A CASCADED CODING SCHEME FOR ERROR CONTROL AND ITS PERFORMANCE ANALYSIS

Technical Report III

to

NASA

Goddard Space Flight Center

Greenbelt, Maryland

Grant Number NAG 5-778

Shu Lin

Principle Investigator

Department of Electrical Engineering

Texas A&M University

College Station, Texas 77843

November 28,1986

A CASCADED CODING SCHEME FOR ERROR CONTROL AND IT'S PERFORMANCE ANALYSIS *

Shu Lin
Department of E.E.
Texas A & M University
College Station, Texas 77843

Tadao Kasami
Faculty of Engineering Science
Osaka University
Toyonaka, Osaka, Japan 560

ABSTRACT

In this paper, we investigate a coding scheme for error control in data communication systems. The scheme is obtained by cascading two error-correcting codes, called the inner and outer codes. The error performance of the scheme is analyzed for a binary symmetric channel with bit-error rate $\epsilon < 1/2$. We show that, if the inner and outer codes are chosen properly, extremely high reliability can be attained even for a high channel bit-error rate. Various specific example schemes with inner codes ranging from high rates to very low rates and Reed-Solomon codes as outer codes are considered, and their error probabilities are evaluated. They all provide extremely high reliability even for very high bit-error rates, say 10^{-1} to 10^{-2}. Several example schemes are being considered by NASA for satellite and spacecraft down-link error control.

* This research is supported by NASA Grants No. NAG 5-407 and No. NAG 5-778, and by the Ministry of Education, Japan, Grant No (C) 61550243

1. Introduction

In this paper we present and analyze a coding scheme for error control for a binary symmetric channel with bit-error rate $\varepsilon < 1/2$. The scheme is achieved by cascading two linear block codes, called the inner and outer codes. The inner code, denoted C_1, is a binary (n_1,k_1) code with minimum distance d_1. It is designed to correct t_1 or fewer errors and simultaneously detect λ_1 ($\lambda_1 \geq t_1$) or fewer errors where $t_1+\lambda_1+1 \leq d_1$ [1-5]. The outer code, denoted C_2, is an (n_2,k_2) code with symbols from the Galois Field $GF(2^\ell)$ and minimum distance d_2. If each code symbol of the outer code is represented by a binary ℓ-tuple based on a certain basis of $GF(2^\ell)$, then the outer code becomes an $(n_2\ell,k_2\ell)$ linear binary code. For the proposed coding scheme, we assume that the following conditions hold:

$$k_1 = m_1\ell \ , \tag{1}$$

and

$$n_2 = m_1m_2 \ , \tag{2}$$

where m_1 and m_2 are two positive integers.

The encoding is performed in two stages as shown in Figures 1 and 2. First a message of $k_2\ell$ binary information digits is divided into k_2 bytes of ℓ information bits each. Each ℓ-bit byte (or binary ℓ-tuple) is regarded as a symbol in $GF(2^\ell)$. These k_2 bytes are encoded according to the outer code C_2 to form an n_2-byte ($n_2\ell$ bits) codeword in C_2. At the second stage of encoding, the n_2-byte codeword at the output of the outer code encoder is divided into m_2 segments of m_1 bytes (or $m_1\ell$ bits) each. Each m_1-byte segment is then encoded according to the inner code C_1 to form an n_1-bit codeword. This n_1-bit codeword in C_1 is called a frame. Thus, corresponding to a message of $k_2\ell$ bits at the input of the outer code encoder, the output of the inner code encoder is a sequence of m_2 frames of n_1 bits each. This sequence

of m_2 frames is called a block. The entire encoding operation results in a binary $(m_2n_1, k_2\ell)$ linear code C which is called a cascaded code. If $m_1=1$ (i.e., each segment consists of a single ℓ-bit byte), the cascaded code C becomes a concatenated code [6]. A concatenated code with varying binary linear block inner code can be regarded as a cascaded code with $n_2=m_1$ and $m_2=1$. Therefore there exist cascaded codes which asymptotically meet the Varshamov-Gilbert bound for all rates [7].

The decoding for the proposed scheme also consists of two stages as shown in Figures 1 and 3. The first stage is the inner code decoding. Depending on the number of errors in a received frame, the inner code decoder performs one of the three following operations: error-correction, erasure and leave-it-alone (LIA) operations. When a frame in a block is received, its syndrome is computed based on the inner code C_1. If the syndrome corresponds to an error pattern $\bar{e}$ of t_1 or fewer errors, error correction is performed by adding $\bar{e}$ to the received frame. The n_1-k_1 parity bits are removed from the decoded frame, and the decoded m_1-byte segment is stored in a receiver buffer for the second stage of decoding. A successfully decoded segment is called a decoded segment with no mark. Note that a decoded segment is error-free, if the number of transmission errors in a received frame is t_1 or less. If the number of transmission errors in a received frame is more than λ_1, the errors may result in a syndrome which corresponds to a correctable error pattern with t_1 or fewer errors. In this case, the decoding will be successful, but the decoded frame (or segment) contains undetected errors. If an uncorrectable error pattern is detected in a received frame, the inner code decoder will perform one of the following two operations (See section 2.2):

1. Erasure Operation -- The erroneous segment is erased. We will call

such a segment an erased segment. Note that this operation creates m_1 symbol erasures.

2. Leave-it-alone (LIA) Operation -- The erroneous segment is stored in the receiver buffer with a mark. Note that a marked segment may contain error-free symbols.

Whether the erasure operation or the LIA-operation is performed depends on the degree of error contamination in the erroneous segment. Since the outer code C_2 has a fixed minimum distance, it is desired to devise a strategy to choose between these two operations so that the minimum distance of the outer code is used most effectively in correcting symbol erasures and errors. A simple strategy may by devised based on the concepts of correcting symbol erasures and errors [2-5]. For a code to be able to correct e or fewer symbol erasures and t or fewer symbol errors, its minimum distance d is at least e+2t+1. This implies that, to correct one symbol erasure, one unit of the minimum distance of the code is needed. However, to correct a symbol error, two units of the minimum distance of the code are needed. In the proposed scheme, when an erasure operation is performed, m_1 symbol erasures are created. To correct these m_1 symbol erasures, m_1 units of the minimum distance of the outer code are needed. When a LIA-operation is performed, the marked segment contains one to m_1 symbol errors. As a result, 2 to $2m_1$ units of the minimum distance of the outer code are required to correct these symbol errors. It is clear that, to minimize the consumption of minimum distance of the outer code, we would perform the LIA-operation when the number of symbol errors in an erroneous segment is less than $\lfloor m_1/2 \rfloor+1$, and perform the erasure operation when the number of symbol errors in an erroneous segment is greater than $\lfloor m_1/2 \rfloor$. Hence we may use the following

strategy to choose between the erasure operation and the LIA-operation: If the probability that an erroneous segment contains more than $\lfloor m_1/2 \rfloor$ symbol errors is relatively small compared to the probability that the erroneous segment contains $\lfloor m_1/2 \rfloor$ or less symbol errors, the LIA-operation is performed. Otherwise, the erasure operation is performed. The joint probability distribution that a received frame is decoded successfully (or detected to contain an uncorrectable error pattern) and the corresponding segment contains w symbol errors is derived in Section 2.1 (or 2.2).

The inner code decoding described above consists of three operations: the error correction, the erasure and the LIA operations. An inner code decoding which performs only the error-correction and erasure operations is called an erasure-only inner decoding. On the other hand, an inner code decoding which performs only the error-correction and LIA operations is called a LIA-only inner decoding. In this paper we mainly consider the erasure-only inner decoding and the LIA-only inner decoding. Which of these two decodings gives better performance will be discussed in Section 2.2. A combined erasure-and-LIA inner decoding is discussed in Section 5.

As soon as m_2 frames in a received block have been processed, the second stage of decoding begins and the outer code decoder starts to decode the m_2 segments which are stored in the buffer. Symbol errors are contained in the segments with or without marks. Each erased segment results in m_1 symbol erasures. The outer code C_2 and its decoder are designed to correct the combinations of symbol erasures and symbol errors. Maximum-distance-separable codes with symbol from $GF(2^\ell)$ are most effective in correcting symbol erasures and errors.

Now we describe outer code decoding process. Let i and h be the numbers of erased segments and marked segments respectively. The outer code decoder

declares an erasure (or raises a flag) for the entire block of m_2 segments if either of the following two events occurs:

(i) The number i is greater than a certain pre-designed threshold T_{es} with $T_{es} \leq (d_2-1)/m_1$.

(ii) The number h is greater than a certain pre-designed threshold $T_{e\ell}(i)$ with $T_{e\ell}(i) \leq (d_2-1-m_1 i)/2$ for a given i.

If none of the above two events occurs, the outer code decoder starts the error-correction operation on the m_2 decoded segments. The $m_1 i$ symbol erasures and the symbol errors in the marked or unmarked segments are corrected based on the outer code C_2. Let $t_2(i)$ be the error-correction threshold for a given i where

$$T_{e\ell}(i) \leq t_2(i) \leq (d_2-1-m_1 i)/2 \ . \qquad (3)$$

If the syndrome of m_2 decoded segments in the buffer corresponds to an error pattern of $m_1 i$ erasures and $t_2(i)$ or fewer symbol errors, error-correction is performed. The values of the erased symbols, and the values and the locations of symbol errors are determined based on a certain algorithm. If more than $t_2(i)$ symbol errors are detected, then the outer code decoder again declares an erasure (or raises a flag) for the entire block of m_2 decoded segments.

When a received block is detected in errors and can not be successfully decoded, the block is erased from the receiver buffer and a retransmission for that block is requested. However, if retransmission is either not possible or not practical and no block is allowed to be discarded, then the erroneous block with all the parity symbols removed is accepted by the user with alarm. An important feature of the proposed scheme is that the decoding information of the inner code decoder is passed to the outer code decoder.

This makes the outer code decoding more efficient.

In the rest of this paper, the error performance of the proposed cascaded coding scheme is analyzed. Interleaving the outer code is considered. We show that, if the inner and outer codes are chosen properly, extremely high reliability can be attained even for high bit-error rate, say $\varepsilon=10^{-2}$. Various specific example schemes with inner codes ranging from high rates to very low rates and Reed-Solomon codes as outer codes are considered, and their error probabilities are evaluated. They all provide extremely high reliability. Several of these specific schemes are being considered by NASA-GSFC for satellite and spacecraft down-link error control [8].

2. Probabilities of Correct Decoding, Incorrect Decoding and Decoding Failure for a Frame

In this section, we analyze the inner code decoding. We assume that the channel is a binary symmetric channel with bit-error rate $\varepsilon \leq 1/2$. Let $P_c^{(1)}$ be the probability that a decoded segment is error-free. A decoded segment is error-free if and only if the corresponding received frame contains t_1 or fewer errors. Thus

$$P_c^{(1)} = \sum_{i=0}^{t_1} \binom{n_1}{i} \varepsilon^i (1-\varepsilon)^{n_1-i}. \tag{4}$$

Let $P_{ic}^{(1)}$ be the probability of an incorrect decoding for a frame. This is actually the probability of an error pattern of λ_1+1 or more errors whose syndrome corresponds to a correctable error pattern of t_1 or fewer errors. Let $P_{es}^{(1)}$ be the probability of a frame erasure, and let $P_{e\ell}^{(1)}$ be the probability that a LIA operation is performed on a frame. Let $P_{er}^{(1)}$ be the

probability that a decoded segment with or without a mark contains errors. Then

$$P_c^{(1)} + P_{ic}^{(1)} + P_{es}^{(1)} + P_{e\ell}^{(1)} = 1, \tag{5}$$

and

$$P_{er}^{(1)} = P_{ic}^{(1)} + P_{e\ell}^{(1)}. \tag{6}$$

Note that $P_c^{(1)} + P_{ic}^{(1)}$ is the probability that a received frame is <u>decoded successfully</u> (correctly or incorrectly), and $P_{es}^{(1)} + P_{e\ell}^{(1)}$ represents the probability of a <u>decoding failure</u>.

Let $A_i^{(1)}$ and $B_i^{(1)}$ be the numbers of codewords of weight i in the inner code C_1 and its dual code $C_1^{\perp}$ respectively. Let $W_{j,s}^{(i)}(n)$ denote the number of binary n-tuples with weight j which are at a Hamming distance s from a given binary n-tuple with weight i. The generating function for $W_{j,s}^{(i)}(n)$ [9] is

$$\sum_{j=0}^{n} \sum_{s=0}^{n} W_{j,s}^{(i)}(n) X^j Y^s = (1+XY)^{n-i}(X+Y)^i. \tag{7}$$

It was proved by MacWilliams [9] that

$$P_c^{(1)} + P_{ic}^{(1)} = \sum_{i=0}^{n_1} A_i^{(1)} \sum_{j=0}^{n_1} \sum_{s=0}^{t_1} W_{j,s}^{(i)}(n_1) \varepsilon^j (1-\varepsilon)^{n_1-j} , \tag{8}$$

$$= 2^{-r_1} \sum_{i=0}^{n_1} B_i^{(1)} (1-2\varepsilon)^i P_{t_1}(i-1, n_1-1), \tag{9}$$

where $r_1 = n_1 - k_1$ is the number of parity-check bits of the inner code, and $P_s(\cdot,\cdot)$ is a Krawtchouk polynomial [4,p.129] whose generating function is

$$\sum_{s=0}^{n} P_s(i,n) Y^s = (1+Y)^{n-i}(1-Y)^i. \tag{10}$$

Equations (8) and (9) are useful for computing $P_c^{(1)} + P_{ic}^{(1)}$ if a formula for $A_i^{(1)}$ or $B_i^{(1)}$ is known, or $\min(k_1,r_1)$ is small enough (say less than 30) to be feasible to compute $A_i^{(1)}$ or $B_i^{(1)}$ by generating all the codewords in C_1 or $C_1^{\perp}$.

Hereafter, we mainly consider the LIA-only inner decoding and the erasure-only inner decoding (A combined inner decoding is discussed in section 5). For the LIA-only inner decoding, the LIA-operation is performed whenever an uncorrectable error pattern in the received frame is detected. In this case, the frame erasure probability $P_{es}^{(1)}$ is "zero". For the erasure-only inner decoding, it is obvious that $P_{e\ell}^{(1)} = 0$.

If $P_{e\ell}^{(1)}$ (or $P_{es}^{(1)}$) is known, then $P_{es}^{(1)}$ (or $P_{e\ell}^{(1)}$) and $P_{er}^{(1)}$ can be computed from (4) to (6) and (8) (or (9)).

