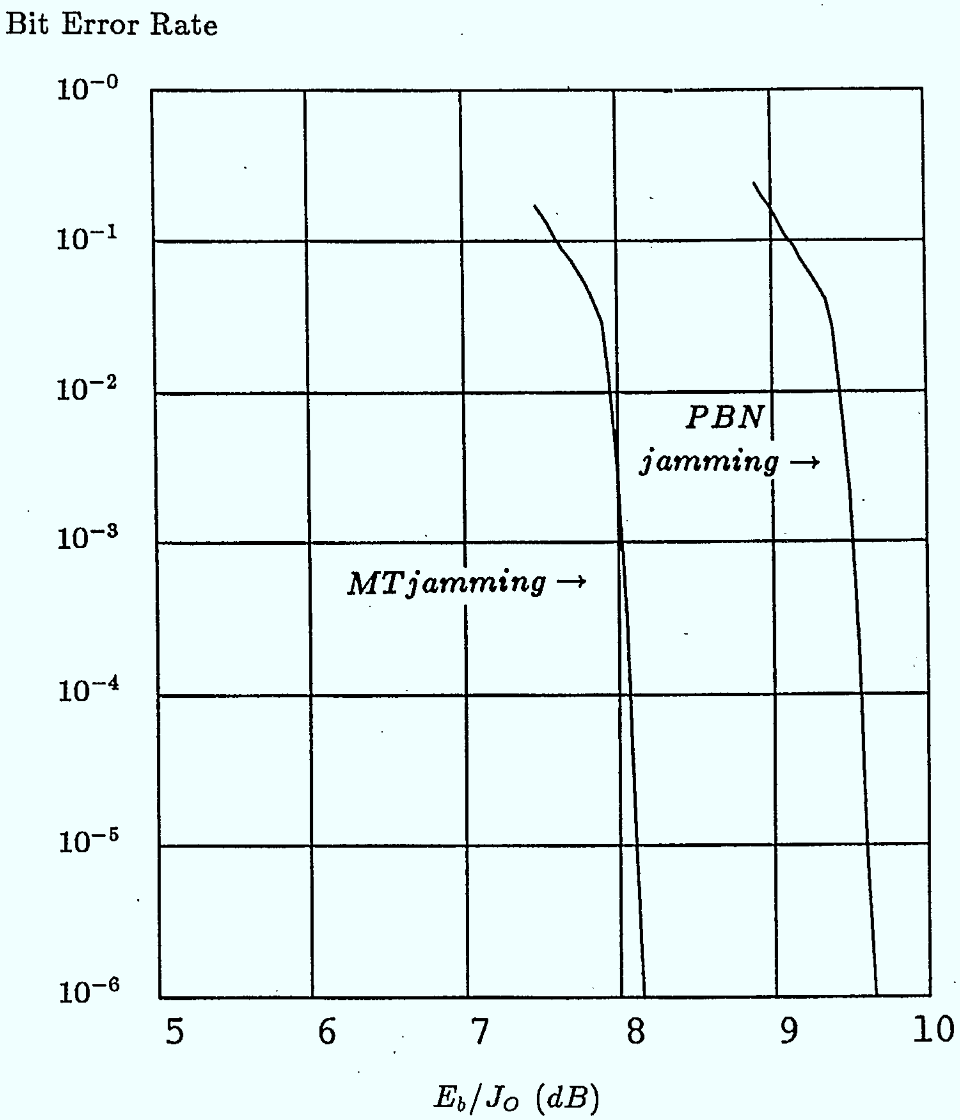

Figure 14: BER performance of the concatenated code with (1023,959) RS outer code and Odenwalder binary rate 1/2 convolutional inner code. $C = 10$. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 1$ for the WC MT jamming.

