Reed-Solomon Codes in Slow Frequency Hop Spread Spectrum Systems

Andrew Bolstad, SURE Program 2002

I. Introduction

In a slow frequency hop spread spectrum system, multiple signals are transmitted over multiple carrier frequencies. Each transmitter sends N_b symbols on a carrier frequency, and then hops to a new frequency. This way, a particular signal will spend a limited amount of time in noisy frequency bands. When multiple users hop between the same frequencies, there is a chance that two or more signals will occupy the same frequency at the same time (a "hit"). When a signal is hit, the N_b symbols transmitted at that frequency will be corrupted. Because the signal continuously hops to different frequencies, only a fraction of transmitted symbols will be completely lost. To recover information lost to hits and other interference, error-correcting codes such as Reed-Solomon codes are employed. In an error correcting code, redundant information is sent to restore lost information. In this analysis, the probability of not decoding is calculated for any (n,k) Reed Solomon code using MPSK (M=2, 4, and 8) and DPSK. Errors only and errors and erasures decoding are analyzed.

II. Properties of Reed-Solomon Codes

Reed-Solomon codes introduce redundancy into a signal allowing the correction of errors made during transmission through a noisy channel. Reed-Solomon codes are specified by two numbers n (the code length) and k. A message is divided into k symbols of m bits each. These k symbols are then encoded as an n-symbol code word. In the basic Reed-Solomon codes, the length of the code n is given by:

$$n = q^m - 1 \tag{1}$$

Generally, q must be a prime number. In many applications, q=2 to facilitate binary computer systems. Thus, n may take on values of 3, 7, 15, 31, 63, etc. The code length may be increased, however, by using extended Reed-Solomon codes. Likewise, code lengths may be shortened through shortening or puncturing. Note that shortening and puncturing involve different ways of setting up the code. Through extending, shortening, and puncturing, any value of n may be achieved. For the purposes of this analysis, it will be assumed that the least amount of extension, shortening, or puncturing is used. Thus, the number of bits per message symbol is:

$$m \approx \log_2 n + 1 \tag{2}$$

An (n,k) Reed-Solomon code can correct up to e code symbol errors and r code symbol erasures as long as $2e+r<n-k+1$ [4]. An error occurs when a code symbol is incorrectly received. An erasure occurs when the receiver can determine that a code symbol was received incorrectly. In order to detect erasures, the receiver must be given information about which symbols to erase. In this analysis, a parity bit will be added to code symbols to facilitate errors and erasures decoding. If there are an odd number of bit errors in a

code symbol, the parity of that symbol will be violated, and the code symbol will be erased.

III. System Description

The system analyzed in this report is shown in Figure 1 below. The message is first encoded using an (n,k) Reed-Solomon code. Parity bits are added when errors and erasures decoding is used. Next the transmission symbols are interleaved such that each transmission symbol can be considered independent of its neighboring symbols. A slow frequency hop transmitter spreads the signal by transmitting N_b symbols on one frequency, then hopping to a new frequency. The transmitted signal experiences additive white Gaussian noise (AWGN) and multiple-access interference when one or more other users transmit on the same frequency at the same time. The analysis given here assumes catastrophic interference when two users transmit on the same frequency at the same time (termed a "hit"). That is, the probability of bit error is 0.5 when a hit occurs. On the receiving end, the work of the transmitter is undone, and the coded message is decoded using errors only or errors and erasures decoding.

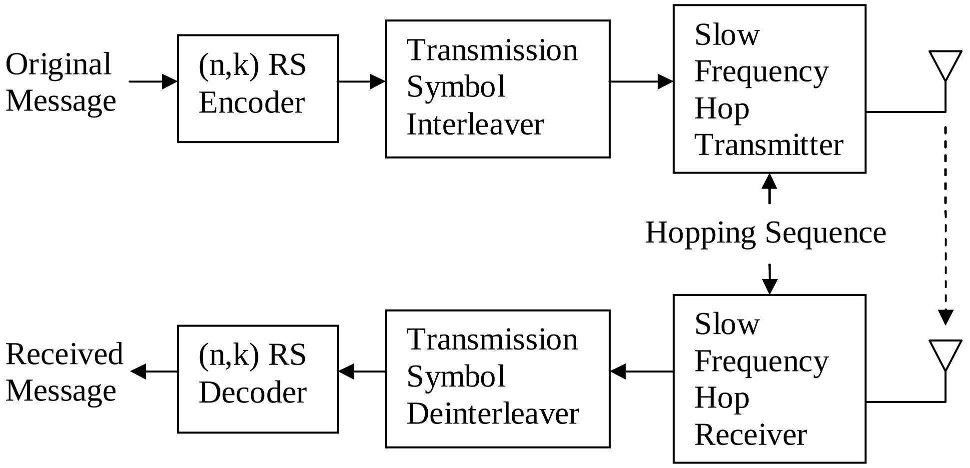


Figure 1

The system was analyzed using BPSK, QPSK, 8PSK, and DPSK modulation schemes. All but DPSK require coherent detection, which may be quite difficult in a frequency hopping system. It is assumed that coherent detection is possible, and that is does not cause any significant errors in the detection of transmitted symbols.

IV. Probability of Transmission symbol Error

The probability of bit error P_b can be computed for BPSK in AWGN using an optimum detector with the formula:

$$P_b = Q\left(\sqrt{\frac{2E_b}{N}}\right) \tag{3}$$

Likewise, the probability of bit error for DPSK in AWGN using an optimum detector is given by:

$$P_b = \frac{1}{2}e^{\frac{-E_b}{N}} \tag{4}$$

The QPSK modulation scheme can be thought of as two BPSK signals transmitted in parallel with one signal on the in-phase part of the carrier, and another on the quadrature part of the carrier. The signals are orthogonal, so errors occur independently in either signal; therefore, QPSK has the same bit error rate as BPSK [2, 3]. The probability of receiving one symbol without error in QPSK is $(1-P_b)^2$.

The probability of error for 8PSK is a bit more difficult to derive. Unlike in QPSK, the probability of bit error is not independent of other bits in the same transmission symbol in 8PSK. Furthermore, the probability of error for a given bit depends on its position in the three bit (8-ary) symbol due to the asymmetrical Gray code mapping onto the signal space.

