# SIMPLE CODING TECHNIQUES FOR HIGH-FREQUENCY RADIO COMMUNICATION

by

HENRY DAVID GOLDFEIN

S. B., Massachusetts Institute of Technology

1965

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREES OF

MASTER OF SCIENCE

AND

ELECTRICAL ENGINEER

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February, 1968

Signature of Author Signature redacted
Department of Electrical Engineering, February 5, 1968

Certified by Signature redacted
Thesis Supervisor

Accepted by Signature redacted
Chairman, Departmental Committe on Graduate Students

# SIMPLE CODING TECHNIQUES FOR HIGH-FREQUENCY RADIO COMMUNICATION

by

HENRY DAVID GOLDFEIN

Submitted to the Department of Electrical Engineering on February 5, 1968 in partial fulfillment of the requirements for the degrees of Master of Science and Electrical Engineer.

## ABSTRACT

The use of cyclic group codes for the correction of bursts of erasures and randomly spaced errors is examined. When the digits of short block length burst erasure correcting codes are separated in time these codes are useful for a large variety of radio channel fading characteristics. The decoders for cyclic codes which are being used to correct long bursts of erasures and small numbers of errors are much less complex than decoders for the correction of randomly spaced erasures or large numbers of errors.

Thesis Supervisor: Robert G. Gallager
Title: Professor of Electrical Engineering

# Table of Contents

# List of Figures and Tables

# Chapter I

# INTRODUCTION

In this thesis a class of relatively easy to implement codes for use on high-frequency ionospheric-scatter radio channels is developed. The approach taken here is to use cyclic group codes in a communication system which corrects both errors and erasures. In Chapters 2 and 3 it is shown that there are several classes of codes which are easy to decode, and which can be used to correct the sets of erasures and errors which are most likely to occur on these radio channels.

## 1.1) A Model of the Radio Channel

A general model for the effects of a high-frequency ionospheric-scatter radio channel on a set of narrow-band, time-limited waveforms is extremely complicated. The channels are dispersive, due principally to multipath propagation, and the received signal amplitude has a Rayleigh or Rician probability density. Amplitudes for successive signals are correlated, and the correlation coefficient depends on both time delay, and difference in frequency. Noise intensity varies slowly with respect to the random fading, but the noise is not white or Gaussian. In this thesis the signaling waveforms to be considered are sets of K equal-energy, narrow-band, time-limited orthogonal signals. The signals must

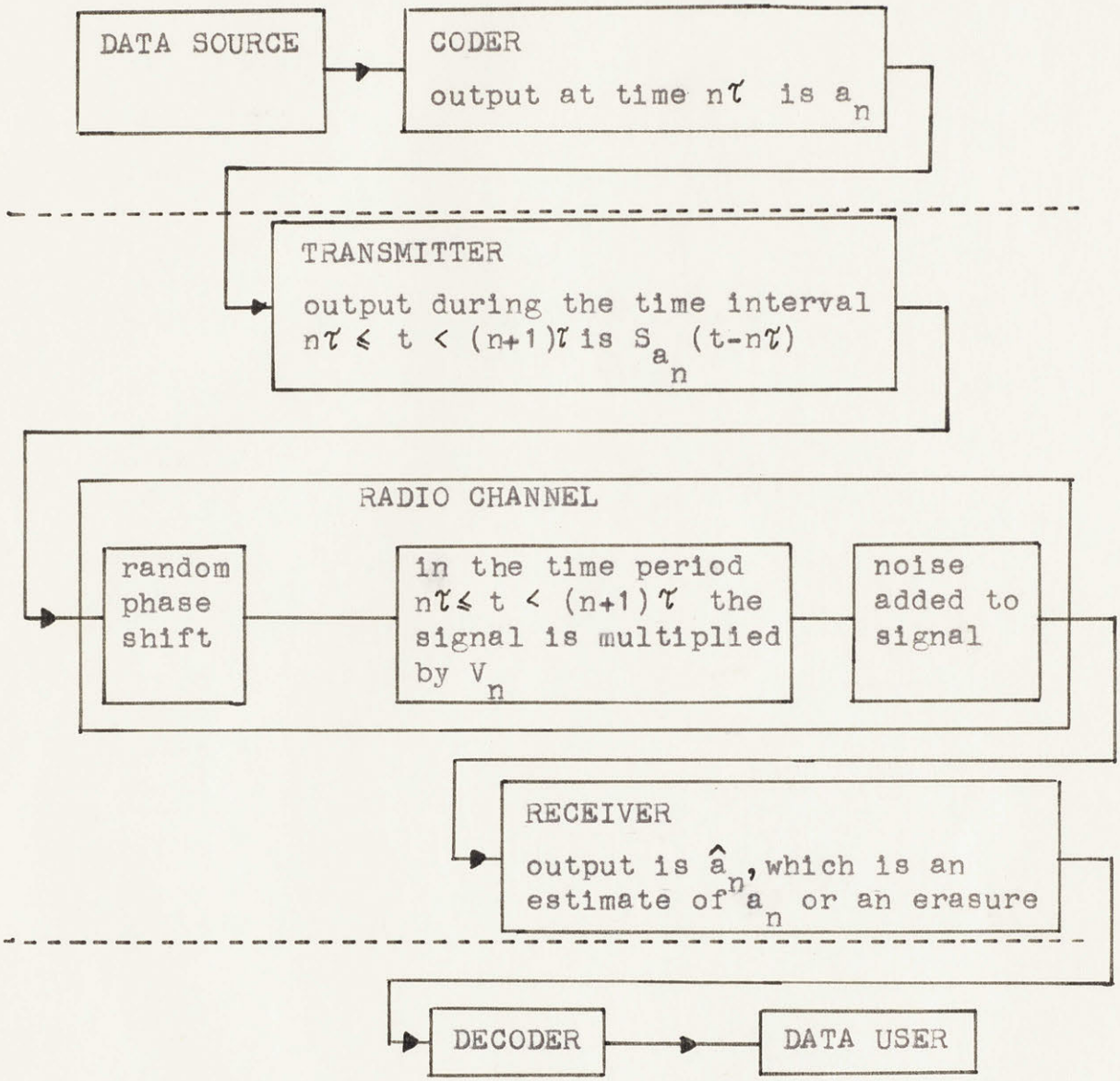


Figure 1-1: Model of a high-frequency radio communication system.

