AN ABSTRACT OF THE THESIS OF

Paul Oprisan for the degree of Doctor of Philosophy in

Electrical and Computer Engineering presented on December 7, 2004.

Title: Error Control Techniques for the Z-channel

Redacted for Privacy

Abstract approved: ____________________

Bella Bose

The asymmetric nature of bit errors in several practical applications provides grounds for efficient error control techniques. The Z-channel model and special classes of codes like asymmetric error detection codes and t-asymmetric error correcting/d-asymmetric error detecting codes can be successfully used in ARQ protocols for feedback error control enhancement.

This thesis presents some efficient feedback error control techniques, suitable for the Z-channel. Precisely, some forms of hybrid ARQ protocols specific to the Z-channel characteristics are introduced. First a diversity combining scheme is presented and analyzed. The undetected error probability and the expected number of retransmissions are calculated for this protocol. Then the Bose-Lin codes are analyzed and feedback error control specific parameters are derived for them. Finally, a type I hybrid ARQ one-code scheme is proposed and analyzed.

The proposed techniques improve the throughput efficiency of feedback error control protocols and decrease their accepted packet error rate. The coding analysis is also of theoretical value, in the sense that it solves some open problems in this area.

Error Control Techniques for the Z-channel

by

Paul Oprisan

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

Presented December 7, 2004
Commencement June 2005

Doctor of Philosophy thesis of Paul Oprisan presented on December 7, 2004

APPROVED:

Redacted for Privacy

Major Professor, representing Electrical and Computer Engineering

Redacted for Privacy

Associate Director of the School of Electrical Engineering and Computer Science

Redacted for Privacy

Dean of the Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Redacted for Privacy

Paul Oprisan, Author

ACKNOWLEDGMENT

I owe more than a word of thanks to the many people who have made my life as a graduate student an enriching experience. I hope to be able to reciprocate someday by giving to others what I have received from them.

First and foremost, I would like to express indebted gratitude to my advisor Prof. Bella Bose for his guidance, inspiration and support for many years. His patient and straightforward approach to every issue set an example for me.

Also, I would like to thank Prof. Paul Cull, Prof. Enrique Thomann, Prof. Mario Magaña and Prof. Dean H. Jensen for their kind agreement to serve on my committee. Their valuable comments and suggestions eliminated many ambiguous points from the manuscript.

Special thanks are due to Prof. Torleiv Kløve, for many hours of stimulating and instructive discussions we had on undetectable errors, as a source and a sounding board for many ideas.

Among the friends I made as a graduate student, a special mention is due to Corina Constantinescu, Ovidiu Iancu and Angela and Catalin Doneanu. I shall cherish their friendship forever.

Finally, I would like to thank my parents for their life-long love and support.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

LIST OF TABLES

GLOSSARY OF SYMBOLS

k	number of information bits
r	number of check bits
n	$= k + r$, code length
$X \cup Y$	union of the sets X and Y
$X \cap Y$	intersection of two sets X and Y
F^k	set of vectors of length k over the finite field F
$\mathbf{H}$	parity-check matrix $((n-k) \times n)$
$\mathbf{x}$	vector in F^k (codeword)
$\mathbf{x} \subseteq \mathbf{y}$	$\mathbf{y}$ covers $\mathbf{x}$
$\|\|\mathbf{x}\|\|$	Hamming weight of $\mathbf{x}$
$u(\mathbf{x})$	number of zeros in $\mathbf{x}$
$\mathbf{x}^T$	the transpose of $\mathbf{x}$
$[a]_n$	the (least non-negative) residue of a modulo n (for any integers a, n)
$O(m)$	a quantity of order m
$D(X,Y)$	Hamming distance between X and Y
$N(X,Y)$	number of crossovers from X to Y
$D_a(X,Y)$	$= \max\{N(X,Y), N(Y,X)\}$, asymmetric distance between X and Y
$H(\cdot)$	Heaviside step function
$(n, k, 2t+1)$	(n,k) t-error correcting code
$D[r,t,d]$	length r tail sequence, part of a t-AEC/d-AED code

DEDICATION

To my parents, Gheorghe and Elisabeta

ERROR CONTROL TECHNIQUES FOR THE Z-CHANNEL

1. INTRODUCTION

Error control coding plays an important role in designing highly reliable digital computer and communication systems. The origin of coding theory comes from a famous theorem of C. Shannon [37]; this channel coding theorem guarantees the existence of codes that transmit information at rates close to capacity with an arbitrarily small probability of error.

In most systems the source signals contain a lot of redundancy. Therefore an encoder performs the important task of eliminating/reducing this redundancy and transforms the message in a suitable form for transmission. This is what is called *source encoding*. Then, data to be transmitted over the channel is again encoded. This is the so called *channel encoding*, which involves the addition of redundancy so as to provide the means for detecting and correcting errors that inevitably occur in any real communication process.

The error model used for most of the binary communication systems is the binary symmetric channel. Let p be the probability that a binary signal is received correctly and then $1-p$ is the probability of incorrect reception. Usually the probabilities of $1 \rightarrow 0$ and $0 \rightarrow 1$ errors are equal, as shown in Figure 1.1.

In general we assume that the elements of a finite field represent the underlying alphabet for coding. Encoding consists of transforming a block of k message symbols $a_1 a_2 \ldots a_i \in F$ into a codeword $\mathbf{x} = x_1 x_2 \ldots x_n$, where for each i, $x_i \in F$. Here the some k symbols are the message symbols, i.e. $x_i = a_j$ for $1 \leq j \leq k$. The remaining $n-k$ elements of $\mathbf{x}$ are *check symbols.* The most common codes used for the binary symmetric channel model are the linear codes. In this case

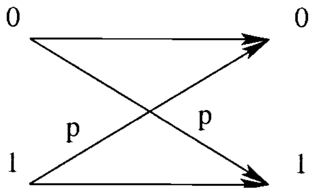


FIGURE 1.1. Binary Symmetric Channel

the check symbols can be obtained from the message symbols in such a way that the codewords $\mathbf{x}$ satisfy the system of linear equations

$$\mathbf{H}\mathbf{x}^T = \mathbf{0},$$

where $\mathbf{H}$ is a given $(n-k) \times n$ matrix with elements in F.

Many techniques for efficient codes design have been developed [28], [34], [4], [25], [27], [5], [41], [35], [29], [36]. Nevertheless, none of these techniques give code rates arbitrarily close to the channel capacity .

In optical networks, which will be one of the dominating communication technologies of the future, 1's are represented by the presence of photons and 0's by their absence. Upon transmission, photons may fade or decay, but new photons cannot be generated. Thus, the observed errors are asymmetric and the error characteristic of such a system can be modeled by the Z-channel [7], [6], as shown in Figure 1.2.

Although linear codes and most of the codes developed for the binary symmetric channel can also be used for the Z-channel, efficient coding calls for different techniques. Many methods of asymmetric and unidirectional encoding and decoding have been proposed over the last two decades ([7], [3], [14], [10], [23], [39], [16], [17], [8]). These codes were proposed to enhance the data rate of the transmission system, or because of simpler encoding/decoding algorithms.

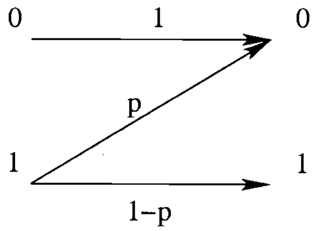


FIGURE 1.2. Z-channel

Two types of errors are mentioned above: asymmetric and unidirectional. When errors of only one type (say 1 → 0) occur during a transmission, they are called asymmetric errors. However, if errors of both types occur during the transmission, but not in the same codeword, then they are called unidirectional errors. Obviously, unidirectional error detecting (UED) codes are also asymmetric error detecting (AED); surprisingly, the converse is also true and it was proven in [10].

1.1. Brief Overview of AED codes

The first asymmetric error detecting code was proposed by Berger [3], [14]. It can be constructed relatively simply by appending to the information word a check symbol which is the number of ones in this information part, in binary. The total number of check bits is $\log_2(k+1)$, where k is the length of the information part. This is a systematic, all asymmetric error detecting code, and it is also optimal.

Borden [7] proposed a d-UED code in which codewords of length n have weight w that is congruent to $\lfloor n/2 \rfloor \bmod (d+1)$. Thus, the number of codewords of this code is $N(n,d)$, where:

$$N(n,d) = \sum_{w=\lfloor n/2 \rfloor \bmod (d+1)} \binom{n}{w}.$$

For $d = 1$, this code is an all single-bit error detecting code, like the parity code. Also, if $d = n/2$, it is a constant weight code (e.g. $n/2$-out-of-n code) and detects all unidirectional errors.

The Borden code is optimal (i.e it has the highest k/n rate, which is called the information rate, for any information block of length k), but its main disadvantage is that it is nonsystematic. This means that, inside a codeword, the information bits cannot be distinguished from the check bits. Thus, in the case of nonsystematic codes, the decoding and data manipulation cannot be done in parallel.

Systematic AED/UED codes have been proposed by Bose and Lin in [10]. These codes can be summarized as follows .

The check symbols for detecting 2 and 3 unidirectional errors are $w_0 \bmod 2^2$ and $w_0 \bmod 2^3$, respectively, where w_0 is the number of 0's in the information word. So, the 2 and 3 asymmetric error detecting codes use 2 and 3 check bits, respectively.

When $r \geq 4$ check bits are used, the code designed by this method can detect up to $2^{r-2} + r - 2$ errors. In order to get the check, first

$$(b_{r-2}, \ldots, b_1, b_0) = w_0 \bmod 2^{r-1}$$

is derived. Then, the check symbol is determined as:

$$(a_{r-1}, a_{r-2}, a_{r-3}, \ldots, a_1, a_0) = (b_{r-2}, \bar{b}_{r-2}, b_{r-3}, \ldots, b_1, b_0).$$

When $r \geq 5$ check bits are used, the following alternate method of encoding, with better detecting capabilities (in terms of the number of errors detected per check bit) is used. First, calculate

$$(b_{r-2}, b_{r-3}, \ldots, b_1, b_0) = w_0 \bmod 3 \cdot 2^{r-3}.$$

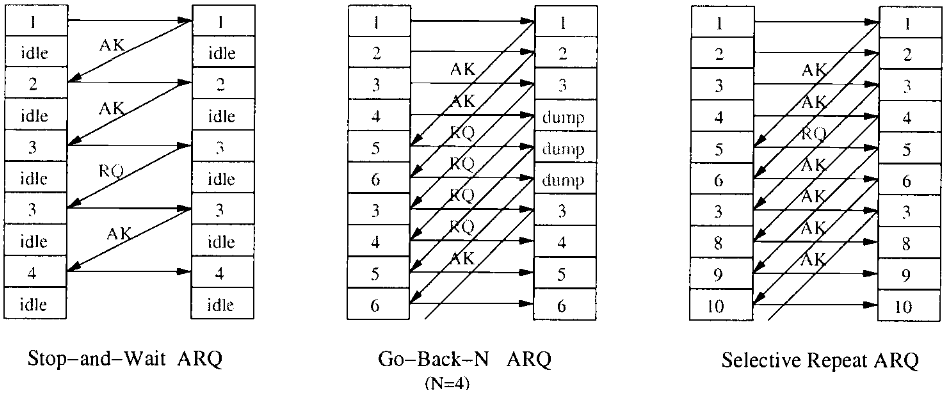
Then, the 3 most significant bits, $(b_{r-2}, b_{r-3}, b_{r-4})$, which can be one of the patterns in the set $\{000, 001, 010, 011, 100, 101\}$, are mapped into a 2-out-of-4 code. A simple example of a mapping function is $f(i) \leq f(j)$ for $i < j$, $0 \leq i, j \leq 5$ i.e. $f(000) = 0011$, $f(001) = 0101$, $f(010) = 0110$, $f(011) = 1001$, $f(100) = 1010$ and $f(101) = 1100$. The concatenation of such a symbol with the remaining $r - 4$ bits $(b_{r-5}, \ldots, b_1, b_0)$ gives the check symbol. This code can detect up to $5 \cdot 2^{r-4} + r - 4$ errors.

A compact description of these codes, which is useful for performance evaluation, is given in Chapter 3.

Comparing Berger-Freiman codes and Bose-Lin codes, we see that Berger-Freiman codes can detect all asymmetric errors, but in most cases at the cost of more check bits (lower rate). The Bose-Lin codes detect all errors up to some weight (as well as some others), but with fewer check bits.

1.2. ARQ Protocols Overview

There are situations where it is more efficient to retransmit a part of a message, given that errors were detected in it, than to correct those errors. In such situations, a great deal of extra protection can be provided by the ARQ (Automatic repeat ReQuest) protocols. This means that the system detects the packet with errors, discards it, and requests a retransmission. These protocols require two-way communication between the transmitter and the receiver and it is desired that the perturbation duration be shorter than the retransmission time, such that the retransmitted packet will pass undisturbed across the channel, thus



Stop–and–Wait ARQ

Go–Back–N ARQ (N=4)

Selective Repeat ARQ

FIGURE 1.3. Pure ARQ protocols

avoiding multiple retransmission attempts. However, the rate of retransmission requests increases as the channel quality deteriorates, which affects the efficiency of the system.

There are three basic retransmission protocols, stop-and-wait (SW-ARQ), go-back-N (GBN-ARQ) and selective repeat (SR-ARQ). Their packet handling is illustrated in Figure 1.3.