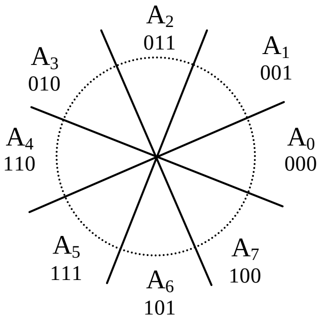


Figure 2

An exact analysis of error rates for 8PSK systems can be accomplished by determining the probability of detecting a symbol in a given decision region. The decision regions and corresponding bit patterns are shown in Figure 2. The boundaries between decision regions occur at angles of ±π/8, ±3π/8, ±5π/8, and ±7π/8 radians. Let $P(A_x)$ denote the probability of detecting the received symbol in region A_x given that the all zero symbol was transmitted in an AWGN channel. The probability of the received symbol falling in a particular region A_x is given by [2]:

$$P(A_x) = \frac{1}{2\pi}\int_{\theta_1}^{\theta_2} e^{\frac{3E_b}{N}}\left(1 + e^{\frac{3E_b\cos^2\theta}{N}}\sqrt{\frac{12\pi E_b}{N}}\cos\theta\left(1 - Q\left(\sqrt{\frac{6E_b}{N}}\cos\theta\right)\right)\right)d\theta \tag{5}$$

where θ_1 and θ_2 are the boundaries of the region in question. Because regions A_1 and A_7 are equidistant from the intended signal and the same size, they occur with the same probability. That is, $P(A_1)=P(A_7)$. Likewise, $P(A_2)=P(A_6)$ and $P(A_3)=P(A_5)$. Furthermore, $P(A_1)$ represents the probability of detecting a signal in a decision region adjacent to the transmitted signal, regardless of what symbol was transmitted. Similarly, $P(A_2)$, $P(A_3)$, and $P(A_4)$ are the probabilities of detecting a symbol two, three, and four decision regions away from the transmitted symbol. For example, if the symbol 011 is transmitted, the probability of detecting the symbol 111 is $P(A_3)$.

Table 1

Transmitted Symbol	**Error Pattern**							
	000	001	010	100	011	101	110	111
000	$P(A_0)$	$P(A_1)$	$P(A_3)$	$P(A_1)$	$P(A_2)$	$P(A_2)$	$P(A_4)$	$P(A_3)$
001	$P(A_0)$	$P(A_1)$	$P(A_1)$	$P(A_3)$	$P(A_2)$	$P(A_2)$	$P(A_4)$	$P(A_3)$
011	$P(A_0)$	$P(A_1)$	$P(A_1)$	$P(A_3)$	$P(A_2)$	$P(A_2)$	$P(A_4)$	$P(A_3)$
010	$P(A_0)$	$P(A_1)$	$P(A_3)$	$P(A_1)$	$P(A_2)$	$P(A_2)$	$P(A_4)$	$P(A_3)$
110	$P(A_0)$	$P(A_1)$	$P(A_3)$	$P(A_1)$	$P(A_2)$	$P(A_2)$	$P(A_4)$	$P(A_3)$
111	$P(A_0)$	$P(A_1)$	$P(A_1)$	$P(A_3)$	$P(A_2)$	$P(A_2)$	$P(A_4)$	$P(A_3)$
101	$P(A_0)$	$P(A_1)$	$P(A_1)$	$P(A_3)$	$P(A_2)$	$P(A_2)$	$P(A_4)$	$P(A_3)$
100	$P(A_0)$	$P(A_1)$	$P(A_3)$	$P(A_1)$	$P(A_2)$	$P(A_2)$	$P(A_4)$	$P(A_3)$
unknown	$P(A_0)$	$P(A_1)$	$\{P(A_1)+P(A_3)\}/2$	$\{P(A_1)+P(A_3)\}/2$	$P(A_2)$	$P(A_2)$	$P(A_4)$	$P(A_3)$

Table 1 shows the probabilities of all eight possible error patterns for all eight possible transmitted symbols. From this table, the probability of any number of bit errors per transmitted symbol can be determined. For example, the probability of one bit error in a transmitted symbol is $2P(A_1)+P(A_3)$. If the position of a particular bit within its three bit transmission symbol is known, the probability of error for that bit can be determined. For example, the probability of an error occurring in bit three is $P(A_1)+ 2P(A_2)+P(A_3)$. Table 2 lists the probabilities of having zero, one, two, or three bit errors per transmission symbol.

Table 2

Bit Errors Per Symbol	**Probability**
0	$P(A_0)$
1	$2P(A_1)+P(A_3)$
2	$2P(A_2)+P(A_4)$
3	$P(A_3)$

When using block codes, there are more bits in the coded message than in the original message. In the formulae given above, E_b is the energy per transmitted bit. Because it takes more bits to send an encoded message than the original message, the bit energy of a transmitted bit will be less than that of a message bit. It is desirable to express the probability of error as a function of the energy per message bit to facilitate comparison between encoded and non-encoded data. In the equations given above, the bit energy to noise ratio must be multiplied by the rate of message bits per code bits. For example, the expression for probability of error in BPSK (and QPSK) becomes:

$$P_b = Q\left(\sqrt{\frac{2RE_b}{N}}\right) \tag{6}$$

where R represents the rate of message bits per code bits.

In the case of errors only decoding, calculating R is simply a matter of dividing the number of symbols (of length m bits) in a message word by the number of symbols in a code word. Thus for an (n,k) code with errors only decoding, R is just k divided by n.

The rate R decreases when errors and erasures decoding is used. In this case, the encoded data contains extra bits which tell the decoder which symbols to erase. For the parity bit method, there is one extra bit in every code symbol. To transmit a message word of km bits, the transmitter must send $n(m+1)$ bits. The rate for the parity bit method is:

$$R = \frac{km}{n(m+1)} \tag{7}$$

Though the probability of error in a single bit is slightly higher for errors and erasures decoding, performance superior to errors only decoding is achieved with the codes ability to correct twice as many erasures as errors.

V. Code Symbol Errors and Erasures

A code symbol is represented by m bits in errors only decoding and $m+1$ bits in errors and erasures decoding with the parity bit method. The probability of successfully transmitting one code symbol is equal to the probability of transmitting all the bits comprising that code symbol correctly. In errors only decoding, a code symbol error occurs if one or more of the m bits comprising that code symbol are in error. Let s denote the probability of successfully transmitting one code symbol. For errors only decoding and modulation schemes where bit errors occur independently of neighboring bits (BPSK, QPSK, and DPSK):

$$s = (1 - P_b)^m \tag{8}$$

Likewise, in errors and erasures decoding, a code symbol is transmitted successfully only if all $m+1$ bits in that code symbol are transmitted successfully. Two possibilities exist, however, when the code symbol is not transmitted correctly. If an odd number of bits are in error, the parity of that code symbol will be violated, and the decoder will erase that code symbol. If an even number of bits is in error, the decoder will select the wrong code symbol, and a code symbol error occurs. Because the probability of more than one bit being in error is so small, code symbol errors are much less likely to occur than code symbol erasures. Let *s* denote the probability of successfully transmitting one code symbol and *t* denote the probability of erasing one code symbol. For errors and erasures decoding with the parity bit method and modulation schemes where bit errors occur independently of neighboring bits:

$$s = (1 - P_b)^{m+1} \tag{9}$$

$$t = \sum_{\substack{x=1 \\ x \ \ odd}}^{m+1} \binom{m+1}{x} P_b{}^{x} (1 - P_b)^{m+1-x} \tag{10}$$