2.1. Detail Error Probabilities for a Decoded Segment with no Mark

A successfully decoded segment may contain errors. For $0 \leq w \leq m_1$, let $P_{e,w}^{(1)}$ be the joint probability that a segment is successfully decoded and the number of symbol (or byte) errors in the decoded segment is w. It is clear that

$$P_c^{(1)} = P_{e,0}^{(1)}$$

and

$$P_{ic}^{(1)} = \sum_{w=1}^{m_1} P_{e,w}^{(1)} \quad . \tag{11}$$

To obtain the probability of a correct block decoding, we need to know $P_{e,w}^{(1)}$ for $0 \leq w \leq m_1$. In this section we will derive a formula for $P_{e,w}^{(1)}$.

For a binary n_1-tuple $\bar{v}$, we divide the first $k_1=m_1\ell$ bits into m_1 ℓ-bit bytes. For $1 \leq h \leq m_1$, let i_h be the weight of the h-th ℓ-bit byte of $\bar{v}$. Let i_{m_1+1} be the weight of the last $r_1=n_1-k_1$ bits. Then the (m_1+1)-tuple, $(i_1,$

$i_2, \cdots, i_{m_1+1})$, is called the weight structure of $\bar{v}$.

Suppose that a frame $\bar{u}$ is transmitted and an error pattern $\bar{e}$ with weight structure $(j_1, j_2, \cdots, j_{m_1+1})$ occurs. The probability of occurrence of $\bar{e}$ is

$$P(\bar{e}) = (1-\varepsilon)^{n_1} \prod_{h=1}^{m_1+1} (\varepsilon/(1-\varepsilon))^{j_h} . \tag{12}$$

Suppose that there is a codeword $\bar{v}$ in C_1 which is at a distance t_1 or less from $\bar{e}$. Since the minimum distance of C_1 is assumed to be greater than $2t_1$, such a codeword $\bar{v}$ in C_1 is uniquely determined. Then the inner decoder assumes that the frame $\bar{u}+\bar{v}$ was sent, and the error pattern $\bar{e}+\bar{v}$ occured. The decoded segment is the first k_1-bit of $\bar{u}+\bar{v}$. If $\bar{v}$ is a nonzero codeword, the decoding is incorrect, and the first k_1-bit of $\bar{v}$ represent the errors introduced by the inner code decoder. If there is no such codeword $\bar{v}$ in C_1, then the inner code decoder performs either the LIA-operation or the erasure-operation. Conversely, for a codeword $\bar{v}$ in C_1 whose weight structure is $(i_1, i_2, \cdots, i_{m_1+1})$, there are

$$\left[\prod_{h=1}^{m_1} W_{j_h, s_h}^{(i_h)}(\ell)\right] \cdot W_{j_{m_1+1}, s_{m_1+1}}^{(i_{m_1+1})}(r_1) \tag{13}$$

error patterns $\bar{e}$'s with weight structure $(j_1, j_2, \cdots, j_{m_1+1})$ such that the weight structure of $\bar{v}+\bar{e}$ is $(s_1, s_2, \cdots, s_{m_1+1})$. Let $A_{i_1, i_2, \cdots, i_{m_1+1}}^{(1)}$ be the number of codewords in C_1 with weight structure $(i_1, i_2, \cdots, i_{m_1+1})$. For $0 \leq w \leq m_1$, let

$$I_w = \{(i_1, i_2, \cdots, i_{m_1+1}) : 0 \leq i_h \leq \ell \text{ for } 1 \leq h \leq m_1,\ 0 \leq i_{m_1+1} \leq r_1,$$
$$\text{and exactly } w \text{ components of } (i_1, i_2, \cdots, i_{m_1}) \text{ are nonzero.}\} . \tag{14}$$

Then, $P_{e,w}^{(1)}$ is given below:

$$P_{e,w}^{(1)} = \sum_{(i_1,i_2,\cdots,i_{m_1+1})\varepsilon I_w} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \sum_{j_1=0}^{\ell} \cdots \sum_{j_{m_1}=0}^{\ell} \sum_{j_{m_1+1}=0}^{r_1}$$

$$\sum_{(s_1,s_2,\cdots,s_{m_1+1})\varepsilon S_{t_1}} \left[\prod_{h=1}^{m_1} W_{j_h,s_h}^{(i_h)}(\ell)\right] \cdot W_{j_{m_1+1},s_{m_1+1}}^{(i_{m_1+1})}(r_1)$$

$$\cdot (1-\varepsilon)^{n_1} \left[\prod_{h=1}^{m_1} (\varepsilon/(1-\varepsilon))^{j_h}\right], \tag{15}$$

where

$$S_{t_1} = \{ (s_1, s_2, \cdots, s_{m_1+1}) : 0 \le s_h \le \ell, \text{ for } 1 \le h \le m_1, \ 0 \le s_{m_1+1} \le r_1$$

$$\text{and } \sum_{h=1}^{m_1+1} s_h \le t_1 \}. \tag{16}$$

The formula given by (15) is useful if either (1) the dimension of C_1, k_1, is small enough (say $k_1 < 30$) to be feasible to compute the detail weight distribution, $\{A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}\}$, by generating all the codewords in C_1, or (2) the dimension of $C_1^{\perp}$, r_1, is small enough to be feasible to compute the detail weight distribution of $C_1^{\perp}$ and the number of element in I_w is small enough to be feasible to enumerate all the elements in I_w and compute $\{A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}\}$ by using the generalized MacWilliams' Identity [4].

Next we will express the probability $P_{e,w}^{(1)}$ in terms of the detail weight distribution of the dual code $C_1^{\perp}$ of C_1. Let H be a subset of $\{1,2,\cdots,m_1\}$. Let $P_e^{(1)}(H)$ be the probability that for $h\varepsilon H$, the h-th ℓ-bit byte of a decoded segment is error-free. Let $\bar{H}$ be the complement of H in $\{1,2,\cdots,m_1+1\}$. Define the following set:

$$I(H) = \{(i_1, i_2, \cdots, i_{m_1+1}): i_h = 0 \text{ for } h\varepsilon H, \ 0 \le i_h \le \ell \text{ for } h\varepsilon\bar{H}-\{m_1+1\},$$

$$\text{and } 0 \le i_{m_1+1} \le r_1\}. \tag{17}$$

Then, we have that

$$P_e^{(1)}(H) = \sum_{(i_1,i_2,\cdots,i_{m_1+1})\in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \sum_{j_1=0}^{\ell} \cdots \sum_{j_{m_1}=0}^{\ell} \sum_{j_{m_1+1}=0}^{r_1}$$

$$\cdot \sum_{(s_1,s_2,\cdots,s_{m_1+1})\in S_{t_1}} \left[\prod_{h=1}^{m_1} W_{j_h,s_h}^{(i_h)}(\ell)\right] \cdot W_{j_{m_1+1},s_{m_1+1}}^{(i_{m_1+1})}(r_1)$$

$$\cdot (1-\varepsilon)^{n_1} \left[\prod_{h=1}^{m_1} (\varepsilon/(1-\varepsilon))^{j_h}\right], \tag{18}$$

Define

$$Q_s(i,n,m,\gamma) = \sum_{j=0}^{s} \gamma^j \binom{m}{j} P_{s-j}(i,n), \tag{19}$$

$$\bar{Q}_t(i,n,m,\gamma) = \sum_{s=0}^{t} Q_s(i,n,m,\gamma). \tag{20}$$

It follows from (10) and (19) that

$$(1+\gamma Y)^m (1+Y)^{n-i} (1-Y)^i = \sum_{s=0}^{n+m} Q_s(i,n,m,\gamma) Y^s. \tag{21}$$

Let $B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$ be the number of codewords in $C_1^{\perp}$ with weight structure $(i_1,i_2,\cdots,i_{m_1+1})$. Then we have Lemma 1.

Lemma 1:

$$P_e^{(1)}(H) = 2^{-r_1} \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \left[\prod_{h\in\bar{H}} (1-2\varepsilon)^{i_h}\right]$$

$$\cdot (1-\varepsilon)^{\ell|H|} \cdot \bar{Q}_{t_1}\left(\sum_{h\in\bar{H}} i_h,\ n_1-\ell|H|,\ \ell|H|,\ \varepsilon/(1-\varepsilon)\right), \tag{22}$$

where $|H|$ denotes the number of elements in H.

Proof: See Appendix A. ΔΔ

For $0 \leq s \leq m_1$, let $\bar{U}_s$ be the sum of $P_e^{(1)}(H)$ where H is taken over all the subsets of $\{1,2,\cdots,m_1\}$ with s elements. Define

$$U_s(i_1,i_2,\cdots,i_{m_1+1};\varepsilon) = \sum_{\substack{H\subseteq\{1,2,\cdots,m_1\} \\ |H| = s}} \left[\prod_{h\in\bar{H}} (1-2\varepsilon)^{i_h}\right] (1-\varepsilon)^{\ell s}$$

$$\cdot \bar{Q}_{t_1}\left(\sum_{h\in\bar{H}} i_h,\ n_1-\ell s,\ \ell s,\ \varepsilon/(1-\varepsilon)\right) . \quad (23)$$

Then it follows from (22) and (23) that

$$\bar{U}_s = 2^{-r_1} \sum_{i_1=0}^{\ell} \sum_{i_2=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1}$$

$$B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}\ U_s(i_1,i_2,\cdots,i_{m_1+1};\varepsilon) . \quad (24)$$

In the sum $\bar{U}_s$, error patterns with m_1-s-1 or less symbol (or byte) errors in a decoded segment are counted more than once. In fact,

$$\bar{U}_s = P^{(1)}_{e,m_1-s} + \binom{s+1}{1} P^{(1)}_{e,m_1-s-1} + \binom{s+2}{2} P^{(1)}_{e,m_1-s-2} + \cdots + \binom{m_1}{m_1-s} P^{(1)}_{e,0} . \quad (25)$$

Using the principle of inclusion and exclusion [10], we have that

$$P^{(1)}_{e,j} = \sum_{h=0}^{j} (-1)^h \binom{m_1-j+h}{h} \bar{U}_{m_1-j+h} . \quad (26)$$

For $0 \leq j \leq m_1$, define

$$T_j(i_1,i_2,\cdots,i_{m_1+1};\varepsilon) = \sum_{h=0}^{j} (-1)^h \binom{m_1-j+h}{h} U_{m_1-j+h}(i_1,i_2,\cdots,i_{m_1+1};\varepsilon). \quad (27)$$

Then it follows from (24) to (27) that we have

Theorem 1:

$$P_{e,j}^{(1)} = 2^{-r_1} \sum_{i_1=0}^{\ell} \sum_{i_2=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B_{i_1,i_2,\cdots,i_{m_1+1}}^{(1)} T_j(i_1,i_2,\cdots,i_{m_1+1};\varepsilon) . \tag{28}$$

ΔΔ

It is feasible to obtain detail weight distribution $\{B_{i_1,i_2,\cdots,i_{m_1+1}}^{(1)}\}$ by generating all the codewords in $C_1^{\perp}$ for relatively small r_1, say less than 30. Note that the number of terms to be added in the right-hand side of (23) is $\binom{m_1}{s}$, and therefore the number of terms to be added or subtracted in the right-hand side of (27) is at most 2^{m_1}. For small m_1, $T_j(i_1,i_2,\cdots,i_{m_1+1};\varepsilon)$ can be easily computed and added for each codeword generated. If the dual code of C_1 contains the all-one vector, then $P_{e,j}^{(1)}$ can be computed by generating every codeword in the even-weight subcode and using

$$T_j(i_1,i_2,\cdots,i_{m_1+1};\varepsilon) + T_j(\ell-i_1,\ell-i_2,\cdots,r_1-i_{m_1+1};\varepsilon)$$

instead of $T_j(i_1,i_2,\cdots,i_{m_1+1};\varepsilon)$. From (11) and (28), $P_{ic}^{(1)}$ can be computed.

2.2. Detailed Error Probability for a Marked Segment

In this section we will evaluate the probability of symbol errors in a marked segment. Let $P_{e\ell,w}^{(1)}$ be the joint probability that a segment is marked and the number of erroneous symbols in the marked segment is w. Then

$$P_{e\ell}^{(1)} = \sum_{w=1}^{m_1} P_{e\ell,w}^{(1)} . \tag{29}$$

In the following, we consider the LIA-only inner decoding. Define

$$J_w = \{(j_1,j_2,\cdots,j_{m_1+1}) : 0 \le j_h \le \ell \text{ for } 1 \le h \le m_1,\ 0 \le j_{m_1+1} \le r_1,$$
$$\text{and there are exactly } w \text{ nonzero components in } (j_1,j_2,\cdots,j_{m_1})\}. \tag{30}$$

Then it follows from the definition of $P_{e\ell,w}^{(1)}$ that

$$P_{e\ell,w}^{(1)} = \binom{m_1}{w}[1-(1-\varepsilon)^{\ell}]^w(1-\varepsilon)^{k_1-\ell w} - \sum_{i_1=0}^{\ell}\cdots\sum_{i_{m_1}=0}^{\ell}\sum_{i_{m_1+1}=0}^{r_1}$$
$$A_{i_1,i_2,\cdots,i_{m_1+1}}^{(1)} \sum_{J_w}\sum_{S_{t_1}}\left[\prod_{h=1}^{m_1} W_{j_h,s_h}^{(i_h)}(\ell)\varepsilon^{j_h}(1-\varepsilon)^{\ell-j_h}\right]$$
$$\cdot W_{j_{m_1+1},s_{m_1+1}}^{(i_{m_1+1})}(r_1)\varepsilon^{j_{m_1+1}}(1-\varepsilon)^{r_1-j_{m_1+1}}, \tag{31}$$

where S_{t_1} is defined by (16). The first term of (31) represents the probability that there are exactly w erroneous symbols (or bytes) in the first m_1 bytes of a received frame, and the second term is the probability that the syndrome of these symbol errors corresponds to an error pattern of t_1 or fewer errors. Define

$$R_w(i_1,i_2,\cdots,i_{m_1};\varepsilon) = \sum_{\substack{H\subseteq\{1,2,\cdots,m_1\}\\ |H| = w}}\prod_{h\in H}\{(1-2\varepsilon)^{i_h} - (1-\varepsilon)^{\ell}\}, \tag{32}$$

where the summation is taken over all the subsets of $\{1,2,\cdots,m_1\}$ with exactly w elements. Then $P_{e\ell,w}^{(1)}$ can be expressed in terms of the detail weight distribution of the dual code of C_1.

