AD-AII 58 AS ARY MATERIEL DEVELOPMENT AND RLADINESS COMMAND ADEL--ETC F/G $17 / 4$ FREGUETICY HOPPING, NULTIPLE FRENUENCY-SHIFT KEYING. COOING. AND-GETC(U) AVG H2 0 J TORRIERI MIPR-N62269/82/MP/00918 (nctistifito $\mathrm{CM} / \mathrm{CCM}-\mathrm{B2}-1$


UNCLASSIFIED
sECUMITY CLASSIFICATION OF THIS PAGE (mhen Dege Entorod)

| REPORT DOCUMENTATION PAGE | READ DNSTRUCTIONS BEFORE COMPLETING FORM |
| :---: | :---: |
| 1. REPORT MUMER   <br> CM/CCM-82-1 AD aOVVT ACCEESSIOM NO | 3. RECIPIENT'S CATALOG MUMIER |
| ```4. TITLE (mad subutlo) Frequency Hopping, Multiple Frequency- Shift Keying, Coding, and Optimal Partial- Band Jamming``` | 3. TYPE OF REPORT \& PEMOO COVEAED Technical Report a. PERFOMMG ORG. REPORT NUMEER |
| 7. Authot(d) Don J. Torrieri | 8. CONTRACT OR GRAMT MUMBER(C) MIPR: N $62269 / 82 / M P / 00918$ |
| 9. perfotming organization name and address CM/CCM Center <br> 2800 Powder Mill Road <br> Adelphi, MD 20783 | 10. PROGRAMELEMENT, PROJECT, TASK |
| 19. controlling office name and addesss <br> Naval Air Systems Command Washington, DC 20361 | 12. REPORT DATE August 1982 |
|  | 13. numeer of pabes |
|  <br> Naval Air Develcoment Center <br> Warminster, PA 18974 | iB. SECUAITY CLASS. (Of Alig repori) UNCLASSIFIED |
|  | ISe. oteclassieication/Downgrading |
| 16. Distrinution statement for thio ropori) |  |
| Approved for public release; distributio | on unlimited. |
|  |  |
| 10. SUPPLEMENTARY NOTES <br> Project No: N9R2N1 |  |
| 15. KEY wonos (Contimue en roveree oldo If nocoesery and lidentity br block min |  |
| Frequency hopping Partial-band jamming |  |
| Error-correcting code Multiple frequency-shift keying |  |
| Chèrnoff bound Concatenated code |  |
|  |  |
| $\checkmark$ The performance of frequency-hopping systems with multiple |  |
| frequency-shift keying is determined for operation against optimal partial-band jamming. The effects of Reed-Solomon, binary block, convolutional, and concatenated codes are analyzed. Con-tinuous-phase frequency-shift keying with limiter-discriminator demodulation is shown to offer potentially improved performance in frequency-hopping systems. |  |
| D. romin ITS EDinow or i wov es is omolete <br> 1/secumitr cla | UNCLASSIFIED |

## CONTENTS

Page

1. INTRODUCTION ..... 5
2. BLOCK CODES .....  7
3. CONVOLUTIONAL CODES ..... 14
4. CONCATENATED CODES ..... 16
5. LIMITER-DESCRIMINATOR DEMODULATION ..... 22
LITERATURE CITED ..... 24
DISTRIBUTION ..... 55
APPENDICES
A.--ERROR PROBABILITIES OF ENCODED SYSTEMS ..... 25
B.--SOFT-DECISION DECODING FOR FREQUENCY-HOPPING SYSTEMS ..... 41
C. --THE CHERNOFF BOUND ..... 49
FIGURES
6. FH/MFSK receiver with hard-decision decoding and multiple frequency-hopping patterns ..... 5
7. FH/MFSK receiver with hard-decision decoding and single frequency-hopping pattern. ..... 6
8. Information bit error probability for no coding, binary hard decisions, and partial-band jamming ..... 11
9. Information bit error probability for Golay $(23,12)$ code, hard-decision decoding, and partial-band jamming ..... 11
10. Worst-case performance for binary block ( $c, w$ ) codes with hard decisions ..... 12
11. Worst-case performance for repetition codes with hard decisions ..... 12
12. Worst-case performance for Reed-Solomon ( $c, w$ ) codes with hard decisions ..... 13

## Figures (Cont'd)

Page
8. Worst-case performance for rate $1 / 2$ convolutional codes with hard decisions15
9. Worst-case performance for rate $1 / 3$ convolutional codes with hard decisions......................................................... 15
10. Worst-case performance for orthogonal convolutional codes with hard decisions16
11. FH/MFSK system with concatenated coding ..... 16
12. Worst-case performance for concatenated codes with outerGolay $(23,12)$ code, inner repetition code, and hard decisions.. 18
13. Worst-case performance for concatenated codes with outer convolutional code ( $K=7, r=1 / 2$ ), inner repetition code, and hard decisions ..... 18
14. Worst-case performance for concatenated codes with outer Reed- Solomon ( $c, w$ ) code, inner binary block ( $c_{1}, w_{1}$ ) code, and hard decisions ..... 20
15. Worst-case performance for concatenated codes with outerReed-Solomon ( $c, w$ ) code, inner convolutional code ( $\mathrm{X}=7$,$r=1 / 2$ ), and hard decisions20
16. Worst-case performance for concatenated codes with outer convolutional code ( $K=7, r=1 / 2$ ), inner repetition code, hard inner decisions, and soft outer decisions22
17. Worst-case performance for limiter-discriminator demodulation
and concatenated codes with outer convolutional code $(K=7$,
17. Worst-case performance for limiter-discriminator demodulation
and concatenated codes with outer convolutional code $(K=7$, $r=1 / 2)$, inner repetition code, hard inner decisions, and soft outer decisions24



## 1. INTRODUCTION

Multiple frequency-shift keying (MFSK) entails choosing one of $N$ frequencies as the carrier or center frequency for each transmitted symbol in a communication system. When frequency hopping is superimposed on MFSK, resulting in an FH/MFSK system, the set of $N$ possible frequencies changes with each hop.

In an ideal FH/MFSK system, each frequency of the frequency sets is randomly selected for each successive hop. This strategy precludes the judicious spacing of jaming signals to exploit the structure of the frequency sets and increases the resistance to repeater jaming.l However, a more practical implementation, which requires only a single frequency synthesizer instead of $N$, selects frequencies having a fixed relation to each other but a randoraly chosen location within the total bandwidth. Figures 1 and 2 depict the main elements of receivers appropriate for these two strategies. Each receiver is noncoherent (a coherent receiver is generally impractical) and implements hard decisions. After the dehopping, separate code symbol decisions are made and the demodulated symbols are applied to a decoder, which produces the decoded message. The $N$ frequencies are separated enough so that the received signal produces negligible responses in the incorrect bandpass filters.


Figure 1. FH/MFSK receiver with hard-decision decoding and multiple frequency-hopping patterns.

[^0]

Figure 2. FH/MFSK receiver with hard-decision decoding and single frequency-hopping pattern.

Soft-decision decoding offers a significant performance advantage for FH/MFSK systems operating in partial-band jamming if the presence or the absence of jamming in each channel can be accurately determined so that symbol erasures can be used. 2,3 However, an accurate measurement of the jamming state in the presence of signal and jamming power variations is not possible in most practical cases. When no information about the jamming is available, a metric can probably be found that yields a performance for a soft-decision system that is slightiy better than the performance of the corresponding hard-decision system. However, it is doubtful that the performance advantage is sufficient to justify the increased implementation complexity of a system with soft decisions, and if the metric depends upon the signal level, as is probable, additional implementation difficulties are entailed. Thus, we consider only hard-decision decoding except for concatenated codes (sect. 4). Appendix A summarizes those aspects of coding theory that are needed subsequently. An analysis of soft-decision decoding for a particular metric is given in appendix $B$.

If the errors in the demodulated symbols are assumed to be independent, the general coding equations and inequalities of appendix $A$ can be used to determine the error-rate performance of an FH/MFSK system with

[^1]hard-decision decoding. This assumption is reasonable for fast frequency hopping, in which there is a frequency hop for every MFSK symbol. For slow frequency hopping, in which there is less than one hop per MFSK symbol, the assumption is reasonable if symbols are interleaved over a sufficient number of hop periods. The deinterleaving in the receiver disperses bursts of errors, thereby facilitating the removal of errors by the decoder.

## 2. BLOCK CODES

When a block code is used, each group of $m$ information bits is encoded as a symbol, and then each group of $w$ symbols is encoded as a codeword of $c$ code symbols that are transmitted. Since a codeword represents mw information bits, there must be $2^{\mathrm{mw}}$ possible codewords. In an FH/MFSK system, one of $N=2^{m}$ frequencies is selected as the carrier for each transmitted symbol.

Let $P_{i b}$ denote the probability of an information bit error in the decoded output and d denote the minimum distance between codewords. For binary frequency-shift keying, let $P_{b}$ denote the channel bit error probability, which is the probability of an error in a demodulated code bit. It is shown in appendix $A$ that for hard-decision decoding of binary block codes, $P_{i b}$ is approximately given by

$$
\begin{align*}
P_{i b}= & \frac{d}{c} \sum_{i=[(d+1) / 2]}^{d}\binom{c}{i} P_{b}^{i}\left(1-P_{b}\right)^{c-i}  \tag{1}\\
& +\frac{1}{c} \sum_{i=d+1}^{c} i\binom{c}{i} p_{b}^{i}\left(1-P_{b}\right)^{c-i},
\end{align*}
$$

where [x] denotes the largest integer less than or equal to $x$. For the nonbinary Reed-Solomon codes, the approximate expression is

$$
\begin{align*}
P_{i b}= & \frac{c+1}{2 c^{2}}\left[d \sum_{i=[(d+1) / 2]}^{d}\binom{c}{i} p_{s}^{i}\left(1-P_{s}\right)^{c-i}\right.  \tag{2}\\
& \left.+\sum_{i=d+1}^{c} i\binom{c}{i} p_{s}^{i}\left(1-P_{s}\right)^{c-i}\right]
\end{align*}
$$

where $c=2^{m}-1, d=c-w+1$, and $P_{s}$ denotes the channel symabol error probability, which is the probability of an error in a demodulated code symbol.

Since an exact derivation of $P_{s}$ is difficult when partial-band jamming causes different amounts of jamming powers to enter the $N$ receiver filters, we use a union bound (app A). A code symbol error occurs if the correct envelope sample does not exceed the other $N-1$ envelope samples. Since the probability that a particular envelope sample exceeds the correct one is a function of only two envelope samples, it is the same as $P_{b}$, the channel bit error probability of a frequency-hopping system with binary frequency-shift keying. Thus, the union bound is

$$
\begin{equation*}
P_{s} \leq(N-1) P_{b}, N \geq 2 \tag{3}
\end{equation*}
$$

If $N>2$, the inequality is strict. If $N=2$, we have $P_{s}=P_{b}$. When this inequality is substituted into equation (2), we obtain an upper bound for $P_{i b}$. This bound becomes tighter as ( $N-1$ ) $P_{b}$ decreases.