be spaced closely enough in frequency so that the amplitude of the received signal will be approximately the same, regardless of which signal was transmitted, and the number of signals per second must be small enough so that the intersymbol interference due to multipath propagation effects can be ignored. Under these conditions the noise may be modeled as approximately white. A model of the communication system to be considered is shown in Figure 1-1. The $V_n$, which are defined in Figure 1-1, are correlated Rayleigh or Rician random variables. The time variation of the $V_n$ is such that the channel produces randomly spaced fades in the received signal strength, which typically occur .1 to 10 seconds apart.

The receiver shown in Figure 1-1 makes independent maximum likelihood decisions on the waveforms received in each time interval. The receiver output is either the number of the waveform which is most likely to have been transmitted, or if the maximum of the energies in each of the K sub-channels is below some threshold, an erasure. The length of time for which the $V_n$ are above or below any threshold is approximately exponentially distributed, which leads, as a rough approximation, to a Markov model for the erasure generation process. A simple model for the properties of the part of the channel of Figure 1-1 between the

dotted lines, which can account for most of the properties of the radio link, under the assumptions made above, is shown in Figure 1-2. A detailed description of the properties of high-frequency ionospheric-scatter radio channels is given in references (1) and (2).

## 1.2) Coding for High-Frequency Radio Channels

Most known codes for the correction of randomly spaced errors and erasures can correct only relatively small numbers of erasures and errors. There is, however, a large class of cyclic codes which can correct long bursts of erasures, or errors, and small numbers of randomly spaced errors. In Chapter 2 several techniques are developed for examining the ability of cyclic codes to correct the most likely error patterns on the channel of Figure 1-2. It is shown that codes with a small block length can efficiently correct a small number of random errors and long bursts of erasures. In Chapter 3 the effects of interspacing the digits of several code words to form a set of codes which are useful for a large range of channel fading characteristics are examined.

Despite the rather extreme simplification involved in the model of the high-frequency radio channel presented above, there are still several rather complex tradeoffs which must be made in the selection of a

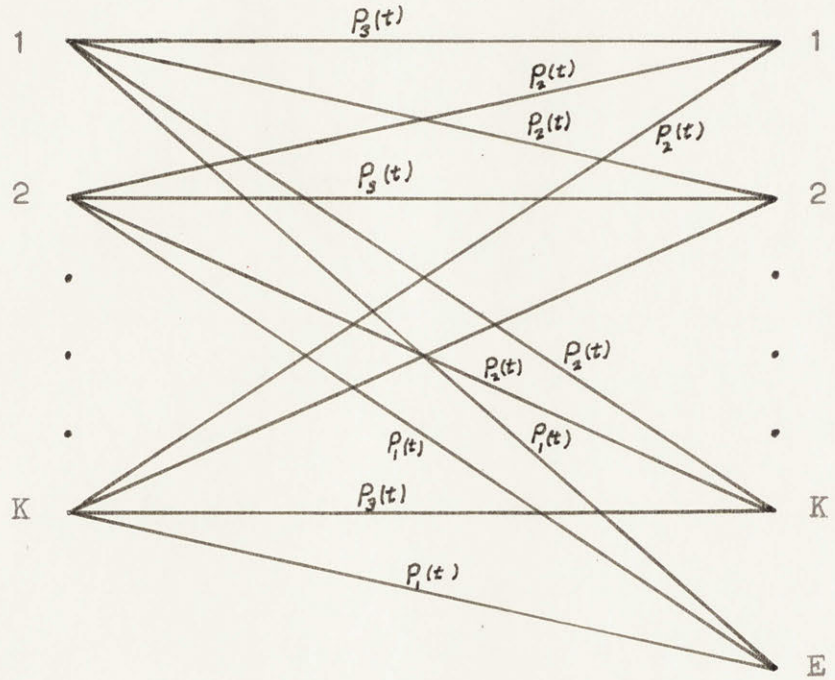


Figure 1-2: Model of a K ary erasure channel with memory.

specific code for use on a given channel. Also, due to the large variation in characteristics that can be observed on one radio link over time periods of only a few hours, it is necessary that any code be able to correct a large variety of error-erasure patterns in order to be useful. In particular the following four variables must be determined:

1. Code Alphabet Size: Because of the restriction on channel symbol rate imposed by multipath propagation the use of large signal sets may be the only way to achieve high data rates.

2. Codeword Length: This involves a tradeoff between short block length and a relatively small number of correctable random errors, and longer block lengths which require more complex decoders but can correct much larger numbers of random errors.

3. The Number of Codewords to be Interspaced: Here the tradeoff is between the length of bursts which can be corrected, and the length of the memory required in the decoder.

4. Receiver Erasure Threshold: The relative numbers of erasures and errors, and the relative lengths of erasure and error bursts can be controlled by setting the erasure threshold. When the code and the number of interspaced codewords to be used have been determined,

the erasure threshold will be the only easily varied parameter which can change the decoder characteristics and thereby permit the minimization of error probability for different sets of channel characteristics.

# Chapter 2

## BLOCK CODES FOR THE CORRECTION OF RANDOM ERRORS AND ERASURE BURSTS

### 2.1) Cyclic Codes

In this chapter it is assumed that the reader is acquainted with most of the material on cyclic codes presented in references (3) or (4). In order to make the conventions and definitions used in the remainder of this chapter more explicit, we review a few of the properties of cyclic codes.

A cyclic code can be defined to be any code with digits selected from a finite field with Q elements, which satisfies the following two conditions: (a) any cyclic shift of the digits of a codeword is a codeword, and (b) any digit by digit sum of two codewords is a codeword.