Theorem 2:

$$P_{e\ell,w}^{(1)} = (1-\varepsilon)^{k_1-\ell w} \{ \binom{m_1}{w} [1-(1-\varepsilon)^{\ell}]^w$$

$$- 2^{-r_1} \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B_{i_1,i_2,\cdots,i_{m_1+1}}^{(1)} (1-2\varepsilon)^{i_{m_1+1}}$$

$$\cdot P_{t_1}\left(\sum_{h=0}^{m_1+1} i_h - 1,\ n_1 - 1\right) R_w(i_1,i_2,\cdots,i_{m_1};\varepsilon) \} \ . \qquad (33)$$

Proof: See Appendix B. ΔΔ

An important question is which provides better performance, "the LIA-only inner decoding," or "the erasure-only inner decoding ?" LIA-only inner decoding may be reasonable only if

$$\sum_{w=\lfloor m_1/2 \rfloor+1}^{m_1} P_{e\ell,w}^{(1)} < P_{es}^{(1)} \ .$$

If

$$\sum_{w=\lfloor m_1/2 \rfloor+1}^{m_1} P_{e\ell,w}^{(1)} << 1 - P_c^{(1)} - P_{ic}^{(1)} \ ,$$

where $P_{e\ell,w}^{(1)}$ is computed under the assumption that the inner code decoding is a LIA-only inner decoding, then a LIA-only inner decoding provides better performance than the erasure-only inner decoding.

3. The Probability of a Correct Block Decoding

In this section, we will evaluate the probability that a block of m_2 segments will be decoded correctly by the outer code decoder. Let $P_e(j,m,h)$ denote the probability that there are h segments with marks and j symbol

errors in a set of consisting of m decoded segments with or without marks. It follows from the definition of $P_e(j,m,h)$ that

$$P_e(j,1,0) = P_{e,j}^{(1)} , \qquad \text{for } 0 \le j \le m_1, \tag{34}$$

$$P_e(j,1,1) = P_{e\ell,j}^{(1)} , \qquad \text{for } 0 \le j \le m_1, \tag{35}$$

$$P_e(j,1,0) = P_e(j,1,1) = 0 , \qquad \text{for } j > m_1, \tag{36}$$

and

$$P_e(j,m,h) = \sum_{w=0}^{\min(j,m_1)} P_e(j-w,m-1,h)\, P_{e,w}^{(1)} + P_e(j-w,m-1,h-1)\, P_{e\ell,w}^{(1)} . \tag{37}$$

From (34) to (37), $P_e(j,m,h)$ can be computed readily.

The probability that, after the inner code decoding of a block of frames, there exist i erased segments, h marked segments and j symbol errors in the marked and unmarked (or decoded) segments is

$$\binom{m_2}{i} [P_{es}^{(1)}]^i\, P_e(j,m_2-i,h) . \tag{38}$$

Therefore, the probability of correct decoding of a block, denoted P_c, is given by

$$P_c = \sum_{i=0}^{T_{es}} \binom{m_2}{i} [P_{es}^{(1)}]^i \sum_{h=0}^{T_{e\ell}(i)} \sum_{j=0}^{t_2(i)} P_e(j,m_2-i,h) . \tag{39}$$

Let P_{es} and P_{er} denote the probabilities of a block erasure and an incorrect decoding respectively. Then

$$P_c + P_{es} + P_{er} = 1 . \tag{40}$$

It follows from definitions that the following equality and bound hold:

$$P_{es} + P_{er} = \sum_{i=0}^{T_{es}} \binom{m_2}{i} [P_{es}^{(1)}]^i \left\{ \sum_{h=0}^{T_{e\ell}(i)} \sum_{j=t_2(i)+1}^{n_2-m_1 i} P_e(j, m_2-i, h) \right.$$

$$\left. + \sum_{h=T_{e\ell}(i)+1}^{m_2-i} \binom{m_2-i}{h} [P_{e\ell}^{(1)}]^h (P_c^{(1)} + P_{ic}^{(1)})^{m_2-i-h} \right\}$$

$$+ \sum_{i=T_{es}+1}^{m_2} \binom{m_2}{i} [P_{es}^{(1)}]^i (1-P_{es}^{(1)})^{m_2-i} , \qquad (41)$$

$$P_{er} \leq \sum_{i=0}^{T_{es}} \binom{m_2}{i} [P_{es}^{(1)}]^i \sum_{h=0}^{T_{e\ell}(i)} \sum_{j=d_2-m_1 i-t_2(i)}^{n_2-m_1 i} P_e(j, m_2-i, h) . \qquad (42)$$

The right-hand side of Eq.(41) provides an upper bound on the probability of a block erasure (or decoding failure), and the right-hand side of (42) gives an upper bound on the probability of an incorrect block decoding.

To the authors' knowledge, no feasible procedure for computing P_{er} or P_{es} has been derived except for the special case where the outer code is a binary code (ℓ=1) and used only for error detection and $n_1-k_1+n_2-k_2$ is small, say less than 25 [11]. If the outer code is used for both error correction and detection, detailed information on the weight distribution of outer codewords with specified bit patterns is required in general.

4. Interleaving

In this section, we investigate how interleaving affects the error performance of the cascaded scheme. Suppose that the outer code C_2 is interleaved in such a way that each symbol (or ℓ-bit byte) in a segment is from a different outer code codeword as shown in Figure 4. Hence the

interleaving depth (or degree) is m_1. Each symbol-column (an $n_2 \times \ell$ submatrix) in the first m_1 columns of the code array is called a section. Note that a section is simply a codeword in the outer code C_2. The $k_1 k_2$ bits in the first k_2 rows and k_1 columns are used as information bits. The code array consists of n_2 frames and is transmitted row by row. As for the decoding, after n_2 received frames have been decoded by the inner code decoder, the n_2 decoded segments are arranged into an array as shown in Figure 5 which is called a decoded segment-array. Note that an erased segment creates one symbol erasure in each section. A decoded segment with or without mark may contain symbol errors which are distributed among the m_1 sections of a decoded segment-array, at most one symbol error in each section. Therefore, each section in a decoded segment-array may contain symbol erasures and errors. Now each section is decoded based on the outer code C_2. Note that buffers are needed to store code arrays at both transmitter and receiver.

For $1 \leq u \leq m_1$, let $\tilde{p}_e(u)$ be the probability that the u-th symbol of a decoded segment with no mark is erroneous. If the inner code C_1 is quasi-cyclic by every s-bit shift where s divides ℓ, then $\tilde{p}_e(u)$ is independent of u. It follows from the definition that

$$\tilde{p}_e(u) = P_c^{(1)} + P_{ic}^{(1)} - P_e^{(1)}(\{u\}) , \tag{43}$$

where $P_e^{(1)}(\{u\})$ is given by (18) or (22). Hence $\tilde{p}_e(u)$ can be computed from either (8) and (18) or (9) and (22).

Let $\tilde{p}_{e\ell}(u)$ be the probability that the u-th symbol of a marked segment is erroneous. For simplicity, the LIA-only inner decoding is considered. Define

$$J(u) = \{ (j_1, j_2, \cdots, j_{m_1+1}) : 0 \leq j_h \leq \ell \text{ for } 1 \leq h \leq m_1,\ j_u \neq 0 \text{ and } 0 \leq j_{m_1+1} \leq r_1 \} . \tag{44}$$

Modifying the derivation of (31) or (33), we have that

$$\tilde{P}_{e\ell}(u) = 1 - (1-\varepsilon)^{\ell} - \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$\cdot \sum_{J(u)} \sum_{S_{t_1}} \left[\prod_{h=1}^{m_1} W^{(i_h)}_{j_h,s_h}(\ell) \varepsilon^{j_h} (1-\varepsilon)^{\ell-j_h} \right]$$

$$\cdot W^{(i_{m_1+1})}_{j_{m_1+1},s_{m_1+1}}(r_1) \varepsilon^{j_{m_1+1}} (1-\varepsilon)^{r_1-j_{m_1+1}} \qquad (45)$$

and

$$\tilde{P}_{e\ell}(u) = 1 - (1-\varepsilon)^{\ell} - 2^{-r_1} \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$\cdot \prod_{h=0}^{m_1+1} (1-2\varepsilon)^{i_h} \left[1-(1-\varepsilon)^{\ell}(1-2\varepsilon)^{-i_u}\right] P_{t_1}\left(\sum_{h=0}^{m_1+1} i_h - 1,\ n_1 - 1\right) . \qquad (46)$$

[See Appendix C for the derivation of (46)].

Since the outer code is interleaved by a depth of m_1, the u-th symbol of every segment is from the u-th section for $1 \le u \le m_1$. Let $\tilde{P}_c(u)$, $\tilde{P}_{es}(u)$ and $\tilde{P}_{er}(u)$ denote the probabilities of a correct decoding, an erasure and an incorrect decoding for the u-th section respectively. Then formulas or bounds for $\tilde{P}_c(u)$, $\tilde{P}_{es}(u)$ and $\tilde{P}_{er}(u)$ can be derived from those for P_c, P_{es} and P_{er} by the following replacement: $m_1 i \to i$, $m_2 \to n_2$ and

$$\sum_h \sum_j P_e(j, m_2-i, h) \to \sum_h \binom{n_2-i}{h} \sum_j \binom{n_2-i-h}{s} \binom{h}{j-s}$$

$$\cdot [\tilde{p}_e(u)]^s [1-P^{(1)}_{es}-P^{(1)}_{e\ell}-\tilde{p}_e(u)]^{n_2-i-h-s}$$

$$\cdot [\tilde{p}_{e\ell}(u)]^{j-s} [P^{(1)}_{e\ell} - \tilde{p}_{e\ell}(u)]^{h-(j-s)} .$$

The restrictions on thresholds T_{es}, $T_{e\ell}(i)$ and $t_2(i)$ can be relaxed as follows:

$$T_{es} \leq d_2-1 \quad , \quad T_{e\ell}(i) \leq (d_2-1-i)/2 \quad \text{and} \quad t_2(i) \leq (d_2-1-i)/2 \ .$$

Let P_c be the probability of a correct decoding for all interleaved m_1 sections. Let P_{er} and P_{es} be the probability that an incorrect decoding occurs for at least one of the interleaved m_1 sections and that of a block erasure, respectively. Then

$$P_{er} \leq \max_{1 \leq u \leq m_1} m_1 \tilde{P}_{er}(u) \ , \tag{47}$$

and

$$1 - P_c = P_{er} + P_{es} \leq \max_{1 \leq u \leq m_1} m_1 (P_{er}(u) + P_{es}(u)) \ . \tag{48}$$

Let $\overline{P_{er}+P_{es}}$ denote the right-hand side of (48).

Next we present a formula for P_c and another upper bound on P_{er}. For simplicity, we only consider the erasure-only inner decoding in which $t_2(i)$ is independent of i and is denoted t_2.

For a binary m_1-tuple $(a_1, a_2, \cdots, a_{m_1})$, let $P^{(1)}_{e,a_1,\cdots,a_{m_1}}$ denote the probability that a segment is not erased and the u-th symbol of the decoding segment is error-free if and only if $a_u=0$ in the inner code decoding. A computing procedure for $P^{(1)}_{e,a_1,\cdots,a_{m_1}}$ is shown in Appendix D. For a positive integer n and integers j_h with $1 \leq h \leq m_1$ such that $0 \leq j_h \leq n$, let $P_{e,j_1,j_2,\cdots,j_{m_1}}(n)$ be defined by

$$\Big[\sum_{(a_1,a_2,\cdots,a_{m_1}) \varepsilon \{0,1\}^{m_1}} P^{(1)}_{e,a_1,a_2,\cdots,a_{m_1}} x_1^{a_1} x_2^{a_2} \cdots x_{m_1}^{a_{m_1}} \Big]^n =$$

$$\sum_{j_1=0}^{n} \sum_{j_2=0}^{n} \cdots \sum_{j_{m_1}=0}^{n} P_{e,j_1,j_2,\cdots,j_{m_1}}(n)\, x_1^{j_1} x_2^{j_2} \cdots x_{m_1}^{j_{m_1}} . \tag{49}$$

Then P_c (= $1-P_{er}-P_{es}$) is given by

$$P_c = \sum_{i=0}^{T_{es}} \binom{n_2}{i} \sum_{j_1=0}^{t_2} \sum_{j_2=0}^{t_2} \cdots \sum_{j_{m_1}=0}^{t_2} P_{e,j_1,j_2,\cdots,j_{m_1}}^{(n_2-i)} . \tag{50}$$

It is feasible to compute P_c for small m_1, t_2 and relatively small $\min\{k_1, n_1-k_1\}$.

For $1 \leq u \leq m_1$ and α in $GF(2^\ell)$, let $p_e(u,\alpha)$ be the probability that a segment is not erased and the u-th error symbol of the decoded segment is α. A procedure for computing $p_e(u,\alpha)$ is stated in Appendix E. Then we have that

$$\tilde{p}_e(u) = \sum_{\alpha \in GF(2^\ell)-\{0\}} p_e(u,\alpha) . \tag{51}$$

In Appendix F, the following upper bound on P_{er} is derived.

$$P_{er} \leq \sum_{i=0}^{T_{es}} \binom{n_2}{i} \sum_{w=d_2-i}^{n_2-i} \binom{n_2-i}{w} \sum_{h=0}^{\min\{t_2, n_2-i-w\}} \binom{n_2-i-w}{h} \sum_{j=w+h-t_2}^{w} \binom{w}{j} \sum_{u=1}^{m_1} \bar{P}(u,i,w,h,j), \tag{52}$$

where

$$\bar{P}(u,i,w,h,j) = [P_{es}^{(1)}]^i [\tilde{p}_e(u)]^{i+w+h-d_2} [p_e(u,0)]^{n_2-i-w-h} \cdot [1-P_{es}^{(1)}]^{w-j} \sum_{q=0}^{2^\ell-2} [p_e(u,\gamma^q)]^{j+d_2-i-w}, \tag{53}$$

where γ is a primitive element of $GF(2^\ell)$.

Let $\bar{P}_{er}$ be defined as follows:

(1) For the case where the outer code is not interleaved, $\bar{P}_{er}$ denotes the right-hand side of (42), and

(2) for the case where the outer code is interleaved by a depth m_1, $\bar{P}_{er}$ denotes the right-hand side of (47), if an erasure-only inner decoding

is used and $t_2(i)$ is independent of i, and otherwise, $\bar{P}_{er}$ denotes the right-hand side of (52).

It follows from (42), (47) and (52) that

$$P_{er} \leq \bar{P}_{er} .$$

For most cases of the example schemes considered in the next section, the right-hand side of (52) is considerably tighter than that of (47).