The total number of frequency channels available for frequency hopping is denoted by $M$, and the number of jamed channels is denoted by $J$. By definition, $J \leq M$. We assume that the jarming power is the same in all jammed channels and that the received signal power is independent of which channel is used for transmission of the signal. We assume either that the possible frequency channels are chosen randomly for each hop (which is true by definition for the system of fig. 1) or that the jammed channels are randomly chosen. Equation (3.13) of Torrieril gives

$$
\begin{equation*}
P_{b}=\sum_{n=n_{0}}^{n_{1}} \frac{\binom{2}{n}\binom{M-2}{J}}{\binom{M}{J}} s_{n} \tag{4}
\end{equation*}
$$

where

$$
\begin{equation*}
n_{0}=\max (0, J+2-M), \quad n_{1}=\min (2, J) \tag{5}
\end{equation*}
$$

The $s_{n}$ depend upon the form of the jamuing. In the referenced text, 1 the $s_{n}$ are determined for narrowband jaming and noise famaing. since it is described by simpler mathematics, noise jamming is considered

[^2]here. The noise jaming is modeled as a Gaussian process with a flat power spectrum over each jammed channel. We assume, as does the referenced text, 1 that the receiver contains ideal nondistorting bandpass filters with disjoint passbands. Consequently, the equations derived for the $S_{n}$ are in terms of signal, thermal noise, and jamming powers. When matched filters are used, it is straightforward to verify (see Haykin ${ }^{4}$ for a similar derivation) that the formulas of the referenced text ${ }^{l}$ for noise jamaing are valid if we replace the signal power by the symbol energy and replace the thermal noise and jamming powers by the corresponding power spectral densities. The value of $S_{n}$ is the same for a bandpass-filter receiver and for a matched-filter receiver if the product of the symbol duration and the noise bandwidth of the bandpass filters is unity. Let $R_{s}$ denote the signal power, $N_{t}$ the thermal and background noise power in a channel, and $N_{j}$ the jamming power in a jammed channel. Equations (3.30) to (3.32) of the referenced textl give
\[

$$
\begin{equation*}
s_{n}=\frac{1}{2} \exp \left(-\frac{R_{s}}{2 N_{t}+n N_{j}}\right), \quad n=1,2,3 \tag{6}
\end{equation*}
$$

\]

Combining equations (4) and (6) yields

$$
\begin{equation*}
P_{b}=\frac{1}{2} \sum_{n=n_{0}}^{n_{1}} \frac{\binom{2}{n}\binom{M-2}{J}}{\binom{M}{J}} \exp \left(-\frac{R_{s}}{2 N_{t}+n N_{j}}\right) \tag{7}
\end{equation*}
$$

The parameters $M_{,} N_{t}, J$, and $N_{j}$ depend upon the coding. Let $M_{u}$ denote the number of channels that are available for frequency hopping if an uncoded binary modulation is used. When MFSK and coding are used but the information rate (or the message duration) and the total hopping bandwidth are preserved, the number of available channels becomes approximately

$$
\begin{equation*}
M=\operatorname{int}\left(r_{s} M_{u}\right) \tag{8}
\end{equation*}
$$

where int( $x$ ) is the largest integer contained in $x$ and $r_{s}$ is the ratio of information bits to transmitted code symbols. For block codes, $r_{s}=$ mw/c. The thermal noise power becomes

[^3]\[

$$
\begin{equation*}
N_{t}=\frac{N_{t u}}{r_{s}} \tag{9}
\end{equation*}
$$

\]

where $N_{t u}$ is the thermal noise power for uncoded binary modulation. The number of jammed channels is approximately

$$
\begin{equation*}
J=\operatorname{int}(\mu M) \tag{10}
\end{equation*}
$$

where $\mu$ is the fraction of the total hopping band that contains jamming. If the jamming power is uniformly distributed and the channels are disjoint, then

$$
\begin{equation*}
N_{j}=\frac{N_{j t}}{J} \tag{11}
\end{equation*}
$$

where $\mathrm{N}_{\text {jt }}$ denotes the total jarming power distributed in the total
hopping band.
In the following examples,* we assume that $M_{u}=1000$. Figures 3 and 4 depict $P_{\text {ib }}$ versus $\mu$ for uncoded binary communications and the Golay $(23,12)$ code, respectively. The improvement due to the coding and the sharpness of the peaks in $P_{i b}$ increases with the signal-to-noise ratio, $R_{g} / N_{t u}$ and decreases with the total jamming-to-signal ratio, $N_{j t} / R_{s}$. The optimal band occupancy for the jammer increases with $\mathrm{N}_{\mathrm{jt}} / \mathrm{R}_{\mathbf{s}}{ }^{\circ} \mathrm{Fig}^{\mathrm{F}}$ ures 5 to 7 depict the maximum value of $P_{i b}$ as a function of $N_{j t} / R_{s}$, assuming the optimal band occupancy for the jammer, $R_{s} / N_{t u}=20 \mathrm{~dB}$, and various block codes. Thus, these figures illustrate the worst-case performance of an FH/MFSK system operating against partial-band jamaing that can be optimized. Instead of using $N_{j t} / R_{B}$, the abscissas can be expressed in terms of $E_{b} / N_{0 j}$, where $E_{b}$ is the energy per information bit and $N_{0 j}$ is the power spectral density that corresponds to uniform jamming over the total hopping band. A straightforward evaluation gives (in decibels)

$$
\begin{equation*}
E_{b} / N_{0 j}(d B)=-N_{j t} / R_{g}(d B)+M_{u}(d B)+B_{u} T_{b}(d B), \tag{12}
\end{equation*}
$$

where $B_{u}$ is the frequency-channel bandwidth for uncoded binary modulation and $T_{b}$ is the information bit duration.

[^4]

Figure 3. Information bit error probability for no coding, binary hard decisions, and partial-band jamming.


Figure 4. Information bit error probability for Golay (23,12) code, hard-decision decoding, and partial-band jamming.


Figure 5. Worst-case performance for binary block ( $c, w$ ) codes with hard decisions.


Figure 6. Worst-case performance for repetition codes with hard decisions.


Figure 7. Worst-case performance for Reed-Solomon ( $c, w$ ) codes with hard decisions.

The Reed-Solomon codes of figure 7 are among those providing the best performance against optimal partial-band jamaing for given values of $N=c+1$. The best codes tend to have rates between one-half and one-third. Since inequality (3) is used, the curves of figure 7 are actually upper bounds for the worst-case performance. A comparison of figures 5 and 7 shows that the Reed-Solomon codes do not offer a significant performance advantange over the Golay (23,12) code unless the required $P_{i b}$ is less than $10^{-5}$ and $N \geq 32$, which requires a complex system implementation.

Communication systems are often required to provide a bit error probability below a specified value. Thus, a measure of performance for these systems is the signal-to-total-jaming ratio required to achieve the specified $P_{i b}$. For example, if an $\mathrm{FH} / \mathrm{MFSK}$ system with repetition coding must provide $P_{i b}=10^{-3}$, then figure 6 indicates that $c=7$ is the optimal choice for minimizing the required value of $\mathrm{R}_{\mathrm{g}} / \mathrm{N}_{\mathrm{jt}}$ or, equivalently, maximtzing the value of $\mathrm{N}_{\mathrm{jt}} / \mathrm{R}_{\mathrm{s}}$ that can be tolerated.

## 3. CONVOLUTIONAL CODES

For convolutional codes and hard-decision Viterbi decoding, $P_{\text {ib }}$ is given by the equations of appendix A and equations (7) to (11). Viterbi decoding is preferable to other convolutional decoding procedures when jamming is capable of causing relatively high error rates. If $v$ bits are transmitted for every b bits shifted into the encoder register, then $r_{s}=b / v$.

Hard-decision decoding of rate $1 / 2$ and rate $1 / 3$ codes results in an error rate approximated by

$$
\begin{equation*}
P_{i b}=\sum_{i=0}^{7} A\left(d_{f}+i\right) Q\left(d_{f}+i\right) \tag{13}
\end{equation*}
$$

where the $A\left(d_{f}+i\right)$ are listed in table $A-2$ and

$$
Q(\delta)=\left\{\begin{array}{l}
\sum_{i=(\delta+1) / 2}^{\delta}\binom{\delta}{i} p_{b}^{i}\left(1-p_{b}\right)^{\delta-i}, \delta \text { is odd },  \tag{14}\\
\sum_{i=\delta / 2+1}^{\delta}\binom{\delta}{i} p_{b}^{i}\left(1-p_{b}\right)^{\delta-i}+\frac{1}{2}\binom{\delta}{\delta / 2}\left[p_{b}\left(1-p_{b}\right)\right]^{\delta / 2}, \\
\delta \text { is even } .
\end{array}\right.
$$

For orthogonal convolutional codes of constraint length $K, r_{s}=2^{-K}$ and $P_{i b}$ is approximated by a truncation of the right-hand side of inequality (A-27).

Figures 8 to 10 illustrate the worst-case performances of an FH/MFSK system with rate $1 / 2$, rate $1 / 3$, and orthogonal convolutional codes, respectively. It is assumed that $M_{u}=1000$ and $R_{s} / N_{t u}=20 \mathrm{~dB}$. In figures 8 and 9, performance always improves with constraint length. In contrast, figure 10 indicates that orthogonal convolutional codes with $K$ $=4$ perform better than codes with $K=3$ only if the required $P_{i b}$ is less than approximately $10^{-4}$.


Figure 8. Worst-case performance for rate $1 / 2$ convolutional codes with hard decisions.


Figure 9. Worst-case performance for rate $1 / 3$ convolutional codes with hard decisions.


Figure 10. Worst-case performance for orthogonal convolutional codes with hard decisions.

## 4. CONCATENATED CODES

A concatenated code uses multiple levels of coding to achieve a large error-correcting capability. Figure 11 is a functional block diagram of an FH/MFSK system with concatenated coding that consiste of two successive stages of coding. The inner interleaver and deinterleaver are unnecessary for fast frequency hopping. For slow frequency hopping, they insure the random distribution of errors at the input of the inner decoder. The outer deinterleaver, which requires a corre-

$\omega$

$\omega$
Figure 11. FH/MFSK system with concatenated coding: (a) transmitter and (b) receiver.
sponding outer interleaver, is usually necessary to redistribute errors in the output of the inner decoder so that symbol errors are distributed randomily at the input of the outer decoder. For the reasons stated in section 1 , hard decisions are desirable in the inner decoder when optimal partial-band jamming is possible.

Analytical expressions can often be derived for $P_{\text {ib }}$, the probability of an information bit error at the output of the outer decoder. If the Inner code is a binary block code, the bit error probability at the output of the inner decoder, $P_{b 1}$, is determined for hard decisions from the right-hand side of equation (1); that is,

$$
\begin{align*}
P_{b 1}= & \frac{d_{1}}{c_{1}} \sum_{i=\left[\left(d_{1}+1\right) / 2\right]}^{d_{1}}\binom{c_{1}}{i} P_{b}^{i}\left(1-P_{b}\right)^{c_{1}-i}  \tag{15}\\
& +\frac{1}{c_{1}} \sum_{i=d_{1}+1}^{c_{1}} i\binom{c_{1}}{i} p_{b}^{i}\left(1-p_{b}\right)^{c_{1}-i}
\end{align*}
$$

where $d_{1}$ and $c_{1}$ refer to the inner code. Equations (7) to (11) give $P_{b}$. The ratio of information bits to transmitted code symbols is

$$
\begin{equation*}
r_{s}=r_{80} r_{s i} \tag{16}
\end{equation*}
$$

where $r_{s o}$ is the ratio of information bits to outer-code symbols and $r_{s i}$ is the ratio of outer-code symbols to inner-code symbols. The deinterleaver provides independent errors at the input of the outer decoder. Thus, if the outer code is a binary block code and hard decisions are made, then $P_{i b}$ is given by equation (1) with $P_{b 1}$ substituted in place of $P_{b}$ and $d$ and $c$ referring to the outer code. If the outer code is a rate $1 / 2$ or rate $1 / 3$ binary convolutional code and hard decisions are made, then $P_{i b}$ is determined from equations $\left(13\right.$ ) and (14) with $P_{b 1}$ replacing $P_{b}$.