All finite fields with Q elements are isomorphic to the Galois Field with Q elements, denoted by GF(Q). Such fields exist only when $Q = q^m$ for some prime number p, and some integer m. Therefore, cyclic codes exist only with digits selected from sets of $q^m$ symbols.

The digits of a codeword can be specified by an N tuple, $(a_{N-1}, a_{N-2}, \ldots a_o)$ and to each such N tuple we can assign a unique polynomial $a(X) = a_{N-1}X^{N-1} + \ldots + a_o$ which also specifies the digits of the codeword. In this thesis

we are dealing with channels with memory, and the order in which the digits of the codeword are transmitted is important. We will assume that $a_o$ is the first digit transmitted, and that $a_{N-1}$ is the last digit.

All of the codewords of a cyclic code of length N can be generated by multiplying some polynomial G(X), with coefficients selected from GF(Q), and which has degree N-k, by each of the $Q^k$ possible polynomials $I(X) = i_{k-1}X^{k-1} + i_{k-2}X^{k-2} + \ldots + i_0$. Also every codeword has a unique representation of the form $a(X) = I(X)G(X)$. In this chapter we will consider I(X) to be the polynomial of the data source digits which we are attempting to transmit.

The length of the cyclic code generated by the polynomial G(X) will be assumed to be the smallest number N for which G(X) divides $X^N-1$. Cyclic codes exist for all N such that G(X) divides $X^N-1$, but if G(X) also divides $X^j-1$, $j<N$, then $X^j-1$ is a codeword in the code of length N, and that code cannot correct any errors. If a code is used to correct only erasures, then this restriction on code length is not necessary.

## 2.2) Channel Model

The channel model of Figure 1-2 can be further simplified as shown in Figure 2-1. Here b(t) is the only time varying quantity, p is a constant: $0 \leq p < \frac{1}{K}$. The

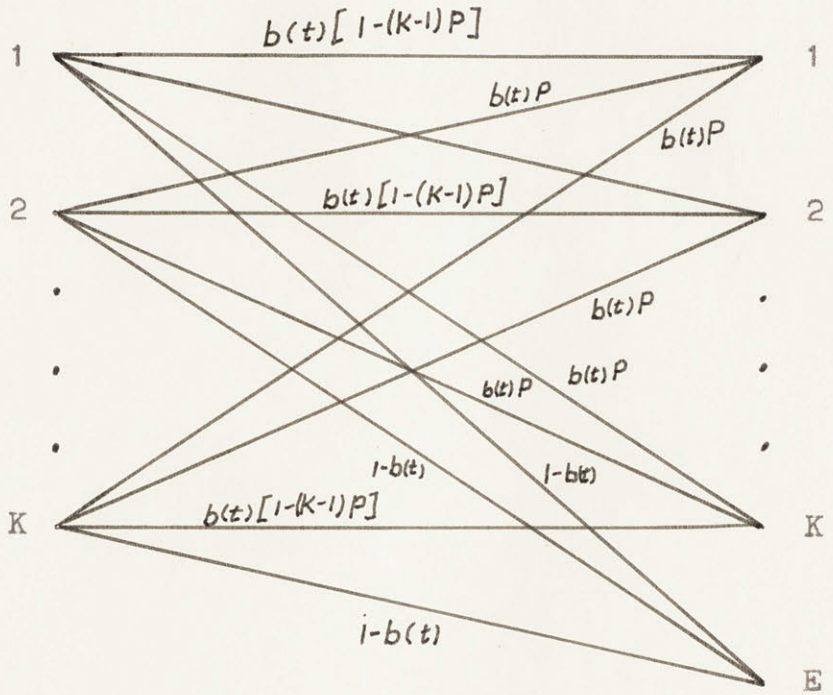


Figure 2-1: Simplified model of a K ary erasure channel with memory.

conditional probabilities $p(j|k,\not E)$, where j is an output digit, k is an input digit, and $\not E$ signifies that the output is not an erasure, are the transition probabilities of a memoryless K-ary symmetric channel. Since we are considering only cyclic codes we will restrict the values of K to $q^m$ for q any prime number, and m any integer.

A cyclic burst of length $\ell$ is defined to be either a set of $\ell$ consecutive digits contained in the codeword of length N, or the first j, and the last $\ell$-j digits of the codeword, for any $j: 0 \leq j \leq \ell$. In the remainder of this thesis, unless otherwise specified, we will mean, when we say a burst of erasures of length $\ell$, any set of erasures such that all of the erased digits are contained in some cyclic burst of length $\ell$.

## 2.3) Codes for Correction of Bursts of Erasures

Assume that no errors occur. If it is possible to decode correctly all received codewords containing erasure bursts of length $\ell$ or less, then the code can have at most $K^{N-\ell}$ distinct codewords, so the dimensionless code rate must be less than $\frac{N-\ell}{N}$. We now demonstrate a large class of codes which meet this bound.

Let G(X) be any polynomial of degree $\ell$ with coefficients from $GF(q^m)$, which divides $X^N-1$. The cyclic code of length N generated by G(x) can correct any erasure burst of length $\ell$ or less. This is shown by specifying a possible correction procedure.

Any cyclic shift of a codeword is also a codeword, and because of the cyclic symmetry of the code, any cyclic shift of a correctable pattern of erasures and errors must also be a correctable pattern. $R_{G(x)}[f(X)]$ is defined to be the remainder of f(X) when divided by G(X). The erasures in the received codeword, r(X), are replaced by zeros, and then the digits of the received codeword are shifted cyclically until the erasure burst is contained in the $\ell$ lowest degree digits. If r'(X) is the shifted codeword, then the erasures can be filled in by adding $-R_{G(X)}[r'(X)]$ to r'(X) and then shifting back to the original position.

A more complicated proof of the same property of cyclic codes is given below. This proof is included because it generalizes to an interesting method for determining other properties of these codes, which will be developed in sections 2.4 and 2.5.