5. Example Schemes

In the following we consider various specific example schemes using cascaded coding for error control. In these example schemes, the inner codes range from high rates to very low rates, and the outer codes are Reed-Solomon (RS) (or a shortened RS) codes with symbols from $GF(2^{\ell})$. The outer code is either interleaved or not interleaved. The inner codes with their parameters and generator polynomials are listed in descending order of the rates in Table 1. The first three inner code, $C_1(1)$ to $C_1(3)$ are shortened distance-4 Hamming codes. The next three codes, $C_1(4)$ to $C_1(6)$ are obtained by shortening the even subcodes of primitive BCH codes of length 63. The forth and fifth codes, $C_1(4)$ and $C_1(5)$, can be decoded with a table look-up decoding. The sixth code $C_1(6)$ is majority-logic decodable in two steps [1], and its decoder can be implemented easily. $C_1(7)$ is a quadruple-error correcting Goppa code [12]. The eighth code is an extended primitive BCH code. In fact, is is also a Reed-Muller code and is majority-logic decodable. $C_1(9)$ is the extended (24,12) Golay code which is widely used for satellite and deep space communications. $C_1(10)$, $C_1(12)$ and $C_1(13)$ are low-rate biorthgonal codes (or first-order Reed-Muller codes). $C_1(11)$ is a quadruple-error correcting one-step majority-logic decodable code [1].

For various combinations of code parameters and bit-error rates, the sum of the probability of a block erasure (decoding failure) and that of a decoding error, $P_{es}+P_{er}$ [given by (41) or (50)], and upper bound $\bar{P}_{er}$ [defined in the previous section] on the probability of a decoding error are given in Tables 2 to 5 and Figures 6 and 7. The degree of interleaving, denoted I_d, is either 1 or m_1. Thresholds, $T_{e\ell}$ and t_2, which are independent of the number of erased segments are considered here. The parameter, m_1T_{es}/I_d+2t_2+1, is used as a measure of the complexity of the outer code.

Symbol "E" (or "L") shown in Tables 2 to 5 indicates that an erasure-only inner decoding (or a LIA-only inner decoding) is used. For a comparison, we also consider a combined erasure and LIA inner decoding where the LIA-operation is performed whenever an uncorrectable error pattern whose weight is even (or odd) is detected in a received frame for odd (or even) t_1. In Table 2 symbol "E-L" indicates that the combined inner decoding is used. For the combined inner decoding, formulas for $P_{e\ell}^{(1)}$, $P_{e\ell,w}^{(1)}$ and $p_{e\ell}(u)$ are given in our NASA Technical Report [8]. In Table 2, the computation results for the combined inner decoding are given only for the cases where either d_2 or m_1T_{es}/I_d+2t_2+1 is smaller than that for either the erasure-only inner decoding or the LIA-only inner decoding.

Example schemes shown in Table 2 are obtained as follows: Given the inner code $C_1(i)$ with $1 \leq i \leq 7$, $n_2=252$ or 255, $I_d=1$ or m_1 and the type of inner code decoding, the values of t_2, T_{es} and $T_{e\ell}$ are chosen to minimize m_1T_{es}/I_d+2t_2+1 under the condition that

$$P_{es} + P_{er} \text{ (or } \overline{P_{es}+P_{er}}) < 10^{-1}$$

for bit-error rate $\varepsilon = 10^{-2}$, and then the minimum value of d_2 is chosen to satisfy the following condition

$$\bar{P}_{er} < 10^{-10}$$

for $\varepsilon = 10^{-2}$. Only the example schemes with rates greater than 0.6 and $d_2 \leq 33$ are listed in Table 2. In the column of $P_{es}+P_{er}$, an entry marked "*" is given by the upper bound of (48).

In Tables 3 to 5, $P_{es}+P_{er}$ and $\bar{P}_{er}$ are shown for cascaded coding schemes in which the inner code is $C_1(i)$ with $1 \leq i \leq 13$, the outer code is an interleaved RS code with a depth of m_1, and an erasure-only inner decoding is used. Parameters T_{es} and t_2 are chosen to minimize the values of $P_{es}+P_{er}$ for a certain bit-error rate ε under the restriction that $\bar{P}_{er} \leq 10^{-10}$ for every bit-error rate ε listed in the Tables.

In Table 3 the outer code is the NASA standard (255,223) RS code over $GF(2^8)$ and the rates are greater than 0.6. For comparison, the case with no inner code is shown in the first row. In Table 4 the rates are less than 0.6 and greater than 0.4, and example schemes with lower rates are given in Table 5.

In Figure 6 (or 7), the curves of $P_{es}+P_{er}$ (or $\bar{P}_{er}$) vs. ε are shown for five representative example schemes listed in Tables 3 to 5.

6. Conclusion

In this paper, we have investigated a cascaded coding scheme for error control. An important feature of the scheme is that the decoding information of the inner code decoder is passed to the outer code decoder. This makes the outer code decoding more effective. Error performance of the scheme is analyzed. If the inner and outer codes are chosen properly, extremely high reliability can be achieved even for a high channel bit-error rate. Many example schemes are being evaluated. Some high-rate example schemes are being considered by NASA for satellite down-link error control, and some low-rate

example schemes are being considered for spacecraft down-link error control.

A major advantage of the proposed cascaded coding scheme, especially with interleaving, is its robustness against unpredictable bursts.

This paper presents first serious effort in analyzing the error performance of a cascaded coding scheme which includes concatenated coding as a special case.

ACKNOWLEDGMENT

The authors wish to thank the anonymous reviewers of this paper for their constructive comments and suggestions, which were helpful in improving its quality.

REFERENCES

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

2. E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

3. W.W. Peterson and E.J. Weldon, Jr., Error-Correcting Codes, Second Edition, The MIT Press, Cambridge, Mass., 1972.

4. F.J. MacWilliams and N.J.A. Sloane, Theory of Error-Correcting Codes, North Holland, Amsterdam, 1977.

5. R.E. Blahut, Theory and Practice of Error Control Codes, Addison Wesley, Reading, Mass., 1983.

6. G.D. Forney, Jr., Concatenated Codes, The MIT Press, Cambridge, Mass., 1966.

7. E.L. Blokh and V.V. Zyablov, "Existence of Linear Concatenated Binary Codes with optimal correcting properties," Probl. Peredach. Inform., Vol.9, pp.3-10, 1973.

8. T. Kasami and S. Lin, "A Cascaded Coding Scheme for Error Control," NASA-GSFC Technical Report, December 10, 1985.

9. J. MacWilliams, "A Theorem on the Distribution of Weights in a Systematic Code," Bell System Technical Journal, Vol.42, pp. 79-94, 1963.

10. J. Riordan, An Introduction to Combinatorial Analysis, John-Wiley and Sons Inc., New York, 1958.

11. T. Kasami, T. Fujiwara and S. Lin, "A Concatenated Coding Scheme for Error Control," IEEE Trans. on Communications, Vol. COM-34, No. 5, pp. 481-488, 1986.

12. V. D. Goppa, "A New Class of Linear Error-Correcting Codes," Problems of Information Transmission, Vol. 6, No. 3, pp.207-212, 1970.

APPENDIX A

Proof of Lemma 1

Let $|H| = u$. It follows from (7) that

$$\sum_{(i_1,i_2,\cdots,i_{m_1+1})\in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \prod_{h=1}^{m_1} \Big[\sum_{j_h=0}^{\ell} \sum_{s_h=0}^{\ell} W^{(i_h)}_{j_h,s_h}(\ell) X^{j_h} Y^{s_h} \Big]$$

$$\cdot \sum_{j_{m_1+1}=1}^{r_1} \sum_{s_{m_1+1}=1}^{r_1} W^{(i_{m_1+1})}_{j_{m_1+1},s_{m_1+1}}(r_1) X^{j_{m_1+1}} Y^{j_{m_1+1}}$$

$$= \sum_{(i_1,i_2,\cdots,i_{m_1+1})\in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$\cdot (1+XY)^{n_1 - \sum_{h=1}^{m_1+1} i_h} (X+Y)^{\sum_{h=1}^{m_1+1} i_h}$$

$$= (1+XY)^{\ell u} \sum_{(i_1,i_2,\cdots,i_{m_1+1})\in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$\cdot (1+XY)^{n_1 - \ell u - \sum_{h=1}^{m_1+1} i_h} (X+Y)^{\sum_{h=1}^{m_1+1} i_h} . \qquad (A\text{-}1)$$

The set of codewords in C_1 whose weight in the h-th ℓ-bit byte is zero for every h in H is a linear $(n_1, k_1 - \ell u)$ subcode of C_1. Let $C_1(H)$ denote the linear $(n_1 - \ell u, k_1 - \ell u)$ code obtained from the above subcode by deleting the u zero ℓ-bit bytes for the u positions in H. Let $A^{(1)}_i(H)$ denote the number of codewords of weight i in $C_1(H)$. Then

$$A_i^{(1)}(H) = \sum_{(i_1,i_2,\cdots,i_{m_1+1})\in I(H;i)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} , \qquad (A\text{-}2)$$

where

$$I(H;i) = \{(i_1,i_2,\cdots,i_{m_1+1}) : (i_1,i_2,\cdots,i_{m_1+1})\in I(H) \text{ and } \sum_{h=1}^{m_1+1} i_h = i \} .$$

The right-hand side of (A-1) can be rewritten as

$$(1+XY)^{\ell u} \sum_{i=0}^{n_1-\ell u} A_i^{(1)}(H)(1+XY)^{n_1-\ell u-i}(X+Y)^i . \qquad (A\text{-}3)$$

Let $B_i^{(1)}(H)$ be the number of codewords of weight i in the dual code of $C_1(H)$. Then, by MacWilliams' identity [4], (A-3) can be rewritten as

$$2^{-r_1}(1+XY)^{\ell u} \sum_{i=0}^{n_1-\ell u} B_i^{(1)}(H)(1+X)^{n_1-\ell u-i}(1-X)^i\,(1+Y)^{n_1-\ell u-i}(1-Y)^i . \qquad (A\text{-}4)$$

It follows from (21), (A-1) and (A-4) that

$$\sum_{(i_1,i_2,\cdots,i_{m_1+1})\in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \prod_{h=1}^{m_1} \Big[\sum_{j_h=0}^{\ell}\sum_{s_h=0}^{\ell} W_{j_h,s_h}^{(i_h)}(\ell)X^{j_h}Y^{s_h}\Big]$$

$$\cdot \sum_{j_{m_1+1}=1}^{r_1}\sum_{s_{m_1+1}=1}^{r_1} W_{j_{m_1+1},s_{m_1+1}}^{(i_{m_1+1})}(r_1)X^{j_{m_1+1}}Y^{j_{m_1+1}}$$

$$= 2^{-r_1} \sum_{i=0}^{n_1-\ell u} B_i^{(1)}(H)(1+X)^{n_1-\ell u-i}(1-X)^i \sum_{s=0}^{n_1} Q_s(i,n_1-\ell u,\ell u,X)Y^s . \qquad (A\text{-}5)$$

Taking the terms on both sides of (A-5) for which the degree of Y is t_1 or

less and substituting "1" for Y, we have that

$$\sum_{(i_1,i_2,\cdots,i_{m_1+1})\in I(H)} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \sum_{j_1=0}^{\ell}\cdots\sum_{j_{m_1}=0}^{\ell}\sum_{j_{m_1+1}=0}^{r_1}$$

$$\cdot \sum_{(s_1,s_2,\cdots,s_{m_1+1})\in S_{t_1}} \Big[\prod_{h=1}^{m_1} W^{(i_h)}_{j_h,s_h(\ell)}\Big]\cdot W^{(i_{m_1+1})}_{j_{m_1+1},s_{m_1+1}(r_1)}\cdot X^{\sum_{h=1}^{m_1+1} j_h}$$

$$= 2^{-r_1}\sum_{i=0}^{n_1-\ell u} B^{(1)}_i(H)(1+X)^{n_1-\ell u-i}(1-X)^i\,\bar{Q}_{t_1}(i,n_1-\ell u,\ell u,X)\ . \qquad \text{(A-6)}$$

Substituting $\varepsilon/(1-\varepsilon)$ for X and multiplying the left-hand side of (A-6) by $(1-\varepsilon)^{n_1}$, we obtain the right-hand side of (18). Therefore we have that

$$P^{(1)}_e(H) = 2^{-r_1}\sum_{i=0}^{n_1-\ell u} B^{(1)}_i(H)(1-2\varepsilon)^i(1-\varepsilon)^{\ell u}\,\bar{Q}_{t_1}(i,n_1-\ell u,\ell u,\varepsilon/(1-\varepsilon))\ . \qquad \text{(A-7)}$$

Since a generator matrix of the dual code of $C_1(H)$ can be obtained from a parity-check matrix of C_1 by deleting all columns corresponding to the h-th ℓ-bit positions for $h\in H$, the following relation holds.

$$B^{(1)}_i(H) = \sum_{I_i(H)} B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} \qquad \text{(A-8)}$$

where

$$I_i(H) = \{(i_1,i_2,\cdots,i_{m_1+1}) : 0 \le i_h \le \ell \text{ for } 1 \le h \le m_1,$$
$$0 \le i_{m_1+1} \le r_1, \text{ and } \sum_{h\in H} i_h = i\ \}\ .$$

Then, expression (22) of Lemma 1 follows from (A-7) and (A-8).

APPENDIX B

Proof of Theorem 2

Let $F(X_1,X_2,\cdots,X_{m_1+1},Y)$ be defined as follows:

$$F(X_1,X_2,\cdots,X_{m_1+1},Y) = \sum_{i_1=0}^{\ell}\cdots\sum_{i_{m_1}=0}^{\ell}\sum_{i_{m_1+1}=0}^{r_1} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$\cdot\prod_{h=1}^{m_1}\Big[\sum_{j_h=0}^{\ell}\sum_{s_h=0}^{\ell} W^{(i_h)}_{j_h,s_h}(\ell)X^{j_h}Y^{s_h}\Big]$$

$$\cdot\Big[\sum_{j_{m_1+1}=1}^{r_1}\sum_{s_{m_1+1}=1}^{r_1} W^{(i_{m_1+1})}_{j_{m_1+1},s_{m_1+1}}(r_1)X_{m_1+1}^{j_{m_1+1}}Y^{j_{m_1+1}}\Big]. \quad (B\text{-}1)$$

It follows from (7) and generalized MacWilliams' identity [4,p.147] that

$$F(X_1,X_2,\cdots,X_{m_1+1},Y) = \sum_{i_1=0}^{\ell}\cdots\sum_{i_{m_1}=0}^{\ell}\sum_{i_{m_1+1}=0}^{r_1} A^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$\cdot\prod_{h=1}^{m_1}(1+X_hY)^{\ell-i_h}(X_h+Y)^{i_h}\,(1+X_{m_1+1}Y)^{r_1-i_{m_1+1}}(X_{m_1+1}+Y)^{i_{m_1+1}}$$

$$= 2^{-r_1}\sum_{i_1=0}^{\ell}\cdots\sum_{i_{m_1}=0}^{\ell}\sum_{i_{m_1+1}=0}^{r_1} B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$\cdot\Big[\prod_{h=1}^{m_1}(1+X_h)^{\ell-i_h}(1-X_h)^{i_h}\Big](1+X_{m_1+1})^{r_1-i_{m_1+1}}(1-X_{m_1+1})^{i_{m_1+1}}$$

$$\cdot(1+Y)^{n_1-\sum_{h=1}^{m_1+1} i_h}\,(1-Y)^{\sum_{h=1}^{m_1+1} i_h}. \quad (B\text{-}2)$$

Let H be a subset of $\{1,2,\cdots,m_1\}$ and $F_{H,t_1}(X_1,X_2,\cdots,X_{m_1+1},Y)$ be the sum of the terms of $F(X_1,X_2,\cdots,X_{m_1+1},Y)$ for which the degree of X_h is nonzero for $h\in H$ and is zero for $h\in\{1,2,\cdots,m_1\}-H$, and the degree of Y is t_1 or less.