For 8PSK, the probability of bit error varies with the position of the bit within the transmission symbol, thus an exact analysis requires consideration of the dependence between bits in the same transmission symbol. When the number of bits per code symbol is an integer multiple of three (for example (31,*k*) codes with parity bit or (7,*k*) codes without parity bits), determining *s* or *t* is relatively easy. In this case for errors only decoding:

$$s = P(A_0)^{\frac{m}{3}} \tag{12}$$

For errors and erasures decoding when the number of bits per code symbol is an integer multiple of three, *s* and *t* are given by:

$$s = P(A_0)^{\frac{m+1}{3}} \tag{13}$$

$$t = \sum_{x_2=0}^{\frac{m+1}{3}} \sum_{\substack{x_1=1 \\ x_1 \ \ odd}}^{\frac{m+1}{3}-x_2} \begin{pmatrix} & \frac{m+1}{3} & \\ \frac{m+1}{3} - x_1 - x_2 & x_1 & x_2 \end{pmatrix} P(A_0)^{\frac{m+1}{3}-x_1-x_2} \left[2\{P(A_1) + P(A_3)\}\right]^{x_1} \left[2P(A_2) + P(A_4)\right]^{x_2} \tag{14}$$

When the number of bits per code symbol is not an integer multiple of three, the values of *s* and *t* will vary from symbol to symbol. Moreover, the values of *s* and *t* will be dependent on those of neighboring symbols. Thus, a more complex method of analysis must be performed. The method described in section VII for calculating the probability of not decoding for 8PSK with multiple-access interference can be used with the probability of a hit (P_h) set to zero.

VI. Decoder Error and Failure

In block codes (e.g. Reed-Solomon codes), there are only 2^{km} valid code words out of 2^{nm} possible received code words. When no errors occur during transmission, a valid code word is detected at the receiver. If the number of errors and number of erasures are within certain limits, the received word will be within Hamming distance of the intended code word, and the receiver can choose the correct code word. If the number of errors and number of erasures exceed the aforementioned limits, two possibilities result. In the more likely case, the received word will not be within Hamming distance of any valid code word. The decoder will not be able to select from the set of valid code word. This condition is termed decoder failure and occurs with probability $P(F)$. (A decoder failure could be resolved by requesting a retransmission of the violating word.) In the less likely case, the number of errors and the number of erasures will be high enough to place the received word within Hamming distance of the wrong valid code word. The decoder will then choose the wrong code word. This condition is termed decoder error and occurs with probability $P(E)$.

The calculation of $P(E)$ is somewhat complicated and code dependant (i.e. a knowledge of the weight distribution $\{A_j\}$ of the code is required). The calculation of $P(F)$ is more straightforward. It is simply one minus the probability that the received word falls within Hamming distance of the intended code word minus the probability that the received word falls within Hamming distance of the incorrect code word ($P(E)$). Thus, for error only decoding [4]:

$$P(F) = 1 - \left[\sum_{x=0}^{\lfloor (n-k)/2 \rfloor} \binom{n}{x} (1-s)^x s^{n-x} \right] - P(E) \tag{15}$$

and for error and erasure decoding [4]:

$$P(F) = 1 - \sum_{v=0}^{\lfloor (n-k)/2 \rfloor} \sum_{w=0}^{n-k-2v} \binom{n}{v} \binom{n-v}{w} s^{n-v-w} t^w (1-s-t)^v - P(E) \tag{16}$$

The probability of not decoding provides a good comparison between different coding schemes. It is defined as the sum of the probability of decoder failure and the probability of decoder error:

$$P(not \quad decoding) \equiv P(E) + P(F) \tag{17}$$

Using the equations above, the probability of not decoding for errors only and errors and erasures decoding are, respectively:

$$P(not \quad decoding) = P(E) + P(F) = 1 - \left[\sum_{x=0}^{\lfloor (n-k)/2 \rfloor} \binom{n}{x} (1-s)^x s^{n-x} \right] \tag{18}$$

$$P(not \quad decoding) = P(E) + P(F) = 1 - \sum_{v=0}^{\lfloor (n-k)/2 \rfloor} \sum_{w=0}^{n-k-2v} \binom{n}{v} \binom{n-v}{w} s^{n-v-w} t^w (1-s-t)^v \tag{19}$$

In Reed-Solomon codes, $P(F)$ is generally much larger than $P(E)$, so $P(\textit{not decoding})$ may serve as an approximation to $P(F)$, especially for large E_b/N.

VII. Multiple-Access Interference

If multiple users transmit in a SFH system, two or more users could transmit on the same carrier frequency at the same time. This event is known as a “hit.” The probability of a hit P_h for a given transmission symbol when random hopping patterns are used is [1]:

$$P_h = 1 - \left(1 - \frac{1}{q}\left(1 + \frac{1}{N_b}\right)\right)^{K-1} \tag{20}$$

where q is the number of carrier frequencies available, N_b is the number of transmission symbols per dwell, and K is the number of users. In actual communication systems, pseudorandom hopping patterns must be used. For these deterministic patterns, an upper bound on the hit probability is [1]:

$$P_h = 1 - \left(1 - \frac{1}{q-1}\left(1 + \frac{1}{N_b}\right)\right)^{K-1} \tag{21}$$

For systems with a large number of available channels (large q), this upper bound is essentially equal to the hit probability for random patterns.

BPSK and DPSK

In BPSK and DPSK, one bit is transmitted per transmission symbol. Because a transmission symbol interleaver is used, the probability of error for a given bit is independent of its neighbors. The probabilities of bit error given multiple-access interference for BPSK and DPSK are, respectively:

$$P_b = (1 - P_h)Q\left(\sqrt{\frac{2RE_b}{N}}\right) + \frac{P_h}{2} \tag{22}$$

and

$$P_b = (1 - P_h)e^{-\frac{RE_b}{N}} + \frac{P_h}{2} \tag{23}$$

The probability of not decoding can then be calculated using (9), (10), (18), and (19).

QPSK

In QPSK, two bits are transmitted per transmission symbol. If a given transmission symbol is hit, two bits will experience catastrophic interference. Because a transmission symbol interleaver is used, the probability of one bit experiencing a hit is dependent on the probability of one of its neighbors experiencing a hit. Let P_0 be the probability of no bit errors in a transmission symbol, P_1 be the probability of one error in a transmission symbol, and P_2 be the probability of two errors in a transmission symbol.

$$P_0 = (1-P_h)\left(1-Q\left(\sqrt{\frac{2RE_b}{N}}\right)\right)^2 + \frac{P_h}{4} \tag{24}$$

$$P_1 = (1-P_h)2Q\left(\sqrt{\frac{2RE_b}{N}}\right)\left(1-Q\left(\sqrt{\frac{2RE_b}{N}}\right)\right) + \frac{P_h}{2} \tag{25}$$

$$P_2 = (1-P_h)Q\left(\sqrt{\frac{2RE_b}{N}}\right)^2 + \frac{P_h}{4} \tag{26}$$

When there is an even number of bits per code symbol, the probability of not decoding can easily be calculated by using (18) and (19) and solving for *s* and, when errors and erasures decoding is used, *t*. For errors only decoding:

$$s = P_0^{\frac{m}{2}} \tag{27}$$

For errors and erasures decoding:

$$s = P_0^{\frac{m+1}{2}} \tag{28}$$

$$t = \sum_{x_2=0}^{\frac{m+1}{2}} \sum_{\substack{x_1=1 \\ x_1 \ odd}}^{\frac{m+1}{2}-x_2} \begin{pmatrix} \frac{m+1}{2} \\ \frac{m+1}{2}-x_1-x_2 \quad x_1 \quad x_2 \end{pmatrix} P_0^{\frac{m+1}{2}-x_1-x_2} P_1^{x_1} P_2^{x_2} \tag{29}$$

When there are an odd number of bits per code symbol, two code symbols must share a transmission symbol, as shown in Figure 3. These two symbols can be divided into three independent random variables. Two of these independent random variables are the number of bit errors in complete transmission symbols in the first and third code symbols. There can be either no bit errors, an odd number of bit errors, or an even number of bit errors in the complete transmission symbols in a code symbol. The third independent random variable is the error pattern of the transmission symbol shared by both code symbols. Four error patterns are possible in QPSK. Thus, there are $3^2 4=36$ possible outcomes for two code symbols that share a transmission symbol.