In general, we measure the performance of an ARQ protocol by two parameters:

1. the accepted packet error rate, P_E, which is the percentage of erroneous packets accepted by the receiver and

2. the throughput, η, which is the average number of data packets accepted by the receiver in the time it takes the transmitter to send one k-bit block.

We define the probability of detected errors, P_d, (which is also the probability that a retransmission request is generated) as the value to which the ratio of blocks with detected errors (N_d) to the number of blocks transmitted over the channel

(N) converges in probability [19]:

$$\lim_{N\to\infty} P\left\{\left|\frac{N_d}{N} - P_d\right| > \epsilon\right\} = 0, \ \forall\, \epsilon > 0. \tag{1.1}$$

Similarly, the probability of undetected errors, P_u, is the value to which the ratio of the number of blocks with undetected errors (N_u) to the total number of blocks transmitted converges in probability:

$$\lim_{N\to\infty} P\left\{\left|\frac{N_u}{N} - P_u\right| > \epsilon\right\} = 0, \ \forall\, \epsilon > 0. \tag{1.2}$$

These probabilities characterize events which occur during the decoding process. P_E can be computed by adding together the probabilities of all the events which result in the acceptance of an erroneous packet:

$$P_E = P_u + P_d P_u + P_d^2 P_u + P_d^3 P_u + \ldots, \tag{1.3}$$

as the erroneous packet can be accepted on the first transmission, or on the second one, third one and so on. The series converges to:

$$P_E = \frac{P_u}{1 - P_d}. \tag{1.4}$$

The throughput is defined as the average number of encoded packets accepted by the receiver in the time it takes the transmitter to send one information word (k-bit packet). In a feedforward system, it is equal to the code rate, k/n. In an ARQ system, it is a function of the average number of times a data packet has to be transmitted before it is accepted. The explicit form of this function depends on the protocol. This is a random variable with a geometric density function (number of transmissions until the first success). Its expected value is:

$$\begin{aligned} T_m = \mathbb{E}T &= \sum_{j=1}^{\infty} jP(T = j) \qquad (1.5) \\ &= (1 - P_d)\sum_{j=1}^{\infty} jP_d^{j-1} = \frac{1}{1 - P_d}. \end{aligned}$$

Throughput expressions for the three basic ARQ protocols are given in [41], [25] and [19].

As already mentioned, if the channel quality deteriorates, the increased frequency of retransmission requests has a severe impact on the throughput. To deal with this problem, several hybrid protocols have been introduced. Although there are major differences between them, they all have one thing in common: they use forward error correction in order to correct the error patterns most frequently caused by the noise on the channel, while the error detection is used to detect the less frequently occurring patterns.

They can be categorized in several (usually overlapping) ways [41], [25], [19]. We only mention here type I and type II hybrid ARQ and packet combining systems. In the case of type I hybrid ARQ, each packet is encoded for both error detection and correction by means of either one code capable of doing both, or two codes, one for correction, the other for detection. When the packet arrives at the receiver, it is first decoded by the feedforward error control (FEC) part, then sent to the error detecting decoder. If errors are detected, a retransmission request is generated. Type II hybrid ARQ protocols adapt to the changing channel conditions through the use of incremental redundancy. This means that, in case of retransmission requests, the transmitter will only send additional parity bits, which are to be appended to the received packet with errors which is stored in the receiver buffer. This allows for increased error correction capability.

Chapters 2 and 4 deal with such protocols for the Z-channel. Nevertheless, the approach is a coding theory one: the transmission protocols are considered as consequences of certain constraints, which are due to the codes which are used. The protocols performance is evaluated by analyzing the codes.

On the same line, in Chapter 3 some bounds on the probability of undetected error for systematic AED codes in general are derived and, more important, this probability is determined for the Bose-Lin codes, thus solving a problem which has been open for a while.

2. DIVERSITY COMBINING

Error detection as part of a feedback error control system is a reliable alternative to feedforward error correction in asymmetric channels. This is because of simpler hardware implementation of the encoding/decoding system and further, the lack of asymmetric error correcting codes with better rates than the corresponding binary symmetric codes.

The method proposed here improves the throughput of a feedback error control for asymmetric channels using *diversity packet combining.* The idea was first introduced by Sindhu in [38] who discussed a scheme that made use of the packets that cause retransmission requests, which are simply discarded in basic and type I hybrid ARQ protocols. Such packets can be stored and combined with additional retransmissions of the packet, thus creating a single packet that is likely to be the correct version of the transmitted one.

There are two basic categories of packet-combining systems: code combining systems and diversity combining systems. In code combining systems the packets are concatenated to form noise corrupted code words from increasingly longer and lower rate codes. This is the basis for type II hybrid ARQ protocols [26]. On the other hand, in diversity combining systems, the individual symbols from identical copies of a packet are combined to create a packet with more reliable constituent symbols. Most of the discussions on diversity combining systems are based on majority logic decoding [40], [11], or on soft channel outputs [15], [12], [2], [18]. The Z-channel error characteristic provides a simple framework which can improve the performance of an ARQ system without adding much to the hardware complexity of the decoder.

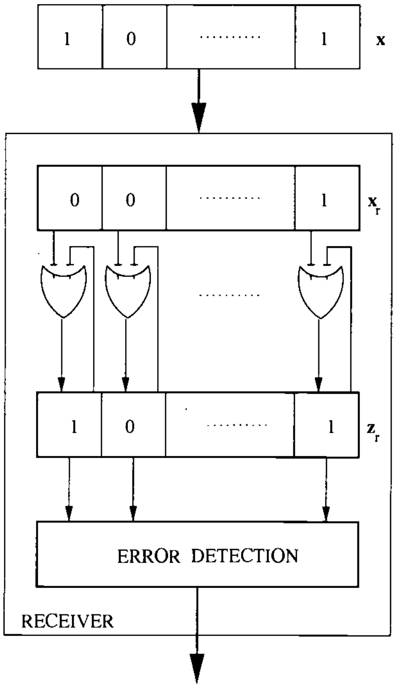


FIGURE 2.1. Packet reusing scheme

First, the proposed asymmetric error correction scheme is introduced. Then the undetected error probability and the average number of transmissions are determined for unordered codewords under the assumption that there are at most $k-1$ retransmission requests for a given codeword [32], [20]. The case of unlimited number of retransmissions, that is a codeword is retransmitted upon error detection until accepted, follows immediately. Furthermore, some bounds are proposed for the more general case when some codewords of the asymmetric error detecting code cover others.

2.1. Diversity combining scheme and problem formulation

The way the saved packets are combined with the retransmitted ones is shown in Figure 2.1.

TABLE 2.1. Retransmission scenario. $\mathbf{x}_r$ is the received vector in the rth transmission, and $\mathbf{z}_r$ is the combined word after r transmissions, that is $\mathbf{z}_r = \mathbf{z}_{r-1} \vee \mathbf{x}_r$ for $r \geq 1$. The bits in error are underlined to make the table easier to read.

r	$\mathbf{x}_r$	$\mathbf{z}_r$
0	-	0000000000000
1	$0100\underline{0}1\underline{0}010\underline{0}01$	$0100\underline{0}1\underline{0}010\underline{0}01$
2	$01001\underline{0}1010\underline{0}01$	$0100111010\underline{0}01$
3	$01001\underline{0}10\underline{0}0101$	0100111010101

Packet combining consists of a bit-by-bit logic OR operation. Assuming only 1 → 0 errors (the 0 → 1 type will require complementing the words prior to the OR operation), note that any bit in error may or may not be corrected, but new errors cannot be created. An example is given in Table 2.1. We assume that $\mathbf{x} = 0100111010101$ is transmitted and suffers three bit errors during the initial transmission. Assuming that the first two retransmissions yield the words shown in Table 2.1, the codeword is recovered after these two retransmissions.

In other words, a codeword is transmitted repeatedly over a Z-channel. At the receiving end, the OR of the received copies is stored (we will call this the combined word). When the combined word becomes a codeword, this is passed on, and a new codeword is transmitted. If the passed codeword is different from the one sent, then we have an *undetected error.* This process is illustrated in Figure 2.2, where the states T, RQ and FWD represent word transmission, retransmission request and next word transmission, respectively. We will further assume that there is a limit k on the number of transmissions of a codeword, that is, if the combined word is not a codeword after k transmissions, it is discarded. A special case of the protocol is a protocol without a limit on the number of transmissions (that is, $k = \infty$).

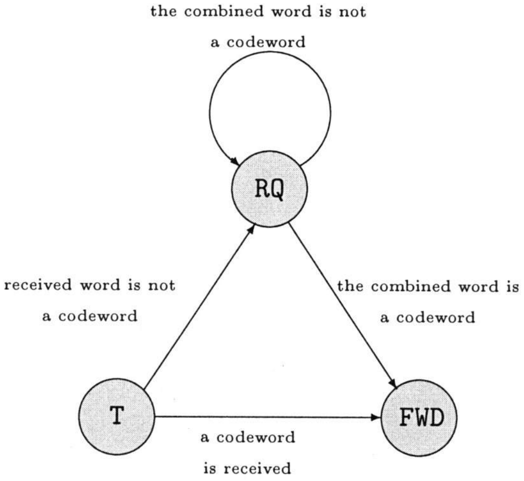


FIGURE 2.2. The graph of the proposed diversity combining scheme

In order to characterize an ARQ system which includes this scheme, we need to consider the following two quantities: N, *the expected number of transmissions* and P, *the probability that the combined word is passed on with an undetected error.* In general, both N and P will depend on the channel error probability p, the codeword transmitted $\mathbf{x}$, the set $X = X_{\mathbf{x}}$ of codewords $\mathbf{y}$ such that $\mathbf{y} \subset \mathbf{x}$ ($\mathbf{y} \subset \mathbf{x}$ denotes that $\mathbf{x}$ covers $\mathbf{y}$ [1]) or, in other words, the support of $\mathbf{y}$ is a proper subset of the support of $\mathbf{x}$, and the maximum number of transmissions k. Therefore, we include these in the notation and write $N_k(\mathbf{x}, X; p)$ and $P_k(\mathbf{x}, X; p)$. Further, we will consider the probability that all errors are corrected, that is, the combined word passed on is the sent codeword. We denote this by $C_k(\mathbf{x}, X; p)$.

We assume that $\mathbf{x} \neq \mathbf{0}$. Note that

$$\begin{aligned} &N_k(\mathbf{x}, X; 0) = 1, \;\; P_k(\mathbf{x}, X; 0) = 0, \\ &N_k(\mathbf{x}, X; 1) = 1, \;\; P_k(\mathbf{x}, X; 1) = 1, \text{ if } \mathbf{0} \in X, \\ &N_k(\mathbf{x}, X; 1) = k, \;\; P_k(\mathbf{x}, X; 1) = 0, \text{ if } \mathbf{0} \notin X. \end{aligned}$$

Therefore, from now on we will assume that $0 < p < 1$. If we introduce more codewords into X, N_k will decrease and P_k will increase, that is, if $X \subset Y$, then $N_k(\mathbf{x}, X; p) > N_k(\mathbf{x}, Y; p)$ and $P_k(\mathbf{x}, X; p) < P_k(\mathbf{x}, Y; p)$. One extreme case is when all $\mathbf{y} \subset \mathbf{x}$ are codewords. Then $N_k = 1$ and $P = 1 - (1-p)^w$ (here $w = ||\mathbf{x}||$, the Hamming weight of $\mathbf{x}$, that is, the number of elements in $\mathbf{x}$ that are 1). The other extreme is when X is empty. Clearly, $P_k(\mathbf{x}, \emptyset; p) = 0$. Since $N_k(\mathbf{x}, \emptyset; p)$ only depends on $w = ||\mathbf{x}||$, p and k, we will use the shorter notation $N_k(w; p) = N_k(\mathbf{x}, \emptyset; p)$ for this particular, important case. As we have noted, $N_k(||\mathbf{x}||; p)$ will be an upper bound on $N_k(\mathbf{x}, X; p)$ in general, and $N_k(\mathbf{x}, X; p)$ will be close to $N_k(||\mathbf{x}||; p)$ if $P_k(\mathbf{x}, X; p)$ is small.

For this scheme we can view the accepted packet error rate P_E as the probability that a forwarded codeword is different from the sent codeword. The probability that a combined word is forwarded is $C_k(\mathbf{x}, X; p) + P_k(\mathbf{x}, X; p)$, and so

$$P_E(\mathbf{x}, X; p) = \frac{P_k(\mathbf{x}, X; p)}{C_k(\mathbf{x}, X; p) + P_k(\mathbf{x}, X; p)}.$$

The throughput efficiency is defined as the ratio of the average number of information symbols, successfully received to the total number of symbols transmitted over the channel. This definition accounts for various delays, protocol specific, such as the time of ACK (NAK) block transmission and the round trip delay (details are given in [41] and [19]). We only consider here the *Selective Repeat* ARQ protocol in conjunction with this diversity combining scheme.

$$\eta = R_C \frac{C_k(\mathbf{x}, X; p) + P_k(\mathbf{x}, X; p)}{N_k(\mathbf{x}, X; p)},$$

where R_C is the information rate of the code.

2.2. The undetected error probability and the average number of transmissions

2.2.1. The special case when X is empty

We consider the following situation: a codeword $\mathbf{x}$ of weight w is transmitted, and there are no codewords $\mathbf{y}$ of lower weight such that $\mathbf{y} \subset \mathbf{x}$. Let $\pi(w, r; p)$ denote the probability that the combined word has weight w after r transmissions

.

