"ON THE UNDETECTED ERROR PROBABILITY OF A CONCATENATED CODING SCHEME FOR ERROR CONTROL"

by

Huijie Deng

Department of Electrical & Computer Engineering
Illinois Institute of Technology
Chicago, IL 60616

and

Daniel J. Costello, Jr.

Department of Electrical & Computer Engineering
Illinois Institute of Technology
Chicago, IL 60616

June 1984

This work was supported by NASA under Grant NAG 5-234.

"ON THE UNDETECTED ERROR PROBABILITY OF A CONCATENATED CODING SCHEME FOR ERROR CONTROL

1. ENCODING-DECODING DESCRIPTION

Consider a concatenated coding scheme for error control on a binary symmetric channel, called the <u>inner channel</u>. The bit error rate (BER) of the channel is correspondingly called the <u>inner BER</u>, and is denoted by ε_i. Two linear block codes, C_f and C_b, are used. The inner code C_f, called the <u>frame code</u>, is an (n,k) systematic binary block code with minimum distance d_f. The frame code is designed to correct t or fewer errors and simultaneously detect λ ($\lambda > t$) or fewer errors, where $t + \lambda + 1 \leq d_f$ [1]. The outer code C_b can be either an (n_b, k_b) binary block code with

$$n_b = mk, \tag{1}$$

or an (n_b, k_b) maximum-distance-separable (MDS) code with symbols from GF(q), where $q = 2^b$ and the code length n_b satisfies

$$n_b b = mk. \tag{2}$$

The integer m in both (1) and (2) is the number of frames. The outer code is designed for error detection only.

The encoding of the concatenated code is achieved in two stages. A message of k_b bits (or symbols) is first encoded into a codeword of n_b bits (or symbols) in the outer code C_b. Then this codeword is interleaved to depth m. After interleaving, the n_b-bit (or symbol) <u>block</u> is divided into m k-bit <u>segments</u>. Each k-bit segment is encoded into an n-bit word in the frame code C_f. This n-bit word is called a <u>frame</u>.

The decoding consists of error correction in frames and error detection in m decoded k-bit segments. When a frame in a block is received, it is decoded based on the frame code C_f. The n-k parity bits are then removed from the decoded frame. If there are t or fewer transmission errors in a received frame, the errors will be corrected, and the decoded segment is error free. If there are more than t errors in a received frame, the decoded segment contains undetected errors. After m frames of a block have been decoded, the m k-bit decoded segments are deinterleaved. Then error detection is performed on these m segments based on the outer code C_b. If no error is detected, the m decoded segments are assumed to be error free, and are accepted by the receiver. If the presence of errors is detected, the m decoded segments are discarded and the receiver requests a retransmission of the rejected block.

2. PROBABILITY OF UNDETECTED ERROR FOR THE FRAME CODE

For a code word $\bar{v}$ in the frame code C_f, let $w(\bar{v})$ denote the Hamming weight of $\bar{v}$. If a decoded frame contains an undetectable error pattern, this error pattern must be a nonzero codeword in C_f. Let $\bar{e}_0$ be a nonzero error pattern after decoding. The probability $P_f(w, \varepsilon_i)$ that a decoded frame contains a nonzero error vector $\bar{e}_0$ after decoding is given by [2]:

$$P_f(w, \varepsilon_i) = \sum_{i=0}^{t} \sum_{j=0}^{\min(t-i,n-w)} \binom{w}{i}\binom{n-w}{j} \varepsilon_i^{w-i+j}(1-\varepsilon_i)^{n-w+i-j}, \quad (3)$$

where $w = w(\bar{e}_0)$, and ε_i is the BER of the inner channel.