The transmitted codeword is I(X)G(X) and the received codeword is denoted by r(X), where the erased digits are replaced by zeros. We choose as a syndrome polynomial S(X), which is defined by

$$S(X) = S_0 + S_1 X + \ldots + S_{\ell-1} X^{\ell-1} \triangleq R_{G(X)}[r(X)] \tag{2-1}$$

Furthermore we define $\alpha_j(X)$ by

$$\alpha_j(X) = \alpha_{j,0} + \alpha_{j,1} X + \ldots + \alpha_{j,\ell-1} X^{\ell-1} \triangleq R_{G(X)}[X^j] \tag{2-2}$$

Then $\alpha_j(X)$ is the syndrome polynomial which would result if the digit -1 were erased in the j+1 th digit of the codeword.

For any codeword $I(X)G(X)$ we know that $R_{G(X)}[I(X)G(X)] = 0$, therefore when $E(X)$ is the polynomial of erased digits;

$$S(X) = R_{G(X)}[r(X)] = R_{G(X)}[I(X)G(X)-E(X)]$$
$$= -R_{G(X)}[E(X)] \qquad (2\text{-}3)$$

To determine $E(X)$ the decoder can solve the equation

$$\sum_{\{j\}} E_j R_{G(X)}[X^j] = \sum_{\{j\}} E_j \alpha_j(X) = -S(X) \qquad (2\text{-}4)$$

where $\{j\}$ is the set of erased digits. When the set of erased digits is a burst extending from the ith to the $i + \ell$-1th digit of the codeword, this equation can be written as

$$\sum_{k=0}^{\ell-1} E_{i+k} \alpha_{i+k}(X) = -S(X) \qquad (2\text{-}5)$$

which is equivalent to the matrix equation

$$\begin{bmatrix} \alpha_{i,0} & \cdots & \alpha_{i+\ell-1,0} \\ \alpha_{i,1} & & \vdots \\ \vdots & & \\ \alpha_{i,\ell-1} & \cdots & \alpha_{i+\ell-1,\ell-1} \end{bmatrix} \begin{bmatrix} E_i \\ \vdots \\ E_{i+\ell-1} \end{bmatrix} = - \begin{bmatrix} S_0 \\ \vdots \\ S_{\ell-1} \end{bmatrix} \qquad (2\text{-}6)$$

This equation has a unique solution if, and only if, the $\underline{\alpha}_i = [\alpha_{i,0},\ldots,\alpha_{i,\ell-1}]$ are linearly independent. We need only show that $\underline{\alpha}_i,\ldots,\underline{\alpha}_{i+\ell-1}$ are linearly independent for all i, and this can be done by induction. First $[\underline{\alpha}_0,\underline{\alpha}_1,\ldots\underline{\alpha}_{\ell-1}] = \underline{I}$, where $\underline{I}$ is the $\ell$ x $\ell$ identity matrix. So $\underline{\alpha}_0,\ldots,\underline{\alpha}_{\ell-1}$ are linearly independent. Assume that $\underline{\alpha}_i,\ldots$ $\underline{\alpha}_{i+\ell-1}$ are linearly independent. Starting from the definition of $\alpha_{i+\ell}$ we have

$$\alpha_{i+\ell}(X) = R_{G(X)}\left[X^{i+\ell}\right]$$

$$= R_{G(X)}\left[X^i\, X^\ell\right]$$

$$= R_{G(X)}\left[X^i\left(-g_0 - g_1X - \ldots - g_{\ell-1}X^{\ell-1}\right)\right]$$

$$= -g_0R_{G(X)}\left[X^i\right] - g_1R_{G(X)}\left[X^{i+1}\right] - \ldots - g_{\ell-1}R_{G(X)}\left[X^{i+\ell+1}\right]$$

$$= -g_0\alpha_i(X) - g_1\alpha_{i+1}(X) - \ldots - g_{\ell-1}\alpha_{i+\ell-1}(X) \qquad (2\text{-}6)$$

or equivalently;

$$\underline{\alpha}_{i+\ell} = -g_0\underline{\alpha}_i - \ldots - g_{i+\ell-1}\underline{\alpha}_{i+\ell-1} \qquad (2\text{-}7)$$

Since g(X) divides $X^N-1$ for some N, $g_0$ cannot be zero. Then, since the vectors $\underline{\alpha}_i, \ldots \underline{\alpha}_{i+\ell-1}$ span an $\ell$ dimensional vector space, the vectors $\underline{\alpha}_{i+1}, \ldots \underline{\alpha}_{i+\ell}$ must span the same space, and must therefore be linearly independent.

There are two particularly interesting sets of cyclic codes for burst erasure correction. The BCH codes have been extensively studied and reasonably simple procedures exist for the simultaneous correction of erasures and errors; these codes are discussed in section 2.3. A second class is the set of codes generated by $G(X) = \frac{X^N-1}{X-1} = 1+X+\ldots+X^{N-1}$, which consist of N repetitions of the same digit. It can be seen that when the code symbols are spaced sufficiently far apart in time this corresponds to N'ple time diversity, with a sub-optimum signal combiner. These codes are useful primarily because of the extremely simple realization of communication systems using them. However, they suffer from a very limited ability to correct errors.

## 2.4) Correction of Erasure Bursts and Errors

There is no loss of generality in assuming that the erasure burst starts at the first digit of the received codeword since any other error and erasure pattern is equivalent to one of this form, except for a cyclic shift. The syndrome is then

$$S(X) = R_{G(X)}\,[-E(X)-e(X)] = -E(X)-R_{G(X)}[e(X)] \qquad (2\text{-}8)$$

where E(X) is the polynomial of erasures, and e(X) is the negative of the polynomial of errors. If there are $\ell$ erasures in the burst, and the degree of G(X) is k, then there are k-$\ell$ linear equations which may be used to correct errors. This is because each of the first $\ell$ digits of S(X) is the sum of a different unknown erased digit and a function of the errors, but the last k-$\ell$ digits are functions of the errors only. This provides a particularly simple technique for testing the ability of a code to correct single errors in addition to erasure bursts. If the coefficients of the k-$\ell$ highest order terms of $\alpha_i(X)$ and $\alpha_j(X)$ are linearly independent, then the code can distinguish between errors in the ith, and jth digits after the first digit of an erasure burst. We examine the properties of the (15, 7) binary BCH code to illustrate this technique. From section 2.3 we know that this code can correct bursts of up to 8 erasures if no errors occur. By using the data in Table 2-1 we can see that if there is a burst of 4 erasures, then the code cannot distinguish between errors in the 4th and 11th, or the 9th and 13th, or the 10th and 14th positions. If there is a burst of 3 erasures then the code cannot distinguish between errors in the 9th and 13th positions. If the burst contains only two erasures, then the code can correct all single errors.