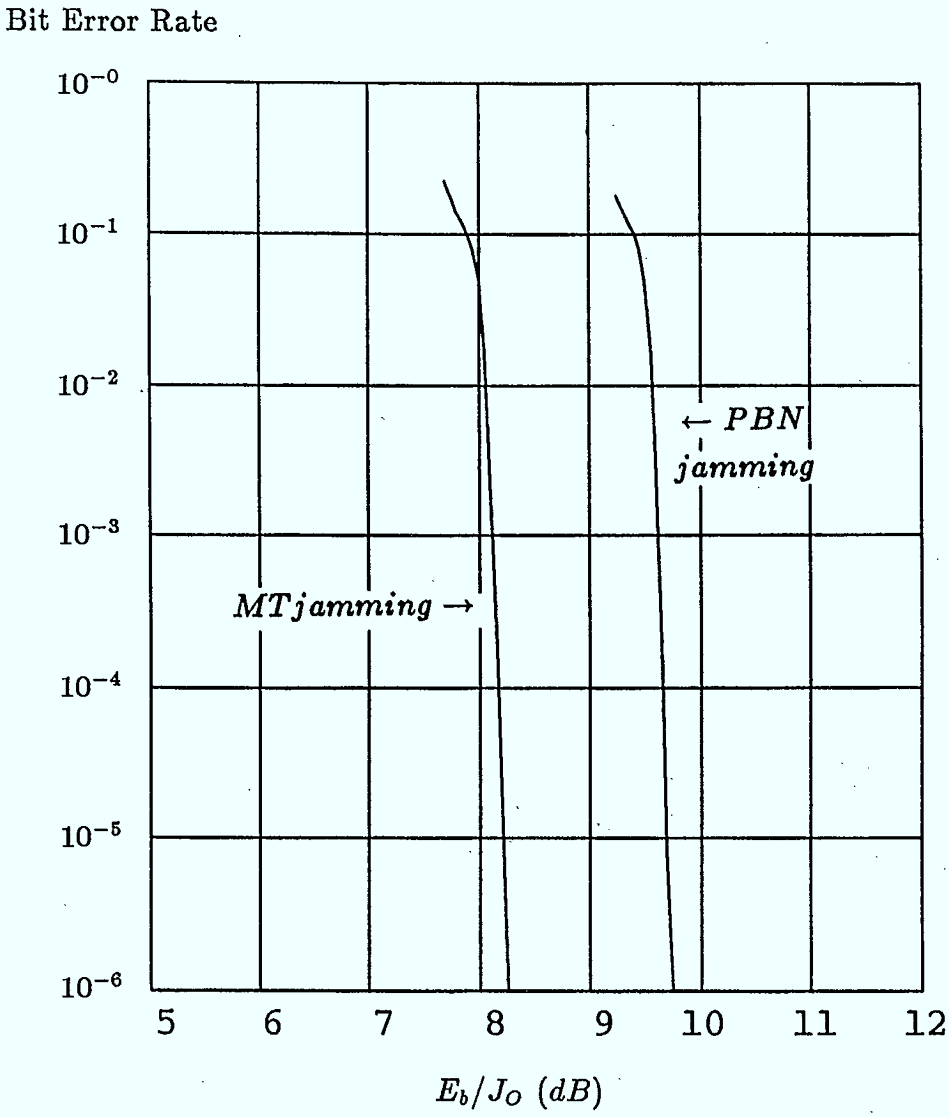

Figure 15: BER performance of the concatenated code with (511,447) RS outer code and Odenwalder binary rate 1/2 convolutional inner code. $C = 9$. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 1$ for the WC MT jamming.