Consider some fixed position. The probability that this is 0 after r transmissions is p^r. The probability that it is 1 after r transmissions is $1 - p^r$. Since errors are independent, the probabilities for the various positions are independent and so

$$\pi(w, r; p) = (1 - p^r)^w.$$

We continue transmitting until the combined word equals $\mathbf{x}$, that is, it has weight w. The probability that this happens after exactly r transmissions is $\pi(w, r; p) - \pi(w, r-1; p)$. Note that this expression is also valid for $r = 1$ since $\pi(w, 0; p) = 0$. If the combined word is not $\mathbf{x}$ after k transmissions, we have used exactly k transmissions. The expected number of transmissions is therefore

$$N_k(w;p) = \sum_{r=1}^{k} r[\pi(w,r;p) - \pi(w,r-1;p)] \tag{2.1}$$

$$+k\Big[1 - \sum_{r=1}^{k}[\pi(w,r;p) - \pi(w,r-1;p)]\Big]$$

$$= k - \sum_{r=0}^{k-1} \pi(w,r;p). \tag{2.2}$$

An alternative useful expression is obtained by expanding $\pi(w,r;p) = (1-p^r)^w$ and changing the order of summation:

$$N_k(w;p) = k - \sum_{r=0}^{k-1}\sum_{j=0}^{w}\binom{w}{j}(-1)^j p^{rj}$$

$$= k - \sum_{j=0}^{w}\binom{w}{j}(-1)^j \sum_{r=0}^{k-1} p^{rj}$$

$$= k - k + \sum_{j=1}^{w}\binom{w}{j}(-1)^{j-1} \sum_{r=0}^{k-1} p^{rj}$$

$$= \sum_{j=1}^{w}\binom{w}{j}(-1)^{j-1}\frac{1-p^{kj}}{1-p^j}. \tag{2.3}$$

An expression for $N_\infty(w;p)$ follows directly from (2.3) since $p^k \to 0$ when $k \to \infty$ (remember that $p < 1$). Hence we get

$$N_\infty(w;p) = \sum_{j=1}^{w}\binom{w}{j}(-1)^{j-1}\frac{1}{1-p^j}.$$

For example, for a balanced code of length $n = 100$ (and $w = 50$), $N_\infty(50, 10^{-2}) \approx 1.400032$. For the same code and a protocol not using diversity combining (the codeword is retransmitted upon error detection, until a codeword is received), the expected number of transmissions is

$$\sum_{r=1}^{\infty} r[1-(1-p)^w]^{r-1}(1-p)^w = \frac{1}{(1-p)^w}.$$

Its' value for $w = 50$ and $p = 10^{-2}$ is 1.652876.

When p is small compared to w^{-1}, we may consider the first few terms of the Taylor series expansion of $N_\infty(w;p)$ to compute good approximations:

$$N_\infty(w;p) = 1 + wp - \left[\binom{w}{2} - w\right]p^2 + \left[\binom{w}{3} + w\right]p^3 + O(p^4).$$

For $w = 50$ and $p = 10^{-2}$, the first four terms of the Taylor series expansion give the value 1.402150.

2.2.2. The case when X contains a single codeword

We now consider the case when X contains exactly one codeword, that is, there is exactly one codeword $\mathbf{y}$ such that $\mathbf{y} \subset \mathbf{x}$. Let $w = ||\mathbf{x}||$, $u = ||\mathbf{y}||$ and $d = w - u$. Since $C_k(\mathbf{x}, \{\mathbf{y}\}; p)$, $P_k(\mathbf{x}, \{\mathbf{y}\}; p)$, and $N_k(\mathbf{x}, \{\mathbf{y}\}; p)$ only depend on w, u, p, and k, we write $C_k(w, u; p)$, $P_k(w, u; p)$, and $N_k(w, u; p)$, respectively.

Suppose that the combined word becomes $\mathbf{y}$ after exactly r transmissions. The d positions not in the support of $\mathbf{y}$ must be in error for all r transmissions and the probability of this happening is p^{dr}. The u positions in the support of $\mathbf{y}$ must become all 1 for the first time after exactly r transmissions. The analysis in Section 2.2.1 shows that the probability for this event is

$$\pi(u, r; p) - \pi(u, r-1; p) = (1 - p^r)^u - (1 - p^{r-1})^u.$$

Hence, the probability that the combined word becomes $\mathbf{y}$ after exactly r transmissions is

$$p^{dr}[(1 - p^r)^u - (1 - p^{r-1})^u]. \tag{2.4}$$

Summing over all r we get

$$P_k(w, u; p) = \sum_{r=1}^{k} p^{dr}[(1 - p^r)^u - (1 - p^{r-1})^u].$$

In particular (if $k \geq d$),

$$P_k(w, u; p) = p^d(1-p)^u + O(p^{2d}).$$

We can rewrite the expression for $P_k(w, u; p)$ in a way similar to what we did for $N_k(w; p)$.

$$\begin{aligned}
P_k(w, u; p) &= \sum_{r=1}^{k} p^{dr} \Big[\sum_{j=0}^{u} \binom{u}{j} (-1)^j p^{jr} - \sum_{j=0}^{u} \binom{u}{j} (-1)^j p^{j(r-1)} \Big] \\
&= \sum_{j=0}^{u} \binom{u}{j} (-1)^{j-1} (1-p^j) p^d \sum_{r=1}^{k} p^{(d+j)(r-1)} \\
&= \sum_{j=0}^{u} \binom{u}{j} (-1)^{j-1} (1-p^j) p^d \frac{1-p^{k(d+j)}}{1-p^{d+j}}.
\end{aligned}$$

For the average number of transmissions, we start by considering that we keep transmitting whether or not the combined word is a codeword.

As explained before, the probability that the combined word is $\mathbf{x}$ after r transmissions is $(1-p^r)^w$, and the probability that the combined word is $\mathbf{x}$ for the first time after r transmissions is $(1-p^r)^w - (1-p^{r-1})^w$.

Let $F(r, s; p)$ denote the probability that the combined word was $\mathbf{y}$ for the first time after s transmissions and $\mathbf{x}$ for the first time after r transmissions, and let $G(r; p) = \sum_{s=1}^{r-1} F(r, s; p)$ denote the probability that the combined word is $\mathbf{x}$ for the first time after r transmissions and it has, at some previous step been $\mathbf{y}$.

If we now return to the situation where we stop when the combined word becomes a codeword, we see that the probability that the combined word is a codeword $\mathbf{x}$ for the first time after r transmissions (this can only occur if the combined word has not been $\mathbf{y}$ earlier) is given by

$$(1-p^r)^w - (1-p^{r-1})^w - G(r; p). \tag{2.5}$$

Combining (2.4) and (2.5), we see that probability that the combined word is a codeword ($\mathbf{y}$ or $\mathbf{x}$) for the first time after r transmissions is

$$p^{dr}[(1-p^r)^u - (1-p^{r-1})^u] + (1-p^r)^w - (1-p^{r-1})^w - G(r;p). \tag{2.6}$$

Before we go on, let us make a small digression. We note that (2.2) could have alternatively been expressed as

$$N_k(w;p) = \sum_{r=1}^{k} r[\pi(w,r;p) - \pi(w,r-1;p)] + k\sum_{r=k+1}^{\infty}[\pi(w,r;p) - \pi(w,r-1;p)]. \tag{2.7}$$

Of course, we could have derived the expression (2.3) from (2.7) also. However, this derivation would have been a little more complicated. For $N_k(w,u;p)$ we similarly have two choices for a starting point, and it seems that, in this case, the second choice gives the simpler derivation and we select it.

From (2.6) we therefore get

$$\begin{aligned} N_k(w,u;p) = {} & \sum_{r=1}^{k} r\Big[p^{dr}[(1-p^r)^u - (1-p^{r-1})^u] \\ & +(1-p^r)^w - (1-p^{r-1})^w - G(r;p)\Big] \\ & +k\sum_{r=k+1}^{\infty}\Big[p^{dr}[(1-p^r)^u - (1-p^{r-1})^u] \\ & +(1-p^r)^w - (1-p^{r-1})^w - G(r;p)\Big] \\ = {} & \Gamma_k(u;p) + N_k(w;p) - \Delta_k(w,u;p), \end{aligned}$$

where

$$\Gamma_k(u;p) = \sum_{r=1}^{k} rp^{dr}[(1-p^r)^u - (1-p^{r-1})^u] + k\sum_{r=k+1}^{\infty} p^{dr}[(1-p^r)^u - (1-p^{r-1})^u]$$

and

$$\Delta_k(w, u; p) = \sum_{r=1}^{k} rG(r; p) + k \sum_{r=k+1}^{\infty} G(r; p).$$

The infinite sums $\Gamma_k(u; p)$ and $\Delta_k(w, u; p)$ can be determined and transformed to finite sums using the binomial expansion in a similar fashion as we have done above.

First,

$$\begin{aligned}\Gamma_k(u; p) &= \sum_{j=0}^{u} \binom{u}{j} (-1)^{j-1}(1-p^j)p^d \Big[\sum_{r=1}^{k} rp^{(r-1)(d+j)} + k \sum_{r=k+1}^{\infty} p^{(r-1)(d+j)}\Big] \\ &= \sum_{j=0}^{u} \binom{u}{j} (-1)^{j-1}(1-p^j)p^d \frac{1-p^{k(d+j)}}{(1-p^{d+j})^2}.\end{aligned}$$

Now, consider $F(r, s)$. The probability that the combined word was $\mathbf{y}$ for the first time after s transmissions is $p^{ds}[(1-p^s)^u - (1-p^{s-1})^u]$ as explained before. For next $r-s$ transmissions, we only have to consider the d positions not in the support of $\mathbf{y}$. The probability that these d positions become all 1 for the first time after $r-s$ transmissions is $(1-p^{r-s})^d - (1-p^{r-s-1})^d$. Hence

$$\begin{aligned}F(r, s) &= p^{ds}[(1-p^s)^u - (1-p^{s-1})^u][(1-p^{r-s})^d - (1-p^{r-s-1})^d] \\ &= p^{ds} \sum_{j=1}^{u} \binom{u}{j} (-1)^j (p^{sj} - p^{(s-1)j}) \sum_{l=1}^{d} \binom{d}{l} (-1)^l (p^{(r-s)l} - p^{(r-s-1)l}) \\ &= \sum_{j=1}^{u} \binom{u}{j} \sum_{l=1}^{d} \binom{d}{l} (-1)^{j+l}(1-p^j)(1-p^l)p^{lr-l-j}p^{(d+j-l)s}.\end{aligned}$$

Therefore

$$\begin{aligned}G(r; p) &= \sum_{j=1}^{u} \binom{u}{j} \sum_{l=1}^{d} \binom{d}{l} (-1)^{j+l}(1-p^j)(1-p^l)p^{lr-l-j} \sum_{s=1}^{r-1} p^{(d+j-l)s} \\ &= \sum_{j=1}^{u} \binom{u}{j} \sum_{l=1}^{d} \binom{d}{l} (-1)^{j+l}(1-p^j)(1-p^l)p^{lr-l-j} \frac{p^{d+j-l} - p^{r(d+j-l)}}{1-p^{d+j-l}} \\ &= \sum_{j=1}^{u} \binom{u}{j} \sum_{l=1}^{d} \binom{d}{l} (-1)^{j+l} \frac{p^{d-l}(1-p^j)(1-p^l)}{1-p^{d+j-l}} [p^{l(r-1)} - p^{(d+j)(r-1)}].\end{aligned}$$

Substituting this into the expression for $\Delta_k(w,u;p)$ (and changing the order of summation), we get

$$\Delta_k(w,u;p) = \sum_{j=1}^{u} \binom{u}{j} \sum_{l=1}^{d} \binom{d}{l} (-1)^{j+l} p^{d-l} \frac{(1-p^j)(1-p^l)}{1-p^{d+j-l}} s_k$$

where

$$\begin{aligned} s_k &= \left[\sum_{r=1}^{k} r p^{l(r-1)} + k \sum_{r=k+1}^{\infty} p^{l(r-1)}\right] - \left[\sum_{r=1}^{k} r p^{(d+j)(r-1)} + k \sum_{r=k+1}^{\infty} p^{(d+j)(r-1)}\right] \\ &= \frac{1-p^{kl}}{(1-p^l)^2} - \frac{1-p^{k(d+j)}}{(1-p^{d+j})^2}. \end{aligned}$$

Similarly

$$\begin{aligned} C_k(w,u;p) &= \sum_{r=1}^{k} \left[(1-p^r)^w - (1-p^{r-1})^w - G(r;p)\right] \\ &= (1-p^k)^w - \sum_{j=1}^{u} \binom{u}{j} \sum_{l=1}^{d} \binom{d}{l} (-1)^{j+l} p^{d-l} \frac{(1-p^j)(1-p^l)}{1-p^{d+j-l}} c_k \end{aligned}$$

where

$$c_k = \sum_{r=1}^{k} p^{l(r-1)} - \sum_{r=1}^{k} p^{(d+j)(r-1)} = \frac{1-p^{kl}}{1-p^l} - \frac{1-p^{k(d+j)}}{1-p^{d+j}}.$$