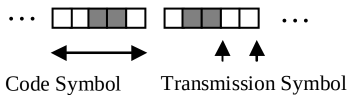


Figure 3

For errors only decoding, these 36 possibilities must be divided into three groups: those that produce zero, one, or two symbol errors per group of two symbols. Let $P_S(x)$ denote the probability of x symbol errors per group of two symbols. The exact calculation of $P_S(x)$ is not given here, but can be easily performed on a computer. It can be seen from the symmetry of a pair of code symbols that a given number of errors is equally likely to occur in the first symbol or the second. The probability of not decoding using errors only decoding is given by:

$$P(not \quad decoding) = \sum_{y=0}^{n \bmod 2} \sum_{x_2=0}^{\frac{1}{2}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y\right)} \sum_{x_1=0}^{\left\lfloor \frac{n-k}{2} \right\rfloor - y - 2x_2} \binom{\left\lfloor \frac{n}{2} \right\rfloor}{x_0 \quad x_1 \quad x_2} P_S(0)^{x_0} P_S(1)^{x_1} P_S(2)^{x_2} \left(P_S(2) + \frac{P_S(1)}{2} \right)^{y} \tag{30}$$

where:

$$x_0 = \left\lfloor \frac{n}{2} \right\rfloor - x_1 - x_2 \tag{31}$$

For errors and erasures decoding, there can be up to two errors or two erasures in a pair of code symbols, but the number of errors plus the number of erasures can be no more than two. The 36 possibilities mentioned above fall into five groups. Let $T_S(x)$ denote the probability that $x=2e+r$ in a pair of code symbols, with x taking values of zero, one, two, three, or four and e and r denoting, respectively, the number of errors and the number of erasures in a pair of code symbols. Let $H(y)$ denote the probability that $y=2e+r$ in one symbol. The exact calculation of $T_S(x)$ and $H(y)$ are not given here, but can be easily performed by a computer. The probability of not decoding using errors and erasures decoding is:

$$P(not \quad decoding) = \sum_{y=0}^{2(n \bmod 2)} \sum_{x_4=0}^{\left\lfloor \frac{n-k-y}{4} \right\rfloor} \sum_{x_3=0}^{\left\lfloor \frac{n-k-y-4x_4}{3} \right\rfloor} \sum_{x_2=0}^{\left\lfloor \frac{n-k-y-4x_4-3x_3}{2} \right\rfloor} \sum_{x_1=0}^{n-k-y-4x_4-3x_3-2x_2} F(x_1, x_2, x_3, x_4) H(y) \tag{32}$$

where:

$$F(x_1, x_2, x_3, x_4) = \binom{\left\lfloor \frac{n}{2} \right\rfloor}{\left\lfloor \frac{n}{2} \right\rfloor - x_1 - x_2 - x_3 - x_4 \quad x_1 \quad \ldots \quad x_4} T_S(0)^{\left\lfloor \frac{n}{2} \right\rfloor - x_1 - x_2 - x_3 - x_4} T_S(1)^{x_1} \ldots T_S(4)^{x_4} \tag{33}$$

8PSK

In 8PSK, three bits are transmitted per transmission symbol. If a transmission symbol is hit during transmission, three bits will be affected. The probability of a symbol falling into a particular decision region must be adjusted to reflect the probability of a hit occurring. Let *P'*(A_x) be the probability of falling into decision region A_x when a hit is possible.

$$P'(A_x) = (1 - P_h)P(A_x) + \frac{P_h}{8} \tag{34}$$

When the number of bits per code symbol is divisible by three, *s* and *t* can easily be calculated, and (18) and (19) can be used to determine the probability of not decoding. For the errors only case, *s* is given by:

$$s = P'(A_0)^{\frac{m}{3}} \tag{35}$$

For errors and erasures decoding:

$$s = P'(A_0)^{\frac{m+1}{3}} \tag{36}$$

$$t = \sum_{x_2=0}^{\frac{m+1}{3}} \sum_{\substack{x_1=1 \\ x_1 \; odd}}^{\frac{m+1}{3}-x_2} \left(\begin{array}{ccc} & \frac{m+1}{3} & \\ \frac{m+1}{3} - x_1 - x_2 & x_1 & x_2 \end{array} \right) P'(A_0)^{\frac{m+1}{3}-x_1-x_2} \left[2\{P'(A_1) + P'(A_3)\}\right]^{x_1} \left[2P'(A_2) + P'(A_4)\right]^{x_2} \tag{37}$$

When the number of bits per code symbol is not an integer multiple of three, adjacent code symbols must share transmission symbols. For example, in Figure 4a the last two bits of the first code symbol and the first bit of the second code symbols are transmitted together as one 8-ary transmission symbol. Similarly, the last bit of the second code symbol and the first two bits of the third code symbol are transmitted together. No matter how many bits per code symbol are used, three sequential code symbols will always contain an integer multiple of 8PSK transmission symbols. Thus, the probability of not decoding can be determined by analyzing groups of three code symbols.

a. **b.**

Figure 4

Any group of three code symbols that share transmission symbols can be divided into five independent events. Three of these events are the number of bit errors in complete transmission symbols in code symbols one, two, and three. There will either be no bit errors, an odd number of bit errors, or an even number of bit errors in any one of these three groups. The other two independent events are the error patterns of the shared transmission symbols. Each transmission symbol will take on one of eight patterns. Thus, there are $3^3 8^2=1728$ possible combinations of these five independent events.

In any group of three code symbols, there can be between zero and three code symbol errors. Let $P_S(x)$ be the probability of x code symbol errors in a group of three code symbols. $P_S(x)$ equals the summation of the probabilities of each of the 1728 possibilities mentioned above that result in x code symbol errors. This summation can be performed by a computer, but no simple method for determining which combinations result in x errors for any group of three was derived.

In errors and erasures decoding, there can be up to three erasures or up to three errors, but the total number of errors plus erasures can be no more than three. Let $T_S(x)$ be the probability that $x=2e+r$, where e is the number errors and r is the number of erasures in a group of three code symbols. As in the calculation of $T_S(x)$, each of 1728 possibilities must be mapped to the appropriate value of x, and no simple method for achieving this mapping is derived.