Using (10), and (B-2), we have that

$$F_{H,t_1}(X_1,X_2,\cdots,X_{m_1+1},Y) = 2^{-r_1} \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$

$$\cdot \Big[\sum_{s=0}^{t_1} P_s\Big(\sum_{h=1}^{m_1+1} i_h, n_1\Big) Y^s \Big] \prod_{h\in H} \big[(1+X_h)^{\ell-i_h}(1-X_h)^{i_h} - 1 \big]$$

$$\cdot (1+X_{m_1+1})^{r_1-i_{m_1+1}}(1-X_{m_1+1})^{i_{m_1+1}} . \qquad \text{(B-3)}$$

Let $F_{w,t_1}(X_1,X_2,\cdots,X_{m_1+1},Y)$ be defined as the sum of $F_{H,t_1}(X_1,X_2,\cdots,X_{m_1+1},Y)$ over all the subsets, H's, of $\{1,2,\cdots,m_1\}$ with exactly w elements. Then the second term of (31) is equal to

$$- (1-\varepsilon)^{n_1} F_{w,t_1}(\varepsilon/(1-\varepsilon),\varepsilon/(1-\varepsilon),\cdots,\varepsilon/(1-\varepsilon),1) . \qquad \text{(B-4)}$$

It follows from (B-3), the definition of R_w given by (32) and the following identity [4, p.153]:

$$\sum_{s=0}^{t} P_s(i,n) = P_t(i-1,n-1) , \qquad \text{(B-5)}$$

that (B-4) is equal to

$$-2^{-r_1}(1-\varepsilon)^{k_1-\ell w} \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}} (1-2\varepsilon)^{i_{m_1+1}}$$

$$\cdot P_{t_1}\Big(\sum_{h=1}^{m_1+1} i_h - 1, n_1 - 1\Big) R_w(i_1,i_2,\cdots,i_{m_1};\varepsilon) .$$

APPENDIX C

Derivation of (46)

Let $F_u(X_1,X_2,\cdots,X_{m_1+1},Y)$ be the sum of terms of $F(X_1,X_2,\cdots,X_{m_1+1},Y)$ defined in Appendix B for which the degree of X_u is nonzero and the degree of Y is t_1 or less. Using (10) and (B-2), we have that

$$F_u(X,X,\cdots,X,Y) = 2^{-r_1} \sum_{i_1=0}^{\ell} \cdots \sum_{i_{m_1}=0}^{\ell} \sum_{i_{m_1+1}=0}^{r_1} B^{(1)}_{i_1,i_2,\cdots,i_{m_1+1}}$$
$$\cdot \Big[\sum_{s=0}^{t_1} P_s\Big(\sum_{h=1}^{m_1+1} i_h, n_1\Big) Y^s \Big] \prod_{\substack{1\le h\le m_1 \\ h\neq u}} (1+X)^{\ell-i_h}(1-X)^{i_h}$$
$$\cdot [(1+X)^{\ell-i_u}(1-X)^{i_u} - 1]\,(1+X)^{r_1-i_{m_1+1}}(1-X)^{i_{m_1+1}} . \qquad (C\text{-}1)$$

The second term of (45) is equal to

$$-(1-\varepsilon)^{n_1} F_u(\varepsilon/(1-\varepsilon),\varepsilon/(1-\varepsilon),\cdots,\varepsilon/(1-\varepsilon),1) .$$

Then (46) follows from (B-5).

APPENDIX D

A formula for computing $P^{(1)}_{e,a_1,a_2,\cdots,a_{m_1}}$

Let H be a subset of $\{1, 2, \cdots, m_1\}$. For small m_1, say less than 11, $\{P_e(H) : H \subseteq \{1, 2, \cdots, m_1\}\}$ can be found as shown in section 2.1. Then it follows from the principle of inclusion and exclusion [10] that

$$P^{(1)}_{e,a_1,a_2,\cdots,a_{m_1}} = \sum_{s=0}^{|W|} (-1)^{|W|-s} \sum_{\substack{\bar{H} \subseteq W \\ |\bar{H}|=s}} P_e(H) \qquad \text{(D-1)}$$

where $W = \{ i \mid a_i = 1, 1 \leq i \leq m_1 \}$ and $\bar{H} = \{1, 2, \cdots, m_1\} - H$.

APPENDIX E

A procedure for computing $p_e(u,\alpha)$

For $1 \le u \le m_1$, $0 \le i \le n_1-\ell$ and $\alpha \in GF(2^\ell)$, let $A_i^{(1)}(u,\alpha)$ (or $B_i^{(1)}(u,\alpha)$) be the number of codewords in C_1 (or the dual code of C_1) whose u-th symbol is α and whose binary weight excluding the u-th symbol is i. Let α_f be the f-th bit of the binary representation of α, and let $|\alpha|$ be the weight of the binary reprensentation of α. It follows from the definition of $p_e(u,\alpha)$ that

$$p_e(u,\alpha) = \sum_{i=0}^{n_1-\ell} A_i^{(1)}(u,\alpha) \sum_{j=0}^{n_1-\ell} \sum_{j'=0}^{\ell} \sum_{s=0}^{t_1} \sum_{s'=0}^{t_1-s} W_{j,s}^{(i)}(n_1-\ell)\, W_{j',s'}^{(|\alpha|)}(\ell)\, \varepsilon^{s+s'}(1-\varepsilon)^{n_1-s-s'}. \quad \text{(E-1)}$$

For relatively small k_1, say less than 25, $\{A_i^{(1)}(u,\alpha) \mid 0 \le i \le n_1-\ell\}$ for an α in $GF(2^\ell)$ can be found by generating $2^{k_1-\ell}$ codewords of C_1.

A procedure for computing $p_e(u,\alpha)$ which is more convenient for $k_1 > n_1-k_1$ will be derived below. By the generalized MacWilliams' identity [4, p.147], we have that

$$A_i^{(1)}(u,\alpha) = 2^{-(n_1-k_1)} \sum_{h=0}^{n_1-\ell} \sum_{\beta \in GF(2^\ell)} B_h^{(1)}(u,\beta) P_i(h,n_1-\ell) \prod_{f=1}^{\ell} P_{\alpha_f}(\beta_f,1). \quad \text{(E-2)}$$

By [4,p.151], we have that

$$\prod_{f=1}^{\ell} P_{\alpha_f}(\beta_f,1) = (-1)^{\sum_{f=1}^{\ell} \alpha_f \beta_f} = (-1)^{(|\alpha|+|\beta|-|\alpha+\beta|)/2}, \quad \text{(E-3)}$$

and

$$\sum_{i=0}^{n_1-\ell} P_i(h,n_1-\ell)(1+XY)^{n_1-\ell-i}(X+Y)^i = (1+X)^{n_1-\ell-h}(1-X)^h\ (1+Y)^{n_1-\ell-h}(1-Y)^h \tag{E-4}$$

It follows from (7), (E-2), (E-3) and (E-4) that

$$\sum_{i=0}^{n_1-\ell} A_i^{(1)}(u,\alpha)\ [\sum_{j=0}^{n_1-\ell}\sum_{s=0}^{n_1-\ell} W_{j,s}^{(i)}(n_1-\ell)\ X^jY^s\ ]\ [\sum_{j'=0}^{\ell}\sum_{s'=0}^{\ell} W_{j',s'}^{(|\alpha|)}(\ell)\ X^{j'}Y^{s'}\ ]$$

$$= 2^{-(n_1-k_1)}\ (1+XY)^{\ell-|\alpha|}(X+Y)^{|\alpha|}\ \sum_{h=0}^{n_1-\ell}\sum_{\beta\in GF(2^\ell)} B_h^{(1)}(u,\beta)$$

$$\cdot\ (-1)^{(|\alpha|+|\beta|-|\alpha+\beta|)/2}\ (1+X)^{n_1-\ell-h}(1-X)^h\ (1+Y)^{n_1-\ell-h}(1-Y)^h$$

$$= 2^{-(n_1-k_1)}\ \sum_{h=0}^{n_1-\ell}\sum_{\beta\in GF(2^\ell)} B_h^{(1)}(u,\beta)$$

$$\cdot\ (-1)^{(|\alpha|+|\beta|-|\alpha+\beta|)/2}\ (1+X)^{n_1-\ell-h}(1-X)^h \sum_{s=0}^{n_1} Q_s'(h,n_1-\ell,|\alpha|,\ell,X)\ Y^s\ , \tag{E-5}$$

where

$$(1+XY)^{m-h}(X+Y)^h(1+Y)^{n-i}(1-Y)^i = \sum_{s=0}^{n+m} Q_s'(i,n,h,m,X)Y^s\ ,$$

$$Q_s'(i,n,h,m,X) = \sum_{f=0}^{s} P_{s-f}(i,n)\ \sum_{j=0}^{m} W_{j,f}^{(h)}(m)X^j\ .$$

Taking the term on both sides of (E-5) for which the degree of Y is t_1 or less substituting $\varepsilon/(1-\varepsilon)$ for X and 1 for Y and multiplying the both sides by $(1-\varepsilon)^{n_1}$, we obtain the following formula from (E-1):

$$p_e(u,\alpha) = 2^{-(n_1-k_1)} (1-\varepsilon)^{\ell} \sum_{h=0}^{n_1-\ell} (1-2\varepsilon)^h$$

$$\sum_{s=0}^{t_1} Q_s'(h,n_1-\ell,|\alpha|,\ell,\varepsilon/(1-\varepsilon))$$

$$\sum_{\beta\in GF(2^{\ell})} B_h^{(1)}(u,\beta) (-1)^{(|\alpha|+|\beta|-|\alpha+\beta|)/2} . \qquad \text{(E-6)}$$

If C_1 is a shortened cyclic code, $\min\{\ell,n_1-k_1\}$ columns of a generating matrix corresponding to the u-th symbol position are linearly independent, and for a symbol β, $\{B_h^{(1)}(u,\beta) \mid 0 \leq h \leq n_1-\ell\}$ can be found by generating $2^{\min\{n_1-k_1-\ell,0\}}$ codewords of the dual code of C_1.

Appendix F

Derivation of (52)

At first an upper bound on $\tilde{P}_{er}(u)$ will be derived. Let us number the segment in a decoded segment-array (Fig. 5) from 1 to n_2. Suppose that the number of erased segments after the inner code decoding is T_{es} or less. Let E_s be the set of the erased segment numbers. For $f \notin E_s$, let e_f be the error symbol at the u-th symbol position of the f-th decoded segment, and let $\bar{e} = (e_1, e_2, \cdots, e_{n_2})$. Note that e_f is the symbol error at the f-th symbol position of the u-th section of a decoded segment-array. Suppose that the u-th section of a segment-array is decoded incorrectly by the outer code decoder. Then the u-th section is decoded into an outer codeword $\bar{v}_c + \bar{v}$, where $\bar{v}_c$ is the actual transmitted outer codeword and $\bar{v}$ is the nonzero outer codeword induced by the outer code decoding. Let v_f be the f-th symbol of $\bar{v}$. Define the following sets associated to $\bar{v}$ and $\bar{e}$.

$$W(\bar{v}) \triangleq \{ f \mid v_f \neq 0, f \notin E_s \}, \tag{F-1}$$

$$H(\bar{e},\bar{v}) \triangleq \{ f \mid e_f \neq 0, v_f = 0, f \notin E_s \}, \tag{F-2}$$

and

$$J(\bar{e},\bar{v}) \triangleq \{ f \mid e_f = v_f \neq 0, f \notin E_s \}. \tag{F-3}$$

When a section is decoded based on the outer code C_2, only t_2 or fewer symbol errors and T_{es} or fewer erasures are corrected. Hence, the following inequality holds:

$$|H(\bar{e},\bar{v})| + |W(\bar{v})| - |J(\bar{e},\bar{v})| \leq t_2 . \tag{F-4}$$

For given $1 \leq u \leq m_1$, $E_s \subseteq \{1,2,\cdots,n_2\}$, $\bar{v} \in C_2$, $H \subseteq \{1,2,\cdots,n_2\}$ and $J \subseteq \{1,2,\cdots,n_2\}$ such that H is disjoint from E_s and $W(\bar{v})$, $J \subseteq W(\bar{v})$ and $|H| + |W(\bar{v})| - |J| \leq t_2$, let $P_e(u,E_s,\bar{v},H,J)$ be the probability of the occurrence of an error pattern $\bar{e}$ induced by the inner code decoding for which $H(\bar{e},\bar{v})=H$ and $J(\bar{e},\bar{v})=J$. Then

$$P_e(u,E_s,\bar{v},H,J) = [P_{es}^{(1)}]^i[\tilde{p}_e(u)]^h[p_e(u,0)]^{n_2-i-w-h}$$

$$\cdot \prod_{f\in J} p_e(u,v_f) \prod_{f\in W(\bar{v})-J} (1-P_{es}^{(1)}-p_e(u,v_f)), \qquad \text{(F-5)}$$

where $i=|E_s|$, $w=|W(\bar{v})|$ and $h=|H|$ (see Figure 8).