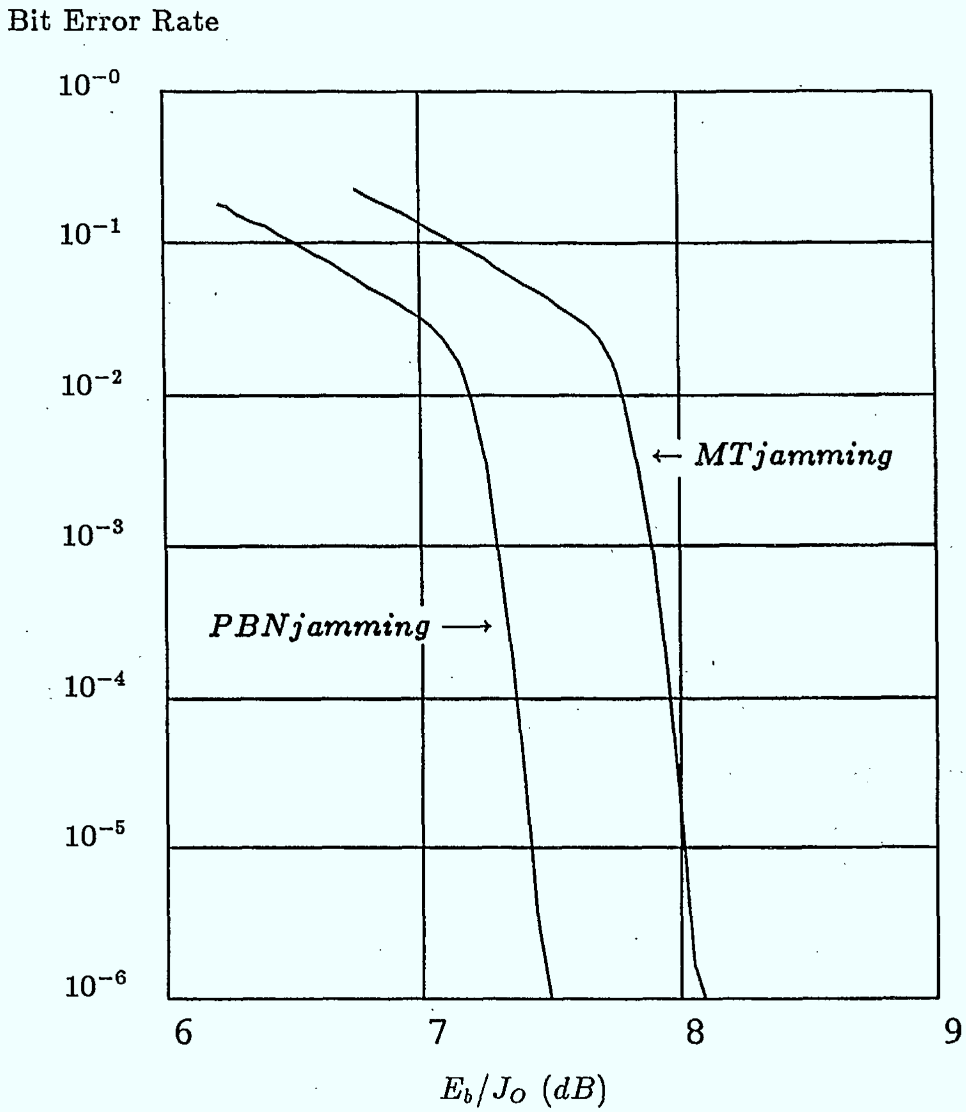

Figure 16: BER performance of the concatenated code with (1023,959) RS outer code and Trumpis 4-ary convolutional inner code. $C = 5$. At 10^{-5}, $\rho_{wc} = 0.75$ for the WC PBN jamming, and $\alpha_{wc} = 0.683$ for the WC MT jamming.

Assume bounded-distance decoding is used for the inner block code. Then we can evaluate the final BER performance of the concatenated RS code with the (n_i, k_i) block inner code by evaluating the BER performance of the outer RS code using formulas developed in Section 2.3, with the exception that Equation 21 which relates P_K and P_{be} is replaced by

$$P_K \approx \frac{1}{n_i} \sum_{j=t_i+1}^{n_i} j \binom{n_i}{j} \left(\frac{2(M-1)}{M} P_{be}\right)^j \left(1 - \frac{2(M-1)}{M} P_{be}\right)^{n_i - j}. \quad (23)$$

We plan to examine cases where binary BCH codes and the (23,12) Golay code are used as inner codes.