As specific examples, figures 12 and 13 depict the worst-case performances against partial-band jamming of systems with repetition codes as the inner codes, $M_{u}=1000$, and $R_{8} / N_{t u}=20 \mathrm{~dB}$. In figure 12 , the outer code is a Golay $(23,12)$ code; In EIgure 13, the outer code is a convolutional code of constraint length 7 and rate $1 / 2$. The figures illustrate that the degree to wich the repetition code improves or degrades the performance of the outer code alone varies with the required $P_{i j}$. In the system implementation, the outer interleaver and the outer deinterleaver are unnecessary.


Figure 12. Worst-case performance for concatenated codes with outer Golay $(23,12)$ code, inner repetition code, and hard decisions.


Figure 13. Morst-case performance for concatenated codes with outer convolutional code ( $K=7, r=1 / 2$ ), inner repetition code, and hard decisions.

Consider a Reed-Solomon outer code and a binary inner code. If there are mits in a Reed-Solomon code symbol, the outer decoder can convert a burst of $m$ errors at the inner-decoder output into a single symbol error, thereby reducing $P_{\text {ib }}$ at the outer-decoder output. The outer deinterleaver operates on symbols, rather than bits, following a serial-to-parallel conversion, and decorrelates errors in successive Reed-Solomon code symbols.

For a block inner code, an efficient design sets the number of information bits in the block codewords, $w_{1}$, equal to an integer times $m$, and symbol deinterleaving prevents an inner codeword error from affecting adjacent symbols in a Reed-Solomon codeword. If $w_{1}=m$, the probability of a Reed-Solomon code symbol error, $P_{s}$, is equal to the word error probability produced by the inner decoder. By analogy with inequality ( $A-1$ ) and equation ( $A-2$ ), we have the approximation or equality

$$
\begin{equation*}
P_{s}=\sum_{i=\left[\left(d_{1}+1\right) / 2\right]}^{c_{1}}\binom{c_{1}}{i} P_{b}^{i}\left(1-P_{b}\right)^{c_{1}-i} \tag{17}
\end{equation*}
$$

when hard decisions are made by the inner decoder. Assuming hard decisions in the outer decoder, $P_{i b}$ is determined from equations (2) and (17). Figure 14 shows examples of the worst-case performance, assuming that $M_{u}=1000$ and $R_{s} / N_{t u}=20 \mathrm{~dB}$.

At the output of a convolutional inner decoder using the viterbi algorithm, the bit errors tend to occur over spans of several constraint lengths. Consequently, the outer deinterleaver should be designed to ensure that two input symbols at a distance less than the usual largest error span result in output symbols that do not beiong to the same ReedSolomon codeword. Assuming that the bit error rate is no more than onehalf in spans with errors, then the bit error probability at the innerdecoder output is less than one-half times $P_{g}$. Thus, for rate $1 / 2$ and rate $1 / 3$ convolutional inner codes with hard decisions,

$$
\begin{equation*}
p_{s}>2 \sum_{i=0}^{7} A\left(d_{f}+i\right) Q\left(d_{f}+1\right) \quad, \quad K>m \tag{18}
\end{equation*}
$$

where the inequality is needed to make the bound reasonably tight. Hard decisions in the outer decoder and ideal symbol interleaving yield a $P_{i b}$ with a lower bound determined by equation (2) and inequality (18). Figure 15 depicts examples of the worst-case lower bounds for $M_{4}=1000$, $R_{8} / \mathrm{N}_{\mathrm{tu}}=20 \mathrm{~dB}$, and an inner convolutional code with $K=7$ and $\mathrm{r}=1 / 2$.


Figure 14. Worst-case performance for concatenated codes with outer Reed-Solomon ( $c, w$ ) code, inner binary block ( $c_{1}, w_{1}$ ) code, and hard decisions.


Figure 15. Worst-case performance for concatenated codes with outer Reed-Solomon ( $C, W$ ) code, inner convolutional code ( $K=7, r=1 / 2$ ), and hard decisions.

Soft-decision decoding in the outer decoder is possible if the inner decoder produces symbol metrics. For a practical example, consider an FH/MFSK system with a repetition code of length $c$, as the inner code. The demodulator produces a series of logical "ones" and "zeros." The inner decoder counts $n_{1}$, the number of ones in each group of $c_{1}$ bits representing an outer-code symbol. The symbol metric associated with an outer-code one is $n_{1}$, whereas $c_{1}-n_{1}$ is associated with an outer-code zero. The outer decoder forms cumulative metrics that are the sums of symbol metrics. The selection of the largest of the cumulative metrics determines the decoded output.

System performance can be determined by first evaluating $Z$, which is defined by equation (A-35). If there are $j$ errors in the $c_{1}$ bits representing outer-code symbol $i$, then the difference between the symbol metric corresponding to the incorrect symbol and the one corresponding to the correct symbol is

$$
\begin{equation*}
m_{1}(2, i)-m_{1}(1, i)=2 j-c_{1} . \tag{19}
\end{equation*}
$$

A stralghtforward calculation yields

$$
\begin{equation*}
z=\min _{0<s} \sum_{j=0}^{c_{1}}\binom{c_{1}}{j} P_{b}^{j}\left(1-P_{b}\right)^{c_{1}-j} \exp \left[s\left(2 j-c_{1}\right)\right] \tag{20}
\end{equation*}
$$

where $P_{b}$ is determined from equations (7) to (11) and (16), and $r_{s i}=$ $1 / c_{1}$. If, for example, the outer code is a rate $r$ convolutional code, then $P_{i b}$ can be determined from inequality $(A-19)$ with $b=1$ and $P_{i s}=$ $P_{i b}$. Since the Chernoff-Jacobs bound of appendix $C$ applies, $\alpha=1 / 2$ and $P_{i b}$ is approximated by

$$
\begin{equation*}
P_{i b}=\frac{1}{2} \sum_{i=0}^{7} A\left(d_{f}+i\right) z^{d_{f}+i} \tag{21}
\end{equation*}
$$

where the $A\left(d_{f}+i\right)$ are listed in table $A-2$. Equation (16) implies that $r_{s}=r / c_{1}$.

As a specific example, figure 16 illustrates the worst-case performances against partial-band jamming of FH/MFSK systems having outer convolutional codes with $K=7$ and $r=1 / 2$, inner repetition codes with $C_{1}=2,3,4$, or $5, M_{M}=1000$, and $R_{8} / N_{t u}=20 \mathrm{~dB}$. For a required $P_{i b}=$ $10^{-5}$, the optimal choice for $c_{1}$ is 3 . Comparing figures 13 and 16 indicates that for $c_{1}=3$, a soft-limiting outer decoder requires a signal power of approximately 1.5 dB less than a hard-limiting one does to provide $P_{i b}=10^{-5}$.


Figure 16. Worst-case performance for concatenated codes with outer convolutional code ( $K=7, r=1 / 2$ ), inner repetition code, hard inner decisions, and soft outer decisions.

## 5. LIMITER-DISCRIMINATOR DEMODULATION

Frequency-hopping systems with continuous-phase frequency-shift keying (CPFSK) offer reduced spectral splatter and a potentially improved performance. ${ }^{1}$ After each frequency hop, a binary CPFSK system shifts between two frequencies separated by $h / T_{b}$, where $h$ is the deviation ratio and $T_{b}$ is the channel bit duration. Demodulation is done by a limiter-discriminator ${ }^{4}$ in general, but differential demodulation is also possible. Thus, the FH/MFSK receiver differs from the receiver of figure 1 or figure 2 in that the envelope detector is replaced by a limiter-discriminator or differential detector.

[^5]The theory of limiter-discriminator demodulation ${ }^{5}$ provides complicated expressions for $P(E)$, the bit error probability in the absence of frequency hopping. However, the theoretical $P(E)$ can often be adequately approximated by a simple equation such as

$$
\begin{equation*}
P(E)=\frac{1}{2} \operatorname{erfc}\left(E \sqrt{\frac{E_{b}}{N_{0}}}\right) \tag{22}
\end{equation*}
$$

where erfc ( ) denotes the complementary error function, $E_{b} / N_{0}$ is the energy-to-noise-density ratio, and $\xi$ is a parameter that depends upon $h$ and the product of $T_{b}$ and the noise bandwidth, $B$. The best performance in white Gaussian nolse results when $h \simeq 0.7$ and $B T_{b}=1$. The corresponding value of $\xi$, obtained by fitting equation (22) to the theoretical curve, is approximately 0.75. In contrast, equation (22) with $\xi=0.78$ gives $P(E)$ for a coherent FSK system with a minimum correlation coefficient. ${ }^{4}$

Although the frequency of a CPFSK signal varies, its compact spectrum allows it to be considered a single-channel modulation for which there is only a single carrier frequency between hops. It follows from equation (22) with $\mathrm{BT}_{\mathrm{b}}=1$ that the channel bit error probability for a frequency-hopping system with binary CPFSK is

$$
\begin{equation*}
P_{b}=\frac{J}{2 M} \operatorname{erfc}\left(\sqrt[\xi]{\frac{R_{s}}{N_{t}+N_{j}}}\right)+\frac{1}{2}\left(1-\frac{J}{M}\right) \operatorname{erfc}\left(\xi \sqrt{\frac{R_{s}}{N_{t}}}\right) . \tag{23}
\end{equation*}
$$

Applications of equation (23) with $\xi=0.75$ (instead of eq (7)) yield wirst-case performances for frequency-hopping systems with limiter-discriminator demodulation that are typically on the order of 4 dB better than the performances of analogous systems with envelopedetector demodulation. Figure 17 illustrates the potential performances against optimal partial-band jamming when the concatenated codes of figure 16 are used with CPFSK and limiter-discriminator demodulation. The improvement increases with the number of inner-code repetitions.

The potental performance of an FH/CPFSK system is significantly degraded in practice by the effects of frequency-hopping transitions, which were ignored in deriving equation (23). The degradation becomes more prounounced as the hopping period decreases. Nevertheless, CPFSK appears to be the most attractive choice for the data modulation of most frequency-hopping systems.

[^6]

Figure 17. Worst-case performance for limiter-discriminator demodulation and concatenated codes with outer convolutional code ( $K=7, r=$ 1/2), inner repetition code, hard inner decisions, and soft outer decisions.


## LITERATURE CITED

(1) D. J. Torrieri, Principles of Military Commication Systems, Artech House, Dedham, MA (1981).
(2) B. K. Levitt and J. K. Omura, Coding Tradeoffs for Improved Performance of FH/MFSK Systems in Partial Band Noise, National Telecommunications Conference, 2 (1981), D.9.1.
(3) A. J. Viterbi and I. M. Jacobs, Advances in Coding and Modulation for Noncoherent Channels Affected by Fading, Partial Band, and Multiple-Access Interference, in A. J. Viterbi, ed., Advances in Comunication Systems, 4, Academic Press, Inc., New York (1975).
(4) S. Haykin, Communication Systems, John Wiley \& Sons, Inc., New York (1978).
(5) R. F. Pawula, On the Theory of Error Rates for Narrow-Band Digital FM, IEEE Trans. Communications, 29 (November 1981), 1634.

APPENDIX A.--ERROR PROBABILITIES OF ENCODED SYSTEMS

In this appendix, the basic facts of coding theory ${ }^{1-3}$ are summarized and used to derive equations for the error probabilities of encoded systems.