Expressions for $P_\infty(w,u;p)$, etc., follow directly from the above expressions by letting $k \to \infty$:

$$\begin{aligned} P_\infty(w,u;p) &= \sum_{j=0}^{u} \binom{u}{j} (-1)^{j-1} p^d \frac{1-p^j}{1-p^{d+j}}, \\ C_\infty(w,u;p) &= 1 - P_\infty(w,u;p), \\ N_\infty(w,u;p) &= \Gamma_\infty(u;p) + N_\infty(w;p) - \Delta_\infty(w,u;p), \\ \Gamma_\infty(u;p) &= \sum_{j=0}^{u} \binom{u}{j} (-1)^{j-1} p^d \frac{1-p^j}{(1-p^{d+j})^2}, \\ \Delta_\infty(w,u;p) &= \sum_{j=1}^{u} \binom{u}{j} \sum_{l=1}^{d} \binom{d}{l} (-1)^{j+l} p^{d-l} \frac{(1-p^j)(1-p^l)}{1-p^{d+j-l}} \\ &\quad \left[\frac{1}{(1-p^l)^2} - \frac{1}{(1-p^{d+j})^2}\right]. \end{aligned}$$

2.2.3. The values of $P_k(\mathbf{x}, X; p)$ and $N_k(\mathbf{x}, X; p)$ when the codewords in X are unordered

We say that the codewords of X are unordered if $\mathbf{y} \not\subset \mathbf{y}'$ and $\mathbf{y}' \not\subset \mathbf{y}$ for all $\mathbf{y}, \mathbf{y}' \in X$, $\mathbf{y} \neq \mathbf{y}' \in X$. We observe that the event that the combined word becomes $\mathbf{x}$ after having been $\mathbf{y}$ and the event that it becomes $\mathbf{x}$ after having been $\mathbf{y}'$, where $\mathbf{y} \neq \mathbf{y}'$, are mutually exclusive. Hence

$$P_k(\mathbf{x}, X; p) = \sum_{\mathbf{y} \in X} P_k(\mathbf{x}, \{\mathbf{y}\}; p)$$

and

$$N_k(\mathbf{x}, X; p) = N_k(||\mathbf{x}||; p) + \sum_{\mathbf{y} \in X} \Gamma_k(||\mathbf{y}||; p) - \sum_{\mathbf{y} \in X} \Delta_k(||\mathbf{x}||, ||\mathbf{y}||; p).$$

In the special case where all the codewords in X have the same weight, u, (and $\mathbf{x}$ has weight w) we get

$$P_k(\mathbf{x}, X; p) = |X| \sum_{j=0}^{u} \binom{u}{j} (-1)^{j-1} (1 - p^j) p^d \frac{1 - p^{k(d+j)}}{1 - p^{d+j}}$$

and

$$N_k(\mathbf{x}, X; p) = N_k(w; p) + |X| \Gamma_k(u; p) - |X| \Delta_k(w, u; p).$$

2.2.4. Bounds on the values of $P_k(\mathbf{x}, X; p)$ and $N_k(\mathbf{x}, X; p)$ when some codewords in X cover others

In the general case when the codewords in X are not unordered, to determine $P_k(\mathbf{x}, X; p)$ and $N_k(\mathbf{x}, X; p)$ becomes more complex and may not even be feasible. Therefore, it is useful to get some bounds. Let T be the smallest value of $||\mathbf{x}|| - ||\mathbf{z}||$ over all codewords $\mathbf{z}$ and $\mathbf{y}$ such that $\mathbf{z} \subset \mathbf{y} \subset \mathbf{x}$, (in particular, $T \geq 2d$ where d is the minimum distance of the code). Define the set Y by

$$Y = \{\mathbf{y} \in X \mid ||\mathbf{y}|| > ||\mathbf{x}|| - T\}.$$

Then the codewords of Y are unordered. Hence $P_k(\mathbf{x}, Y; p)$ and $N_k(\mathbf{x}, Y; p)$ can be computed as explained above. Moreover,

$$N_k(\mathbf{x}, X; p) \leq N_k(\mathbf{x}, Y; p).$$

Further, if p^T is small, then $P_k(\mathbf{x}, Y; p)$ is a good approximation for $P_k(\mathbf{x}, X; p)$. We will make this last claim more precise. On one hand, we know that $P_k(\mathbf{x}, X; p) \geq P_k(\mathbf{x}, Y; p)$. On the other hand, if the combined word becomes a codeword not in Y, then after the first transmission, the combined word must have weight $w - T$ or less. The probability that the combined word is *some* vector of weight $w - T$ or less (not necessarily a codeword) after the first transmission is

$$\sum_{j=0}^{w-T} \binom{w}{j} p^{w-j}(1-p)^j \leq p^T(1-p)^{w-T} \sum_{j=0}^{w-T} \binom{w}{j} < p^T(1-p)^{w-T} 2^w.$$

Therefore,

$$P_k(\mathbf{x}, Y; p) \leq P_k(\mathbf{x}, X; p) < P_k(\mathbf{x}, Y; p) + 2^w p^T (1-p)^{w-T}.$$

Then, the corresponding quantities for the code are given by

$$P_k(C; p) = \frac{1}{|C|} \sum_{\mathbf{x} \in C} P_k(\mathbf{x}, X_{\mathbf{x}}; p)$$

and similarly for $N_k(C, p)$ (assuming that each codeword is equally likely).

In practice we may be able to calculate exactly the probability of undetected error and the expected number of transmissions for some codes, but most generally we can give bounds on these two parameters.

3. SYSTEMATIC AED CODES

In [10] it is shown that the multiplicity of errors that can be detected by an unidirectional error detecting code depends on how the check bits are derived. Moreover, it is shown that a code capable of detecting t asymmetric errors is also capable of detecting t unidirectional errors.

An upper bound for the undetected error probability is derived in Section 3.1 [33], [31], [30]. This is done starting with estimating the probability of detected errors in the case of asymmetric errors. Section 3.2 compares these bounds for different versions of AED codes. Then the Bose-Lin codes are analyzed: a new construction description is introduced (in Section 3.3), their probability of undetected error is determined using this new description (in Section 3.5), and the undetected error minimal weight problem is generalized (in Section 3.7) [22], [21]. Finally, a couple of detailed examples are presented.

3.1. General bounds for the detected and undetected error probability

Let us denote by q and $1-q$ the probabilities of the source generating 1's and 0's, respectively. If Z is the number of bit errors in the code word, then:

$$P_z = P(Z=z) = \binom{w}{z} p^z (1-p)^{w-z}. \tag{3.1}$$

The weight of the code word w in (3.1) can be written as the sum of corresponding weights in the information part in and the check symbol. Thus, (3.1) becomes:

$$P_z = \binom{w_{inf}+w_{cs}}{z} p^z (1-p)^{w_{inf}-z} (1-p)^{w_{cs}}. \tag{3.2}$$

Note that the functions $\binom{w_{inf}+w_{cs}}{z}$ and $(1-p)^{w_{cs}}$ are increasing and decresing, respectively, in w_{cs}, so:

$$P_z \geq \binom{w_{inf}+w_{cs_{min}}}{z} p^z (1-p)^{w_{inf}-z} (1-p)^{w_{cs max}}. \tag{3.3}$$

Because the '1' and '0' bits are independently distributed in the information part, equation (3.3) can be rewritten as:

$$P_z \geq \sum_{i=0}^{k-z} \binom{k}{i} q^{k-i}(1-q)^i \binom{k-i+w_{cs_{min}}}{z} p^z (1-p)^{k-i-z}(1-p)^{w_{cs max}}. \tag{3.4}$$

Note that:

$$\begin{aligned}\binom{k-i+w_{cs_{min}}}{z} &= \binom{k-i}{z} \frac{(k-i+1)(k-i+2)\dots(k-i+w_{cs_{min}})}{(k-i-z+1)(k-i-z+2)\dots(k-i-z+w_{cs_{min}})} \\ &= \binom{k-i}{z} \frac{(k-i+w_{cs_{min}}-z+1)(k-i+w_{cs_{min}}-z+2)\dots(k-i+w_{cs_{min}})}{(k-i-z+1)(k-i-z+2)\dots(k-i)},\end{aligned}$$

for $w_{cs_{min}} \geq z$ (the other case is similar). But,

$$\frac{k-i+w_{cs_{min}}-z+1}{k-i-z+1} \geq \frac{k-i+w_{cs_{min}}-z+2}{k-i-z+2} \geq \dots \geq \frac{k-i+w_{cs_{min}}}{k-i},$$

so

$$\begin{aligned}\binom{k-i+w_{cs_{min}}}{z} &\geq \binom{k-i}{z} \left(\frac{k-i+w_{cs_{min}}}{k-i}\right)^z = \binom{k-i}{z}\left(1+\frac{w_{cs_{min}}}{k-i}\right)^z \\ &\geq \binom{k-i}{z}\left(1+\frac{w_{cs_{min}}}{k}\right)^z.\end{aligned}$$

Thus:

$$P_z \geq \sum_{i=0}^{k-z} \binom{k}{i} q^{k-i}(1-q)^i \left(1+\frac{w_{cs_{min}}}{k}\right)^z \binom{k-i}{z} p^z (1-p)^{k-i-z}(1-p)^{w_{cs max}}, \tag{3.5}$$

or, by using

$$\binom{k-i}{z}\binom{k}{i} = \binom{k}{z}\binom{k-z}{i},$$

$$P_z \geq \binom{k}{z} q^z p^z (1-p)^{w_{cs max}} \left(1+\frac{w_{cs_{min}}}{k}\right)^z \sum_{i=0}^{k-z} \binom{k-z}{i} (1-q)^i q^{k-z-i}(1-p)^{k-z-i}. \tag{3.6}$$

Equation (3.6) gives a lower bound for P_z, which is:

$$P_z \geq \binom{k}{z}\left(1+\frac{w_{cs_{min}}}{k}\right)^z q^z p^z (1-p)^{w_{cs_{max}}}(1-pq)^{k-z}. \tag{3.7}$$

The probability of detected errors can be related to P_z by using the following well known inequality:

$$P_d \geq \sum_{z=1}^{m} P_z, \tag{3.8}$$

where m is the error detection capability of the code. There is no equality here, because an AED code can detect more than the guaranteed number of errors, m, in some situations. However, the two sides of this inequality become very close for small p, thus (3.8) may be used as a good estimate of the probability of detected errors in cases like optical communications, where the bit error rate is indeed very small ($p \leq 10^{-5}$).

The undetected error probability is given by:

$$P_u = 1 - P_d - P_{ef}, \tag{3.9}$$

where P_{ef} is the probability of error free transmission. Using (3.7) and (3.8) we can also obtain an upper bound for P_u:

$$P_u \leq 1 - \sum_{z=0}^{m} P_z. \tag{3.10}$$

3.2. Error detection performance

Equations (3.7) and (3.10) can be particularized for a Bose-Lin code. The following examples are considered:

Case 1: 2 check bits

Since $w_{cs_{min}} = 0$ and $w_{cs_{max}} = 2$, we have that:

$$P_d \geq \sum_{z=1}^{2} \binom{k}{z} q^z p^z (1-p)^2 (1-pq)^{k-z} \tag{3.11}$$

and

$$P_u \leq 1 - \sum_{z=0}^{2} \binom{k}{z} q^z p^z (1-p)^2 (1-pq)^{k-z}. \qquad (3.12)$$

Case 2: 3 check bits

Similarly, $w_{cs_{min}} = 0$ and $w_{cs_{max}} = 3$:

$$P_d \geq \sum_{z=1}^{3} \binom{k}{z} q^z p^z (1-p)^3 (1-pq)^{k-z} \qquad (3.13)$$

and

$$P_u \leq 1 - \sum_{z=0}^{3} \binom{k}{z} q^z p^z (1-p)^3 (1-pq)^{k-z}. \qquad (3.14)$$

Case 3: 4 check bits

In this case, $w_{cs_{min}} = 1$ and $w_{cs_{max}} = 3$ so:

$$P_d \geq \sum_{z=1}^{6} \binom{k}{z} \left(1 + \frac{1}{k}\right)^z q^z p^z (1-p)^3 (1-pq)^{k-z} \qquad (3.15)$$

$$P_u \leq 1 - \sum_{z=0}^{6} \binom{k}{z} \left(1 + \frac{1}{k}\right)^z q^z p^z (1-p)^3 (1-pq)^{k-z}. \qquad (3.16)$$

Case 4: 5 and more check bits

Because of the mapping, $w_{cs_{min}} = 2$ and $w_{cs_{max}} = r - 2$:

$$P_d \geq \sum_{z=1}^{5 \cdot 2^{r-4}+r-4} \binom{k}{z} \left(1 + \frac{2}{k}\right)^z q^z p^z (1-p)^{r-2} (1-pq)^{k-z} \qquad (3.17)$$

and

$$P_u \leq 1 - \sum_{z=0}^{5 \cdot 2^{r-4}+r-4} \binom{k}{z} \left(1 + \frac{2}{k}\right)^z q^z p^z (1-p)^{r-2} (1-pq)^{k-z}. \qquad (3.18)$$

The above bounds for P_d and P_u are compared for different codes in Fig. 3.1 and Fig. 3.2.