If the length of the code n is divisible by three, there are an integer number of groups of three code symbols in one code word. Thus, the probability of not decoding is given by:

$$P(not \quad decoding)=1-\sum_{x_3=0}^{\frac{1}{3}\left\lfloor\frac{n-k}{2}\right\rfloor}\;\sum_{x_2=0}^{\frac{1}{2}\left(\left\lfloor\frac{n-k}{2}\right\rfloor-3x_3\right)}\;\sum_{x_1=0}^{\left\lfloor\frac{n-k}{2}\right\rfloor-3x_3-2x_2}\begin{pmatrix} & \frac{n}{3} & \\ x_0 \quad x_1 & & x_2 \quad x_3\end{pmatrix}P_S(0)^{x_0}P_S(1)^{x_1}P_S(2)^{x_2}P_S(3)^{x_3} \tag{38}$$

where:

$$x_0=\frac{n}{3}-x_1-x_2-x_3 \tag{39}$$

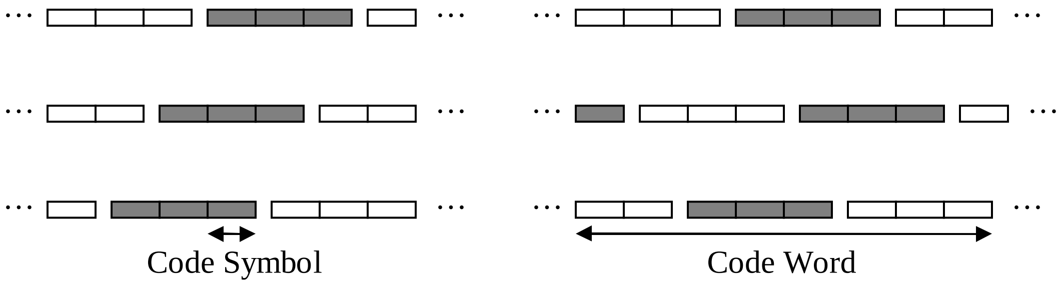
For errors and erasures decoding, the probability of not decoding is given by:

$$P(not \quad decoding)=1-\sum_{x_6=0}^{\frac{n-k}{6}}\;\sum_{x_5=0}^{\frac{n-k-6x_6}{5}}\cdots\sum_{x_1=0}^{n-k-6x_6-\ldots-2x_2}\begin{pmatrix} & \frac{n}{3} & \\ x_0 \quad x_1 & & \ldots \quad x_6\end{pmatrix}T_S(0)^{x_0}T_S(1)^{x_1}\ldots T_S(6)^{x_6} \tag{40}$$

where:

$$x_0=\frac{n}{3}-x_1-x_2-x_3-x_4-x_5-x_6 \tag{41}$$

If the code length n is not divisible by three, there are two possible results. These are illustrated in Figure 5 for a codes of lengths n=7 and n=8.



a. **b.**

Figure 5

In Figure 5a, the first code word contains two groups of three code words and the first symbol from another group of three. The second code word contains one group of three code symbols, the last two symbols of one group of three, and the first two symbols from another group of three. The last code word contains two groups of three code symbols and the last symbol from another group of three. Any of these three code words is equally likely. Let P_i denote the probability of not decoding for the i^{th} code word in Figure 5a. Let $H_x(y)$ represent the probability of y symbol errors in symbol(s) x. The calculation of $H_x(y)$ is not given here, but can be calculated in a similar manner as $P_S(x)$.

$$P_1 = 1 - \sum_{y=0}^{1} \sum_{x_3=0}^{\frac{1}{3}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y\right)} \sum_{x_2=0}^{\frac{1}{2}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y - 3x_3\right)} \sum_{x_1=0}^{\left\lfloor \frac{n-k}{2} \right\rfloor - y - 3x_3 - 2x_2} \binom{\left\lfloor \frac{n}{3} \right\rfloor}{x_0 \quad x_1 \quad x_2 \quad x_3} F(x_0, x_1, x_2, x_3) H_1(y) \qquad (42)$$

$$x_0 = \left\lfloor \frac{n}{3} \right\rfloor - x_1 - x_2 - x_3 \qquad (43)$$

$$P_2 = 1 - \sum_{y_1=0}^{1} \sum_{y_2=0}^{1} \sum_{x_3=0}^{\frac{1}{3}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y_1 - y_2\right)} \sum_{x_2=0}^{\frac{1}{2}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y_1 - y_2 - 3x_3\right)} \sum_{x_1=0}^{\left\lfloor \frac{n-k}{2} \right\rfloor - y_1 - y_2 - 3x_3 - 2x_2} \binom{\frac{n-4}{3}}{x_0 \quad x_1 \quad x_2 \quad x_3} F(x_1, x_2, x_3) H_1(y_1) H_3(y_2)$$

$$(44)$$

$$x_0 = \frac{n-4}{3} - x_1 - x_2 - x_3 \qquad (45)$$

$$P_3 = 1 - \sum_{y=0}^{1} \sum_{x_3=0}^{\frac{1}{3}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y\right)} \sum_{x_2=0}^{\frac{1}{2}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y - 3x_3\right)} \sum_{x_1=0}^{\left\lfloor \frac{n-k}{2} \right\rfloor - y - 3x_3 - 2x_2} \binom{\left\lfloor \frac{n}{3} \right\rfloor}{x_0 \quad x_1 \quad x_2 \quad x_3} F(x_{0,} x_1, x_2, x_3) H_3(y) \qquad (46)$$

$$x_0 = \left\lfloor \frac{n}{3} \right\rfloor - x_1 - x_2 - x_3 \qquad (47)$$

where:

$$F(x_0 . x_1, x_2, x_3) = P_S(0)^{x_0} P_S(1)^{x_1} P_S(2)^{x_2} P_S(3)^{x_3} \tag{48}$$

For errors only decoding, the probability of not decoding is the average of P_1, P_2, and P_3:

$$P(not \quad decoding) = \frac{P_1 + P_2 + P_3}{3} \tag{49}$$

Similar calculations give the probability of not decoding for errors and erasures decoding. Let G$_x$(y) represent the probability that y=2e+r in symbol(s) x.