## A-1. BLOCK CODES

In digital communication systems using block codes, information is transmitted as blocks of symbols called codewords. Each symbol is selected from an alphabet of possible symbols. In binary communications, the two possible symbols are the logical "one" and the logical "zero." If each of the codewords can be expressed as linear algebraic sums of linearly independent code vectors (sequences having the same length as the codewords), the code is called a linear block code. For binary data, the code bits generated by a linear block code are modulotwo sums of the information bits. A systematic block code is a code in which the information symbols appear unchanged in the codeword, which also has additional parity symbols. The code rate is defined as the ${ }^{-}$ ratio of information symbols to the total number of symbols in a codeword.

The Hamming distance between two sequences with an equal number of symbols is defined as the number of positions in which the symbol of one sequence differs from the corresponding symbol of the other sequence. The minimum Hamming distance between any two possible codewords is called the minimum distance of the code.

After the waveform representing a codeword is received and demodulated, the decoder uses the demodulator output to determine the information symbols corresponding to the codeword. If the demodulator produces a sequence of discrete symbols and the decoding is based on these symbols, the process is called hard limiting or a hard decision. Conversely, if the decoding is based on analog or multilevel quantized samples of the waveform, the process is called soft limiting or a soft decision. The advantage of soft-decision decoding is that reliability or quality indicators are used in making the decisions.

When hard decisions are made, a maximum-likelihood decoder assumes that the correct codeword is the one that differs in the least number of positions from the demodulator output sequence. Correct decoding occurs if the number of incorrect symbols in the demodulator output is less

[^7]than half the ninimum distance, $d$, between codewords. For some codes, it is possible to decode correctly in some cases where the number of errors exceeds $d / 2$ because of the sparseness of the codewords in the vector space. By ignoring this possibility, we can bound the probability of error in a decoded word, which is denoted by $P_{w}$. In a ( $c, w$ ) block code, c code symbols represent $w$ information symbols. We assume the statistical independence of errors in demodulated code symbols, which can often be ensured, if necessary, by appropriate symbol interleaving. Since there are $\binom{c}{i}$ distinct ways in which $i$ errors may occur among c symbols,
\[

$$
\begin{equation*}
P_{w} \leq \sum_{i=[(d+1) / 2]}^{c}\binom{c}{i} p_{s}^{i}\left(1-p_{s}\right)^{c-i} \tag{A-1}
\end{equation*}
$$

\]

where $[x]$ denotes the largest integer less than or equal to $x$, and $p_{s}$ is the channel symbol error probability, which is the probability of error in a demodulated code symbol. The tightness of this bound depends upon the decoding algorithm. If the algorithm makes no attempt to correct $[(d+1) / 2]$ or more errors, then $P_{w}$ is equal to the bound.

A perfect code is a block code such that every c-symbol sequence is at a distance of at most $\varepsilon$ from some c-symbol codeword, and the sets of all sequences at distance $\varepsilon$ from each codeword are disjoint. Therefore, perfect codes correct exactly $\varepsilon=(d-1) / 2$ errors, where $d$ is odd, and fail to correct more than $\varepsilon$ errors. Assuming the independence of symbol errors, we can replace inequality (A-1) with

$$
\begin{equation*}
P_{w}=\sum_{i=(d+1) / 2}^{c}\binom{c}{i} P_{s}^{i}\left(1-p_{s}\right)^{c-i} \tag{A-2}
\end{equation*}
$$

The only known perfect binary codes are the Hamming codes, repetition codes of odd length, and the Golay $(23,12)$ code. In a Hamming ( $c, w$ ) code, the numbers of code bits and information bits are related by $c=2^{c-w}-1$. Since $d=3$ for Hamming codes, they are capable of correcting all single errors and detecting two or fewer errors. Equation (A-2) applies with $P_{s}=P_{b}$, where $P_{b}$ is the channel bit error probability, which is the probability of error in a demodulated code bit.

Repetition codes have one information bit represented by code bits. For hard-decision decoding, $c$ is odd and the decoder decides the logical state of the information bit according to the states of the majority of the demodulated bits. Thus, the decoder can correct all combinations of ( $c-1$ )/2 or fewer errors, but no patterns of more errors. In this case, $P_{w}$ is the probability of error in a decoded information bit, which is denoted by $P_{i b}$. Since $d=c$, equation (A-2) becomes

$$
\begin{equation*}
P_{i b}=\sum_{i=(c+1) / 2}^{c}\binom{c}{i} P_{b}^{i}\left(1-p_{b}\right)^{c-i} \tag{A-3}
\end{equation*}
$$

The Golay $(23,12)$ code has $d=7$ and, thus, can correct three bit errors. The extended Golay (24,12) code is formed by adding an overall parity bit to the perfect Golay $(23,12)$ code, thereby increasing the minimum distance to $d=8$. As a result, three or fewer errors can always be corrected and one-sixth of the code vectors with four errors can be corrected.l Five or more errors are never corrected. Thus, assuming the independence of bit errors, the word error probability for the extended Golay code is

$$
P_{W}=\frac{5}{6}\binom{24}{4} P_{b}^{4}\left(1-P_{b}\right)^{20}+\sum_{i=5}^{24}\binom{24}{i} P_{b}^{i}\left(1-P_{b}\right)^{24-i} \quad(A-4)
$$

The extended Golay $(24,12)$ code is usually preferable to the Golay $(23,12)$ code, which usually gives a slightly better performance in the presence of white Gaussian noise, because it allows a less complex decoding implementation and it has a code rate of exactly one-half, which simplifies the system timing. The design of an extended Golay decoder may be simplified if no attempt is made to correct four errors. In this case, equation (A-4) must be replaced by inequality ( $A-1$ ) with $c=24, d=8$, and $P_{s}=P_{b}$.

The most important nonbinary block codes are probably the ReedSolomon codes, 2,3 which provide the largest possible minimum code distance of any linear code with specified values of $c$ and w. A ReedSolomon code has an alphabet of $2^{m}$ symbols and $c=2^{m}-1$ symbols per codeword, where $m$ is the number of bits per symbol. If the codeword represents $w$ information symbols, the minimum distance is $d=c-w+$ 1. Since the Reed-Solomon codes are not perfect codes, inequality (A-1) applies to hard-decision decoding.

To compare codes with different numbers of information symbols represented by the codewords, we need the probability of an information symbol error, $P_{i g}$, at the output of the decoder. Since not every word error results in a symbol error, $P_{i s} \leq P_{w}$. Since for every inear block code there exists a systematic linear block code that is equivalent in performance, 1.3 practical block codes are usually systematic
${ }^{1}$ A. J. Viterbi and J. K. Omura, Principles of Digital Communication and Coding, McGraw-Hill Book Co., New York (1979).
${ }^{2}$ G. C. Clark and J. B. Cain, Error-Correction Coding for Digital Communications, Plenum Press, New York (1981).
${ }^{3}$ W. W. Peterson and E. J. Weldon, Error-Correcting Codes, 2nd ed., The MIT Press, Cambridge, MA (1972).

## APPENDIX A

and, thus, systematic codes are assumed in the subsequent analysis. Given that a word error occurred, the probability of an information symbol error for a systematic code is the same as the probability of error in any symbol of the codeword. The latter probability is at least d/c because an incorrectly chosen codeword is at least a distance d from the correct codeword, assuming that the decoder attempts to decode all possible received sequences. Thus,

$$
\begin{equation*}
\frac{d}{c} P_{w} \leq P_{i s} \leq P_{w} \tag{A-5}
\end{equation*}
$$

Since an incorrectly chosen codeword is often exactly a distance d from the correct codeword, the lower bound is usually tight unless $P_{w}$ is large.

Consider practical codes for which $P_{w}$ is given approximately or exactly by equation (A-2). Let $A(i)$ denote the event that $i$ symbol errors occur in a demodulated word of $c$ code symbols at the decoder input. Then $P_{i s}$ is equal to the summation over $i$ of the product of the probability of $A(i)$ and the probability of an error in a decoded information symbol given $A(i)$. For $[(d+1) / 2] \leq i \leq d$, the latter probability is approximated by $d / c$; for $d<i \leq c$, it is approximated by i/c, the probability of an error in a demodulated code symbol at the decoder input given $A(i)$. Therefore, for hard-decision decoding,

$$
\begin{equation*}
P_{i s}=\frac{d}{c} \sum_{i=[(d+1) / 2]}^{d}\binom{c}{i} p_{s}^{i}\left(1-P_{s}\right)^{c-i} \tag{A-6}
\end{equation*}
$$

$$
+\frac{1}{c} \sum_{i=d+1}^{c} i\binom{c}{i} p_{s}^{i}\left(1-p_{s}\right)^{c-i}
$$

The right-hand side of this equation is always within the bounds of inequality $(A-5)$ and gives $P_{i s}=1$ when $P_{s}=1$, as desired.

For binary communications, $P_{\text {is }}$ is equal to the probability of an information bit error, $\mathrm{P}_{\mathrm{ib}}$. Thus,

$$
\begin{align*}
P_{i b}= & \frac{d}{c} \sum_{i=[(d+1) / 2]}^{d}\binom{c}{i} p_{b}^{i}\left(1-P_{b}\right)^{c-i}  \tag{A-7}\\
& +\frac{1}{c} \sum_{i=d+1}^{c} i\binom{c}{i} p_{b}^{i}\left(1-p_{b}\right)^{c-1} .
\end{align*}
$$

For repetition codes, equation (A-7) reduces to equation ( $A-3$ ), as desired. Equation (A-7) and the bounds of inequality (A-5) are compared in figure A-1 for the Golay $(23,12)$ code.


Figure A-1. Information bit error probability as function of channel bit error probability for Golay $(23,12)$ code.

In nonbinary communications, an information symbol represents $m$ information bits. We assume that an incorrectly decoded information 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. Thus, when there are $2^{m}-1$ equally likely incorrect symbols,

$$
\begin{equation*}
P_{i b}=\frac{2^{m-1}}{2^{m}-1} P_{i s} \tag{A-8}
\end{equation*}
$$

For Reed-Solomon codes, equations $(A-6)$ and $(A-8)$ and $c=2^{m}-1$ imply that

APPENDIX A

$$
\begin{aligned}
P_{i b} & =\frac{c+1}{2 c^{2}}\left[d \sum_{i=\left[\left(\frac{d+1}{d}\right) / 2\right]}^{d}\binom{c}{i} p_{s}^{i}\left(1-p_{s}\right)^{c-i}\right. \\
& \left.+\sum_{i=d+1}^{c} i\binom{c}{i} p_{s}^{i}\left(1-p_{s}\right)^{c-i}\right]
\end{aligned}
$$

for hard-decision decoding.
The Hamming weight of a codeword is defined as the number of nonzero symbols in a codeword. For binary codes, the Hamming weight is the number of ones in a codeword. The set of Hamming distances from a given binary codeword to the other valid codewords is the same for all codewords.1,3 since the set of distances from the all-zero codeword is the same as the set of weights of the nonzero codewords, the set of weights is equivalent to the set of distances. Analytical expressions for the weight distribution are known for the Hamming and Reed-Solomon codes. 2,3 The weight distributions of other codes can be determined by examining all $2^{W}$ valid codewords if $w$, the number of information bits, is not too large. The weight distribution of the Golay codes is listed in table A-1.