Let W be a subset of $\{1,2,\cdots,n_2\}-E_s-H$ such that $W \supseteq J$, $d_2-i \leq |W|$ and $|W|+h-j \leq t_2$. Let $C_2(E_s,W)$ be defined as the following subset of codewords in C_2:

$$C_2(E_s,W) = \{ (v_1, v_2, \cdots, v_{n_2}) \in C_2 \mid$$

$$v_f \neq 0 \text{ if } f \in W \text{ and only if } f \in W \cup E_s\}. \qquad \text{(F-6)}$$

For $\bar{v} \in C_2(E_s,W)$, $W(\bar{v}) = W$. Let w denote $|W|$. Next we estimate

$$\sum_{\bar{v}\in C_2(E_s,W)} P_e(u,E_s,\bar{v},H,J).$$

Since $i \leq T_{es}$ and $t_2 \leq (d_2-1-T_{es})/2$, we have that

$$d_2 \geq i + 2t_2 + 1 . \qquad \text{(F-7)}$$

Since $d_2 \leq w+i$ and $h+w-j \leq t_2$, it follows from (F-7) that

$$j \geq i+w-d_2 \geq 0 \ . \tag{F-8}$$

Let J' be a subset of J such that

$$|J'| = i + w - d_2 \ . \tag{F-9}$$

For any $a_f \in GF(2^\ell)-\{0\}$ with $f \in J'$, consider two different codewords $\bar{v} = (v_1, v_2, \cdots, v_{n_2})$ and $\bar{v}' = (v_1', v_2', \cdots, v_{n_2}')$ in $C_2(E_s,W)$ such that $v_f = v_f' = a_f$ for $f \in J'$. Since the weight of $\bar{v}-\bar{v}'$ is at least d_2, we have that

$$v_f \neq v_f' \ , \quad \text{for } f \in E_s \cup W - J'. \tag{F-10}$$

It follows from a well known inequality and (F-10) that

$$\begin{aligned}
&\sum_{\bar{v}\in\{\bar{v}\in C_2(E_s,W) \,|\, v_f=a_f \text{ for } f\in J'\}} \prod_{f\in J} p_e(u,v_f) \\
&= \prod_{f\in J'} p_e(u,a_f) \sum_{\bar{v}\in\{\bar{v}\in C_2(E_s,W) \,|\, v_f=a_f \text{ for } f\in J'\}} \prod_{f\in J-J'} p_e(u,v_f) \\
&\leq \prod_{f\in J'} p_e(u,a_f) \sum_{\bar{v}\in\{\bar{v}\in C_2(E_s,W) \,|\, v_f=a_f \text{ for } f\in J'\}} \\
&\qquad \sum_{f\in J-J'} [p_e(u,v_f)]^{j+d_2-i-w} / (j+d_2-i-w) \\
&\leq \prod_{f\in J'} p_e(u,a_f) \sum_{q=0}^{2^\ell-2} [p_e(u,\gamma^q)]^{j+d_2-i-w} \ .
\end{aligned} \tag{F-11}$$

It follows from (51) and (F-11) that

$$\sum_{\bar{v}\in C_2(E_s,W)} \prod_{f\in J} p_e(u,v_f) \leq [\tilde{p}_e(u)]^{i+w-d_2} \sum_{q=0}^{2^{\ell}-2} [p_e(u,\gamma^q)]^{j+d_2-i-w}. \quad \text{(F-12)}$$

Thus it follows from (53) that

$$\sum_{\bar{v}\in C_2(E_s,W)} P_e(u,E_s,\bar{v},H,J) \leq \bar{P}(u,i,w,h,j) \quad \text{(F-13)}$$

Since $\tilde{P}_{er}(u)$ is the sum of $\sum_{\bar{v}\in C_2(E_s,W)} P_e(u,E_s,\bar{v},H,J)$ taken over all possible E_s, W, H and J, we have that

$$\tilde{P}_{er}(u) \leq \sum_{i=0}^{T_{es}} \binom{n_2}{i} \sum_{w=d_2-i}^{n_2-i} \binom{n_2-i}{w} \sum_{h=0}^{\min\{t_2,n_2-i-w\}} \binom{n_2-i-w}{h} \sum_{j=w+h-t_2}^{w} \binom{w}{j} \bar{P}(u,i,w,h,j). \quad \text{(F-14)}$$

P_{er} is bounded above by the expression obtained from the right-hand side of (F-14) by replacing $\bar{P}(u,i,w,h,j)$ with $\sum_{u=1}^{m_1} \bar{P}(u,i,w,h,j)$.