Table 2-1

The coefficients of $R_{G(X)}\left[X^i\right]$ represented as column vectors. G(X) is the generator polynomial for a (15,7) binary BCH code; $G(X) = X^8+X^7+X^6+X^4+1$.

| i= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |

The set of all possible single error syndrome sequences when there is a burst of 4 erasures.

The set of all possible single error syndrome sequences when there is a burst of 3 erasures.

An equivalent technique is to examine the alternate syndrome polynomial,

$$S(X) = R_{X^N-1}[h(X)\, r(X)] \tag{2-9}$$

where h(X) is defined by

$$h(X) = \frac{X^N-1}{G(X)} \tag{2-10}$$

We have already stated that G(X) must be a factor of $X^N-1$. Then we have

$$\begin{aligned} S(X) &= R_{X^N-1}[I(X)\, G(X)\, h(X) - e(X)\, h(X) - E(X)\, h(X)] \\ &= -R_{X^N-1}[e(X)\, h(X)] - R_{X^N-1}[E(X)\, h(X)]. \end{aligned} \tag{2-11}$$

As in the previous case we can cycle the received codeword until all erasures are contained in the smallest possible burst which starts at the first digit of the received codeword. If $\ell$ digits are erased and the degree of h(X) is k, the coefficients $s_0, s_1, \ldots, s_{\ell+k-1}$ of the lowest order terms of S(X) will be functions of the erased digits, but $S_{\ell+k}, s_{\ell+k+1}, \ldots, s_{N-1}$ will not be functions of the erased digits. Then if $s_{\ell+k}, s_{\ell+k+1} \ldots s_{N-1}$ differ for two sets of errors, the code generated by G(X) can distinguish between those two sets of errors. This provides another technique for determining the ability of

a code to correct single errors when a burst of $\ell$ erasures has occurred. If a single error occurs in the ith digit after the first digit of the erasure burst, then the code can distinguish between all single errors for which one or more of the $N-\ell-k$ highest order coefficients of $R_{X^N-1}[X^i h(X)]$ are different. We use as an example the binary (31, 21) BCH code. The coefficients of the polynomials $R_{X^N-1}[X^i h(X)]$ are given in Table 2-2. Each row of this table is a one-step cyclic shift of the previous row, and the first row consists of the coefficients of h(X). If there are 4 erasures, then the code can distinguish between all single errors except those which occur in the 19 or 27th and 21 or 26th positions after the first digit of the erasure burst. If there are 3 erasures the code can correct all single errors.

Clearly the determination of the properties of a code by the examination of the individual possible syndrome sequences can become extremely complicated if any but the simplest information about short codes is required. We now develop a technique for providing some insight into the classes of error sequences which a code can reasonably be expected to handle.

We consider codes with generator polynomials which can be written in the form $G_1(X)G_2(X)$, where $G_1(X)$ and

Table 2-2

The coefficients of the seven highest degree terms of $R_{X^{31}-1}[h(X)\,X^i]$.

$$h(X) = 1 + X^3 + X^5 + X^8 + X^{11} + X^{12} + X^{13} + X^{14} + X^{16} + X^{18} + X^{20} + X^{21}$$

| i = | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 6 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 7 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| 8 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 9 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 10 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 11 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 12 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| 13 | 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| 14 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |
| 15 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| 16 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| 17 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| 18 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 19 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 20 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 21 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 22 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 23 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 24 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 25 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 26 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 27 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 28 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 29 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 30 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

The set of all possible single error syndrome sequences when there is a burst of 3 erasures

The set of all possible single error syndrome sequences when there is a burst of 5 erasures

$G_2(X)$ are relatively prime polynomials of degree $\ell$, and the smallest N for which $G_1(X)G_2(X)$ divides $X^N-1$ is the codeword length. We use two syndrome polynomials;

$$S_1(X) \triangleq R_{G_1(X)}[r(X)], \quad S_2(X) \triangleq R_{G_2(X)}[r(X)] \tag{2-12}$$

These two syndromes together are equivalent to the single syndrome, $S_0(X) = R_{G(X)}[r(X)]$, used above in the sense that either syndrome can be determined from the other.

$$S_1(X) = R_{G_1(X)}[S_0(X)], \quad S_2(X) = R_{G_2(X)}[S_0(X)] \tag{2-13}$$

And therefore we can write

$$S_0(X) = a_1(X)G_1(X) + S_1(X) \tag{2-14A}$$

$$= a_2(X)G_2(X) + S_2(X) \tag{2-14B}$$

If we are given $S_1(X)$ and $S_2(X)$ we can solve for $a_1(X)$ and $a_2(X)$ to find $S_0(X)$ by using the equation

$$a_1(X)G_1(X)-a_2(X)G_2(X) = S_2(X)-S_1(X) \tag{2-15}$$

If this equation does not have a unique solution for $a_1(X)$ and $a_2(X)$, both of degree less than or equal to $\ell-1$, then there must be some nonzero $a_3(X)$ and $a_4(X)$, both of degree less than or equal to $\ell-1$ such that

$$a_3(X)G_1(X)-a_4(X)G_2(X) = 0 \tag{2-16}$$

or

$$a_3(X) = \frac{G_2(X)}{G_1(X)} \; a_4(X) \tag{2-17}$$

For equation 2-17 to have a solution $G_1(X)$ must divide $a_4(X)$ since $G_1(X)$ and $G_2(X)$ are relatively prime. But the degree of $a_4(X)$ is less than the degree of $G_1(X)$. Therefore $a_1(X)$ and $a_2(X)$ are uniquely determined and $S_0(X)$ must be uniquely determined by $S_1(X)$ and $S_2(X)$. The same proof requires only minor modification when the degrees of $G_1(X)$ and $G_2(X)$ are not the same.