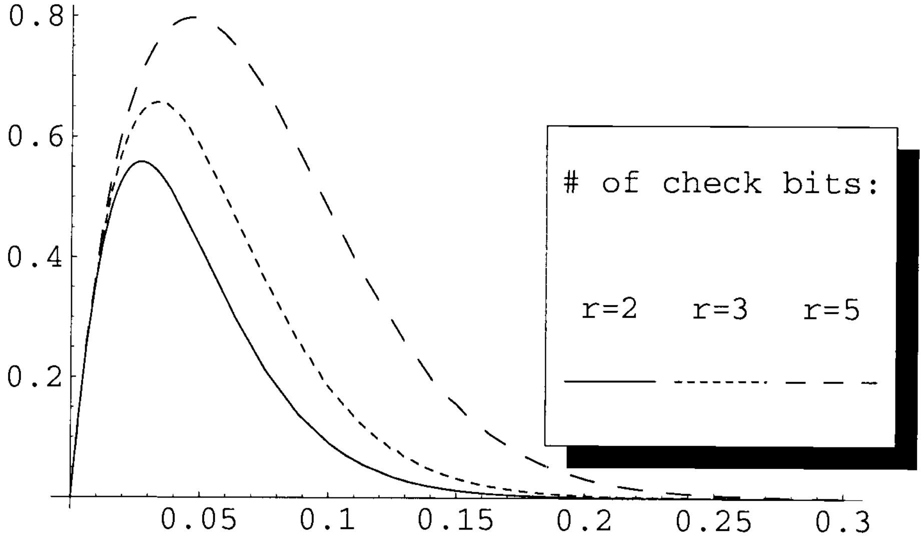


FIGURE 3.1. Lower bounds on P_d for $k = 100$

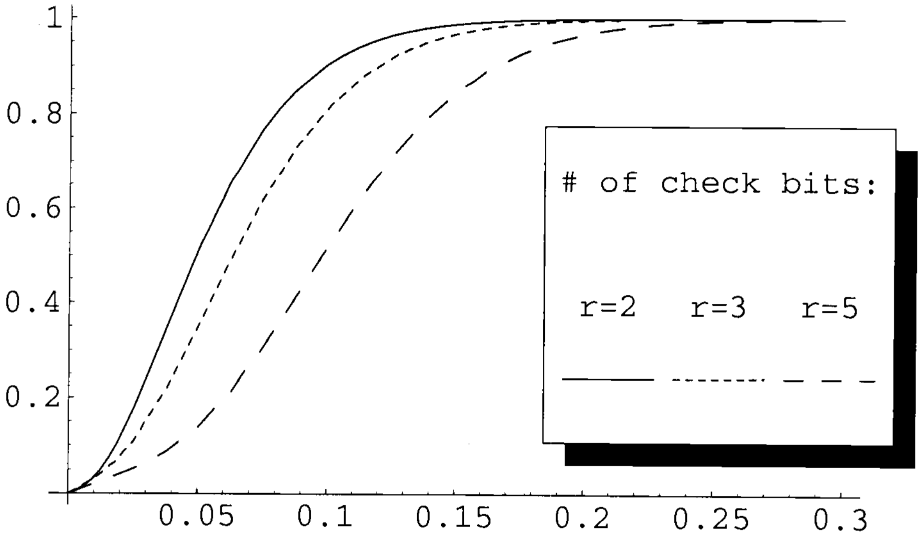


FIGURE 3.2. Upper bounds on P_u for $k = 100$

3.3. The Bose-Lin codes - An alternative description

In this section the Bose-Lin codes are described using a somewhat different notation than the one used in [10]. A common characteristic of the codes is that the check bits are determined as a function of the number of zeros in the information bits.

We first introduce some notation. Let $F = \{0,1\}$ and let F^k be the set of all binary vectors of length k, and for $\mathbf{x} \in F^k$, let $u(\mathbf{x})$ denote its number of zeros and $||\mathbf{x}||$ its number of ones (the Hamming weight). For a non-negative integer a, $||a||$ denotes the number of ones in its binary expansion. For example, $u((011101)) = 2$, $||(011101)|| = 4$, $||21|| = 3$ (since $21 = 2^4 + 2^2 + 1$).

For two vectors $\mathbf{x}$ and $\mathbf{y}$, $\mathbf{x} \subseteq \mathbf{y}$ denotes that $\mathbf{y}$ covers $\mathbf{x}$, that is, $x_i \leq y_i$ for all i.

For integers a and n, let $[a]_n$ denote the (least non-negative) residue of a modulo n.

For non-negative integers a and s, where $a < 2^s$, let

$$\mathbf{B}_s(a) = (a_{s-1}, a_{s-2}, \ldots, a_0) \in F^s$$

where

$$a = \sum_{i=0}^{s-1} a_i 2^i, \quad a_i \in F.$$

The Bose-Lin codes are systematic. A codeword consists of a k bits information vector and an r bits check vector. In addition, there is another (integer) parameter ν satisfying $0 \leq 2\nu \leq r$. Let

$$\sigma = \binom{2\nu}{\nu}, \quad \theta = 2^{r-2\nu}, \text{ and } \mu = \sigma\theta.$$

Finally, let $\mathbf{b}_\nu(0), \mathbf{b}_\nu(1), \ldots, \mathbf{b}_\nu(\sigma - 1)$ be a listing of all the balanced vectors of length 2ν, that is, the vectors of Hamming weight ν.

For an information vector $\mathbf{x}$, let $u = u(\mathbf{x})$, and define α by

$$[u]_\mu = \alpha\theta + [u]_\theta \text{ where then } 0 \leq \alpha < \sigma.$$

The *check vector* is given by $(\mathbf{b}_\nu(\alpha), \mathbf{B}_{r-2\nu}([u]_\theta))$.

Bose and Lin showed that this code detects all asymmetric errors of weights up to $(\sigma - 1)\theta + r - 2\nu$, whereas some errors of weight $(\sigma - 1)\theta + r - 2\nu + 1$ are not detected.

For $k \leq 2^r$, the code with $\nu = 0$ is optimal (it reduces to the all error detecting Berger-Freiman code [3], [14] in this case).

The following lemma was known to Bose and Lin, but not explicitly stated. This lemma was the reason they only considered $\nu \leq 2$.

Lemma 1. *For $k > 2^r$, $(\sigma - 1)\theta + r - 2\nu$ is maximal for $\nu = 0$ when $r = 1, 2, 3$, and for $\nu = 1$ when $r = 4$, and for $\nu = 2$ when $r \geq 5$.*

Proof. Suppose r is fixed, and for $0 \leq 2\nu \leq r$ let

$$A(\nu) = (\sigma - 1)\theta + r - 2\nu = \left\{\binom{2\nu}{\nu} - 1\right\} 2^{r-2\nu} + r - 2\nu.$$

Then simple algebraic manipulations show that

$$A(\nu + 1) - A(\nu) = 2^{r-2\nu-2}\left\{3 - \frac{2}{\nu + 1}\binom{2\nu}{\nu}\right\} - 2.$$

Hence for $\nu \geq 2$, $A(\nu + 1) < A(\nu)$. Further,

$$A(2) - A(1) = 2^{r-4} - 2 \geq 0$$

for $r \geq 5$ and

$$A(1) - A(0) = 2^{r-2} - 2 > 0$$

for $r \geq 4$. □

In the following , we will consider the general ν, since it does not yield more complex derivations.

3.4. Undetectable errors

Suppose $\mathbf{x} \in F^k$ is encoded using the Bose-Lin code and transmitted over a Z-channel. An undetectable error occurs if the received vector is another codeword. The next theorem characterizes the undetectable errors.

Theorem 1. *Suppose that a codeword*

$$(\mathbf{x}, \mathbf{b}_\nu(\alpha), \mathbf{B}_{r-2\nu}([u]_\theta))$$

has been transmitted over the Z-channel and $l > 0$ errors occured in the information part $\mathbf{x}$. Let $u = u(\mathbf{x})$ and $\lambda = [-l]_\mu$; then $l = j\mu - \lambda$ where $j \geq 1$. An undetectable error has occured if and only if

i) $\mathbf{b}_\nu(\alpha)$ *is not changed in the transmission,*

ii) $\lambda \leq [u]_\theta$,

iii) $\mathbf{B}_{r-2\nu}(\lambda) \subseteq \mathbf{B}_{r-2\nu}([u]_\theta)$,

iv) $\mathbf{B}_{r-2\nu}([u]_\theta)$ *is changed in exactly the positions where* $\mathbf{B}_{r-2\nu}(\lambda)$ *is 1.*

Proof. Since the information part of the corrupted codeword has $u + l$ zeros, the errors are undetectable if and only if the check part $\mathbf{c}(u)$ has been changed to $\mathbf{c}(u+l)$ during the transmission. We will show that this is equivalent to conditions i–iv. Clearly, this is possible only if

$$\mathbf{c}(u + l) \subseteq \mathbf{c}(u) \tag{3.19}$$

First we note that $\mathbf{c}(u+l) = \mathbf{c}(u-\lambda)$ since $[u+l]_\mu = [u-\lambda]_\mu$. By definition

$$\mathbf{c}(u) = (\mathbf{b}_\nu(\alpha), \mathbf{B}_{r-2\nu}([u]_\theta)),$$

$$\mathbf{c}(u - \lambda) = (\mathbf{b}_\nu(\alpha'), \mathbf{B}_{r-2\nu}([u - \lambda]_\theta)),$$

where α and α' are defined by

$$[u]_\mu = \alpha\theta + [u]_\theta,$$

$$[u-\lambda]_\mu = \alpha'\theta + [u-\lambda]_\theta.$$

Hence (3.19) is satisfied if and only if

$$\alpha = \alpha' \tag{3.20}$$

(this is condition i) and

$$\mathbf{B}_{r-2\nu}([u-\lambda]_\theta) \subseteq \mathbf{B}_{r-2\nu}([u]_\theta). \tag{3.21}$$

If $\lambda \geq \theta$, then $\alpha \neq \alpha'$ and so (3.20) and hence (3.19) are not satisfied. If $[u]_\theta < \lambda < \theta$, then $[u-\lambda]_\theta > [u]_\theta$ and so (3.21) and hence (3.19) are not satisfied. This proves ii. Further, if $0 \leq \lambda \leq [u]_\theta$, then (3.21) is satisfied exactly when $\mathbf{B}_{r-2\nu}(\lambda) \subseteq \mathbf{B}_{r-2\nu}([u]_\theta)$. This proves iii. Finally, we observe that under condition iii, $\mathbf{B}_{r-2\nu}([u]_\theta)$ is changed to $\mathbf{B}_{r-2\nu}([u]_\theta - \lambda)$ exactly when condition iv is satisfied. This completes the proof of the theorem. □

3.5. The probability of undetected error

Suppose that an information vector $\mathbf{x}$ is chosen from F^k according to some probability distribution P, then $\mathbf{x}$ is encoded by a Bose-Lin code and transmitted over a Z-channel with error probability p (that is, a 1 can change to 0 with probability p). The probability that the received vector is another codeword (i.e. that an undetectable error has occured) depends only on $u = u(\mathbf{x})$ and p, and we denote it by $P_{\text{ue}}(u,p)$. Then the probability of undetected error for the code is

$$\begin{aligned} P_{\text{ue}}(C,p) &= \sum_{\mathbf{x}\in F^k} P(\mathbf{x}) P_{\text{ue}}(u(\mathbf{x}),p) \\ &= \sum_{u=0}^{k} P_{\text{ue}}(u,p) \sum_{\mathbf{x}\in F^k, u(\mathbf{x})=u} P(\mathbf{x}). \end{aligned}$$

The part $\sum_{\mathbf{x}\in F^k, u(\mathbf{x})=u} P(\mathbf{x})$ is the probability that the information vector contains u zeros, and it depends on the distribution P. An important special case is when the bits in the information vector are i.i.d. with probability q of being a zero. In this case

$$\sum_{\mathbf{x}\in F^k, u(\mathbf{x})=u} P(\mathbf{x}) = \binom{k}{u} q^u (1-q)^{k-u}.$$

In particular, if the codewords are uniformly distributed, (i.e. $q = 1/2$), then $\sum_{\mathbf{x}\in F^k, u(\mathbf{x})=u} P(\mathbf{x}) = \binom{k}{u} 2^{-k}$.

3.6. Determining $P_{\text{ue}}(u,p)$

Suppose $(\mathbf{x}, \mathbf{c}(u))$ is transmitted and $l = j\mu - \lambda > 0$ errors occur in $\mathbf{x}$. The probability of this event is $\binom{w}{l} p^l (1-p)^{w-l}$ (recall that $w = k-u$). By Theorem 1, an undetected error has occured if and only if i–iv are satisfied, and if so, then there are $||\mathbf{B}_{r-2\nu}(\lambda)|| = ||\lambda||$ errors in the check part (all of them in the part $\mathbf{B}_{r-2\nu}([u]_\theta)$). Since $||\mathbf{b}_\nu(\alpha)|| = \nu$, the probability of this is $p^{||\lambda||}(1-p)^{\nu+||[u]_\theta||-||\lambda||}$ (note that by iv), the locations of the errors are determined by λ).

From these facts we get:

$$\begin{aligned} P_{\text{ue}}(u,p) = \sum_{j\geq 1} \sum_{\substack{\lambda \\ \mathbf{B}_{r-2\nu}(\lambda)\subseteq \mathbf{B}_{r-2\nu}([u]_\theta)}} &\binom{w}{j\mu-\lambda} p^{j\mu-\lambda}(1-p)^{w-j\mu+\lambda} \\ &\cdot p^{||\lambda||}(1-p)^{\nu+||[u]_\theta||-||\lambda||} \end{aligned}$$

$$\begin{aligned}
&= \sum_{\substack{\lambda \\ \mathbf{B}_{r-2\nu}(\lambda)\subseteq\mathbf{B}_{r-2\nu}([u]_\theta)}} p^{||\lambda||}(1-p)^{\nu+||[u]_\theta||-||\lambda||} \\
&\qquad \cdot \sum_{j\geq 1}\binom{w}{j\mu-\lambda} p^{j\mu-\lambda}(1-p)^{w-j\mu+\lambda}.
\end{aligned}$$

Thus we have the following theorem:

Theorem 2. *For $0 \leq u \leq k$ the probability of undetected error, $P_{\text{ue}}(u,p)$ is given by*

$$\sum_{\substack{\lambda \\ \mathbf{B}_{r-2\nu}(\lambda)\subseteq\mathbf{B}_{r-2\nu}([u]_\theta)}} p^{||\lambda||}(1-p)^{\nu+||[u]_\theta||-||\lambda||} f_{\lambda,m,k-u}(p),$$

where

$$f_{\lambda,\mu,w}(p) = \sum_{j\geq 1}\binom{w}{j\mu-\lambda} p^{j\mu-\lambda}(1-p)^{w-j\mu+\lambda}$$

for $\lambda = 0, 1, \ldots, \mu-1$.