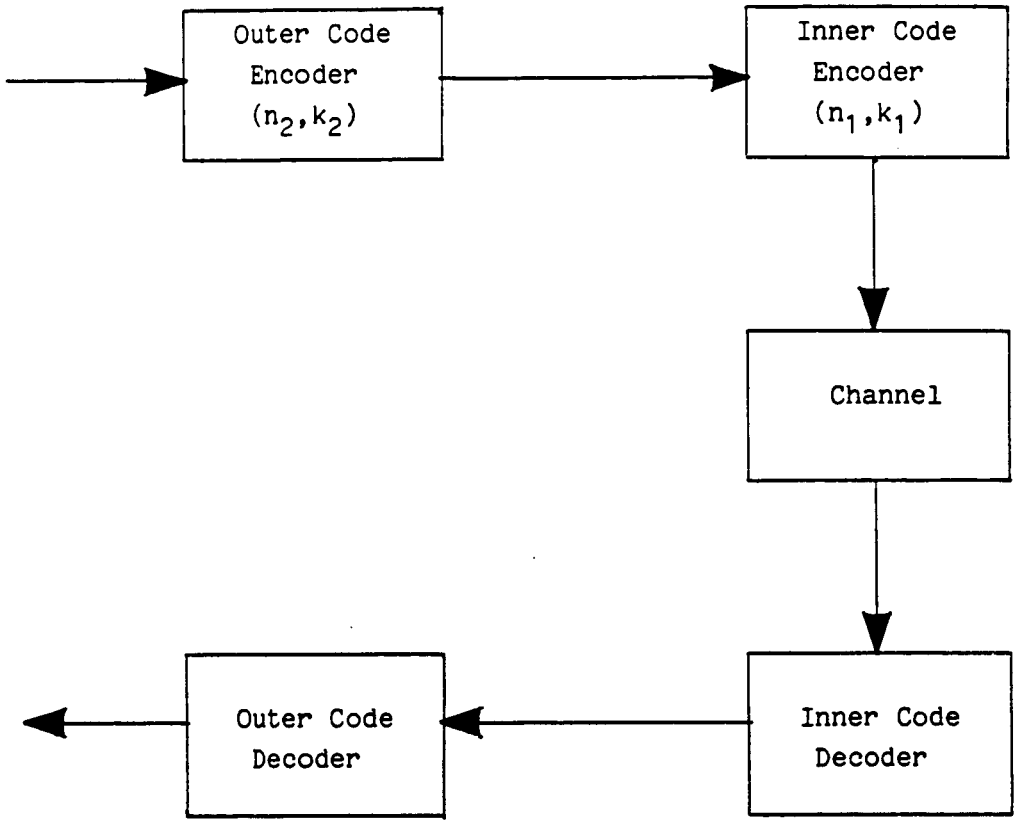

Figure 1 A cascaded coding system

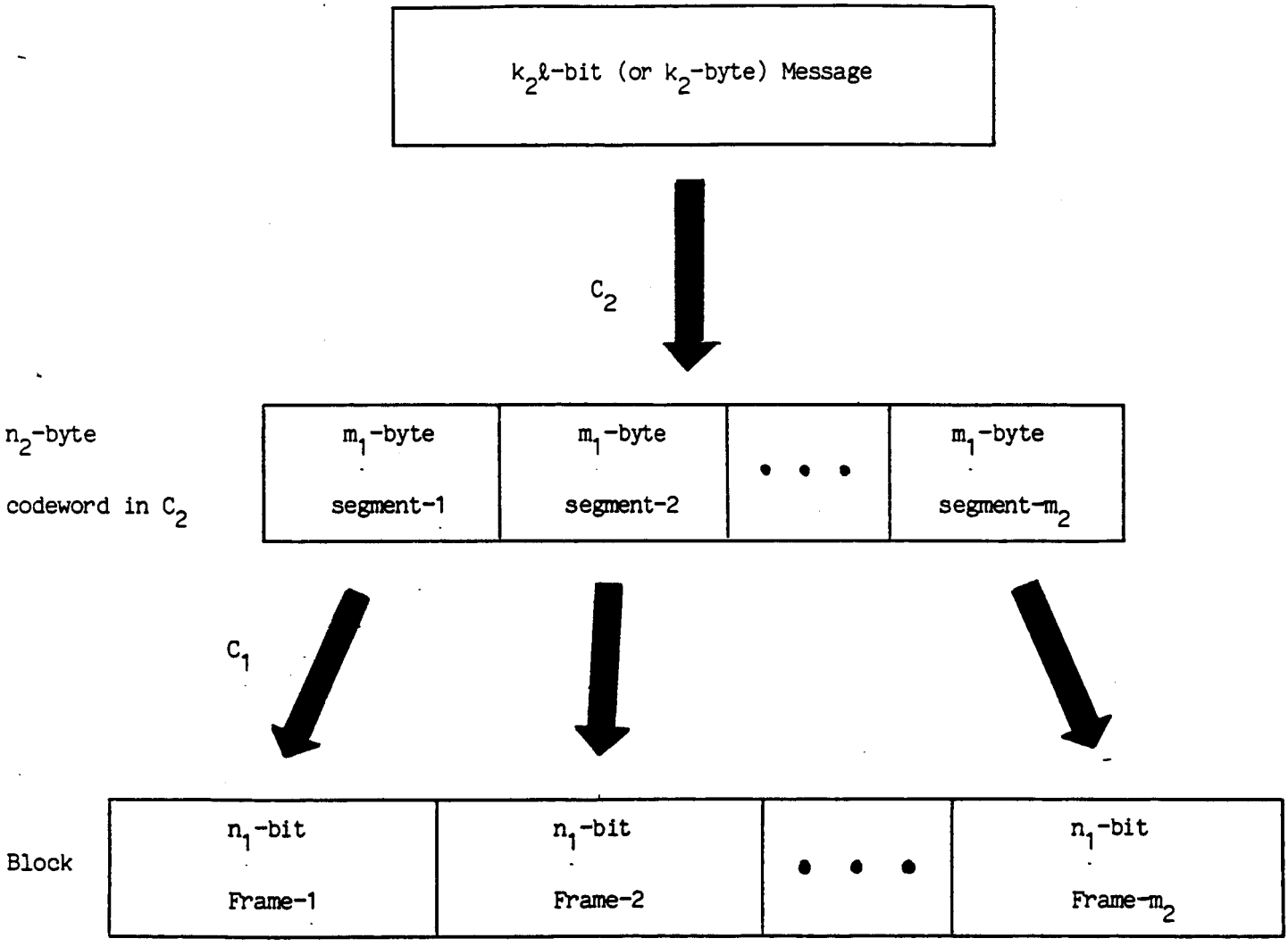

Figure 2 Encoding Operation

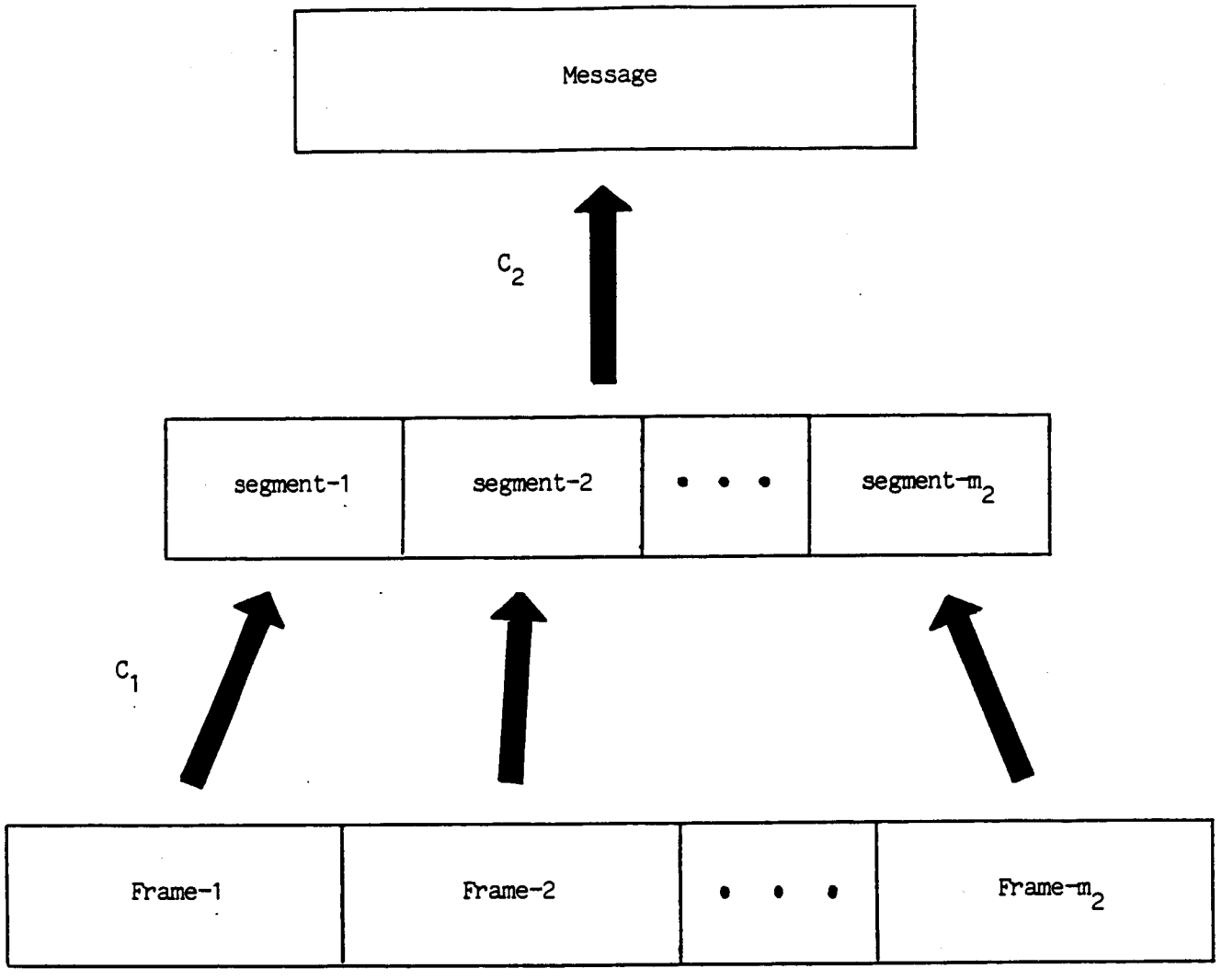

Figure 3 Decoding operation

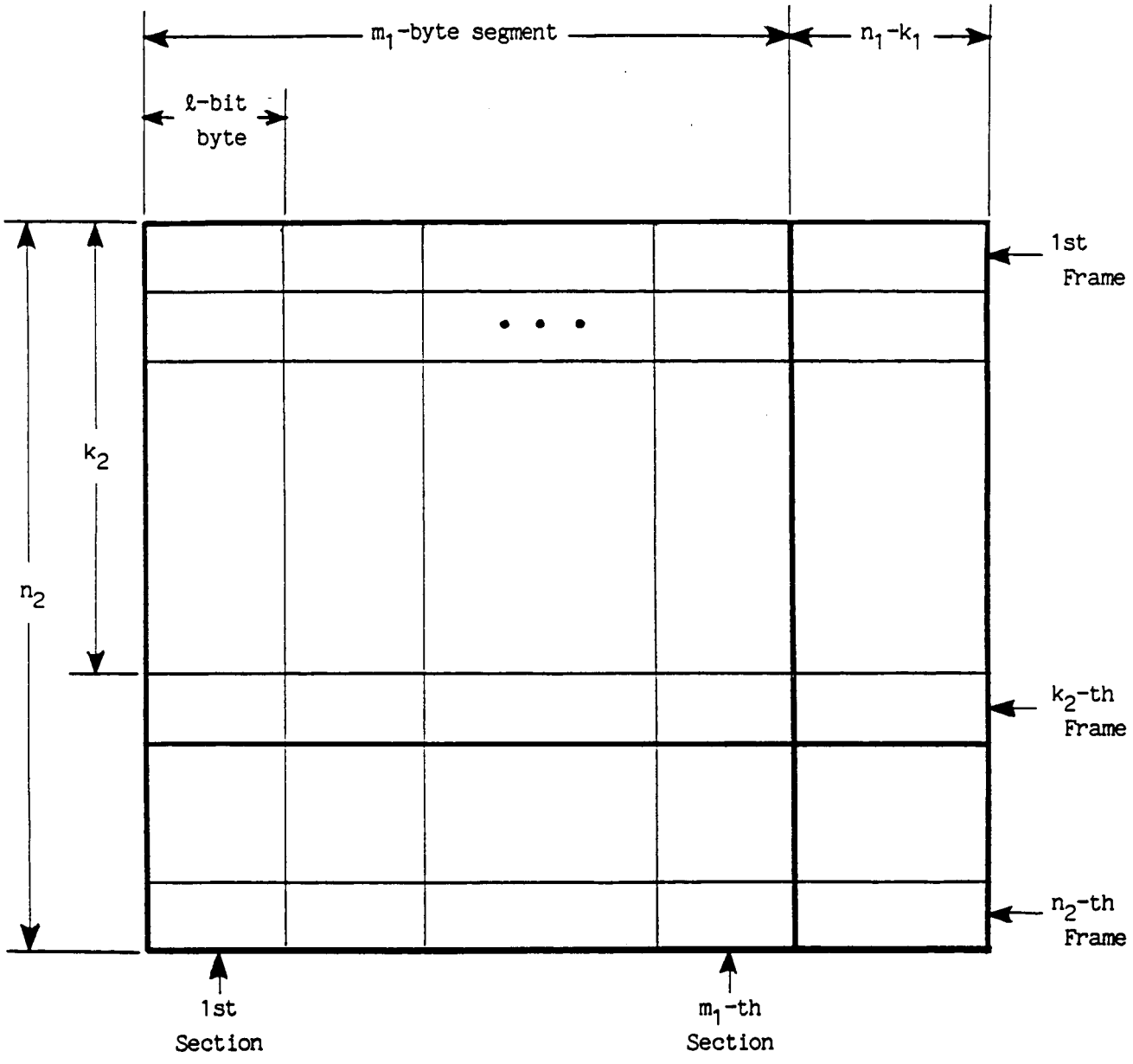

Figure 4 An interleaved code block

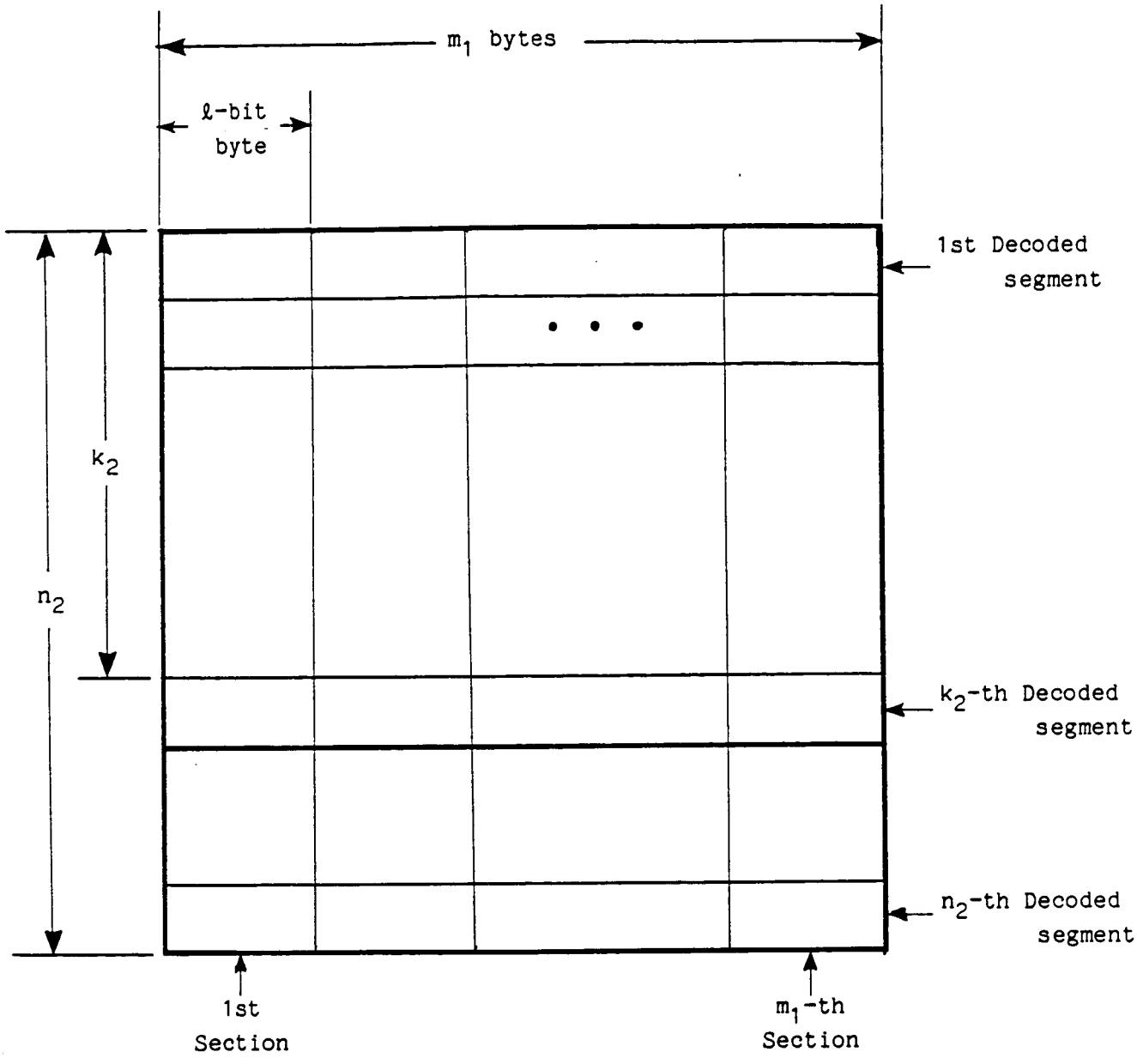

Figure 5 A decoded segment-array

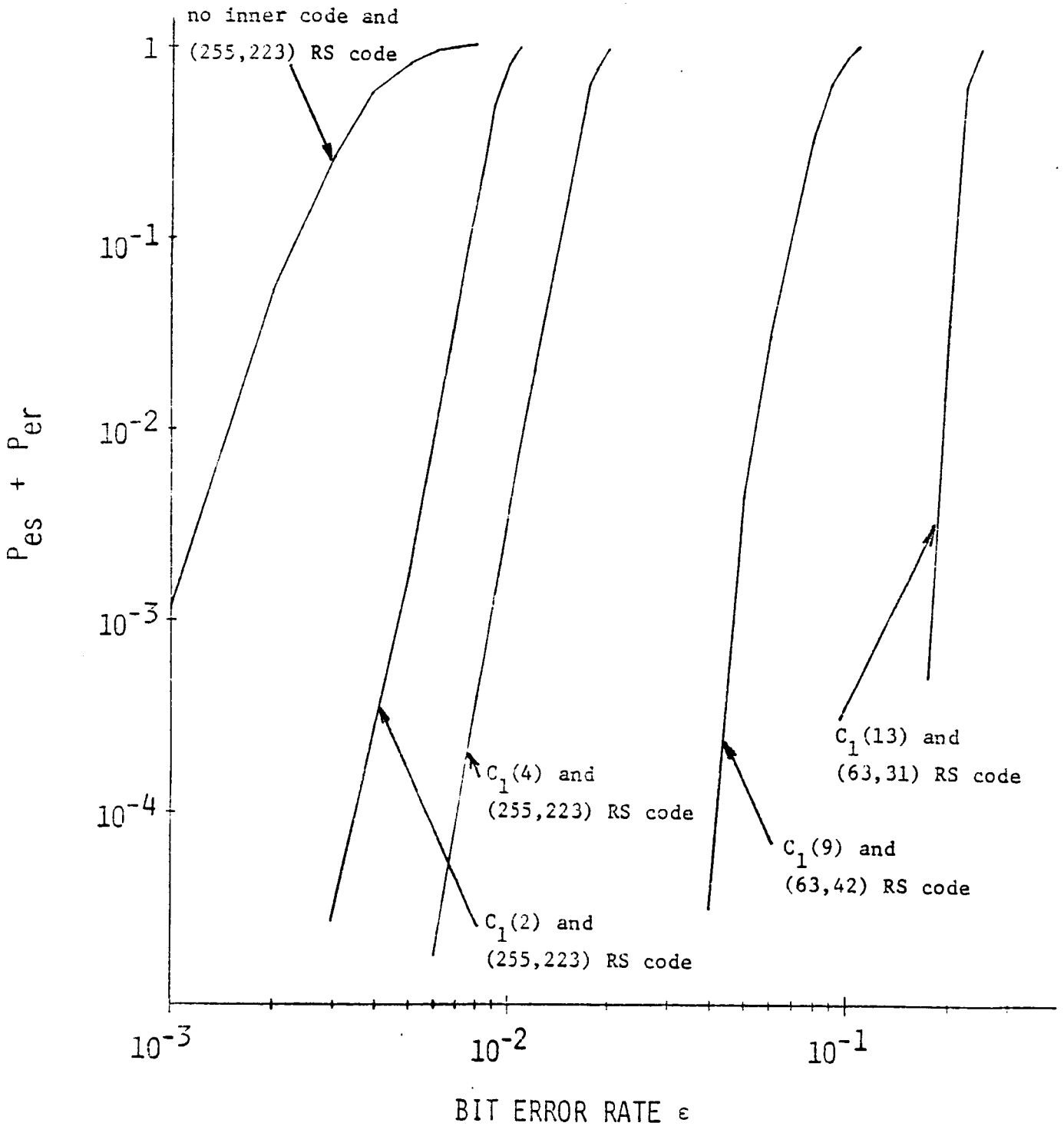

Figure 6 The sum of probabilities of a block erasure and a decoding error.

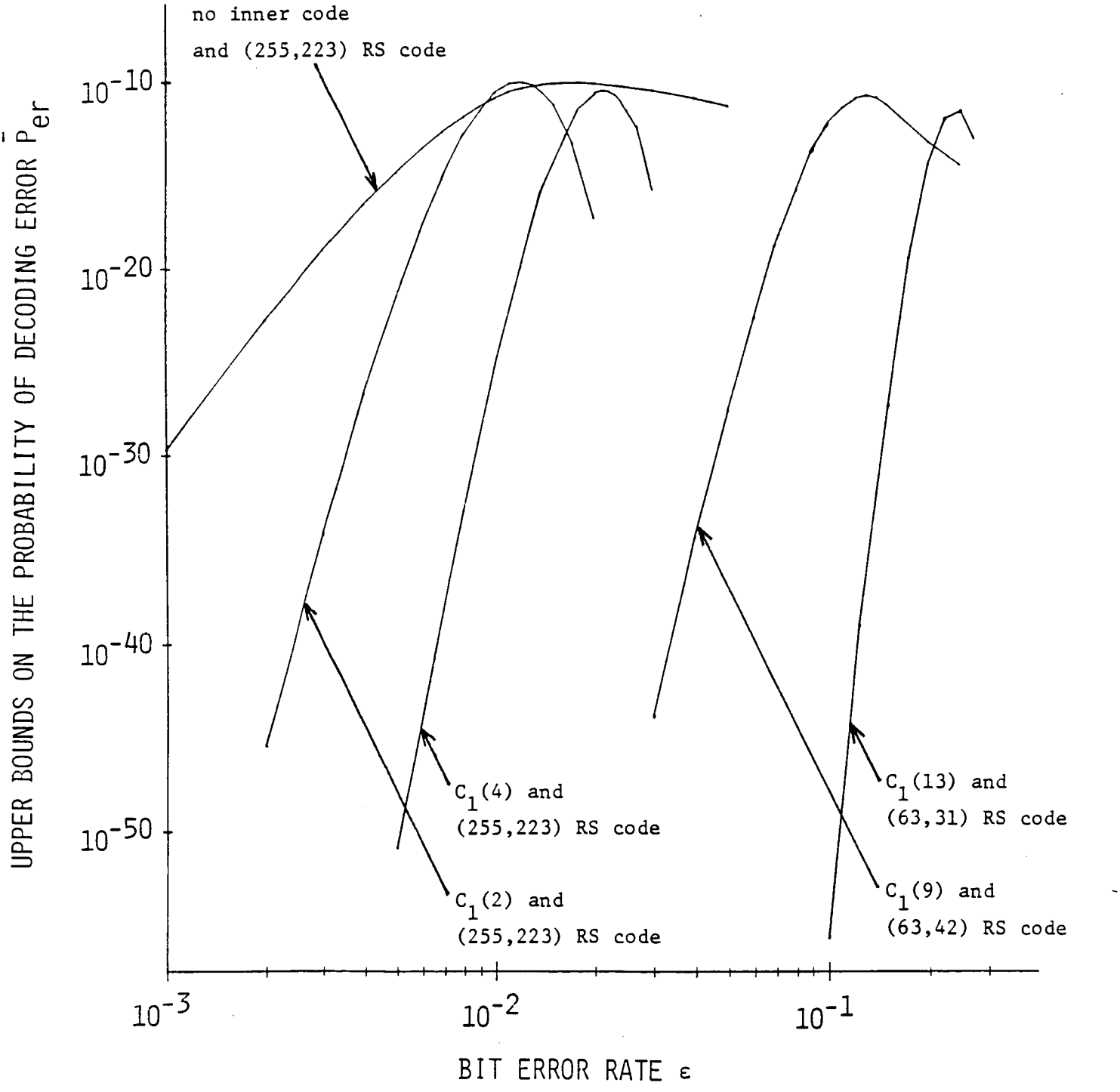

Figure 7 Upper bounds on the probability of decoding error for cascaded codes.