We can now derive an equation which must be satisfied by the error polynomial. We again assume that the erasure burst begins at the first digit of the codeword. $r(X)$ is given by

$$r(X) = G_1(X)G_2(X)I(X) - e(X) - E(X) \tag{2-18}$$

The two syndrome polynomials satisfy the equations:

$$S_1(X) = R_{G_1(X)}[r(X)] = -R_{G_1(X)}[e(X)] - R_{G_1(X)}[E(X)] \tag{2-19A}$$

$$S_2(X) = R_{G_2(X)}[r(X)] = -R_{G_1(X)}[e(X)] - R_{G_2(X)}[E(X)] \tag{2-19B}$$

Since we have assumed that the erasures occur in the first $\ell$ digits of the codeword these equations are equivalent to

$$-S_1(X) = R_{G_1(X)}[e(X)] + E(X) \tag{2-20A}$$

$$-S_2(X) = R_{G_2(X)}[e(X)] + E(X) \tag{2-20B}$$

Subtracting $S_1(X)$ from $S_2(X)$ we have

$$S_2(X)-S_1(X) = -R_{G_2(X)}[e(X)] + R_{G_1(X)}[e(X)] \tag{2-21}$$

If we define $\alpha_i(X) = R_{G_1(X)}[X^i]$, $\beta_i(X) = R_{G_2(X)}[X^i]$ then these equations can be rewritten as

$$S_2(X)-S_1(X) = \sum_{i=\ell}^{N-1} e_i(\alpha_i(X)-\beta_i(X)). \tag{2-22}$$

Or equivalently we have the matrix equation

$$\underline{S}_2-\underline{S}_1 = \begin{bmatrix} S_{2,1}-S_{1,1} \\ \vdots \\ S_{2,\ell-1}-S_{1,\ell-1} \end{bmatrix} = \begin{bmatrix} \alpha_{\ell,0}-\beta_{\ell,0},\ldots,\alpha_{N-1,0}-\beta_{N-1,0} \\ \vdots \\ \alpha_{\ell,\ell-1}-\beta_{\ell,\ell-1} \end{bmatrix} \begin{bmatrix} e_\ell \\ \vdots \\ e_{N-1} \end{bmatrix} \tag{2-23}$$

The minimum hamming distance between two $\underline{e}$ which satisfy this equation is equal to the number of members of the smallest set of linearly independent $(\alpha_i-\beta_i)$, $\ell \leq i \leq N-1$.

If $G_1(X)$ has degree $\ell$, $G_2(X)$ has degree L, $\ell < L$, and a burst of $\ell$ erasures occurs at the beginning of a code-word, then the syndrome polynomials still satisfy equation 2-22, but the matrix equation becomes

$$\underline{S}_2-\underline{S}_1 = \begin{bmatrix} \alpha_{\ell,0}-\beta_{\ell,0},\ldots,\alpha_{N-1,0}-\beta_{N-1,0} \\ \vdots \\ \alpha_{\ell,\ell-1}-\beta_{\ell,\ell-1} \\ 0-\beta_{\ell,\ell} \\ \vdots \\ 0-\beta_{\ell,L-1},\ldots,0-\beta_{N-1,L-1} \end{bmatrix} \begin{bmatrix} e_\ell \\ \vdots \\ e_{N-1} \end{bmatrix} \tag{2-24}$$

Equation 2-23 or equation 2-24 can be used to determine the ability of any code, which is generated by the product of two relatively prime polynomials, to distinguish between two sets of errors when a burst of $\ell$ erasures occurs. For example if each of the $(\underline{\alpha}_i - \underline{\beta}_i)$: $i \geqslant \ell$ is different , then the code can distinguish between all single errors. Therefore, the code can be used to correct all single errors when a burst of $\ell$ or fewer erasures occurs. As an example of this technique we use equation 2-23 to examine the properties of the (15,7) binary BCH code.

The $(\underline{\alpha}_i - \underline{\beta}_i)$ are tabulated in Table 2-3. Examination of this table shows the same result as the previous example using this code.

Table 2-3

Values of $(\underline{\alpha}_i - \underline{\beta}_i)$ for the (15,7) binary BCH code generated by $G(X) = G_1(X)G_2(X)$; $G_1(X) = X^4+X+1$, $G_2(X) = X^4+X^3+X^2+X+1$

| i = | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| | erased digits | | | | | | | | | | | | | | |

If the generator polynomial of a cyclic code is the product of three relatively prime polynomials of degree $\ell$; $G_1(X)$, $G_2(X)$ and $G_3(X)$, then there are three equations which the errors must satisfy;

$$S_2 - S_1 = [\underline{\alpha}_\ell - \underline{\beta}_\ell, \ldots, \underline{\alpha}_{N-1} - \underline{\beta}_{N-1}] \underline{e} \tag{2-26A}$$

$$S_2 - S_3 = [\underline{\gamma}_\ell - \underline{\beta}_\ell, \ldots, \underline{\gamma}_{N-1} - \underline{\beta}_{N-1}] \underline{e} \tag{2-26B}$$

$$S_1 - S_3 = [\underline{\gamma}_\ell - \underline{\beta}_\ell, \ldots, \underline{\gamma}_{N-1} - \underline{\beta}_{N-1}] \underline{e} \tag{2-26C}$$

A code of this type can distinguish between any single errors which can be distinguished between by use of any one of the three equations above. Each of the three syndrome pairs will have a set of single errors which it cannot be used to distinguish between, but since each of the three syndrome pairs satisfies a different equation the sets of indistinguishable errors will be different for each equation.