3 Implemention of Error Correcting Codes

As a prelude to implementing complex EC codes, the (24,12) extended Golay code is considered. This code is equivalent to a rate 1/2 quasi-cyclic code with minimum distance 8. The encoder is implemented as a twelve-stage linear feedback shift register (LFSR). In the decoder the twelve bit syndrome is computed using a 12-stage LFSR and acts as the address for the corresponding error pattern stored in a read-only memory (ROM). The error pattern is added modulo-2 to the received information to produce the correct transmitted information.

Simple computations reveal that this code is capable of correcting all error patterns of up to three errors and 1771 error patterns of four or more errors. The bit error rate P_b at the output of the decoder (i.e. as seen by the user) is related to the bit error rate p of the digital communication channel by the relation

$$P_b \leq 3695p^4. \tag{24}$$

Thus a raw channel error rate of 10^{-3} will be improved to about 4×10^{-9} by the use of this enCOder-DECoder (CODEC).

The encoder is contained entirely on one Xilinx chip (XC2064). The decoder is contained in three chips. The syndrome computer is contained on one Xilinx chip, while the table with the error pattern data is on two 32 kilobyte EPROMs (AM2732A). The minimum read time for the EPROMs is 250 ns which is the limiting factor for the speed of operation. The address for the EPROMs is valid at the rising clock pulse and the data is used at the next clock pulse, thus one half of a clock cycle is a minimum of 250 ns (or 500 ns for a clock cycle). This limits the speed of the system to 2 MHz. Due to the control circuitry the actual maximum speed of operation is 1.8 MHz. Further technical details of the CODEC may be found in [10].

4 Suggestions for Further Work

During the next few months we propose to undertake the following:

1. Develop software to examine the performance of error correcting codes for the slow frequency hopped, differentially coherent modulation technique in the presence of worst case jamming.

2. Examine the performance of some very low rate codes that can tolerate a large symbol error rate at the input to the decoder.

3. An in depth examination of hard-decision vs soft-decision and reliability of side information.

4. Search for M-ary convolutional codes ($M > 8$).

5. Continue work on implementation aspects of error correcting codes.

References

[1] Viterbi, A. J. and Jacobs, I. M.: 'Advances in coding and modulation for noncoherent channels affected by fading, partial band, and

multiple access interference',in *Advances in Communication Systems* , Vol. 4, New York: Academic Press, 1975, pp 279-308.

[2] Bird, J. S. and Felstead, E. B.: 'Antijam performance of fast frequency-hopped M-ary NCFSK – An overview", *IEEE J. on Selected Areas on Commun.*, Vol. SAC-4, No. 2, March 1986, pp 216-233.

[3] Simon, M. K., Omura, J. K., Scholtz, R. A. and Levitt, B. K.: *Spread spectrum communications, Vol. II*, Rockville, Maryland: Computer Science Press, 1985.

[4] Ma, H. H. and Poole, M. A.: 'Error correcting codes againt the worst-case partial-band jammer', *IEEE Trans. on Commun.*, Vol. COM-32, No. 2, February 1984, pp 124-133.

[5] Odenwalder, J. P. : 'Optimal decoding of convolutional codes', Ph.D. Dissertation, University of California, Los Angeles, 1970.

[6] Trumpis, B. D. : 'Convolutional coding for M-ary channels', Ph.D. Dissertation, University of California, Los Angeles, 1975.

[7] Viterbi, A. J. and Omura, J. K.: *Principles of digital communications and coding*, New York: McGraw-Hill, 1979.

[8] Ziemer, R. E. and Peterson, R. L.: *Digital communications and spread spectrum systems*, New York: Macmillan, 1985.

[9] Blahut, R. E. : *Theory and practice of error control codes*, Addison-Wesley, 1983.