Let $P_{ud}^{(f)}(\varepsilon_i)$ denote the probability of undetected error for the frame code and let $\{A_w^{(f)}, d_f \leq w \leq n\}$ be the weight distribution of C_f. Then it follows from (3) that

$$P_{ud}^{(f)}(\varepsilon_i) = \sum_{w=d_f}^{n} A_w^{(f)} P_f(w, \varepsilon_i). \tag{4}$$

If $\varepsilon_i << \frac{1}{n}$, a close approximation of $P_{ud}^{(f)}(\varepsilon_i)$ is given by

$$P_{ud}^{(f)}(\varepsilon_i) \simeq A_{d_f} P_f(d_f, \varepsilon_i), \tag{5}$$

and from (3) we have

$$P_f(d_f, \varepsilon_i) \simeq \binom{d_f}{t} \varepsilon_i^{d_f - t} (1-\varepsilon_i)^{n-d_f+t} . \tag{6}$$

For convenience, we first consider the case of a binary linear block outer code. The result is then generalized for MDS outer codes.

Now consider any one of the m frames, say the $i^{\underline{th}}$ frame. Let ε_a be the BER of the frame after decoding. Then we have

$$\varepsilon_a = \frac{1}{n} \sum_{w=d_f}^{n} w A_w^{(f)} P_f(w, \varepsilon_i). \tag{7}$$

If $\varepsilon_i << \frac{1}{n}$, then

$$\varepsilon_a \simeq \frac{1}{n} d_f A_{d_f}^{(f)} P_f(d_f, \varepsilon_i) \tag{8}$$

will be a good approximation to ε_a. Let E be defined as the event that the $j^{\underline{th}}$ frame contains undetected errors. Then from (4) we have

$$\Pr\{E\} = P_{ud}^{(f)}(\varepsilon_i). \tag{9}$$

Now let $\varepsilon_{a/E}$ denote the BER embedded in the $j^{\underline{th}}$ decoded frame conditioned on the occurrence of event E. Then from (7) and (9), it follows that

$$\varepsilon_{a/E} = \varepsilon_a / \Pr\{E\}$$

$$= \frac{\frac{1}{n} \sum_{w=d_f}^{n} w A_w^{(f)} \; P_f(w, \varepsilon_i)}{P_{ud}^{(f)}(\varepsilon_i)} \; . \qquad (10)$$

For $\varepsilon_i << \frac{1}{n}$, substituting (5) and (8) into (10) yields

$$\varepsilon_{a/E} \simeq \frac{\frac{1}{n} \, d_f A_{d_f}^{(f)} \; P_f(d_f, \varepsilon_i)}{A_{d_f}^{(f)} \; P_f(d_f, \varepsilon_i)} = \frac{d_f}{n} \; . \qquad (11)$$

Now define S to be a random variable such that when h of the m frames contain undetected errors, S = h, h = 0, 1, 2, $\cdots$, m. It follows from (4) that

$$\Pr\{S=h\} = \binom{m}{h} [P_{ud}^{(f)}(\varepsilon_i)]^h [1 - P_{ud}^{(f)}(\varepsilon_i)]^{m-h}. \qquad (12)$$

After deinterleaving of the m decoded segments (with the n-k parity bits removed from each frame), the BER embedded in the n_b-bit block, given that S = h, (i.e., h frames contain undetected errors) is given by

$$\varepsilon_0(h) = \varepsilon_{a/E} \cdot \frac{h}{m} \quad , \qquad h = 0, 1, 2, \cdots, m. \qquad (13)$$

We call the channel specified by (12) and (13) the <u>outer channel</u>, and it is depicted in Figure 1. Note that $\varepsilon_0(0) = 0$. This channel can be viewed as a <u>block interference</u> (BI) channel, as described in [3]. Δh, h = 0, 1, 2, $\cdots$, m, is called the h^{th} component channel of the BI channel. Each block of n_b bits (n_b