TABLE A-1. WEIGHT DISTRIBUTION OF GOLAY CODES

| Weight | Number of codewords |  |
| :---: | :---: | :---: |
|  | $(23,12)$ code | $(24,12)$ code |
| 0 | 1 | 1 |
| 7 | 253 | 0 |
| 8 | 506 | 759 |
| 11 | 1288 | 0 |
| 12 | 1288 | 2576 |
| 15 | 506 | 0 |
| 16 | 253 | 759 |
| 23 | 1 | 0 |
| 24 | 0 | 1 |
|  | 4096 | 4096 |

[^8]A soft-decision decoder makes decisions by selecting the largest of the cumulative metrics, which are measures of the likelihoods of codewords. An upper bound for $P_{w}$ follows from fundamental considerations. Because of the countable subadditivity of probability measures, the probability of a finite or countable union of events $A_{n}, n=1$, 2 , . . ., satisfies

$$
\begin{equation*}
P\left(\bigcup_{n} A_{n}\right) \leq \sum_{n} P\left(A_{n}\right) \tag{A-10}
\end{equation*}
$$

In communication theory, a bound obtained from this inequality is called a union bound. Let $N(\delta)$ denote the number of codewords having weight $\delta$. Let $Q(\delta)$ denote the probability that the cumulative metric for an incorrect codeword at distance $\delta$ from the correct codeword exceeds the cumulative metric for the correct codeword. The union bound and the relation between weights and distances imply that

$$
\begin{equation*}
\mathrm{P}_{\mathrm{w}} \leq \sum_{\delta} \mathrm{N}(\delta) Q(\delta), \tag{A-11}
\end{equation*}
$$

where the summation is over all values of $\delta$ for which there are valid codewords. Metrics are defined so that $Q\left(\delta_{1}\right) \leq Q\left(\delta_{2}\right)$ if $\delta_{1} \geq \delta_{2}$. Thus, in terms of the minimum distance, $d$, we have the much weaker bound

$$
\begin{equation*}
P_{w} \leq(v-1) Q(d) \tag{A-12}
\end{equation*}
$$

where $v$ is the number of valid codewords. This bound is useful when the only known parameter of a code is the minimum distance between codewords. The bound is tight if the distances from a given codeword are all close to d.

For a repetition code, $P_{i b}=Q(c)$, where $c$ may be even or odd for soft-decision decoding. In other cases, approximate expressions for $P_{i b}$ and $P_{\text {is }}$ can be obtained by combining inequality ( $A-11$ ) or (A-12) with the lower bound of inequality $(A-5)$ and equation (A-8). For example, using table A-1, we obtain

$$
\begin{equation*}
P_{i b}=\frac{1}{3}[759 Q(8)+2576 Q(12)+759 Q(16)+Q(24)] \tag{A-13}
\end{equation*}
$$

for the extended Golay (24,12) code.

## APPENDIX A

## A-2. CONVOLUTIONAL CODES

A convolutional encoder converts an input of $b$ information symbols into an output of $v$ code symbols that are a function of both the current input and preceding information symbols. A convolutional encoder can be implemented with a shift register and linear logic. The outputs of selected register stages are added modulo-two to form the code symbols. After $b$ symbols are shifted into the register and b symbols are shifted out, a commutating switch reads out $v$ code symbols in sequence. The code rate, which is the ratio of input symbols to output symbols, is $r=b / v$. The constraint length, $K$, is defined as the total number of shift register stages in the encoder.

We assume that a Viterbi decoder is used to generate the information bits in the receiver. Let $a(\delta, i)$ denote the number of paths diverging at a node from the correct path, having Hamming distance $\delta$ and $i$ information symbol errors over the unmerged segment. Let $d_{f}$ denote the mininum free distance, which is the minimum distance of any unmerged segment from the correct path. Let $Q(\delta)$ denote the probability of an error in comparing the correct path segment with a path segment that differs in $\delta$ symbols. From the union bound, it can be shown that the probability of an information symbol error after Viterbi decoding is bounded by ${ }^{1,2}$

$$
\begin{equation*}
P_{i s} \leq \frac{1}{b} \sum_{i=1}^{\infty} \sum_{\delta=d_{f}}^{\infty} i a(\delta, i) Q(\delta) \tag{A-14}
\end{equation*}
$$

For binary codes, $P_{i s}$ is equal to the probability of an information bit error, $\mathrm{P}_{\mathrm{ib}}$.

Among the convolutional codes of a given code rate and constraint length, the one with the best distance properties can sometimes be determined by a complete computer search. After elimination of the catastrophic codes, for which a finite number of demodulated bit errors can cause an infinite number of decoded information bit errors, the codes with the largest value of $d_{f}$ are selected. Then the values of the total information weights,

$$
\begin{equation*}
A(\delta)=\sum_{i=1}^{\infty} i a(\delta, i), \delta \geq d_{f} . \tag{A-15}
\end{equation*}
$$

[^9]are examined for each of the selected codes. All codes that do not have the minimum value of $A\left(d_{f}\right)$ are eliminated. If more than one code remains, codes are eliminated on the basis of the minimal values of $A\left(d_{f}+\right.$ 1), $A\left(d_{f}+2\right)$, . .. until one code remains. For binary codes of rate $1 / 2$ and rate $1 / 3$ and constraint lengths up to 9 and 8 , respectively, the optimal codes have been determined. ${ }^{4}$ For these codes, table A-2 lists the corresponding values of $d_{f}$ and $A\left(d_{f}+i\right), i=0,1, \ldots, \ldots$. In terms of $A\left(d_{f}+i\right)$, equation $(A-14)$ becomes
\[

$$
\begin{equation*}
P_{i s} \leq \frac{1}{b} \sum_{i=0}^{\infty} A\left(d_{f}+i\right) Q\left(d_{f}+i\right) \tag{A-16}
\end{equation*}
$$

\]

TABLE A-2. PARNMETK:R VALUES FOR BEST CONVOLUTIONAL CODES

| Code |  | $d_{\text {f }}$ | $\boldsymbol{A}\left(\mathbf{d}_{\mathbf{E}}\right)$ | $A\left(d_{f}+1\right)$ | $\boldsymbol{A}\left(d_{1}+2\right)$ | $A\left(d_{t}+3\right)$ | $A\left(d_{t}+4\right)$ | $A\left(d_{f}+5\right)$ | $A\left(d_{f}+6\right)$ | $\lambda\left(d_{f}+7\right)$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| E | $\underline{7}$ |  |  |  |  |  |  |  |  |  |
| 3 | 1/2 | 5 | 1 | 4 | 12 | 32 | 80 | 192 | 448 | 1024 |
| 4 | $1 / 2$ | 6 | 2 | 7 | 18 | 49 | 130 | 333 | 836 | 2069 |
| 5 | 1/2 | 7 | 4 | 12 | 20 | 72 | 225 | 500 | 1.324 | 3680 |
| 6 | 1/2 | 8 | 2 | 36 | 32 | 62 | 332 | 701 | 2,342 | 5503 - |
| 7 | 1/2 | 10 | 36 | 0 | 211 | 0 | 1404 | 0 | 11.633 | 0 |
| 8 | 1/2 | 10 | 2 | 22 | 60 | 148 | 340 | 1008 | 2,642 | 6748 |
| 9 | 1/2 | 12 | 33 | 0 | 281 | 0 | 2179 | 0 | 15,035 | 0 |
| 3 | 1/3 | 8 | 3 | 0 | 15 | 0 | 58 | 0 | 201 | 0 |
| 4 | 1/3 | 10 | 6 | 0 | 6 | 0 | 58 | 0 | 118 | 0 |
| 5 | 1/3 | 12 | 12 | 0 | 12 | 0 | 56 | 0 | 320 | 0 |
| 6 | 1/3 | 13 | 1 | 8 | 26 | 20 | 19 | 62 | 86 | 204 |
| 7 | 1/3 | 14 | 1 | 0 | 20 | 0 | 53 | 0 | 184 | 0 |
| 8 | 1/3 | 16 | 1 | 0 | 24 | 0 | 113 | 0 | 287 | 0 |

If a binary code is used and the Viterbi decoder makes a hard decision on each demodulator output bit, an exact expression for $Q(\delta)$ can be written. When the correct path is compared with an incorrect one, correct decoding results if the number of incorrect bits in the demodulator output is less than half the number of bits in which the two paths differ. If the number of incorrect bits is exactly half the number of differing bits, then either of the two paths is chosen with equal probability. Assuming the independence of bit errors, it follows that


[^10]where $P_{b}$ is the probability of error in choosing between the correct bit and an incorrect one.

It is shown below that when soft decisions are made, $Q(\delta)$ can often be bounded by a function of the form

$$
Q(\delta) \leq \alpha z^{\delta}
$$

where $\alpha$ and $z$ are independent of $\delta$. Inequalities ( $A-16$ ) and -18 ) imply that

$$
\begin{equation*}
P_{i s} \leq \frac{a}{b} \sum_{i=0}^{\infty} A\left(d_{f}+i\right) z^{d_{f}+i} \tag{A-19}
\end{equation*}
$$

In principle, $A(\delta)$ can be determined from the augmented generating function, $T(D, I)$, which depends upon the structure of the convolutional code. 1,2 An expansion of the augmented generating function has the form

$$
\begin{equation*}
T(D, I)=\sum_{i=1}^{\infty} \sum_{\delta=d_{f}}^{\infty} a(\delta, i) D^{\delta} I^{i} \tag{A-20}
\end{equation*}
$$

The derivative at $I=1$ is

$$
\begin{align*}
\left.\frac{\partial T(D, I)}{\partial I}\right|_{I=1} & =\sum_{i=1}^{\infty} \sum_{\delta=d_{f}}^{\infty} i a(\delta, i) D^{\delta}  \tag{A-21}\\
& =\sum_{i=0}^{\infty} A\left(d_{f}+i\right) D^{d_{f}+i}
\end{align*}
$$

Thus, the bound for $P_{\text {is }}$, given by inequality ( $A-16$ ), is determined by substituting $Q(\delta)$ in place of $D^{\delta}$ in this expansion and multiplying the result by 1/b. For soft-decision decoding, equation (A-21) and inequality (A-19) imply that

[^11]\[

$$
\begin{equation*}
P_{1 s} \leq\left.\frac{\alpha}{b} \frac{\partial T(D, I)}{\partial I}\right|_{I=1, D=Z} \tag{A-22}
\end{equation*}
$$

\]

Closed-form expressions for $T(D, I)$ are known for the orthogonal and the dual-k convolutional codes. The encoder for an orthogonal convolutional code of constraint length $K$ generates one of $2^{K}$ orthogonal binary sequences of lenath $v=2^{K}$ for each input bit. Thus, the rate of the code is $2^{-K}$. The augmented generating function can be shown to bel

$$
\begin{equation*}
T(D, I)=\frac{I D^{K v / 2}\left(1-D^{V / 2}\right)}{1-D^{V / 2}\left\{1+I\left[1-D^{(v / 2)(K-1)}\right]\right\}} . \tag{A-23}
\end{equation*}
$$

Differentiation yields

$$
\begin{equation*}
\left.\frac{\partial T(D, I)}{\partial I}\right|_{I=1}=\frac{D^{K v / 2}\left(1-D^{v / 2}\right)^{2}}{\left(1-2 D^{v / 2}+D^{K v / 2}\right)^{2}} \tag{A-24}
\end{equation*}
$$

Since $b=1$ and $P_{i s}=P_{i b}$, equation (A-24) and inequality (A-22) give

$$
\begin{equation*}
P_{i b} \leq a \frac{z^{K v / 2}\left(1-z^{v / 2}\right)^{2}}{\left(1-2 z^{v / 2}+z^{K v / 2}\right)^{2}}, v=2^{K} \tag{A-25}
\end{equation*}
$$

for soft-decision decoding.
To determine $P_{i b}$ for hard-decision decoding, we must first expand equation (A-24) in powers of $D$ because equation (A-17) does not have the form of inequality (A-18). We use the identity

$$
\begin{equation*}
[1-(x+y)]^{-2}=\sum_{n=1}^{\infty} n(x+y)^{n-1}=\sum_{n=1}^{\infty} n \sum_{i=0}^{n-1}\binom{n-1}{i} x^{i} y^{n-i-1} \tag{A-26}
\end{equation*}
$$

and substitute $Q(\delta)$ in place of $D^{\delta}$. The result is

$$
\begin{align*}
P_{i b} \leq & \sum_{n=1}^{\infty} n \sum_{i=0}^{n-1}\binom{n-1}{i}(-1)^{i} 2^{n-i-1}\left\{Q\left[2^{K-1}(n-i-1+K i+K)\right]\right.  \tag{A-27}\\
& \left.-2 Q\left[2^{K-1}(n-i+K i+K)\right]+Q\left[2^{K-1}(n-i+1+K i+K)\right]\right\}
\end{align*}
$$

where Q[ ] is given by equation (A-17).

