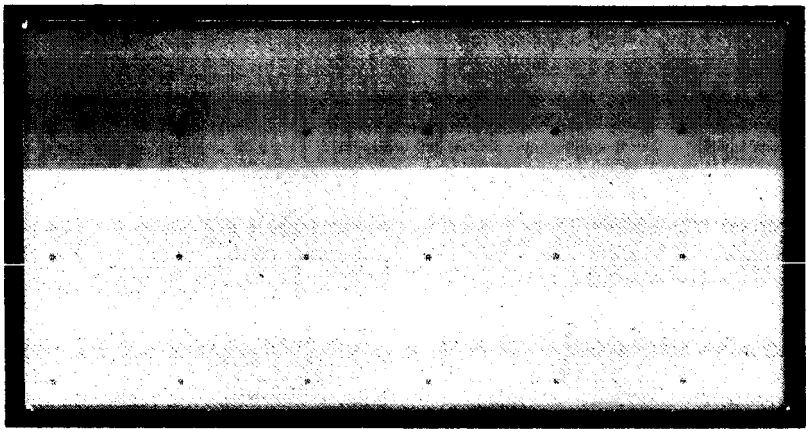
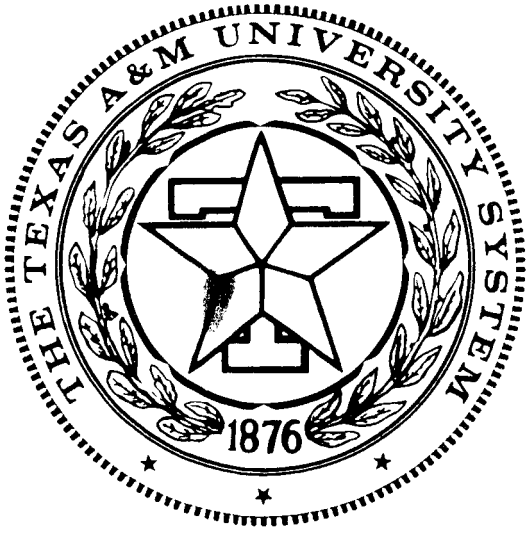
GRANT/GODDARD

IN-35698

P-21

TELECOMMUNICATION and CONTROL SYSTEMS LABORATORY





ELECTRICAL ENGINEERING DEPARTMENT
TEXAS A&M UNIVERSITY
College Station, Texas

PERFORMANCE ANAYLSIS

OF

A CASCADED CODING SCHEME WITH INTERLEAVED OUTER CODE

Technical Report II

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 10, 1986

PERFORMANCE ANALYSIS
OF
A CASCADED CODING SCHEME WITH INTERLEAVED OUTER CODE

Tadao Kasami
Osaka University
Toyonaka, Osaka 560
Japan

Shu Lin
Texas A&M University
College Station, TX 77843
USA

ABSTRACT

In this report, we analyzed a cascaded coding scheme for a random error channel with a bit-error rate ϵ. In this scheme, the inner code C_1 is an $(n_1, m_1\ell)$ binary linear block code which is designed for simultaneous error correction and detection. The outer code C_2 is a linear block code with symbols from the Galois field $GF(2^\ell)$ which is designed for correcting both symbol errors and erasures, and is interleaved with a degree m_1. A procedure for computing the probability of a correct decoding is presented and an upper bound on the probability of a decoding error is derived. The bound provides much better results than our previous bound [1] for a cascaded coding scheme with an interleaved outer code. Example schemes with inner codes ranging from high rates to very low rates are evaluated. Several schemes provide extremely high reliability even for very high bit-error rates say 10^{-1} to 10^{-2}.

1. Introduction

In this paper we investigate a coding scheme for error control for a random error channel with bit-error rate ϵ. 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 $(n_1, m_1\ell)$ code with minimum distance d_1 which is designed to correct t_1 or fewer errors and simultaneously detect $\lambda_1 (\lambda_1 \geq t_1)$ or fewer errors where $t_1 + \lambda_1 + 1 \leq d_1$ [2]. The outer code is an (n_2, k_2) code with symbols from the Galois field $GF(2^\ell)$ and minimum distance d_2. Each code symbol of the outer code is represented by a binary ℓ-tuple (called a ℓ-bit byte) based on a certain basis of $GF(2^\ell)$. The outer code is interleaved with a degree (or depth) m_1.