[10] Fels, S., Little, W. D. and Bhargava, V. K. : 'Implementation of an encoder/decoder system for the (24,12) extended Golay code with XILINX chips', *Technical Report ECE-87-1* , Department of Electrical and Computer Engineering, University of Victoria, April 1987.

UNCLASSIFIED

Security Classification

KEY WORDS

Fast frequency hopping, spread spectrum, error-correcting codes, anti-jamming, fading

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the organization issuing the document.

2a. DOCUMENT SECURITY CLASSIFICATION: Enter the overall security classification of the document including special warning terms whenever applicable.

2b. GROUP: Enter security reclassification group number. The three groups are defined in Appendix 'M' of the DRB Security Regulations.

3. DOCUMENT TITLE: Enter the complete document title in all capital letters. Titles in all cases should be unclassified. If a sufficiently descriptive title cannot be selected without classification, show title classification with the usual one-capital-letter abbreviation in parentheses immediately following the title.

4. DESCRIPTIVE NOTES: Enter the category of document, e.g. technical report, technical note or technical letter. If appropriate, enter the type of document, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the document. Enter last name, first name, middle initial. If military, show rank. The name of the principal author is an absolute minimum requirement.

6. DOCUMENT DATE: Enter the date (month, year) of Establishment approval for publication of the document.

7a. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7b. NUMBER OF REFERENCES: Enter the total number of references cited in the document.

8a. PROJECT OR GRANT NUMBER: If appropriate, enter the applicable research and development project or grant number under which the document was written.

8b. CONTRACT NUMBER: If appropriate, enter the applicable number under which the document was written.

9a. ORIGINATOR'S DOCUMENT NUMBER(S): Enter the official document number by which the document will be identified and controlled by the originating activity. This number must be unique to this document.

9b. OTHER DOCUMENT NUMBER(S): If the document has been assigned any other document numbers (either by the originator or by the sponsor), also enter this number(s).

10. DISTRIBUTION STATEMENT: Enter any limitations on further dissemination of the document, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this document from their defence documentation center."

(2) "Announcement and dissemination of this document is not authorized without prior approval from originating activity."

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document, even though it may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall end with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (TS), (S), (C), (R), or (U).

The length of the abstract should be limited to 20 single-spaced standard typewritten lines; 7½ inches long.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a document and could be helpful in cataloging the document. Key words should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context.

UNCLASSIFIED
Security Classification

DOCUMENT CONTROL DATA – R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATING ACTIVITY University of Victoria	2a. DOCUMENT SECURITY CLASSIFICATION UNCLASSIFIED 2b. GROUP

3. DOCUMENT TITLE
CODING FOR FREQUENCY HOPPED SPREAD SPECTRUM SATELLITE COMMUNICATIONS

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)
Annual Report, December 1, 1986 to April 15, 1987

5. AUTHOR(S) (Last name, first name, middle initial)
Wang, Qiang; Gulliver Aaron T., Bhargava, Vijay K., and Little, Warren D.

6. DOCUMENT DATE April 1987	7a. TOTAL NO. OF PAGES 44	7b. NO. OF REFS 10

8a. PROJECT OR GRANT NO. 32A99	9a. ORIGINATOR'S DOCUMENT NUMBER(S) ECE-87-2
8b. CONTRACT NO. SSC #27ST.36001-6-3539	9b. OTHER DOCUMENT NO.(S) (Any other numbers that may be assigned this document)

10. DISTRIBUTION STATEMENT
Unlimited

11. SUPPLEMENTARY NOTES	12. SPONSORING ACTIVITY Communications Research Centre

13. ABSTRACT

Performance of various types of error correcting codes is examined under partial band noise jamming and multitone jamming using the fast frequency hopping, noncoherent M-ary frequency-shift-keying technique. Some results are compared to those previously published to ensure the reliability of the software package developed. Several errors in previously published results, some of which are not trivial, are identified and corrected. As a prelude to implementing more complex codes, we report on the hardware implementation of the well known (24,12) extended Golay code.

DSIS
77-065