[^12]
## APPENDIX A

A dual-k code is a nonbinary convolutional code. The encoder shifts one k-bit information symbol at a time into a shift register of $2 k$ binary stages (two symbol stages). For each information symbol, a rate $1 / v$ encoder generates $v$ code symbols. Each code symbol is one of $2^{k}$ possible symbols and may be transmitted as one of $2^{k}$ modulated signals.

Among the dual-k codes, the codes with the best distance properties can be shown to have ${ }^{5}$

$$
\begin{equation*}
T(D, I)=\frac{\left(2^{k}-1\right) D^{2 v} I}{1-I\left[v D^{v-1}+\left(2^{k}-1-v\right) D^{V}\right]} . \tag{A-28}
\end{equation*}
$$

which implies that

$$
\begin{equation*}
\left.\frac{\partial T(D, I)}{\partial I}\right|_{I=1}=\frac{\left(2^{k}-1\right) D^{2 v}}{\left[1-v D^{v-1}-\left(2^{k}-1-v\right) D^{v}\right]^{2}} \tag{A-29}
\end{equation*}
$$

Analogously to equation (A-8), the probability of an information bit error is related to the probability of an information symbol error by

$$
\begin{equation*}
P_{i b}=\frac{2^{k-1}}{2^{k}-1} P_{i s} \tag{A-30}
\end{equation*}
$$

For soft-decison decoding, equations (A-29) and (A-30) and inequality (A-22) with $b=1$ give

$$
\begin{equation*}
P_{i b} \leq \frac{\alpha 2^{k-1} z^{2 v}}{\left[1-v z^{v-1}-\left(2^{k}-1-v\right) z^{v}\right]^{2}} \tag{A-31}
\end{equation*}
$$

## A-3. SOFT-DECISION DECODING

The function $Q(\delta)$ can be defined in general as the probability that the cumulative metric for an incorrect sequence at distance $\delta$ from the correct sequence exceeds the cumulative metric for the correct sequence. For block codes, the sequence is a codeword; for convolutional codes, the sequence is a path segment. In soft-decision decoding, the sequence with the largest associated metric is converted into the decoded output. Let $m_{0}(k, L)$ denote the value of the cumulative metric associated with sequence $k$ of length $L$. To derive inequality (A- 18), we consider additive metrics of the form

[^13]\[

$$
\begin{equation*}
m_{0}(k, L)=\sum_{i=1}^{L} m_{1}(k, i) \tag{A-32}
\end{equation*}
$$

\]

where $m_{1}(k, i)$ is the symbol metric determined from code symbol i. Let $k$ $=1$ label the correct sequence and $k=2$ label an incorrect one at distance $\delta$. By suitably relabeling the $\delta$ symbol metrics that may differ for the two sequences, we obtain

$$
\begin{align*}
Q(\delta) & =P\left[m_{0}(2, L)>m_{0}(1, L)\right] \\
& =P\left[\sum_{i=1}^{\delta}\left[m_{1}(2, i)-m_{1}(1, i)\right]>0\right] . \tag{A-33}
\end{align*}
$$

where $P[A]$ denotes the probability of event $A$. The right-hand side of this equation can be bounded by the inequalities of appendix $C$. We obtain

$$
\begin{equation*}
Q(\delta) \leq \alpha \min _{0<s<s_{1}} E\left[\exp \left\{s \sum_{i=1}^{\delta}\left[m_{1}(2, i)-m_{1}(1, i)\right]\right\}\right] . \tag{A-34}
\end{equation*}
$$

If inequalities ( $C-8$ ) and ( $C-9$ ) are satisfied, which is the usual case in practice, then inequality (A-34) represents the Chernoff-Jacobs bound and $\alpha=1 / 2$; otherwise, inequality ( $A-34$ ) represents the Chernoff bound and $\alpha=1$. The assumption that the $m_{1}(2, i)-m_{1}(1, i), i=1$, 2, . . .. $\delta$, are independent, identically distributed random variables and the definition

$$
\begin{equation*}
z=\min _{0<s<s_{1}} E\left[\exp \left\{s\left[m_{1}(2, i)-m_{1}(1, i)\right]\right\}\right] \tag{A-35}
\end{equation*}
$$

yleld

$$
\begin{equation*}
Q(\delta) \leq \alpha z^{\delta} \tag{A-36}
\end{equation*}
$$

The assumptions required to establish this inequality are reasonable in most practical cases, especially when symbol interleaving is used.

Calculations for specific communication systems operating in white Gaussian noise have shown that soft-decision decoding gives a superior
performance relative to hard-decision decoding. Approximately 2 dB of additional signal power is required for a hard-decision receiver to produce the same error rates as the corresponding soft-decision receiver. However, soft-decision systems are much more complex to implement and may be too slow for the processing of high information rates. Quantization is necessary in soft-decision receivers because digital computations are perforned in the decoders. Since the appropriate quantization levels depend on the signal, thermal noise, and interference levels, automatic gain control is required. Finally, when the interference is not similar to white Gaussian noise and has unknown parameters, the appropriate soft-decision metric is of ten difficuit to determine, may be a function of the signal level, and may not yield a significant performance advantage relative to hard-decision systems.

## onconerionomoresemoncones

## LITERATURE CITED

(1) A. J. Viterbi and J. K. Omura, Principles of Digital Commanication and Coding, McGraw-Hill Book Co., New York (1979).
(2) G. C. Clark and J. B. Cain, Error-Correction Coding for Digital Communications, Plenum Press, New York (1981).
(3) W. W. Peterson and E. J. Weldon, Error-Correcting Codes, 2nd ed., The MIT Press, Cambridge, MA (1972).
(4) J. P. Odenwalder, Optimal Decoding of Convolutional Codes, Doctoral Dissertation, University of California at Los Angeles (1970).
(5) J. P. Odenwalder, Dual-k Convolutional Codes for Noncoherently Demodulated Channels, International Telemetering Conference (1976), 165.

APPENDIX B.--SOFT-DECISION DECODING FOR FREQUENCY-HOPPING SYSTEMS

Figure B-1 depicts a noncoherent frequency-hopping multiple frequency-shift keying (FH/MFSK) receiver that implements soft decisions. After the dehopping, the received signal passes through an MFSK demodulator. The detector outputs are sampled once every code symbol. After each sampling time, the appropriate quantized sample value is added to the stored values in one or more accumulators in the decoder. When block codes are used, each accumulator is associated with a possible codeword. All the code symbols in a received sequence are sampled, and then the final accumulator outputs, which are called the cumulative metrics, are compared. The codeword associated with the largest metric value is then converted into the decoded output. When convolutional codee are used, each cumulative metric is associated with a particular code path. The decoded output is the sequence corresponding to the path having the largest cumulative metric.


Figure B-1. FH/MFSK receiver with soft-decision decoding.

Let $R_{k i}$ represent the $i$ th quantized sample value that enters accumulator $k$. We consider the cumulative metric defined by

$$
\begin{equation*}
m_{0}(k, L)=\sum_{i=1}^{L} R_{k i}^{2}, \tag{B-1}
\end{equation*}
$$

where $L$ is the number of samples used. This metric is chosen because it is mathematically tractable and it is known to be optimal for Rayleigh fading.

To apply the general coding results of appendix $A$, we must evaluate $Z$, which is defined in equation (A-35). In the subsequent analysis, the degradation due to imperfect quantization is neglected. Let $\mathrm{R}_{1 i}$ denote a sample value from the detector that receives the intended signal plus noise and interference. Let $R_{2 i}$ denote a sample value from a detector
that receives only noise and interference, which are approximated by band-limited white Gaussian processes. Suppose that an intended signal with power $R_{s}$ and form

$$
\begin{equation*}
s_{1}(t)=\sqrt{2 R_{s}} \cos \omega t \tag{B-2}
\end{equation*}
$$

is received during each hop. It is shown elsewhere that

$$
\begin{align*}
& R_{1 i}^{2}=z_{1 i}^{2}+z_{2 i}^{2} \\
& R_{2 i}^{2}=z_{3 i}^{2}+z_{4 i}^{2} \tag{B-3}
\end{align*}
$$

where the $z_{n i}, n=1,2,3,4$, are independent Gaussian random variables. The expected values are

$$
\begin{align*}
& E\left[z_{1 i}\right]=\sqrt{2 R_{s}} \\
& E\left[z_{2 i}\right]=E\left[z_{3 i}\right]=E\left[z_{4 i}\right]=0 \tag{B-4}
\end{align*}
$$

The variances are

$$
\begin{align*}
& \operatorname{VAR}\left(z_{1 i}\right)=\operatorname{VAR}\left(z_{2 i}\right)=N_{1} \\
& \operatorname{VAR}\left(z_{3 i}\right)=\operatorname{VAR}\left(z_{4 i}\right)=N_{2},
\end{align*}
$$

where $N_{1}$ is the total noise power (thermal noise plus interference) accompanying the signal and $N_{2}$ is the total noise power in the other detector output. The conditions for the Chernoff-Jacobs bound with $s_{0}$ > 0 (see app C) are satisfied by $\sum_{i} R_{2 i}^{2}-R_{1 i}^{2}$.