$$P_1 = 1 - \sum_{y=0}^{2} \sum_{x_6=0}^{\frac{n-k-y}{6}} \cdots \sum_{x_1=0}^{\frac{n-k-y-6x_6-\ldots-2x_2}{6}} \begin{pmatrix} & \left\lfloor \frac{n}{3} \right\rfloor & \\ x_0 \quad x_1 & \ldots & x_6 \end{pmatrix} F(x_0, x_1, x_2, x_3, x_4, x_5, x_6) G_1(y) \tag{50}$$

$$x_0 = \left\lfloor \frac{n}{3} \right\rfloor - x_1 - x_2 - x_3 - x_4 - x_5 - x_6 \tag{51}$$

$$P_2 = 1 - \sum_{y=0}^{4} \sum_{y=0}^{4} \sum_{x_6=0}^{\frac{n-k-y}{6}} \cdots \sum_{x_1=0}^{\frac{n-k-y-6x_6-\ldots-2x_2}{6}} \begin{pmatrix} & \frac{n-4}{3} & \\ x_0 \quad x_1 & \ldots & x_6 \end{pmatrix} F(x_0, x_1, x_2, x_3, x_4, x_5, x_6) G_{12}(y_1) G_{23}(y_2) \tag{52}$$

$$x_0 = \frac{n-4}{3} - x_1 - x_2 - x_3 - x_4 - x_5 - x_6 \tag{53}$$

$$P_3 = 1 - \sum_{y=0}^{2} \sum_{x_6=0}^{\frac{n-k-y}{6}} \cdots \sum_{x_1=0}^{\frac{n-k-y-6x_6-\ldots-2x_2}{6}} \begin{pmatrix} & \left\lfloor \frac{n}{3} \right\rfloor & \\ x_0 \quad x_1 & \ldots & x_6 \end{pmatrix} F(x_0, x_1, x_2, x_3, x_4, x_5, x_6) G_3(y) \tag{54}$$

$$x_0 = \left\lfloor \frac{n}{3} \right\rfloor - x_1 - x_2 - x_3 - x_4 - x_5 - x_6 \tag{55}$$

where:

$$F(x_0, x_1, x_2, x_3, x_4, x_5, x_6) = T_S(0)^{x_0} T_S(1)^{x_1} T_S(2)^{x_2} T_S(3)^{x_3} T_S(4)^{x_4} T_S(5)^{x_5} T_S(6)^{x_6} \tag{56}$$

The probability of not decoding is then given by:

$$P(not \quad decoding) = \frac{P_1 + P_2 + P_3}{3} \tag{57}$$

In Figure 5b, the first code word contains two groups of three code symbols and the first two symbols from another group of three. Likewise, the second code word contains two groups of three code symbols and two code symbols from two other groups of three. Finally, the third code symbol contains two groups of three code symbols plus the third code symbol from another group of three. All three code words are equally likely. Calculating the probability of not decoding is similar to the method used for code words in Figure 5a. Let P_i denote the probability of not decoding for the i^{th} code word in Figure 5b. For errors only decoding:

$$P_1 = 1 - \sum_{y=0}^{2} \sum_{x_3=0}^{\frac{1}{3}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y\right)} \sum_{x_2=0}^{\frac{1}{2}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y - 3x_3\right)} \sum_{x_1=0}^{\left\lfloor \frac{n-k}{2} \right\rfloor - y - 3x_3 - 2x_2} F(x_1, x_2, x_3) H_{12}(y) \tag{58}$$

$$P_2 = 1 - \sum_{y_1=0}^{1} \sum_{y_2=0}^{1} \sum_{x_3=0}^{\frac{1}{3}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y_1 - y_2\right)} \sum_{x_2=0}^{\frac{1}{2}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y_1 - y_2 - 3x_3\right)} \sum_{x_1=0}^{\left\lfloor \frac{n-k}{2} \right\rfloor - y_1 - y_2 - 3x_3 - 2x_2} F(x_1, x_2, x_3) H_1(y_1) H_3(y_2) \tag{59}$$

$$P_3 = 1 - \sum_{y=0}^{2} \sum_{x_3=0}^{\frac{1}{3}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y\right)} \sum_{x_2=0}^{\frac{1}{2}\left(\left\lfloor \frac{n-k}{2} \right\rfloor - y - 3x_3\right)} \sum_{x_1=0}^{\left\lfloor \frac{n-k}{2} \right\rfloor - y - 3x_3 - 2x_2} F(x_1, x_2, x_3) H_{23}(y) \tag{60}$$

where:

$$F(x_1, x_2, x_3) = \binom{\left\lfloor \frac{n}{3} \right\rfloor}{\left\lfloor \frac{n}{3} \right\rfloor - x_1 - x_2 - x_3 \quad x_1 \quad x_2 \quad x_3} P_S(0)^{\left\lfloor \frac{n}{3} \right\rfloor - x_1 - x_2 - x_3} P_S(1)^{x_1} P_S(2)^{x_2} P_S(3)^{x_3} \tag{61}$$

Because all three code words are equally likely, the probability of not decoding is the average of the probability of not decoding for each word:

$$P(not \quad decoding) = \frac{P_1 + P_2 + P_3}{3} \tag{62}$$

The probability of not decoding for errors and erasures decoding can be found with similar calculations.

$$P_1 = 1 - \sum_{y=0}^{4} \sum_{x_6=0}^{\frac{n-k-y}{6}} \cdots \sum_{x_1=0}^{n-k-y-6x_6-\ldots-2x_2} F(x_1, x_2, x_3, x_4, x_5, x_6) G_{12}(y) \tag{63}$$

$$P_2 = 1 - \sum_{y_1=0}^{2} \sum_{y_2=0}^{2} \sum_{x_6=0}^{\frac{n-k-y}{6}} \ldots \sum_{x_1=0}^{n-k-y-6x_6-\ldots-2x_2} F(x_1, x_2, x_3, x_4, x_5, x_6) G_1(y_1) G_3(y_2) \tag{64}$$

$$P_1 = 1 - \sum_{y=0}^{4} \sum_{x_6=0}^{\frac{n-k-y}{6}} \ldots \sum_{x_1=0}^{n-k-y-6x_6-\ldots-2x_2} F(x_1, x_2, x_3, x_4, x_5, x_6) G_{12}(y) \tag{65}$$

where:

$$F(x_1, x_2, x_3, x_4, x_5, x_6) = \begin{pmatrix} & \left\lfloor \frac{n}{3} \right\rfloor & & \\ \left\lfloor \frac{n}{3} \right\rfloor - x_1 - \ldots - x_6 & x_1 & \ldots & x_6 \end{pmatrix} T_S(0)^{\left\lfloor \frac{n}{3} \right\rfloor - x_1 - \ldots - x_6} T_S(1)^{x_1} \ldots T_S(6)^{x_6} \tag{66}$$

The probability of not decoding is then given by:

$$P(not \quad decoding) = \frac{P_1 + P_2 + P_3}{3} \tag{67}$$

VIII. Results

The calculations described were implemented in a series of Matlab functions which calculate the probability of not decoding for any (*n*,*k*) Reed-Solomon code with errors only decoding or errors and erasures decoding using BPSK, QPSK, 8PSK, or DPSK. In 8PSK modulation, the error probabilities were determined by numerically integrating (5).

Figure 6 compares errors only decoding, errors and erasures decoding, and no coding for a (16,10) Reed-Solomon code. For the multiple-access interference (MAI) case, the probability of a hit was calculated using eq. (21) with ten users, ten symbols per hop, 1600 channels for the no coding case, 1000 channels for the errors only decoding case, and 800 channels for the errors and erasures case. The change in the number of available channels reflects the fact that the coding schemes must send redundant information in the same amount of time and, therefore, require more bandwidth. One minus the probability of not decoding is the probability of sending all *km* bits flawlessly. Thus, the traces for no coding scheme are the probability of one or more errors occurring in *km*=40 bits.