For the sums $f_{\lambda,\mu,w}(p)$, $\lambda = 0, 1, \ldots, \mu-1$, there are alternative expressions that will be more suitable for computation when w is large. Let $\varepsilon = e^{2\pi i/\mu}$. For $0 \leq s \leq \mu - 1$ we get

$$\begin{aligned}
&(1+(\varepsilon^s-1)p)^w \\
&= (\varepsilon^s p + (1-p))^w \\
&= \sum_{l=0}^{w}\binom{w}{l}\varepsilon^{sl}p^l(1-p)^{w-l} \\
&= (1-p)^w \\
&\quad + \sum_{\lambda=0}^{\mu-1}\sum_{j\geq 1}\binom{w}{j\mu-\lambda}\varepsilon^{s(j\mu-\lambda)}p^{j\mu-\lambda}(1-p)^{w-j\mu+\lambda} \\
&= (1-p)^w + \sum_{\lambda=0}^{\mu-1}\varepsilon^{-s\lambda}f_{\lambda,\mu,w}.
\end{aligned}$$

Solving these μ equations for $f_{\lambda,\mu,w}$, $\lambda = 0, 1, \ldots, \mu - 1$, we get the following lemma.

Lemma 2. *Let* $\varepsilon = e^{2\pi i/\mu}$. *Then*

$$f_{0,\mu,w}(p) = \frac{1}{\mu}\sum_{s=0}^{\mu-1}(1+(\varepsilon^s-1)p)^w - (1-p)^w,$$

$$f_{\lambda,\mu,w}(p) = \frac{1}{\mu}\sum_{s=0}^{\mu-1}\varepsilon^{s\lambda}(1+(\varepsilon^s-1)p)^w \textit{ for } 0<\lambda<\mu.$$

3.7. The minimal weight undetectable errors

As mentioned in Section 3.3, Bose and Lin [10] showed that the minimal weight of an undetectable error is $(\sigma-1)\theta + r - 2\nu + 1$ (they only considered $\nu \leq 2$). For completeness we prove this for general ν. Moreover, we determine the exact number of errors of minimal weight.

Theorem 3. *For a Bose-Lin code with parameters* k, r, *and* ν, *where* $2\nu < r$, *the minimal weight of an undetectable error is* $(\sigma-1)\theta + r - 2\nu + 1$, *and the number of undetectable errors of this weight is* $\sum_{t\geq 1}\binom{k+1}{t\theta-1}\binom{k-t\theta+2}{m-\theta+2}$.

Proof. From the proof of Theorem 1, we see that for a given u, the weight of an undetectable error is of the form

$$||\lambda|| + j\mu - \lambda = j\mu - (\lambda - ||\lambda||) \tag{3.22}$$

where $j \geq 1$, $0 \leq \lambda \leq [u]_\theta \leq \theta - 1$ and

$$\mathbf{B}_{r-2\nu}(\lambda) \subseteq \mathbf{B}_{r-2\nu}([u]_\theta)). \tag{3.23}$$

For a minimal weight, clearly $j=1$. Further, if

$$\lambda = \sum_{i=0}^{r-2\nu-1} a_i 2^i,$$

then

$$\lambda - ||\lambda|| = \sum_{i=0}^{r-2\nu-1} a_i(2^i - 1).$$

Hence, if $\mathbf{B}_{r-2\nu}(\lambda') \subseteq \mathbf{B}_{r-2\nu}(\lambda)$ where $\lambda' = \sum_{i=0}^{r-2\nu-1} a_i' 2^i$, then

$$(\lambda - ||\lambda||) - (\lambda' - ||\lambda'||) = \sum_{i:a_i=1,a_i'=0} (2^i - 1) > 0$$

except if λ is odd and $\lambda' = \lambda - 1$. Hence, for fixed $[u]_\theta$,

$$\min_{\lambda:\mathbf{B}_{r-2\nu}(\lambda)\subseteq\mathbf{B}_{r-2\nu}([u]_\theta)} \{\mu - (\lambda - ||\lambda||)\} = \mu - ([u]_\theta - ||[u]_\theta||),$$

and the minimum is obtained for $\lambda = [u]_\theta$ and, if $[u]_\theta$ is odd, also for $\lambda = [u]_\theta - 1$. Since $\theta - 1 = 2^{r-2\nu} - 1$ is odd and $\mathbf{B}_{r-2\nu}([u]_\theta) \subseteq \mathbf{B}_{r-2\nu}(\theta - 1)$ for all u,

$$\begin{aligned}\min_u\{\mu - ([u]_\theta - ||[u]_\theta||)\} &= \mu - (\theta - 1 - (r - 2\nu)) \\ &= (\sigma - 1)\theta + r - 2\nu + 1,\end{aligned}$$

and this minimum is obtained in three cases:

$$\begin{aligned}&[u]_\theta = \theta - 1 \;\; \lambda = \theta - 1, \\ &[u]_\theta = \theta - 1 \;\; \lambda = \theta - 2, \\ &[u]_\theta = \theta - 2 \;\; \lambda = \theta - 2.\end{aligned}$$

We note that $[u]_\theta = \theta - 1$ if and only if $u = t\theta - 1$ for some $t \geq 1$ and similarly for $\theta - 2$. The number of minimal weight undetectable errors where $u = t\theta - 1$ or $u = t\theta - 2$ is therefore 2^{-k} times

$$\begin{aligned}&\binom{k}{t\theta - 1}\binom{k - t\theta + 1}{\mu - \theta + 1} \\ &+ \binom{k}{t\theta - 1}\binom{k - t\theta + 1}{\mu - \theta + 2} \\ &+ \binom{k}{t\theta - 2}\binom{k - t\theta + 2}{\mu - \theta + 2} = \binom{k+1}{t\theta - 1}\binom{k - t\theta + 2}{\mu - \theta + 2}.\end{aligned}$$

Summing over all $t \geq 1$, the theorem follows. □

From our discussion we see that there are detectable errors of all weights (up to the maximum weight of a codeword), but undetectable errors of only some of these weights. The exact determination of these weights was first done by El-Mougy and Gorshe [13] (for $\nu \leq 2$). In the general case, a complete description of the possible weights of undetected errors is determined by (3.22) and (3.23) above.

For small p, the cases where undetectable errors have minimal weight will provide the main contribution to $P_{\text{ue}}(C,p)$. Since $1-p \approx 1$, we get the following corollary.

Corollary 1. *For small p and $q = 1/2$,*

$$P_{\text{ue}}(C,p) \approx p^{(\sigma-1)\theta+r-2\nu+1} \sum_{t\geq 1} \binom{k+1}{t\theta-1} \binom{k-t\theta+2}{\mu-\theta+2} 2^{-k}.$$

3.8. A couple of examples

Example 1. *In this example $\nu = 2$ and $r = 5$. For these parameters, $\sigma = 6$, $\theta = 2$, and $\mu = 12$. The minimal weight of uncorrectable errors is $(\sigma-1)\theta+r-2\nu+1 = 12$. From Theorem 2 we get:*

$[u]_2$	$P_{\text{ue}}(u,p)$
0	$(1-p)^2 f_0$
1	$(1-p)^3 f_0 + p(1-p)^2 f_1$

Here $f_\lambda = f_{\lambda,12,k-u}(p)$ for $\lambda = 0,1$.

The values of $P_{\text{ue}}(C,p)$ and its approximation given in Corollary 1 for $q = 1/2$ and $k = 50$ are given in the Table 1 for some values of p.

TABLE 3.1. $P_{\text{ue}}(C,p)$, k=50

p	$P_{\text{ue}}(C,p)$	*approx.*
0.00001	$0.3874981970 \cdot 10^{-52}$	$0.3875815183 \cdot 10^{-52}$
0.0001	$0.3867490905 \cdot 10^{-40}$	$0.3875815183 \cdot 10^{-40}$
0.001	$0.3793352274 \cdot 10^{-28}$	$0.3875815183 \cdot 10^{-28}$
0.01	$0.3124162376 \cdot 10^{-16}$	$0.3875815183 \cdot 10^{-16}$
0.1	$0.4246867240 \cdot 10^{-5}$	$0.3875815183 \cdot 10^{-4}$
0.2	$0.1668633091 \cdot 10^{-2}$	0.1587533899
0.425	0.4001579456	
0.5	0.3180626249	
1	0	

TABLE 3.2. $P_{\text{ue}}(C,p)$, k=100

p	$P_{\text{ue}}(C,p)$	*approx.*
0.00001	$0.2908927440 \cdot 10^{-48}$	$0.2910280410 \cdot 10^{-48}$
0.0001	$0.2896778669 \cdot 10^{-36}$	$0.2910280410 \cdot 10^{-36}$
0.001	$0.2778016844 \cdot 10^{-24}$	$0.2910280410 \cdot 10^{-24}$
0.01	$0.1825826102 \cdot 10^{-12}$	$0.2910280410 \cdot 10^{-12}$
0.1	$0.2453695931 \cdot 10^{-2}$	0.2910280410
0.2277	$0.7190816340 \cdot 10^{-1}$	
0.5	$0.2364620679 \cdot 10^{-1}$	
1	0	

The function $P_{\mathrm{ue}}(C,p)$ has its maximum for $p \approx 0.425$. We see that the approximation is reasonably good for $p \leq 0.01$. For $p > 0.235$ (approximately), the approximation has a value larger than 1.

For $k = 100$ the situation is similar. The maximum is obtained for $p \approx 0.2277$. The approximation is larger than 1 for $p > 0.1109$. Some selected values are given in Table 1.

Example 2. *For $\nu = 1$ and $r = 5$ we get:*

$[u]_8$	$P_{\mathrm{ue}}(u,p)$
0	$(1-p)f_0$
1	$(1-p)^2 f_0 + p(1-p)f_1$
2	$(1-p)^2 f_0 + p(1-p)f_2$
3	$(1-p)^3 f_0 + p(1-p)^2(f_1+f_2) + p^2(1-p)f_3$
4	$(1-p)^2 f_0 + p(1-p)f_4$
5	$(1-p)^3 f_0 + p(1-p)^2(f_1+f_4) + p^2(1-p)f_5$
6	$(1-p)^3 f_0 + p(1-p)^2(f_2+f_4) + p^2(1-p)f_6$
7	$(1-p)^4 f_0 + p(1-p)^3(f_1+f_2+f_4)$ $+p^2(1-p)^2(f_3+f_5+f_6) + p^3(1-p)f_7$

Here $f_\lambda = f_{\lambda,16,k-u}(p)$, $\lambda = 0, 1, \ldots, 7$.

4. A ONE-CODE TYPE I HYBRID ARQ SYSTEM

Hybrid protocols use forward error correction in conjunction with error detection. Thus, the FEC part of the protocol is designed to correct the most frequent error patterns, caused by noise on the channel, while the error detection part deals with the less frequently occurring error patterns. These patterns are generally most likely to cause decoder errors in the FEC system. The most common approach is the type I hybrid ARQ which can be implemented as a one code or a two code system. The first method may use only a FEC code and retransmission requests are generated either if the number of errors exceeds a certain threshold, or in the event of FEC decoder failure. A two code system uses separate feedforward error correcting and feedback error detecting codes.

The existence of high information rate t-AEC/d-AED codes suggests a good opportunity for using type I hybrid ARQ protocols for the Z-channel. Moreover, these codes can correct t asymmetric errors, and simultaneously detect d ($d > t$), and their encoding/decoding complexity is comparable to the existing error correcting codes.

4.1. Reliability and Efficiency

The reliability of any ARQ protocol is given by the final error probability (or the accepted packet error rate), by definition, the value to which the ratio of the number N_u of received blocks with undetected errors to the total number of received blocks N converges in probability [19]:

$$\lim_{N\to\infty} P\left\{\left|\frac{N_u}{N} - P_E\right| > \epsilon\right\} = 0, \ \forall\, \epsilon > 0. \tag{4.1}$$

We have given some bounds on the final error probability for the Z-channel with ARQ in [33]. Essentially, it does not depend on the delays introduced by any specific basic ARQ protocol and it may be calculated as:

$$P_E = \frac{P_u}{1 - P_d} \tag{4.2}$$

where P_d is the probability of detected errors and P_u the undetected error probability). For a hybrid ARQ protocol, we also need to consider P_c (the probability of corrected errors), which is a characteristic of the feedforward part of the ARQ system. Note that $P_u + P_d + P_c = 1$ and we include the error free codeword probability into P_c. The final error probability is given again by (4.2). However, in this case P_u and P_d are related in a different way and we may also write:

$$P_E = \frac{P_u}{P_u + P_c}. \tag{4.3}$$

The delivery time is characterized by the expected number of channel symbols required to deliver one information symbol to a user. This is called the throughput efficiency, or short throughput, and it does depend on the delays introduced by various ARQ protocols. For analysis purposes we will consider here only SR-ARQ, for which these delays are not important. Since each retransmission request results in the retransmission of only one packet it follows:

$$\eta = \frac{k}{n}(1 - P_d). \tag{4.4}$$

4.2. t-AEC/d-AED codes construction and performance

The necessary and sufficient conditions for a code C to be t-EC/d-UED are given by either of the following [24, 1]:

(a) $N(X, Y) \geq t + 1$ and $N(Y, X) \geq t + 1$,

(b) $D(X,Y) \geq t+d+1$,

for any distinct $X, Y \in \mathcal{C}$. Here, $N(X,Y)$ is the number of crossovers from X to Y and $D(X,Y)$ is the Hamming distance between X and Y.