Two well-known classes of codes which appear to be useful for the correction of erasure bursts and errors are the BCH codes ( 3,4 ) and the fire codes ( 3 ). In most cases the generator polynomial of a member of either of these classes of codes can be written as the product of two or more polynomials. General methods for correction of erasures and errors in BCH codes have been described by Forney (7), Berlekamp (6) and Massey (5). When short

codes are used, the simplest decoding procedure may be to generate the syndrome of equation 2-1 or equation 2-9, and correct all correctable errors on the basis of the syndrome digits which are not functions of the erased digits. The erasure burst may then be filled in by use of the shift register circuit described in section 2.3.

It would be convenient to find a method whereby erasures can be filled in first, and then the errors corrected by use of a separate decoder. One approach to this is to use cyclic codes generated by polynomials of the form $G_1(X)G_2(X)$. The shift register circuit of section 2.3 is used with $G_1(X)$ to fill in erasures, and then the errors are corrected using the second polynomial, $G_2(X)$. Unfortunately the test given by equation 2-23 indicates that many codes of this form will not even be able to correct single errors when a burst of $\ell$ erasures occurs. The error corrector, which follows the erasure corrector, cannot be a minimum hamming distance decoder since most single errors will result in two or more errors when the erasure correction is finished. If the correction procedure is to first cycle the erasure burst to the beginning of the codeword, next fill in the erasure burst, then correct errors, and finally cycle the codeword back to its original position, then the input to the error corrector is

$$r'(X)-R_{G_1(X)}[r'(X)]$$

If r'(X) contains a single error, in the ith order term, then the polynomial of the errors at the input to the error corrector is

$$-e_iX^i+R_{G_1(X)}[e_iX^i] = -e_iX^i+e_i\alpha_i(X) \tag{2-27}$$

The number of errors in the input to the error corrector is equal to one plus the number of non-zero coefficients of $\alpha_i(X)$.

A generalization of this technique, which leads to non-cyclic codes, is to transmit $\ell$ additional digits with a codeword of length N. Each of the additional digits $a_{N+i}$: $0 \leq i \leq \ell-1$, is the sum of every $\ell$th digit of the codeword.

$$a_{N+i} = \sum_{j=0}^{(k:\ \ell k+i < N)} a_{j\ell+i} \tag{2-28}$$

The erasure burst can be filled in by using the $\ell$ additional check digits, and then the errors in the N digit codeword corrected. This type of code suffers from the same difficulty as the cyclic codes; when an erasure is filled in, many single errors in the N+$\ell$ digit codeword will result in two errors in the N digit codeword, so the decoder cannot be a minimum hamming distance decoder.

There are at least a few codes of this type which can correct all single errors in addition to erasure bursts of length $\ell$, for example, the (15,11) cyclic hamming code generated by $X^4+X+1$ with five additional parity checks.

## 2.5) Correction of Two Bursts of Erasures

Assume that the degrees of $G_1(X)$ and $G_2(X)$ are both equal to $\ell$, and that there are two bursts of $\ell$ or fewer erasures, one of which is at the beginning of the receive codeword. $r(X)$ is given by

$$r(X) = G_1(X)G_2(X)I(X) + E_1(X) + E_2(X) \tag{2-29}$$

Using the syndromes defined by equation 2-12, we have

$$S_1(X) = -E_1(X) - R_{G_1(X)}[E_2(X)], \tag{2-30A}$$

$$S_2(X) = E_1(X) - R_{G_2(X)}[E_2(X)], \tag{2-30B}$$

$$S_2(X) - S_1(X) = R_{G_1(X)}[E_2(X)] - R_{G_2(X)}[E_1(X)] \tag{2-31}$$

From this we get the matrix equation

$$S_2(X) - S_1(X) = [\underline{\alpha}_{j-1} - \underline{\beta}_{j-1}, \ldots, \underline{\alpha}_{j+\ell-2} - \underline{\beta}_{j+\ell-2}]\underline{E}_2 \tag{2-32}$$

when $E_2(X)$ extends from the jth to the $j+\ell-1$th digit of the received codeword. If the matrix above is non-singular for all j, the code can correct all double bursts

of $\ell$ or fewer erasures. There appear to be very few codes which satisfy this condition. These codes can correct one burst of $\ell$ erasures and one burst of L erasures, starting at the jth digit of the codeword if

$$[\underline{\alpha}_{j-1}-\underline{\beta}_{j-1}, \ldots, \underline{\alpha}_{j+L-2}-\underline{\beta}_{j+L-2}] \tag{2-33}$$

has degree L. L must be less than or equal to $\ell$. If the degree of $G_1(X)$ is $\ell$, and the degree of $G_2(X)$ is L, then the matrix which must be examined is

$$\begin{bmatrix} \alpha_{j-1,0}-\beta_{j-1,0} & \cdots & \alpha_{j+L-2,0}-\beta_{j+L-2,0} \\ \vdots & & \vdots \\ \alpha_{j-1,\ell}-\beta_{j-1,\ell-1} & & \\ 0-\beta_{j-1,\ell} & & \\ \vdots & & \\ 0-\beta_{j-1,L-1} & & \end{bmatrix} \tag{2-34}$$

and the code can correct one burst of $\ell \leq L$ erasures, and one burst of m erasures starting in the jth position where m is the number of consecutive linearly independent vectors starting from $(\underline{\alpha}_{j-1}-\underline{\beta}_{j-1})$.

# Chapter 3

# BLOCK LENGTH AND PROBABILITY OF ERROR

## 3.1) Channel Model

In this chapter the erasures generated by the channel of Figure 2-1 are modeled as being generated by a two state Markov process. When the channel is in state G no erasures occur, in state B all code digits are erased.