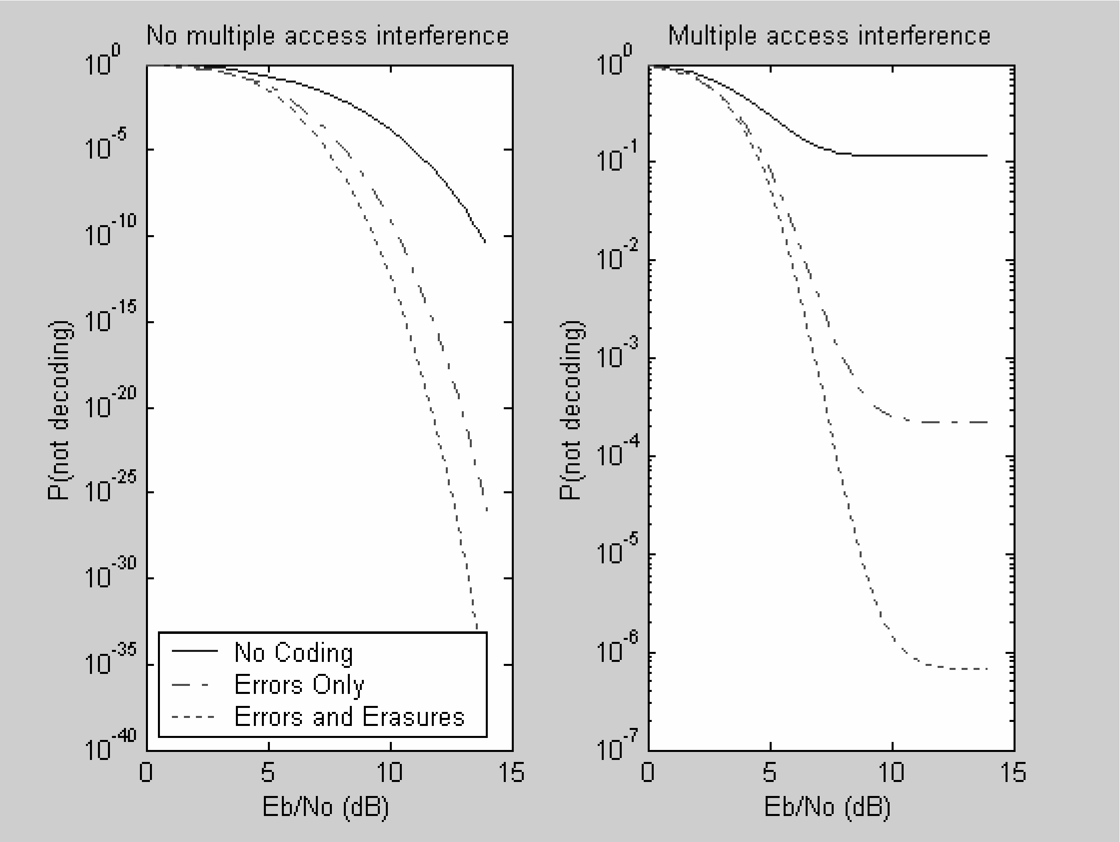


Figure 6: (16,10) R-S Code with BPSK

Three results of interest should be noted from Figure 6. First, Reed-Solomon encoding produces fewer errors than no coding. Second, multiple-access interference can greatly increase the probability of not decoding. Third, in the presence of multiple-access interference, there exists a lower limit to the probability of not decoding that depends on the probability of a hit and the specific code used (i.e. length *n* and errors only vs. errors and erasures). This limit arises from the fact that, as the bit energy to noise ratio increases, the probability of error due to AWGN decrease to zero, but the probability of a hit stays the same.

Figure 7 shows the result of using BPSK, QPSK, 8PSK, and DPSK and a (31,17) code. The BPSK and DPSK signals have 1000 available frequencies, while the QPSK and 8PSK signals use 2000 and 3000 frequencies respectively. This reflects the smaller bandwidth of QPSK and 8PSK modulation. As in the (16,10) case described above, there are ten symbols per hop.