We assume that $R_{1 i}^{2}$ and $R_{2 i}^{2}$ are statistically independent of each other and from hop to hop, that is, for all values of i. Then equation (A-35) becomes

[^14]\[

$$
\begin{equation*}
\mathrm{z}=\min _{0<s<s_{1}} \mathrm{E}\left[\exp \left(s R_{2 i}^{2}\right)\right] \mathrm{E}\left[\exp \left(-s R_{1 i}^{2}\right)\right] \tag{B-6}
\end{equation*}
$$

\]

where $s_{1}$ is the largest value of $s$ for which the expected values remain finite. For a Gaussian random variable $X$ with mean $m$ and variance $\sigma^{2}$, a direct calculation yields

$$
\begin{equation*}
E\left[\exp \left(s x^{2}\right)\right]=\frac{1}{\sqrt{1-2 s \sigma^{2}}} \exp \left(\frac{s m^{2}}{1-2 s \sigma^{2}}\right) \quad, \quad s<\frac{1}{2 \sigma^{2}} \tag{B-7}
\end{equation*}
$$

Using equations ( $B-3$ ) to ( $B-5$ ) and ( $B-7$ ) in equation ( $B-6$ ), we can evaluate the conditional expectations given the values of $N_{1}$ and $N_{2}$. Substituting $\lambda=\mathbf{2 s N _ { 1 }}$, we obtain

$$
z=\min _{0<\lambda<N_{1} / N_{2}} C(\lambda)
$$

where

$$
C(\lambda)=E\left\{\frac{\exp \left[\left(\frac{\lambda}{1+\lambda}\right) \frac{R_{s}}{N_{1}}\right]}{(1+\lambda)\left(1-\frac{\lambda N_{2}}{N_{1}}\right)}\right\}, 0<\lambda<\frac{N_{1}}{N_{2}},
$$

and the expected value is with respect to $N_{1}$ and $N_{2}$.
There are four possible values of the pair $\left(N_{1}, N_{2}\right)$, depending upon which of the two detectors are jammed. For $J$ jammed channels out of $M$ total channels, the associated probabilities, $P[$ ], are derived from elementary combinatorial analysis. The results are

$$
\begin{align*}
& P\left[N_{1}=N_{2}=N_{t}\right]=\frac{\binom{M-2}{J}}{\binom{M}{J}} F(0, M-2),  \tag{B-10}\\
& P\left[N_{1}=N_{t}+N_{j}, N_{2}=N_{t}\right]=\frac{\binom{M-2}{J}}{\binom{M}{J}} F(1, M-1),  \tag{B-11}\\
& P\left[N_{1}=N_{t}, N_{2}=N_{t}+N_{j}\right]=\frac{\binom{M-2}{J}}{\binom{M}{J}} F(1, M-1), \tag{B-12}
\end{align*}
$$

$$
\begin{equation*}
P\left[N_{1}=N_{2}=N_{t}+N_{j}\right]=\frac{\binom{M-2}{J-2}}{\binom{M}{J}} F(2, M) \tag{B-13}
\end{equation*}
$$

where $N_{t}$ is the thermal and background noise power in a channel, $N_{j}$ is the jamming power in a jammed channel, and

$$
F(a, b)= \begin{cases}1, & a \leq J \leq b  \tag{B-14}\\ 0, & \text { otherwise }\end{cases}
$$

Combining equations ( $B-9$ ) to ( $B-14$ ) gives

$$
\begin{aligned}
& C(\lambda)= \frac{\binom{M-2}{J} F(0, M-2) \exp \left[\left(\frac{\lambda}{1+\lambda}\right) \frac{R_{s}}{N_{t}}\right]}{\binom{M}{J}\left(1-\lambda^{2}\right)} \\
&+\frac{\binom{M-2}{J-1} F(1, M-1) \exp \left[\left(\frac{\lambda}{1+\lambda}\right) \frac{R_{s}}{N_{t}+N_{j}}\right]}{\binom{M}{J}(1+\lambda)\left(1-\frac{\lambda N_{t}}{N_{t}+N_{j}}\right)} \\
&+\frac{\binom{M-2}{J-1} F(1, M-1) \exp \left[\left(\frac{\lambda}{1+\lambda}\right) \frac{R_{s}}{N_{t}}\right]}{\binom{M}{J}(1+\lambda)\left[1-\frac{1\left(N_{t}+N_{j}\right)}{N_{t}}\right]} \\
&+\frac{\binom{M-2}{J} F(2, M) \exp \left[\left(\frac{\lambda}{1+\lambda}\right) \frac{R_{s}}{N_{t}+N_{j}}\right]}{\binom{M}{J}\left(1-\lambda^{2}\right)}, \\
& 0<\lambda<\frac{N_{t}}{N_{t}+N_{j}}
\end{aligned},
$$

This equation can be expressed in terms of $\mu, M_{u}, N_{t u}$, and $N_{j t}$ by using equations (8) to (11) in the main body of the text. The upper bound on $\lambda$ is the smallest value of $N_{1} / N_{2}$ out of the three possibilities. By using numerical analysis, $\lambda$ can be chosen to minimize $C(\lambda)$, thus providing $z$.

Soft-decision decoding with the metric of equation (B-1) provides a poor performance relative to hard-decision decoding against optimal partial-band jamming. As an example, figure B-2 shows the upper bound of $P_{i b}$ for a dual-k convolutional code and $0 \leq \mu \leq 0.1$. Equations ( $B-15$ ). ( $B-8)$, (8) to (11), and inequality ( $A-31$ ) are applied with $\alpha=1 / 2, k=3, v=4, r_{s}=3 / 4, M_{u}=1000$, and $R_{s} / N_{t u}=20 \mathrm{~dB}$. The graph illustrates the vulnerability of the soft-decision decoding to jamming concentrated over a small portion of the total hopping band.


Figure B-2. Information bit error probability for dual-3 convolutional code ( $v=4$ ), soft-decision decoding, and partial-band jamming.

Decoding errors are primarily due to interference that causes a single term in the summation to dominate the cumulative metric of equation ( $B-1$ ). Clipping the $R_{k i}$ would improve performance, but an effective implementation requires an accurate measurement of the signal power, which is often impractical.

The moment generating function of the random variable $X$ is defined as ${ }^{1}$

$$
\begin{equation*}
M(s)=E\left[e^{s X}\right]=\int_{-\infty}^{\infty} \exp (s x) d F(x) \tag{C-1}
\end{equation*}
$$

for all $s$ for which the integral is finite, where $E[$ ] denotes the expected value, $s$ is a constant, and $F(x)$ is the distribution function of $X$. In general, $M(s)$ is defined for some interval including the origin. Let $P[$ ] denote the probability of the event in the brackets. For all nonnegative s,

$$
\begin{equation*}
P[x \geq 0]=\int_{0}^{\infty} d F(x) \leq \int_{0}^{\infty} \exp (s x) d F(x) \tag{C-2}
\end{equation*}
$$

Comparing equations $(C-1)$ and ( $C-2$ ), we conclude that

$$
\begin{equation*}
P[x \geq 0] \leq M(s) \quad, \quad 0 \leq s<s_{1} \tag{C-3}
\end{equation*}
$$

where $s_{1}$ is the upper limit of the interval in which $M(s)$ is defined. To make this bound as tight as possible, we choose the value of $s$ that minimizes $M(s)$, which we denote by $s_{0}$. Thus,

$$
\begin{equation*}
P[x \geq 0] \leq M\left(s_{0}\right), \tag{c-4}
\end{equation*}
$$

where $s_{0} \geq 0$ and

$$
\begin{equation*}
M\left(s_{0}\right)=\min _{0 \leq s^{\prime}<s_{1}} M(s) \tag{C-5}
\end{equation*}
$$

The right-hand side of inequality (C-4) is called the Chernoff bound. Since $M(0)=1$, the Chernoff bound is not useful unless $M\left(s_{0}\right)<M(0)$.

If the moment generating function is finite in some neighborhood of $s=0$, we may differentiate under the integral in equation ( $C-1$ ) to obtain the derivative of $M(s)$, which is

[^15]
## APPENDIX C

$$
\begin{equation*}
M^{\prime}(s)=\int_{-\infty}^{\infty} x \exp (s x) d F(x) \tag{c-6}
\end{equation*}
$$

It follows that $M^{\prime}(0)=E[x]$. Differentiating equation (C-6) gives the second derivative,

$$
\begin{equation*}
M^{\prime \prime}(s)=\int_{-\infty}^{\infty} x^{2} \exp (s x) d F(x) \tag{C-7}
\end{equation*}
$$

This equation shows that $M^{\prime \prime}(s) \geq 0$, which implies that $M(s)$ is convex in its interval of definition. Suppose that

$$
\begin{equation*}
E(X)<0, \quad P(X>0)>0 \tag{c-8}
\end{equation*}
$$

Then $M^{\prime}(0)<0$ by the first assumption, and $M(s) \rightarrow \infty$ as $s \rightarrow \infty$ by the second. Since $M(s)$ is convex, it has its minimum value at some positive $s=s_{0}$. We conclude that if $s_{1}>0$, inequalities ( $C-8$ ) are sufficient to ensure that the Chernoff bound is less than unity and $s_{0}>0$.

The Chernoff bound can be tightened if we assume that $x$ has a density function, $f(x)$, that satisfies

$$
\begin{equation*}
f(-x) \geq f(x) \tag{C-9}
\end{equation*}
$$

for all $x_{0} \quad$ Suppose that $M(s)$ is defined in the interval $s_{2}<s<s_{1}$,
where $s_{2} \leq 0$ and $s_{1} \geq 0$. Then

$$
\begin{aligned}
M(s) & =\int_{-\infty}^{\infty} \exp (8 x) f(x) d x \\
& =\int_{0}^{\infty} \exp (8 x) f(x) d x+\int_{-\infty}^{0} \exp (s x) f(x) d x \\
& \geq \int_{0}^{\infty}[\exp (s x)+\exp (-8 x)] f(x) d x
\end{aligned}
$$

[^16]\[

$$
\begin{aligned}
& =\int_{0}^{\infty} 2 \cosh (s x) f(x) d x \\
& \geq 2 \int_{0}^{\infty} f(x) d x \\
& =2 P[x \geq 0] .
\end{aligned}
$$
\]

Thus, we obtain the Chernoff-Jacobs bound:

$$
\begin{equation*}
P[x \geq 0] \leq \frac{1}{2} M\left(s_{0}\right) \tag{C-10}
\end{equation*}
$$

where

$$
\begin{equation*}
M\left(s_{0}\right)=\min _{s_{2}<s<s_{1}} M(s) \tag{C-11}
\end{equation*}
$$

The parameter $s_{0}$ is not required to exceed zero in this case. However, if $s_{1}>0$ and inequalities ( $\mathrm{C}-8$ ) hold, then the Chernoff-Jacobs bound is less than $1 / 2$ and $s_{0}>0$.

## DISTRIBUTION

## ADMINISTRATOR

OEFENSE TECHNICAL INFORMATION CENTER ATHA DTIC-DDA ( 12 COPIES)
CAMERON STATION, BUILDING 5
aLEXANDRIA, VA 22314

COMMANDER
US ARMY RSCH \& STD GP (EUR)
ATTN CHIEF, PHYSICS \& MATH BRANCH
FPO. NY 09510

COMMANDER
US ARMY MISSILE \& MUNITIONS CENTER
\& SCHOOL
ATHN ATSK-CTD-F
REDSTONE ARSENAL, AL 35809
DIRECTOR
US ARMY MATERIEL SYSTEMS ANALXSIS
ACTIVITY
ATTN DRXSY-MP
ATTN DRXSY-CT
ABERDEEN PROVING GROUND, MD 21005
DIRECTOR
US ARMY BALLISTIC RESEARCH LABORATORY ATTN DRDAR-TSE-S
ABERDEEN PROVING GROUND, MD 21005
US ARMY ELECTRONICS \& TECHNOLOGY DEVICES LABORATORY
ATTN DELET-DD
FT MONMOUTH, NJ 07703
HQ USAF/SAMI
WASHINGTON, DC 20330
TELEDYNE BROWN ENGINEERING
CUMMINGS RESEARCH PARK
ATIN DR. MELVIN L. PRICE, MS-44
HUNTSVILLE, AL 35807
ENGINEERING SOCIETIES LIBRARY
ATIN ACQUISITIONS DEPARTMENT
345 EAST 47TH STREET
NEW YORK, NY 10017
DIRECTOR
DEFENSE ADVANCED RESEARCH PROJBCTS
Agency
tactical technology office
ARCHITECT BUILDING
1400 WILSON BLVD
ARLINGTON, VA 22209