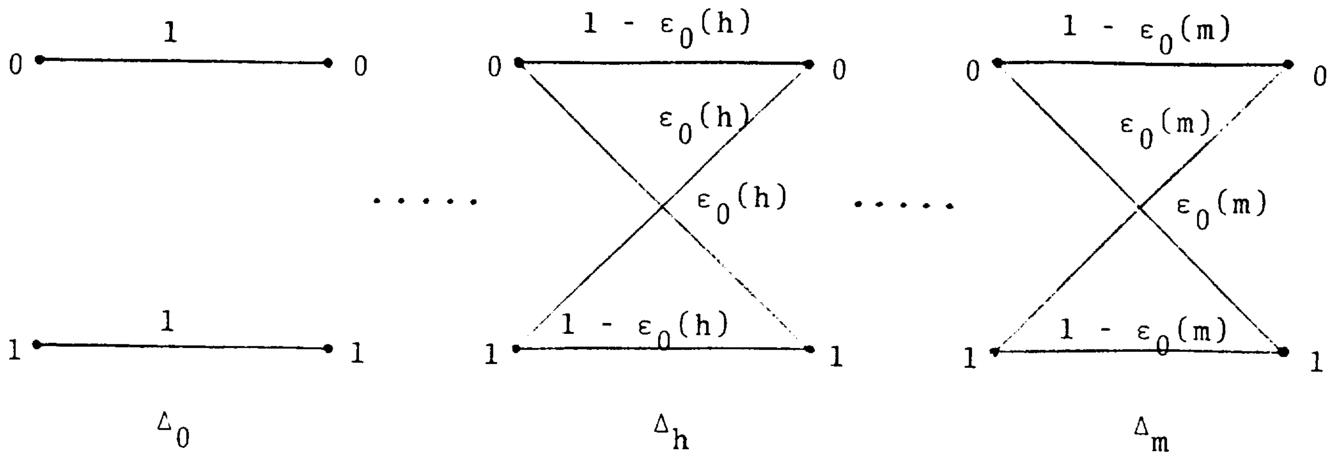

Figure 1. The outer channel.

is the length of the outer code) is transmitted over one of the m component channels. The random variable S determines which component channel is used to transmit a given n_b-bit block.

3. PROBABILITY OF UNDETECTED ERROR FOR THE OUTER CODE

Let $P_{ud}^{(b)}(\varepsilon)$ be the probability of undetected error for the outer code C_b. Let $\{A_i^{(b)}, d_b \leq i \leq n_b\}$ be the weight distribution of the outer code C_b, where d_b is the minimum distance of C_b.

Case 1. An (n_b, k_b) binary block outer code is used.

If the n_b-bit block is transmitted over the h^{th} component channel Δh of the outer channel, it follows from (13) that

$$P_{ud}^{(b)}(\varepsilon_0(h)) = \sum_{i=d_b}^{n_b} A_i^{(b)} \varepsilon_0(h)^i (1 - \varepsilon_0(h))^{n_b - i}. \qquad (14)$$

Let $P_{ud}^{(1)}(\varepsilon_i)$ be the average probability of undetected error of the concatenated code. From (12) and (14) we obtain

$$P_{ud}^{(1)}(\varepsilon_i) = \sum_{h=0}^{m} Pr\{S=h\} P_{ud}^{(b)}(\varepsilon_0(h))$$

$$= \sum_{h=0}^{m} \{ \binom{m}{h} [P_{ud}^{(f)}(\varepsilon_i)]^h [1 - P_{ud}^{(f)}(\varepsilon_i)]^{m-h} \sum_{i=d_b}^{n_b} A_i^{(b)} \varepsilon_0(h)^i (1-\varepsilon_0(h))^{n_b - i} \} , \qquad (15)$$

where $P_{ud}^{(f)}(\varepsilon_i)$ is given in (4).

<u>Case 2</u>. An (n_b, k_b) MDS outer code is used.