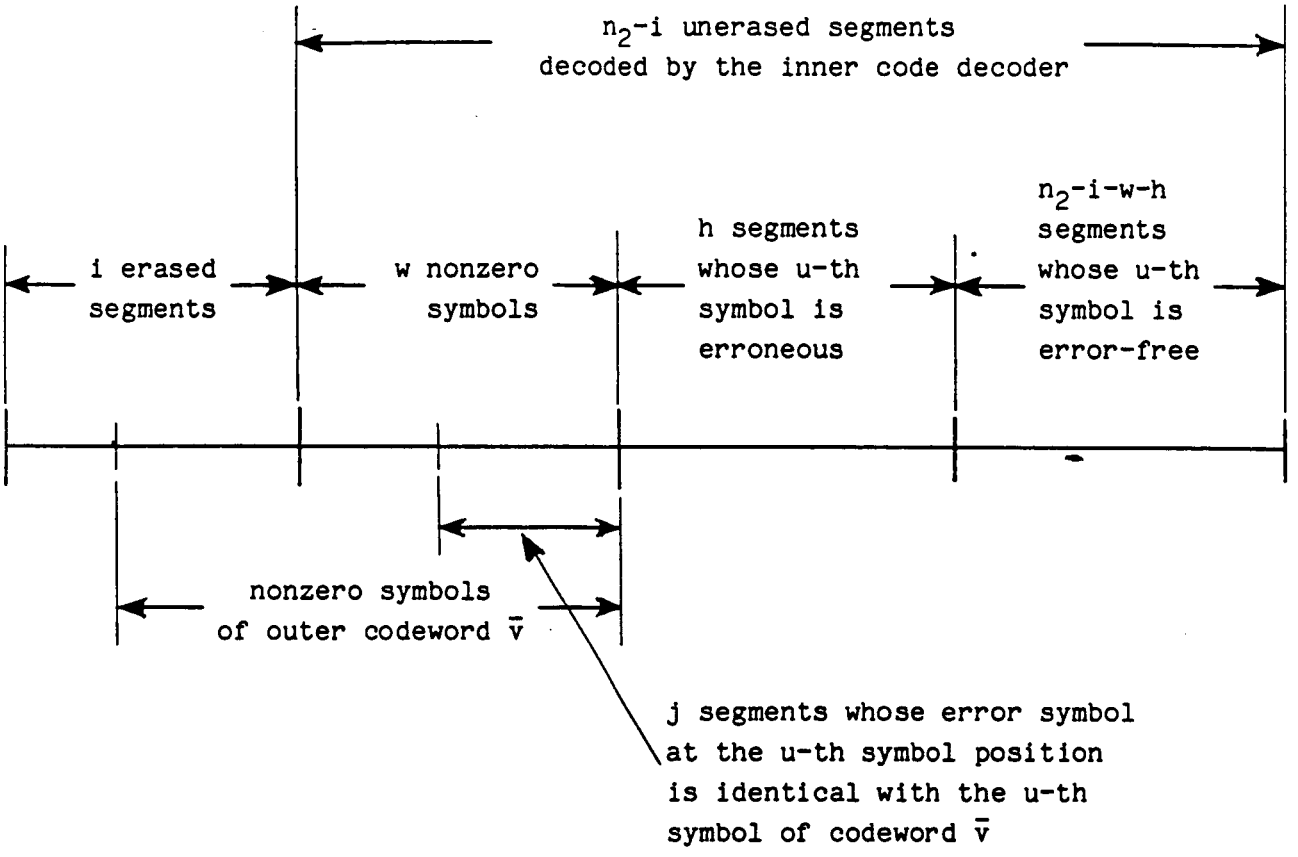

Figure 8 Illustration for Equation (F-5)

Table 1 Inner Codes

	Inner codes	(n_1,k_1)	Rate of the inner code	ℓ	m_1	d_1	t_1	Generator polynomial
$C_1(1)$	shortened Hamming code	(55,48)	0.873	8	6	4	1	$(1+X)\phi_1(X)$
$C_1(2)$	shortened Hamming code	(56,48)	0.857	8	6	4	1	$(1+X)(1+X+X^7)$
$C_1(3)$	shortened Hamming code	(30,24)	0.800	8	3	4	1	$(1+X)(1+X^2+X^5)$
$C_1(4)$	shortened BCH code	(61,48)	0.787	8	6	6	2	$(1+X)\phi_1(X)\phi_3(X)$
$C_1(5)$	shortened BCH code	(53,40)	0.755	8	5	6	2	$(1+X)\phi_1(X)\phi_3(X)$
$C_1(6)$	shortened BCH code	(59,40)	0.678	8	5	8	3	$(1+X)\phi_1(X)\phi_3(X)\phi_5(X)$
$C_1(7)$	Goppa code	(64,40)	0.625	8	5	9	4	
$C_1(8)$	extended BCH code	(32,16)	0.500	8	2	4	3	
$C_1(9)$	extended Golay code	(24,12)	0.500	6	2	8	3	
$C_1(10)$	biorthogonal code	(8, 4)	0.500	4	1	4	1	
$C_1(11)$	shortened Type 0 DTI code	(51,24)	0.471	8	3	10	4	$(1+X)\phi_1(X)\phi_3(X)\phi_5(X)$ $\cdot\phi_7(X)\phi_{21}(X)$
$C_1(12)$	biorthogonal code	(16, 5)	0.313	5	1	8	3	
$C_1(13)$	biorthogonal code	(32, 6)	0.188	6	1	16	7	

The generator polynomials are given only for shortened cyclic codes, and $\phi_i(X)$ is the minimum polynomial of α^i with α as a root of $1+X+X^6$.

Table 2 Probabilities of Decoding Failure or Decoding Error and Upper Bounds on the Probability of Decoding Error For Cascaded Codes with High Rates

Rate	n_2	d_2	I_d	E/L	T_{es}	$T_{e\ell}$	t_2	$m_1 T_{es}/I_d + 2t_2 + 1$	Inner code	Bit-error rate $\varepsilon=10^{-2}$		$\varepsilon=0.5\times10^{-2}$		$\varepsilon=10^{-3}$	
										$P_{es}+P_{er}$	$\bar{P}_{er}$	$P_{es}+P_{er}$	$\bar{P}_{er}$	$P_{es}+P_{er}$	$\bar{P}_{er}$
0.731	255	23	3	E	13	0	2	18	$C_1(3)$	7.97E-2	2.88E-12	1.51E-4	1.80E-23	1.14E-10	1.74E-56
0.712	255	28	3	E-L	1	15	8	18	$C_1(3)$	7.91E-2*	7.69E-11	9.22E-5*	6.41E-22	7.22E-9*	1.07E-51
0.706	255	30	3	L	0	15	9	19	$C_1(3)$	7.64E-2*	3.50E-11	1.70E-6*	2.84E-22	8.38E-20*	5.04E-54
0.740	252	16	6	E	9	0	1	12	$C_1(4)$	9.43E-2	1.35E-11	3.35E-4	2.76E-23	1.37E-9	3.23E-57
0.721	252	22	6	L	0	11	6	13	$C_1(4)$	9.87E-2*	3.50E-12	3.46E-7*	1.02E-24	2.69E-21*	4.43E-60
0.690	252	32	1	L	0	3	5	11	$C_1(4)$	9.39E-2	4.77E-11	1.60E-3	8.39E-18	1.31E-7	1.06E-33
0.716	255	14	5	E	7	0	1	10	$C_1(5)$	5.72E-2	1.47E-13	6.52E-5	1.94E-24	2.47E-10	1.22E-54
0.704	255	18	5	L	0	9	5	11	$C_1(5)$	6.68E-2*	7.16E-11	1.31E-6*	2.39E-21	9.16E-19*	3.05E-50
0.678	255	27	1	E	2	0	0	11	$C_1(5)$	7.30E-2	4.55E-11	2.59E-3	6.45E-17	4.52E-6	8.83E-32
0.678	255	27	1	L	0	3	4	9	$C_1(5)$	9.97E-2	5.28E-11	2.49E-3	3.38E-17	3.85E-7	1.04E-31
0.665	255	6	5	E	2	0	0	3	$C_1(6)$	4.97E-2	2.72E-14	4.97E-4	8.97E-22	1.85E-7	8.60E-41
0.657	255	9	5	L	0	3	2	5	$C_1(6)$	5.10E-2*	2.82E-12	1.69E-5*	6.96E-21	1.05E-13*	1.25E-42
0.635	255	17	1	E	1	0	0	6	$C_1(6)$	1.20E-2	6.71E-11	1.59E-4	4.02E-16	3.72E-8	4.83E-29
0.630	255	19	1	L	0	2	2	5	$C_1(6)$	6.22E-2	2.83E-11	4.57E-3	2.17E-16	8.44E-6	9.98E-29
0.615	255	5	5	E	1	0	0	2	$C_1(7)$	4.46E-2	1.28E-12	6.11E-4	1.43E-19	2.17E-7	1.28E-36

Table 3 Probabilities of Decoding Failure or Decoding Error and Upper Bounds on the Probability of Decoding Error for Cascaded Codes with (255,223) RS Outer Code

Rate	n_2	k_2	d_2	I_d	E/L	T_{es}	t_2	Inner code		Bit-error rate $\varepsilon=0.2\times10^{-2}$	$\varepsilon=0.5\times10^{-2}$	$\varepsilon=1\times10^{-2}$	$\varepsilon=2\times10^{-2}$	$\varepsilon=3\times10^{-2}$
0.875	255	223	33	1	E	0	7	No inner code	$P_{es}+P_{er}$	5.29E-2	7.88E-1	1.00E0	1.00E0	------
									$\bar{P}_{er}$	1.81E-23	1.45E-15	9.93E-12	5.83E-11	------
0.764	255	223	33	6	E	20	2	$C_1(1)$	$P_{es}+P_{er}$	6.13E-6	1.11E-2	8.83E-1	1.00E0	1.00E0
									$\bar{P}_{er}$	4.83E-49	2.01E-24	1.06E-12	1.49E-16	1.02E-29
0.750	255	223	33	6	E	22	2	$C_1(2)$	$P_{es}+P_{er}$	8.35E-7	1.74E-3	7.98E-1	1.00E0	------
									$\bar{P}_{er}$	4.04E-46	2.97E-22	2.04E-11	4.22E-18	------
0.700	255	223	33	3	E	20	2	$C_1(3)$	$P_{es}+P_{er}$	5.35E-8	1.50E-4	3.38E-2	9.80E-1	1.00E0
									$\bar{P}_{er}$	1.15E-66	1.70E-39	7.74E-22	1.06E-11	2.41E-13
0.688	255	223	33	6	E	21	2	$C_1(4)$	$P_{es}+P_{er}$	7.10E-11	2.52E-6	3.69E-3	9.65E-1	1.00E0
									$\bar{P}_{er}$	3.00E-90	1.19E-51	6.15E-26	1.99E-11	1.20E-16
0.660	255	223	33	5	E	22	2	$C_1(5)$	$P_{es}+P_{er}$	5.65E-12	2.17E-7	3.95E-4	4.95E-1	1.00E0
									$\bar{P}_{er}$	9.74E-95	4.18E-56	1.72E-29	1.03E-11	1.59E-12

Table 4 Probabilities of Decoding Failure or Decoding Error and Upper Bounds on the Probability of Decoding Error

Rate	n_2	k_2	d_2	I_d	E/L	T_{es}	t_2	Inner code		Bit-error rate $\varepsilon=1\times10^{-2}$	$\varepsilon=2\times10^{-2}$	$\varepsilon=3\times10^{-2}$	$\varepsilon=4\times10^{-2}$	$\varepsilon=5\times10^{-2}$
0.593	255	223	33	5	E	21	3	$C_1(6)$	$P_{es}+P_{er}$	5.69E-10	7.26E-5	7.55E-1	1.00E0	------
									$\bar{P}_{er}$	6.24E-51	6.38E-21	1.85E-11	1.36E-13	------
0.547	255	223	33	5	E	23	2	$C_1(7)$	$P_{es}+P_{er}$	8.38E-9	6.17E-5	5.57E-3	8.21E-1	1.00E0
									$\bar{P}_{er}$	8.06E-74	1.47E-34	4.28E-17	2.15E-11	1.80E-14
0.437	255	223	33	3	E	24	2	$C_1(8)$	$P_{es}+P_{er}$	5.04E-11	7.36E-7	1.38E-4	3.97E-3	9.93E-2
									$\bar{P}_{er}$	3.44E-83	2.61E-47	1.51E-28	1.22E-17	8.21E-12
0.412	255	223	33	3	E	25	2	$C_1(11)$	$P_{es}+P_{er}$	6.40E-15	4.45E-10	1.75E-7	1.03E-3	6.89E-1
									$\bar{P}_{er}$	2.10E-93	1.45E-50	6.19E-29	1.59E-17	3.02E-13

Table 5 Probabilities of Decoding Failure or Decoding Error and Upper Bounds on the Probability of Decoding Error

rate	n_2	k_2	d_2	I_d	E/L	T_{es}	t_2	inner code		bit-error rate				
										$\varepsilon=0.2\times10^{-1}$	$\varepsilon=0.5\times10^{-1}$	$\varepsilon=1\times10^{-1}$	$\varepsilon=2\times10^{-1}$	$\varepsilon=3\times10^{-1}$
0.333	63	42	22	2	E	10	2	$C_1(9)$	$P_{es}+P_{er}$ $\bar{P}_{er}$	3.22E-8 1.25E-58	4.49E-3 2.41E-28	8.74E-1 3.64E-13	1.00E0 4.39E-14	1.00E0 4.61E-16
0.200	15	6	10	1	E	2	0	$C_1(10)$	$P_{es}+P_{er}$ $\bar{P}_{er}$	6.50E-3 9.08E-35	1.17E-1 2.16E-24	6.63E-1 2.14E-17	9.99E-1 3.07E-12	1.00E0 7.31E-11
0.151	31	15	17	1	E	7	2	$C_1(12)$	$P_{es}+P_{er}$ $\bar{P}_{er}$	3.72E-13 5.56E-65	1.34E-7 4.88E-40	1.30E-3 1.80E-23	9.28E-1 7.00E-13	1.00E0 6.68E-13
0.092	63	31	33	1	E	25	2	$C_1(13)$	$P_{es}+P_{er}$ $\bar{P}_{er}$	5.00E-25 ********	3.76E-15 1.15E-117	1.87E-8 2.31E-56	3.67E-2 8.07E-15	1.00E0 6.99E-17