DIRECTOR
OEFENSE COMMUNICATIONS ENGINEERING
CENTER
ATHN RED OFFICE, ASST DIR FOR TECH 1860 WI EHLE AVE
RESTON, VA 22090

UNDER SECRETARY OF DEFENSE FOR RESEARCH \& ENGINEERING
ATTN DEP UNDER SECRETARY (TACTICAL WARFARE PROGRAM)
WASHINGTON, DC 20301
ASSISTANT SECRETARY OF THE ARMY
(RES, DEV, \& ACQ)
ATTN DEP FOR COMM \& TARGET ACQ
ATTN DEP FOR AIR \& MISSILE DEFENSE WASHINGTON, DC 20310

COMMANDER
US ARMY COMMUNICATIONS-ELEC. COMMAND
ATTN STEEP-MT-M
FT HUACHUCA, AZ 85613
OFFICE, DEPUTY CHIEF OF STAFF FOR
OPERATIONS \& PLANS
DEPARMENT OF THE ARMY
ATTN DAMO-TCD, ELECTRONIC/WARFARE SIGNAL SECURITY
WASHINGTON, DC 20310
COMMANDER
US ARMY CONCEPTS ANALYSIS AGENCY
8120 WOODMONT AVENUE
ATTN MDCA-SMS
BETHESDA, MD 20014

## COMMANDER

US ARMY COMMUNICATIONS R\&D COMMAND
ATTN DRSEL-CE, COMMUNICATIONS-ELECTRONIC
SYS INTEG OFFICE
FT MONMOUTH, NJ 07703

DIRECTOR, ELECTRONIC WARFARE LABORATORY
ATTN DELEET-V
ATTIN DELEN-C
ATTN DELEN-E
ATTN DELEN-M-ST
FTT MONMOUTH, NJ 07703

COMMANDER
ELECTRONICS WARFARE LABORATORY
OFFICE OF MISSILE ELECTRONIC WARFARE
WHITE SANDS MISSILE RANGE, NM 88002

## COMMANDER

NAVAL WEAPONS CENTER
ATIN CODE 35, ELECTRONIC WARFARE DEPT
CHINA LAKE, CA 93555
DIRECTOR
NAVAL RESEARCH LABORATORY
ATTN CODE 5700, TACTICAL ELE WARFARE DIVISION
WASHINGTON, DC 20375

COMMANDER
NAVAL SURFACE WEAPONS CENTER ATIN DF-20, ELECTRONICS WARFARE DIV ATTN DK, WARFARE ANALYSIS DEPT DAHLGREN, VA 22448

DIRECTOR
af avionics laboratory
ATIN KL (WR), ELECTRONIC WARFARE DIV WRIGHT-PATTERSON AFB, OH 45433

## COMMANDER

HQ, TACTICAL AIR COMMAND
ATTN DOR, DIR OF ELECTRONIC WARFARE OPNS
LANGLEY AFB, VA 23665
COMMANDER
hQ USAF tactical air warfare CENTER (TAC)
ATTW ER, DCS/ELECTRONIC WARFARE c RECONNAISSANCE
ATTN ERW, DIR OF ELECTRONIC WARFARE
EGLIN AFB, FL 32542
INSTITUTE POR DEFENSE ANALYSIS
400 ARMY NAVY DRIVE
ARLINGTON, VA 22209
DIA
DEP DIR OF SCIENTIFIC \& TECH INST
ELECTRONICS WARPARE BRANCH
1735 N. LYNN STREET
ARLINGTON, VA 22209
DEPT OF NAVY
OPFICE OF RES, DEV, TEST \& EVAL
ATYN TACTICAL AIR SURFACE \& EN DEV DIV ( NOP-98E5)
ATHN CEC EM SENSORS SEC (NOP-982F3)
THE PENTAGON
WASHINGTON, DC 20350

## COMMANDER

US ARMY TRAINING \& DOCTRINE COMMAND ATTN ATDC (DCS, COMBAT DEVELOPMENTSS)
FT MONROE, VA 23651
OPFICE OF THE DEPUTY CHIEF OF Staff
FOR RES, DEV, ACQ
DEPARTMEST OF THE ARMY
ATHN DMMA-WS
ATTM DAMA-CS
ATIM DANA-AR
ATM DAMA-SCS, LLECTRONIC WARFARE TEAM
WASHIWGTON, DC 20310

US ARMY COMBINED ARMS COMBAT DEV ACTIVITY ATTN ATZLCA-CA
attin atzlca-co
ATTN ATZLCA-FS
ATTN ATZLCA-SW
ATTN ATZLCA-COM-G
FT LEAVENWORTH, KS 66027
DIRECTOR
ELECTRONICS TECHNOLOGY \& DEV LAB
ATTN DELET
FT MONMOUTH, NJ 07703
COMMANDER
US ARMY MATERIEL DEV \& READINESS COMMAND
ATTN DRCPP
ATTN DRCPS
ATTN DRCDE
ATTN DECDE-D
ATTN DRDMD-ST
5001 EISENHOWER AVENUE
ALEXANDRIA, VA 22333
DIRECTOR
US ARMY NIGHT VISION \& ELECTRO-OPTICS LABORATORY
FT BELVOIR, VA 22060
COMMANDER/DIRECTOR
COMBAT SURVEILLANCE \& TARGET
ACQUISITION LAB
US ARMY ERADCOM
FT MONMOUTH, NJ 07703
DIRECTOR
US ARMY SIGNALS WARFARE LAB
VINT HILL FARMS STATION
WARRENTON, VA 22186
COMMANDER
US ARMY INTELLIGENCE \& SECURITY COMMAND
ARLINGTON HALL STATION
ATIN IARDA (DCS, RDA)
ATTN IAITA (DIR, threat analysis)
4000 ARLINGTON BLVD
ARLINGTON, VA 22212
US ARMY TRADOC SYSTEMS ANALYSIS ACTIVITY
ATTN ATAA-TDB
WHITE SANDS MISSILE RANGE, NM 88002
DIRECTOR
NATIONAL SECURITY AGENCY
ATTN S65
FT MEADE, MD 20755
NAVAL AIR DEVELOPMENT CERNTER
ATTN DR. GERALD PALATUCCI (404B) (30 COPIES)
WARMINSTER, PA 18974

US ARMY ELECTRONICS RESEARCH \&
development command
ATTN TECHNICAL DIRECTOR, DRDEL-CT
ATTN DRDELLCM
ATTN DRDEL-PO
ATTN TORRIERI, D., DRDEL-CM ( 20 COPIES)
HARRY OIAMOND LABORATORIES
ATTN CO/TD/TSO/DIVISION DIRECTORS
ATTN RECORD COPY, 81200
ATTN HDL LIBRARY, 81100 (2 COPIES)
ATIN HDL LIBRARY, 81100 (WOODBRIDGE)
ATTN TECHNICAL REPORTS BRANCH, 81300 ( 3 COPIES)
ATTN LEGAL OFFICE, 97000
ATIN CHARIMAN, EDITORIAL COMMITTEE
ATTN MORRISON, R. E., 13500 (GIDEP)
INGERSOLL, P., 34300
GOODMAN, R., 34400
MAK, T., 21300
TOZZI, L., 30000
Chase, R., 15300
GIGLIO, D., 15300
DENT, J., 36100
FEMENIAS, R., 21100

$$
\underset{=1}{D}
$$


[^0]:    D. J. Torrieri, Principles of Military Commaication Systems, Artech House, Dedham, MA (1981).

[^1]:    ${ }^{2}$ B. K. Levitt and J. K. Omura, Coding Tradeoffs for Improved Performance of FH/MFSK Systems in Partial Band Noise, National Telecoamunications Conference, 2 (1981), D.9.1.

    3A. J. Viterbi and I. M. Jacobs, Advances in Coding and Modulation $^{\text {A }}$ for Noncoherent Channels Affected by Fading, Partial Band, and MultipleAccess Interference, in A. J. Viterbi, ed., Advances in Communication Systems, 4, Academic Press, Inc., New York (1975).

[^2]:    ID. J. Torrieri, Principles of Military Communication Systems, Artech Rouse, Dedham, MA (1981).

[^3]:    ${ }^{1}$ D. J. Torrieri, Principles of Military Communication Systems, Artech House, Dedham, MA (1981).
    ${ }^{4}$ S. Haykin, Communication Systems, John Wiley \& Sons, Inc., New York (1978).

[^4]:    *The computer programming was provided by Thomas Wright of the Countermeasures/Counter-Countermeasures Center.

[^5]:    ${ }^{1}$ D. J. Torrieri, Principles of Military Communication Systems, Artech House, Dedham, MA (1981).
    ${ }^{4}$ S. Haykin, Communication Systems, John Wiley \& Sons, Inc., New York (1978).

[^6]:    ${ }^{4}$ S. Haykin, Communication Systems, John Wiley \& Sons, Inc., New York (1978).

    5R. F. Pawula, On the Theory of Error Rates for Narrow-Band Digital FM, IEEE Trans. Communications, 29 (November 1981), 1634.

[^7]:    ${ }^{1}$ A. J. Viterbi and J. K. Omura, Principles of Digital Comunication and Coding, McGraw-Hill Book Co., New York (1979).
    ${ }^{2}$ G. C. Clark and J. B. Cain, Error-Correction Coding for Digital Communications, Plenum Press, New York (1981).
    ${ }^{3}$ W. W. Peterson and E. J. Weldon, Error-Correcting Codes, 2nd ed., The MIT Press, Cambridge, MA (1972).

[^8]:    ${ }^{1}$ A. J. Viterbi and J. K. Omura, Principles of Digital Communication and Coding, McGraw-Hill Book Co., New York (1979).
    ${ }^{2}$ G. C. Clark and J. B. Cain, Error-Correction Coding for Digital Communications, Plenum Press, New York (1981).
    ${ }^{3}$ W. W. Peterson and E. J. Weldon, Error-Correcting Codes, 2nd ed., The MIT Press, Cambridge, MA (1972).

[^9]:    ${ }^{1}$ A. J. Viterbi and J. K. Omura, Principles of Digital Communication and Coding, McGraw-Hill Book Co., New York (1979).
    ${ }^{2}$ G. C. Clark and J. B. Cain, Error-Correction Coding for Digital Communications, Plenum Press, New York (1981).

[^10]:    ${ }^{4}$ J. P. Odenwalder, Optimal Decoding of Convolutional Codes, Doctoral Dissertation, University of California at Los Angeles (1970).

[^11]:    1A. J. Viterbi and J. K. Omura, Principles of Digital Communication and Coding, McGraw-Hill Book Co., New York (1979).
    ${ }^{2}$ G. C. Clark and J. B. Cain, Error-Correction Coding for Digital Communications, Plenum Press, New York (1981).

[^12]:    1A. J. Viterbi and J. K. Omura, Princlples of Digital Communication and Coding, McGraw-Hill Book Co., New York (1979).

[^13]:    5J. P. Odenwalder, Dual-k Convolutional Codes for Noncoherently Demodulated Channels, International Telemetering Conference (1976), 165.

[^14]:    ${ }^{1}$ D. J. Torrieri, Principles of Military Communication Systems, Artech House, Dedham, MA (1981).

[^15]:    ${ }^{1}$ P. Billingsley, Probability and Measure, John Wiley a Sons, Inc., New York (1979).

[^16]:    ${ }^{2}$ I. M. Jacobs, Probability-of-Error Bounds for Binary Transmission on Slowly Fading Rician Channel, IEEE Trans. Inform. Theory, 12 (October 1966). 431.