The codes discussed in Chapter 2 can simultaneously correct long bursts of erasures and a small number of errors. We now develop a procedure which permits the use of codes of this type on channels which, with high probability generate bursts of erasures which are too long to be corrected by one codeword. The coder forms n codewords simultaneously and transmits sequentially the first digit of each codeword followed by the second digit from each codeword, etc. The effective block length for this code is nN, and the code can correct error and erasure bursts n times as long as those corrected by the individual codewords. The receiver decodes each of the n component codewords independently of all other codewords.

When n is too small for a given code and channel the system will make errors because too many digits have been erased. If n is too large the erasure probability for successive code digits becomes independent.

Then the erasures will not necessarily be concentrated in bursts, and the only useful bound on the number of erasures and errors which can be corrected is $2t + s < d_{min}$, where t is the number of errors, s is the number of erasures, and $d_{min}$ is the minimum hamming distance between two codewords. In general $d_{min}$ is much smaller than half of the number of parity checks, so the code cannot correct as many erasures as it can when the erasures occur in bursts. Also decoders which can correct any pattern of erasures in addition to randomly spaced errors are much more complex than decoders which correct erasure bursts and only limited numbers of errors.

## 3.2) Selection of Code Block Length

The state transition matrix for the erasure generating Markov Process is;

$$\underline{P} \triangleq \begin{bmatrix} P_{G|G} & P_{B|G} \\ P_{G|B} & P_{B|B} \end{bmatrix} \triangleq \begin{bmatrix} a & 1-a \\ 1-b & b \end{bmatrix} \tag{3-1}$$

When n codewords are interlaced, the effective state transition matrix for each codeword is the n step transition matrix of the Markov Process, is given by ( 8 );

$$\underline{\Phi}(n) = \underline{P}^n = \frac{1}{2-a-b} \left\{ \begin{bmatrix} 1-b & 1-a \\ 1-b & 1-a \end{bmatrix} + (a+b-1)^n \begin{bmatrix} 1-a & a-1 \\ b-1 & 1-b \end{bmatrix} \right\} \tag{3-2}$$

For the burst erasure channel we have the constraints $\frac{1}{2} < a \leqslant 1$, $\frac{1}{2} < b \leqslant 1$. For convenience we define

$$\epsilon = a+b-1$$

$$\pi_g = \frac{1-b}{2-a-b}$$

$$\pi_b = \frac{1-a}{2-a-b}$$

We can now derive the probability of a cyclic burst of $\ell$ or fewer erasures. There are four classes of erasure bursts which must be considered. We list the probability of a burst of length $\ell$ or less, where it is known that the ith digit of the codeword is erased, and the ith digit is the first digit of the erasure burst.

$$i = 1; \qquad \left[\Phi_{G|G}(n)\right]^{N-\ell-1} \frac{1-a}{2-a-b} \Phi_{G|B}(\ell n) \tag{3-3}$$

$$2 \leqslant i \leqslant N-\ell; \qquad \left[\Phi_{G|G}(n)\right]^{N-\ell-2} \frac{(1-a)(1-b)}{2-a-b} \Phi_{G|B}(\ell n) \tag{3-4}$$

$$i = N-\ell+1; \qquad \left[\Phi_{G|G}(n)\right]^{N-\ell-1} \frac{(1-a)(1-b)}{2-a-b} \tag{3-5}$$

$$N-\ell+1+k \leqslant i, \quad 1 \leqslant k \leqslant \ell-1;$$

$$\left[\Phi_{G|G}(n)\right]^{N-\ell-2} (1-a)\left[\frac{1-b}{2-a-b} \Phi_{G|G}((k-1)n) + \frac{1-a}{2-a-b} \Phi_{G|B}((k-1)n)\right] \tag{3-6}$$

The $\Phi_{i|j}(m)$ are elements of the m step transition matrix of the Markov Process.

The probability of a burst which starts in any position between the N-$\ell$+2 and the Nth is found by summing the $\ell$-1 terms represented by equation 3-6, and it is equal to:

$$(\ell-1)\left[\Phi_{G|G}(n)\right]^{N-\ell-2}(1-a)(1-b) \tag{3-7}$$

Then by summing equations 3-3, 3-5, 3-7 and N-$\ell$-1 times equation 3-4, we have the probability that some erasures occur, and that they are confined to a burst of length $\ell$. If we denote this by $P_\ell$ then we have

$$P_\ell = (1-b)\pi_b(\pi_g+\epsilon^n\pi_b)^{N-\ell-1}\left[\pi_g(1-\epsilon^{n\ell})\left(1+\frac{N-\ell-1}{\pi_g+\epsilon^n\pi_b}\right)+1+(\ell-1)(1-\epsilon)\right] \tag{3-8}$$

The probability that there are no erasures in an N digit codeword is

$$P_0 = \pi_g(\Phi_{G|G}(n))^{N-1} = \pi_g^N\left(1+\epsilon^n\frac{1-a}{1-b}\right)^{N-1} \tag{3-9}$$

Equations 3-8 and 3-9 can be used to estimate the probability of error for a communication system of the form described in section 3.1 when the individual codewords can correct erasure bursts and simple sets of errors.

# Bibliography


1 K. Davies, Ionospheric Radio Propagation, National Bureau of Standards, U.S. Government Printing Office, Washington, D.C., 1965.

2 CCIR Report 322, 1964, "World Distributions and Characteristics of Atmospheric Noise,"

3 W.W. Peterson, Error-Correcting Codes, M.I.T. Press, Cambridge, Mass., 1961.

4 R.G. Gallager, Information Theory and Reliable Communication, Wiley, New York, 1968.

5 J.L. Massey, "Notes in Coding Theory," Text for course 6.575 as offered in the spring semester of academic year 1966-67 at M.I.T.

6 E.R. Berlekamp, "Non Binary BCH Decoder," IEEE International Symposium on Information Theory, Sept., 1967.

7 G.G. Forney, "On Decoding BCH Codes," IEEE Trans. on Information Theory, IT-10, pp. 549-557, October 1965.

8 D.R. Cox, and H.D. Miller, The Theory of Stochastic Processes, Wiley, New York, 1965.