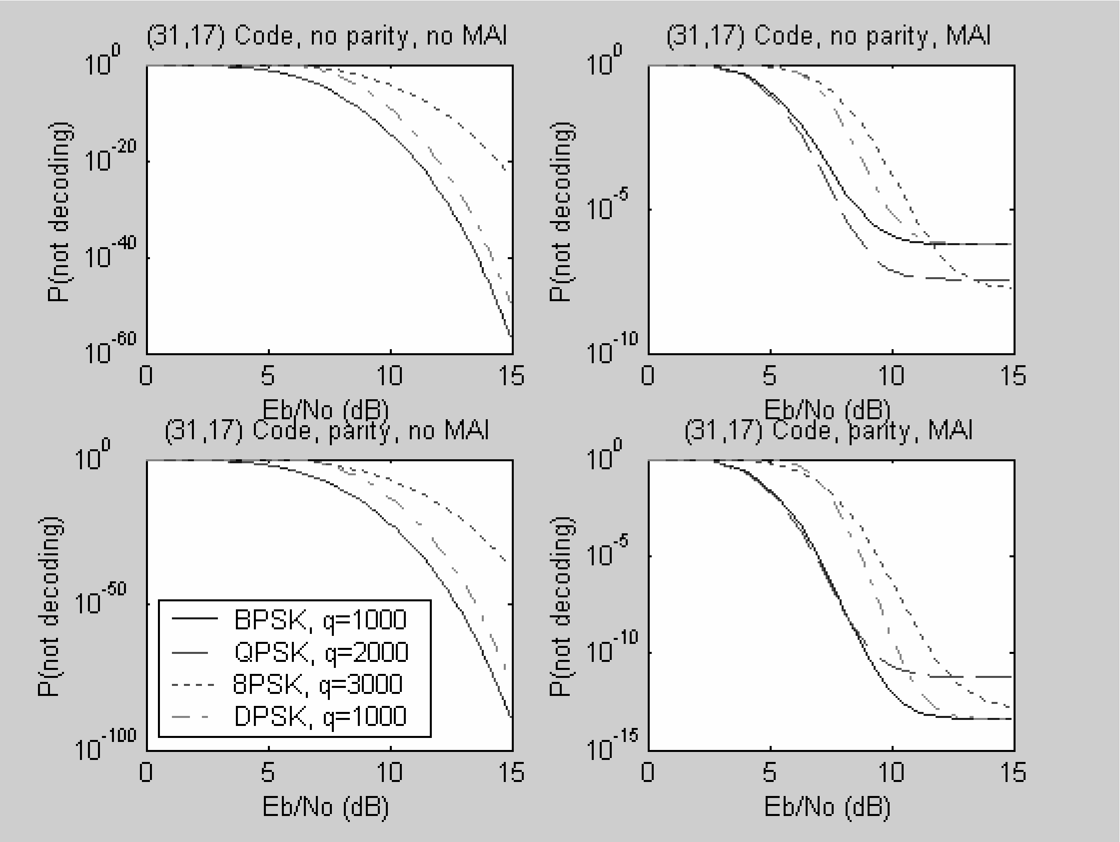


Figure 7: (31,17) R-S Code

The plot in the upper left of the figure gives the probability of not decoding using errors only decoding when there is no multiple-access interference. Notice that the traces for BPSK and QPSK are the same because they have the same probability of bit error. The 8PSK scheme is worse when there is no multiple-access interference because there is a higher probability of bit error in 8PSK. In the upper right, multiple-access interference is added. The bandwidth advantage from using QPSK or 8PSK becomes clear in this case at high bit energy to noise ratios. The two plots in the bottom half of the figure show the same situation when errors and erasures decoding is used. Surprisingly, it appears that BPSK is the best choice in this situation. This result may seem incorrect, but there is a major difference between the upper and lower plots: the number of bits per code symbol. For errors only decoding, there are five bits per code signal. Because five is neither divisible by two nor three, neighboring code symbols are not independent for QPSK and 8PSK. When errors and erasures decoding is used, there are six bits per code symbol. Because six is divisible by two and three, neighboring code symbols are independent in every case. Thus, there is no reason to expect the best scheme in the no parity case to also be the best scheme in the parity case.

Figure 8 illustrates the probability of not decoding for a (15,9) code with 10 users and with 100 users. As described above, the BPSK and DPSK signals use 1000 frequencies, while the QPSK and 8PSK signals use 2000 and 3000 frequencies, respectively. Ten symbols are transmitted per hop. The two plots on the upper half of the figure illustrate an errors only system. When only 10 users are present, the probability of a hit for the DPSK and BPSK signals are about 1%. For QPSK, the hit probability is about .5%, and for 8PSK it is about .3%. At these low hit probabilities, it is nearly impossible to predict which modulation scheme will be best. When 100 users are present, the probability of a hit increases by more than ten times. At high levels of multiple-access interference, the bandwidth reduction gained with QPSK and 8PSK systems results in a much lower probability of not decoding.

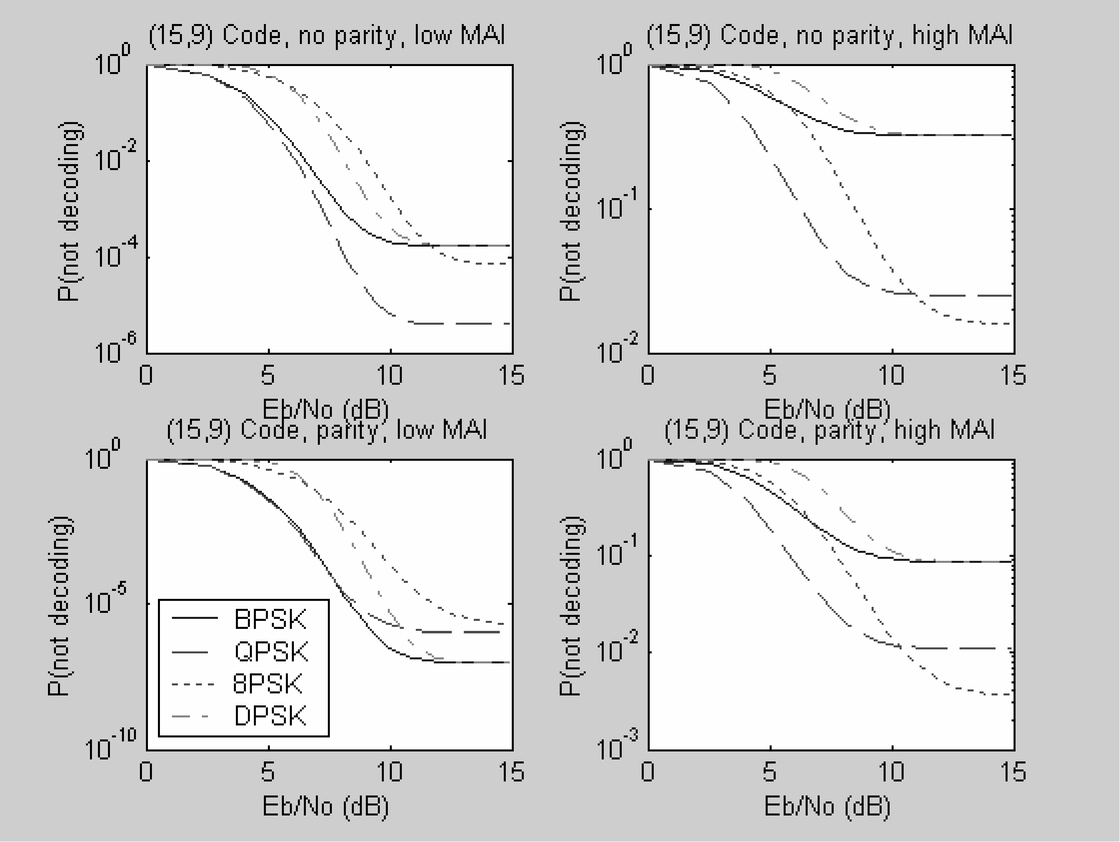


Figure 8: (15,9) RS Code

IX. Conclusions

Reed-Solomon codes provide effective defense against AWGN and, especially, multiple-access interference. Without some form of error correcting code, even a small amount of multiple-access interference can cause extremely high error rates.

There is lower limit to the probability of not decoding which depends only on the probability of a hit, the amount of redundancy in the code (*n*-*k*), and whether errors only or errors and erasures decoding is used. Future work may seek to find an algorithm to determine these limits for a given modulation method and coding scheme.

When no multiple-access interference exists, BPSK and QPSK produce the lowest probabilities of not decoding, because they have the smallest probability of bit error. For low levels of MAI, the best modulation method cannot be easily predicted. When high levels of MAI exist, 8PSK provides the lowest probability of not decoding given a high enough bit energy to noise ratio.

The exact calculation of the probability of not decoding is tedious when transmission symbol interleaving is used. Simulation of the system would provide an easy check on the results obtained here. Investigation of different methods of interleaving (bit level, no interleaving) may provide useful comparisons with the system analyzed here.

References

[1] E. O. Geraniotis and M. B. Pursley, "Error Probabilities for Slow-Frequency-Hopped Spread-Spectrum Multiple-Access Communications Over Fading Channels" IEEE Trans. on Communication, vol. Com-30, no. 5, pp. 996-1009, May 1982.

[2] Lathi, B.P., Modern Digital and Analog Communication Systems, 3rd. Ed., New York and Oxford: Oxford University Press: 1998.

[3] Lee, P.J., "Computation of the BER of Coherent M-ary PSK with Gray Code Bit Mapping," IEEE Transactions on Communications, vol. COM-34, no. 5, May 1986, pp. 488-491.

[4] Wicker, Stephen B., *Error Control Systems for Digital Communication and Storage*, Upper Saddle River, New Jersey: Prentice Hall, 1995.