A somewhat weaker condition (b') $D_a(X,Y) \geq d+1$ (D_a stands for the asymmetric distance) replaces (b) for the necessary and sufficient conditions of t-AEC/d-AED.

Encoding and decoding procedures for these codes are given in [1]. Although good AEC codes exist [9], their information rate is not much better than that of some error correcting codes for the binary symmetric channel. Moreover, efficient encoding procedures are not known yet. In this paper we will concentrate on t-AEC/d-AED codes construction, which can be summarized as follows:

Let $\mathcal{C}'$ be any $(n', k, 2t+1)$ systematic code where n' is the length of the code word, k is the length of the information part and t is the number of correctable errors. Define the D-sequence of length r with parameters t and d by $D[r,t,d] \in \{s_0, s_1, \ldots, s_{m-1}\}$, where each s_i is of length r. Then $\mathcal{C} = \{Y(X,m) | X \in \mathcal{C}'\}$, where $Y(X,m)$ is the codeword obtained by appending $s_{w(X) \bmod m}$ to X, is a t-AEC/d-AED code of length $n = n' + r$.

Moreover, in [1] it is also shown that any t-EC code can be changed into a t-EC/$t+r$-AED code by adding an extra tail of r check bits. For small values of r, the resultant code is an efficient one. This tail sequence can be constructed as:

$$D[r,t,t+r] = \{\underbrace{11\ldots1}_{r-1-i}\,\underbrace{00\ldots0}_{i}\,1,\ \underbrace{11\ldots1}_{r-1-i}\,\underbrace{00\ldots0}_{i}\,0 \mid 0 \leq i \leq r-1\}. \tag{4.5}$$

This specific construction suggests that P_c depends only on the inner systematic code $\mathcal{C}'$. On the other hand, P_u and P_d, are related only to the D tail sequence. However, in order to determine them, the weight distribution of the codewords needs to be considered, thus they depend on $\mathcal{C}'$ in this manner.

4.2.1. t-AEC/d-AED weight distribution

The weight distribution of a t-AEC/d-AED code using D tail sequences (4.5), is given by the following theorem:

Theorem 4. *Let $A'_i, i = 0 \dots n'$, be the weight distribution of C', where C' is a $(n', k, 2t+1)$ systematic code. The t-AEC/$t+r$-AED code $\mathcal{C}$, constructed by appending the $D[r,t,d]$ tail sequence (4.5) to the codewords of C', has the weight distribution given by:*

$$A_i = \begin{cases} 0, & \text{if } 2jr \leq i < (2j+1)r; \\ A'_{2i-(2j+2)r} + A'_{2i-(2j+2)r+1}, & \text{if } (2j+1)r \leq i \leq (2j+2)r - 1, \end{cases} \tag{4.6}$$

for all $j = 0, 1, \dots, \lfloor n'/2 \rfloor$.

Proof. Because the tail check of any word of weight i is $s_{i \bmod 2r}$, the weights of the codewords of $\mathcal{C}$ are at least r. Moreover, they take values which belong to discrete sets of r elements. This is shown in Table 4.1.

TABLE 4.1. The weights of the codewords in $\mathcal{C}$ are given by adding the corresponding check sequence weights to the weights of the codewords in $\mathcal{C}'$

$w_{C'}$	0	1	2	3	$\dots$	$2r-2$	$2r-1$	$2r$	$2r+1$	$\dots$
w_D	r	$r-1$	$r-1$	$r-2$	$\dots$	1	0	r	$r-1$	$\dots$
w_C	r	r	$r+1$	$r+1$	$\dots$	$2r-1$	$2r-1$	$3r$	$3r$	$\dots$

The weight of any codeword in $\mathcal{C}$ is in a set of the form $\{ir, ir+1, \dots, 2ir-1\}$, where i is odd. Note the 'gaps' in the weight distribution of C which are due to the D-sequence "re-adjustments" of weight. They correspond to $\{ir, ir+1, \dots, 2ir-1\}$ sets, where i is even. Taking into account these considerations, equation (4.6) follows directly. □

4.2.2. FEC decoder

Let P_j^w be the probability that a received word has j crossovers from a weight w code word. Assuming only '1 ⟶ 0' errors, with probability p we have:

$$P_j^w = \binom{w}{j} p^j (1-p)^{w-j}. \tag{4.7}$$

Let us assume a codeword X of weight w is received. The probability that it contains correctable errors (or no errors at all) is then:

$$P_c(X, w, p) = \sum_{j=0}^{t} P_j^w. \tag{4.8}$$

Then the probability of correctable errors for this system can be calculated by multiplying the probability of correctable errors for a codeword of a certain weight with the probability that the information word corresponding to that codeword is generated. Assuming that each information word is equally likely we have:

$$P_c(\mathcal{C}, p) = \frac{1}{2^k} \sum_{i=0}^{n} A_i \sum_{j=0}^{t} P_j^i. \tag{4.9}$$

The FEC decoder errors occur whenever the received codewords become valid codewords after more than d errors occur during the transmission. Note that if less than d errors occur in the received codeword, a retransmission request is always generated. Some patterns with more than d errors may also be detected; however not all such patterns are valid codewords. The decoder failure (that is, passing codewords with undetectable errors) only happens when the received codeword is a valid codeword that is different from the transmitted one .

If more than d errors occur during the transmission, the received word Y is at an asymmetric distance of more than $d+1$ from the transmitted word X. The probability of a word passing with undetected errors is upper bounded by:

$$P(\{w_Y \leq w_X - d - 1\} \cap \{Y \in \mathcal{C}\}).$$

However, not all the received words with $d+1$ crossovers are undetectable as mentioned above. In order to select those which are valid codewords, we need to consider the weight distribution of the received words.

A listing of all the codewords of C from the lowest to the highest weight looks like:

$$\left.\begin{array}{c} 0\ 0\ \ldots\ 0 \\ \cdots\cdots\cdots \\ 0\ 0\ \ldots\ 1 \end{array}\right\} r\ldots 2r-1$$

$$\left.\begin{array}{c} 0\ 0\ \ldots\ 1 \\ \cdots\cdots\cdots \\ \cdots\cdots\cdots \end{array}\right\} 3r\ldots 4r-1$$

$$\vdots$$

$$\left.\begin{array}{c} \cdots\cdots\cdots \\ \cdots\cdots\cdots \\ 1\ 1\ \ldots\ 1 \end{array}\right\} qr\ldots qr+s,$$

where

$$(q,s)=\begin{cases} \left(\left\lfloor \frac{w'_{max}}{r}\right\rfloor, w'_{max} \bmod r+r+1\right) & \text{if } \left\lfloor \frac{w'_{max}}{r}\right\rfloor \text{ is odd} \\ \left(\left\lfloor \frac{w'_{max}}{r}\right\rfloor+1, w'_{max} \bmod r+1\right) & \text{if } \left\lfloor \frac{w'_{max}}{r}\right\rfloor \text{ is even,} \end{cases}$$

and w'_{max} is the maximum weight of C'.

The right column gives the weight range of the codewords from C corresponding to the C' codewords in the left column. Because of the nature of errors (only $1 \longrightarrow 0$), a received word contains undetectable errors and thus produces a FEC decoder error only if the transmitted codeword belongs to a lower weight group. Any error pattern with a weight within the gaps between legal codeword weights is detectable. In other words, if the received word Y has a legal codeword weight and is at a distance of more than $d+1$ from the transmitted codeword X, then the decoder will pass it with undetected errors.

We can rewrite the bound on undetected error probability as

$$P_u \leq P\Big(w_Y \in \{r,\dots,2r-1\} \cup \{3r,\dots,4r-1\} \cup \cdots \cup \{vr,\dots,w_X-d-1\}\Big),$$

if $v = \lfloor \frac{w_X-d-1}{r} \rfloor$ is odd, or,

$$P_u \leq P\Big(w_Y \in \{r,\dots,2r-1\} \cup \{3r,\dots,4r-1\} \cup \cdots \cup \{(v-1)r,\dots,vr-1\}\Big),$$

if v is even.

In a compact notation:

$$P_u \leq \begin{cases} P\Big(w_{X'} \in \bigcup_{\substack{1\leq i\leq v-2 \\ i \text{odd}}}\{ir,\dots,(i+1)r-1\} \cup \{vr,\dots,w_X-d-1\}\Big), \\ \hfill \text{if } v \text{ is odd} \\ P\Big(w_{X'} \in \bigcup_{\substack{1\leq i\leq v-1 \\ i \text{odd}}}\{ir,\dots,(i+1)r-1\}\Big), \qquad \text{if } v \text{ is even.} \end{cases}$$

In other words, this upper bound is given by the probability that the number of errors occurred during transmission yields a valid codeword of lower weight.

$$P_u(w,d,r,p) \leq \begin{cases} \sum_{\substack{i=1 \\ i \text{odd}}}^{v-2} \sum_{j=ir}^{(i+1)r-1} H(A_{w-j}-1)P_j^w + \sum_{j=vr}^{w-d-1} H(A_{w-j}-1)P_j^w, \\ \hfill \text{if } v \text{ is odd} \\ \sum_{\substack{i=1 \\ i \text{odd}}}^{v-1} \sum_{j=ir}^{(i+1)r-1} H(A_{w-j}-1)P_j^w, \qquad \text{if } v \text{ is even.} \end{cases} \tag{4.10}$$

Here, $H(\cdot)$ is the Heaviside step function, and it has the role of 'filtering out' the words which are not legal codewords from each $\{ir,\dots,(i+1)r-1\}$ set. Thus, if the word of weight $w-j$ is not a codeword, the probability to reach its weight is not counted.

Assuming that each codeword is equally likely to be transmitted, the undetected error probability for the code $\mathcal{C}$ is then:

$$P_u(\mathcal{C}, r, p) \leq \frac{1}{2^k} \sum_{i=0}^{n} A_i P_u(i, d, r, p). \tag{4.11}$$

4.3. Examples

4.3.1. A SEC/3-AED code

We consider the $(7, 4)$ Hamming code to be the inner error correcting code. As explained in Section 4.2, we can obtain a SEC-3AED code by appending a tail sequence of $r = 2$ check bits.

TABLE 4.2. The weight distribution of the SEC/3-AED code constructed from the (7,4) Hamming code

$w_{C'}$	0	3	4	7
w_D	2	0	2	0
w_C	2	3	6	7

The (7,4) Hamming code contains the all zero and all one codewords, thus $A'(0) = A'(1) = 1$. All the other codewords are of either 3 or 4 weight. It follows $A'(3) = A'(4) = 7$ and $A'(i) = 0$ for $i = 1, 2, 5, 7$. Then, equation (4.6) and Table 4.1 give the weight distribution as shown in Table 4.2.

The probability of undetected error can then be upper bounded according to equation (4.11) as:

$$P_u(\mathcal{C}, 2, p) \leq \frac{1}{16} \sum_{i=0}^{11} A_i P_u(i, 2, p).$$

TABLE 4.3. The probability of undetected error of 2 t-EC/d-AED codes

$\log_{10} p$	-7	-6	-5	-4	-3	-2	-1
$P_u(C, 4, p)$ SEC/3-AED	8.25×10^{-28}	8.74×10^{-24}	8.74×10^{-20}	8.74×10^{-16}	8.73×10^{-12}	8.56×10^{-8}	8.74×10^{-4}
$P_u(C, 6, p)$ 2-EC/8-AED	9.33×10^{-61}	9.33×10^{-52}	9.33×10^{-43}	9.31×10^{-34}	9.16×10^{-25}	7.75×10^{-16}	1.35×10^{-7}

Because of the weight distribution of this code, the summation has only four nonzero terms. $P_u(i, 4, p)$ is the probability that the weight of the received codeword belongs to the set of legal weights of C and it is at distance more than 3 from the transmitted one. Then,

$$\begin{aligned} P_u(C,4,p) \leq \frac{1}{16}\sum_{i=4}^{7} A_i P_u(i,2,p) &= \frac{1}{16}\left[A_7(P_4^7 + P_5^7) + A_6 P_4^6\right] \\ &= \frac{1}{16}A_7\Big[\binom{7}{4}p^4(1-p)^3 \\ &+ \binom{7}{5}p^5(1-p)^2\Big] \\ &+ \frac{1}{16}A_6\binom{6}{4}p^4(1-p)^2. \end{aligned}$$

This probability of undetected error is shown in Table 4.3 for some values of p.