The (n_b, k_b) MDS outer code is specified by (2). In this case, $\varepsilon_0(h)$ in (13) is replaced by

$$\varepsilon_0(h) = [1 - (1-\varepsilon_{a/E})^b] \frac{h}{m} , \quad h = 0, 1, \cdots, m, \qquad (16)$$

where $\varepsilon_{a/E}$ remains the same as given in (10). Then

$$P_{ud}^{(b)}(\varepsilon_0(h)) = \sum_{i=d_b}^{n_b} A_i^{(b)} (\frac{\varepsilon_0(h)}{q - 1})^i (1-\varepsilon_0(h))^{n_b - i}, \qquad (17)$$

where $\{A_i^{(b)}, d_b \leqq i \leqq n_b\}$. The weight distribution of the MDS code is given by [4]

$$A_i^{(b)} = \binom{n_b}{i} \{ \sum_{j=0}^{i-d_b} (-1)^j \binom{i}{j} q^{i-j+1-d_b} + \sum_{j=i-d_b+1}^{i} (-1)^j \binom{i}{j} \} . \qquad (18)$$

Let $P_{ud}^{(2)}(\varepsilon_i)$ be the average probability of undetected error of the concatenated code. From (12) and (17) we have

$$P_{ud}^{(2)}(\varepsilon_i) = \sum_{h=0}^{m} Pr\{S=h\} P_{ud}^{(b)}(\varepsilon_0(h))$$

$$= \sum_{h=0}^{m} \{ \binom{m}{h} [P_{ud}^{(f)}(\varepsilon_i)]^h [1 - P_{ud}^{(f)}(\varepsilon_i)]^{m-h}$$

$$\sum_{i=d_b}^{n_b} A_i^{(b)} \left(\frac{\varepsilon_0(h)}{q-1} \right)^i (1-\varepsilon_0(h))^{n_b - i} \}. \qquad (19)$$

4. Examples

Example 1.

Consider a concatenated coding scheme. The frame code C_f is a distance-4 Hamming code with generator polynomial,

$$g(x) = (x+1)(x^6 + x + 1) = x^7 + x^6 + x^2 + 1, \qquad (20)$$

where $x^6 + x + 1$ is a primitive polynomial of degree 6. The maximum length of this code is 63. This code is used for single error correction and is capable of detecting all error patterns of weight two and some higher odd weight error patterns. The outer code is a distance-4 shortened Hamming code with generator polynomial

$$g(x) = x^{16} + x^{12} + x^5 + 1. \qquad (21)$$

The natural length of this code is $2^{15}-1 = 32,767$, but it is shortened to $n_b = 2048$. This code is used for error detection only.

Evaluation of $P_{ud}^{(1)}(\varepsilon_i)$, based on (4), (13), and (15) for various values of ε_i, is given in Table 1, where we have used the method in [5] to obtain $P_{ud}^{(b)}(\varepsilon_0(h))$.

Example 2.

This time the frame code we choose is the same as in example 1, but the outer code is a (256, 254) $d_b = 3$ MDS code over $GF(2^8)$. Evaluation of $P_{ud}^{(2)}(\varepsilon_i)$, based on (4), (16), and (19) for various ε_i, is given in Table 2.

Table 1. $P_{ud}^{(1)}(\varepsilon_i)$, with number of frames m = 36

ε_i	$P_{ud}^{(1)}(\varepsilon_i)$
10^{-4}	1.677×10^{-11}
10^{-5}	1.686×10^{-14}
10^{-6}	1.687×10^{-17}
10^{-7}	1.687×10^{-20}

Table 2. $P_{ud}^{(2)}(\varepsilon_i)$, with number of frames m = 36

ε_i	$P_{ud}^{(2)}(\varepsilon_i)$
10^{-4}	1.271×10^{-11}
10^{-5}	1.278×10^{-14}
10^{-6}	1.278×10^{-17}
10^{-7}	1.279×10^{-20}

REFERENCES

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

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

[3]. R.J. McEliece and W.E. Stark, "Channels with Block Interference", **IEEE Trans. on Inform. Theory**, IT-30, pp. 44-53, Jan. 1984.

[4]. T. Kasami, S. Lin, and W.W. Peterson, "Some Results on Weight Distributions of BCH Codes", **IEEE Trans. on Inform. Theory**, IT-12, p. 274, 1966.

[5]. T. Fujiwara, T. Kasami, A. Kitai, and S. Lin, "On the Undetected Error Probability for Shortened Hamming Codes", Technical Report, NASA Grant NAG 5-234, August 1983.