4.3.2. A 2-AEC/8-AED code

Let us consider the (31,21) binary BCH double correcting code, given by the the following generator polynomial:

$$g(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1.$$

TABLE 4.4. A 2-EC/8-AED code weight distribution

w'	$\mathcal{C}'$ weight distribution	w	$\mathcal{C}$ weight distribution
0	1	6	A_6=1
5	186	8	A_8=1
6	806	9	$A_9 = 3441$
7	2635	9	
8	7905	10	$A_{10} = 26815$
9	18910	10	
10	41602	11	$A_{11} = 127162$
11	85560	11	
12	142600	18	$A_{18} = 337900$
13	195300	18	
14	251100	19	$A_{19} = 553071$
15	301971	19	
16	301971	20	$A_{20} = 553071$
17	251100	20	
18	195300	21	$A_{21} = 337900$
19	142600	21	
20	85560	22	$A_{22} = 127162$
21	41602	22	
22	18910	23	$A_{23} = 26815$
23	7905	23	
24	2635	30	$A_{30} = 3441$
25	806	30	
26	186	31	A_{31}=186
31	1	33	A_{33}=1

Note that this is a primitive narrow-sense BCH code and thus, apart from the all zero codeword, its dual has [25, 41]:

$$\begin{cases} (2^5-1)(2^3+2) & \text{codewords of weight } 2^5-2^2, \\ 2^9+2^4-1 & \text{codewords of weight } 2^4, \text{ and} \\ (2^5-1)(2^3-2) & \text{codewords of weight } 2^5+2^2. \end{cases}$$

The weight distribution of the BCH code can be determined by using the MacWilliams equation [25, 41] and it is shown in Table 4.4. The weight distribution of the 2-AEC/8-AED code is determined according to Theorem 4 and it is also shown in Table 4.4. The probability of undetected error is shown in Table 4.3.

5. CONCLUSION AND FURTHER RESEARCH DIRECTIONS

5.1. Summary

In this thesis, results that are both of theoretical and practical interest are derived for AED and t-AEC/d-AED codes. Also, feedback error control techniques are proposed and analyzed. Specifically, new results are given on:

- The probability of undetected error for the Bose-Lin code.
- Bounds on the probability of undetected error for general classes of systematic AED codes and for t-AEC/d-AED codes.
- Diversity combining for the Z-channel.

Chapter 2 introduced a particular scheme of diversity combining, specific to the Z-channel. The stored result of a bit-by-bit OR operation between any retransmitted codeword and the result of the previous transmissions was used towards increasing both the reliability and the throughput at the receiving end. First the probability of undetected error $P_k(\mathbf{x}, X; p)$ and the average number of transmissions $N_k(\mathbf{x}, X; p)$ were considered for each codeword $\mathbf{x}$, with its set X of covered codewords. Assuming that each codeword is equally likely, the probability of undetected error for an AED code can be calculated as:

$$P_k(C;p) = \frac{1}{|C|}\sum_{\mathbf{x}\in C} P_k(\mathbf{x}, X_{\mathbf{x}}; p).$$

A similar equation was derived for $N_k(C, p)$. In realistic situations, we will be able to compute $P_k(\mathbf{x}, X_{\mathbf{x}}; p)$ exactly for some $\mathbf{x}$'s, and give bounds for other $\mathbf{x}$'s.

Lower and upper bounds for the probabilities of detected and undetected errors in the received words, respectively, were determined in Chapter 3. These bounds may be very useful tools for characterizing ARQ systems performance by providing good starting points for estimating the throughput and the accepted packet error rate. Then, in the same chapter, the Bose-Lin codes were analyzed by providing a new parameterized form for them which includes all the method designs, for any number of check bits. Based on this approach, their probability of undetected error was calculated.

The type I hybrid ARQ protocol with t-AEC/d-AED coding was analyzed for the the Z-channel transmission in Chapter 4. The parameters which characterize this protocol, the final error probability and the throughput were introduced in Section 4.1. Both can be completely determined by the undetected error probability and the probability of error correcting. For t-AEC/d-AED codes with a $D[r, t, d]$ tail sequence as check symbol, the probability of error correcting was calculated and an upper bound on the probability of undetected error was also determined. This bound took into account the weight distribution of these codes, which was determined in Section 4.2 based on the inner error correcting code weight distribution. A couple of detailed examples were given, starting with Hamming and binary BCH codes as inner codes.

5.2. Further Research

In Chapter 3, a powerful class of AED codes has been investigated and analyzed: the Bose-Lin codes. A new parametrized description and the complete derivation of the probability of undetected errors, leaves only one open problem: the complete optimality investigation. Thus, we know that these codes are optimal in the cases of 2, 3 or 4 bits check sequences. However , a generalization to any number of check bits (if true) is highly desireable.

Because of the difficulty in designing systematic t-AEC codes with a better information rate than the corresponding t-error correcting BCH codes, there is an alternate direction one may take; namely, to design t-AEC codes with simpler encoding/decoding techniques.

A t-AEC code design is briefly described in the following [9].

Let $\{\alpha_0 = 0, \alpha_1, \alpha_2, \ldots \alpha_n\}$ be the elements of $GF(n+1)$. We define the function F from the binary n-tuples to $GF(n+1)$ as:

$$F : GF(2^n) \longrightarrow GF(n+1)$$

by

$$F(x) = \begin{bmatrix} F_1(x) \\ F_2(x) \\ \vdots \\ F_t(x) \end{bmatrix},$$

where

$$F_1(x) = F_1((x_1 x_2 \ldots x_n)) = \sum_{x_i=1} \alpha_i$$

and

$$F_i(x) = \sum_{\substack{j_1<j_2<\ldots<j_i \\ x_{j_1}=x_{j_2}=\ldots=x_{j_i}=1}} \alpha_{j_1}\alpha_{j_2}\ldots\alpha_{j_i},$$

for $i = 2, 3, \ldots, t$. Now, F partitions 2^n tuples into $(n+1)^t$ classes $C_1, C_2, \ldots C_{(n+1)^t}$, such that, if $X, Y \in C_i$, then $F(X) = F(Y)$. It can be proven that each of C_i, $i = 1, 2, \ldots, (n+1)^t$ is a t-AEC code and there exists a class which contains at least $\frac{2^n}{(n+1)^t}$ codewords.

Suppose we choose the C_1 code such that:

$$F(x) = \begin{bmatrix} F_1(x) \\ F_2(x) \\ \vdots \\ F_t(x) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let X and X' be the transmitted and the received words, respectively, and X' has s, $s < t$, $0 \rightarrow 1$ errors (similar results hold for $1 \rightarrow 0$ errors). Then, it can be proven that:

$$\begin{aligned} F_1(X') &= S_1 = \sigma_1 \neq 0 \\ F_2(X') &= S_2 = \sigma_2 \neq 0 \\ &\vdots \\ F_s(X') &= S_s = \sigma_s \neq 0 \\ F_{s+1}(X') &= S_{s+1} = 0 \\ &\vdots \\ F_t(X') &= S_t = 0, \end{aligned}$$

where the σ_i's are the symmetric functions of the error location values. Thus, from the syndromes, it is possible to find the number of errors and, furthermore, the syndromes directly give the symmetric functions of the error location values. Then, the errors location can be determined by using Chien search ([4], [25], [34]).

In the case of BCH codes decoding, the major step is to find the symmetric functions of the error location values from the syndromes. Thus, these t-AEC codes have a much simpler decoding procedure.

One possible research goal is to find simple encoding methods for these codes; in particular, methods of encoding in a systematic form. The analysis of these codes within the frame of feedback error control systems is another goal. Thus, a combination of AEC with Bose-Lin codes may provide a valuable hybrid ARQ technique for the Z-channel.

BIBLIOGRAPHY

[1] S. Al-Bassam and B. Bose. Asymmetric/unidirectional error correcting and detecting codes. *IEEE Trans. Comput.*, 43:590–597, May 1994.

[2] G. Benelli. An ARQ scheme with memory and soft error detection. *IEEE Trans. Commun.*, 33:285–288, March 1985.

[3] J.M. Berger. A note on error detecting codes for asymmetric channels. *Information and Control*, 4:68–73, March 1961.

[4] E.R. Berlekamp. *Algebraic Coding Theory.* Aegean Park Press, 1984.

[5] J.E. Blahut. *Theory and Practice of Error Control Codes.* Addison Wesley, Reading, MA, 1983.

[6] M. Blaum. *Codes for Detecting and Correcting Unidirectional Errors.* IEEE Computer Society Press, Los Alamitos, CA, 1993.

[7] J.M. Borden. Optimal asymmetric error detecting codes. *Inform. Control*, 53:66–73, April 1982.

[8] B. Bose. On unordered codes. *IEEE Trans. Comput.*, 40:125–131, February 1991.

[9] B. Bose and S. Cunningham. Asymmetric error correcting codes. In *Methods in Communication, Security and Computer Science.* Springer-Verlag, New York, 1993.

[10] B. Bose and D.J. Lin. Systematic unidirectional error-detecting codes. *IEEE Trans. Comput.*, 34:1026–1032, November 1985.

[11] S.S. Chakraborty, E. Yli-Juuti, and M. Liinaharja. An ARQ scheme with packet combining. *IEEE Commun. Lett.*, 2:200–202, July 1998.

[12] D. Chase. Code combining - A maximum-likelihood decoding approach for combining an arbitrary number of noisy packets. *IEEE Trans. Commun.*, 33:385–393, May 1985.

[13] S. El-Mougy and S. Gorshe. Some error detecting properties of bose-lin codes. *IEEE Trans. Comput.* Submitted paper.

[14] C.V. Freiman. Optimal error detecting codes for completely asymmetric binary channels. *Information and Control*, 5:66–71, March 1962.

[15] B.A. Harvey and S.B. Wicker. Packet combining systems based on the Viterbi decoder. *IEEE Trans. Commun.*, 42:1544–1557, April 1994.

[16] N.K. Jha. Separable codes for detecting unidirectional errors. *IEEE Trans. Computer-Aided Design*, 8:571–574, May 1989.

[17] N.K. Jha and M.B. Vora. A t-unidirectional error detecting systematic code. *Computers and Mathematics with Applications*, pages 705–714, 1988.

[18] S. Kallel. Analysis of an ARQ scheme with code combining. *IEEE Trans. Commun.*, 38:1133–1137, August 1990.

[19] T. Kløve and V. Korzhik. *Error Detecting Codes. General Theory and their Application in Feedback Communication Systems.* Kluwer Academics, Boston/London/Dordrecht, 1995.

[20] T. Kløve, P. Oprisan, and B.Bose. Diversity combining for the Z-channel. *IEEE Trans. Inform. Theory*, March 2005. To be published.

[21] T. Kløve, P. Oprisan, and B.Bose. Probability of undetected error for a class of asymmetric error detecting codes. *IEEE Trans. Information Theory*, March 2005. To be published.

[22] T. Kløve, P. Oprisan, and B. Bose. Probability of undetected error for a class of unidirectional error detecting codes. *Proc. IEEE Int. Symposium. on Inform. Theory*, page 481, July 2004.

[23] D.E. Knuth. Efficient balanced codes. *IEEE Trans. Inform. Theory*, 32:51–53, January 1986.

[24] D.J. Lin and B. Bose. Theory and design of t-error correcting and $d(d > t)$-unidirectional error detecting (t-EC d-UED) codes. *IEEE Trans. Comput.*, 47:433–439, April 1998.

[25] S. Lin and D. J. Costello. *Error Control Coding, Fundamentals and Applications.* Prentice Hall, New Jersey, 1983.

[26] S. Lin and P.S. Yu. A Hybrid-ARQ scheme with parity retransmission for error control of satellite channels. *IEEE Trans. Commun.*, 30:1701–1719, July 1982.

[27] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes.* North-Holland, 1977.

[28] R.J. McEliece. *The Theory of Information and Coding - A Mathematical Framework for Communication.* Addisson-Wesley, 1977.

[29] A.M. Michelson and A.H. Levesque. *Error Control Techniques for Digital Communication.* John Willey & Sons, New York, 1985.

[30] P. Oprisan and B. Bose. ARQ in optical networks. *Proc. PRDC2001*, December 2001.

[31] P. Oprisan and B. Bose. On asymmetric error detection with feedback. In *Information, Coding and Mathematics.* Kluwer Academic Publishers, Boston/Dordrecht/London, 2002.

[32] P. Oprisan and B. Bose. Z-channel feedback error control. *Proc. IEEE Inform. Theory Workshop*, October 2002.

[33] P. Oprisan and B. Bose. On asymmetric error detection performance. *Proc. IEEE Int. Symposium. on Inform. Theory*, page 188, July 2003.

[34] W.W. Peterson and E.J. Weldon Jr. *Error Correcting Codes.* MIT Press, Cambridge, MA, 2^{nd} edition, 1972.

[35] T.R.N. Rao and E. Fujiwara. *Error Control Coding for Computer Systems.* Englewood Cliffs, Prentice Hall, NJ, 1989.

[36] K. A. Schoenhamer-Immink. *Coding Techniques for Digital Recorders.* Prentice Hall International (UK), New York London, 1991.

[37] C.E. Shannon. A mathematical theory of communication. *Bell Systems Technical Journal*, pages 379–423, 1948. Part I.

[38] P. Sindhu. Retransmission error control with memory. *IEEE Trans. Commun.*, 25:473–479, May 1977.

[39] J.E. Smith. On separable unordered codes. *IEEE Trans. Comput.*, 33:741–743, August 1984.

[40] S.B. Wicker. Adaptive rate error control through the use of diversity combining and majority-logic decoding in a Hybrid-ARQ protocol. *IEEE Trans. Commun.*, 39:380–385, March 1991.

[41] S.B. Wicker. *Error Control Systems for Digital Communication and Storage.* Prentice Hall, New Jersey, 1995.

INDEX