The encoding is performed in two stages as shown in Figure 1. First a message of $k_2\ell$ binary information digits is divided into k_2 ℓ-bit bytes. Each ℓ-bit byte 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 codeword in C_2. This outer codeword is then temporarily stored in a buffer as a row in an array. After m_1 outer codewords have been formed, the buffer stores a $m_1 \times n_2$ array of code symbols as shown in Figure 2, which is called a segment-array. Each row of a segment-array is called a section. Each column of a segment-array consists of m_1 ℓ-bit bytes (or $m_1\ell$ bits), and is called a segment. There are k_2 data segments and $n_2 - k_2$ parity segments. At the second stage of encoding, each segment of a segment-array is encoded according to the inner code C_1 to form an n_1-bit codeword, which is called a frame. The n_2 frames corresponding to the n_2 segments of a segment-array form a code block. The two-dimensional format of a code block is shown in Figure 3. A code block is transmitted column by column (or frame by frame). In fact each frame is transmitted as soon as it has been formed. Note that the outer code is interleaved with a degree (or depth) m_1.

The decoding for the proposed scheme also consists of two stages, the inner and outer decodings. When a frame in a code 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

as a column in a receiver buffer for the second stage of decoding. 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 segment contains undetected errors. If an uncorrectable error pattern is detected in a received frame, then the erroneous segment is declared to be erased. We call such a segment an erased segment. An erased segment is not necessarily being erased from the received buffer, it is simply ignored during the second stage of decoding (the outer code decoding). After n_2 frames of a received code block have been processed, the decoder buffer contains a $m_1 \times n_2$ decoded segment-array. Each column of this decoded segment-array is either a decoded segment or an erased segment. A decoded segment may contain symbol (or byte) errors which are distributed among the m_1 sections, at most one symbol error in each section. An erased segment creates m_1 symbol erasures, one in each section. Therefore, each section in the decoded segment-array may contain symbol errors and erasures. Now the decoder starts the second stage of decoding, each section is decoded based on the outer code C_2. The outer code is designed to correct both symbol errors and erasures. Maximum distance-separable codes (or Reed-Solomon codes) with symbols from $GF(2^\ell)$ are most effective for this purpose.

Let i be the number of erased segments in a decoded segment-array. If i is greater than a certain pre-designed erasure threshold $T_{es}(T_{es} \leq d_2 - 1)$, the outer code decoder stops the decoding process and declares an erasure (or raises a flag) for the entire segment-array. Otherwise the outer code decoder starts the error-correction operation on each of the m_1 sections. Let t_2 be the designed error-correction capability of the outer code C_2 with

$$t_2 \leq (d_2 - 1 - T_{es})/2. \tag{1}$$

If the syndrome of a section in the decoded segment-array corresponds to an error pattern of i erasures and t_2 or fewer symbol errors, error correction is performed. The values of the erased symbols and the values and locations of symbol errors are determined based on a certain algorithm. If more than t_2 symbol errors are detected, the receiver stops the

decoding process and declares an erasure (or raises a flag) for the entire segment-array. If all the m_1 sections of a segment-array are successfully decoded, then the k_2 decoded data segments are accepted by the receiver and delivered to the user in proper order.

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.

In the next three sections, the error performance of the proposed scheme is analyzed and an upper bound on the probability of a block decoding error is derived. In Section 5, various example schemes are considered and their error probabilities are evaluated. The inner codes being used in these example scheme range from high rates to very low rates. High rate inner codes are suitable for near-earth satellite communications for large file transfer. Low rate inner codes such as biorthogonal codes or the (24,12) Golay code are suitable for low data rate deep space communications. All the example schemes provide extremely high reliabilty even for very high bit-error rates, e.g., 10^{-1} to 10^{-2}.

2. Probabilities Related to the Inner Code Decoding

For $1 \leq u \leq m_1$ and α in $GF(2^\ell)$, let $p_e(u,\alpha)$ be the joint probability that a segment is not erased and the u-th symbol of the segment contains an error whose value is α. Clearly, if $\alpha = 0$, the u-th symbol is error-free. The probability $p_e(u,\alpha)$ can be computed if we know the detail weight distribution of the inner code C_1. A procedure for computing $p_e(u,\alpha)$ is given in Appendix-I.

Let $P_c^{(1)}(u)$, and $P_{er}^{(1)}(u)$ be defined as follows:

$$P_c^{(1)}(u) = p_e(u,o), \tag{2}$$

$$P_{er}^{(1)}(u) = \sum_{\substack{\alpha \epsilon GF(2^\ell) \\ \alpha \neq 0}} p_e(u,\alpha), \tag{3}$$

Clearly, $P_c^{(1)}(u)$ is simply the probability that a segment is not erased and its u-th symbol is error-free; and $P_{er}^{(1)}(u)$ is the probability that a segment is not erased and its u-th symbol is erroneous. Let $P_{es}^{(1)}$ be the probability that a segment is being erased. Then

$$P_c^{(1)}(u) + P_{er}^{(1)}(u) + P_{es}^{(1)} = 1. \tag{4}$$

Once $P_c^{(1)}(u), P_{er}^{(1)}(u)$ and $P_{es}^{(1)}$ are known we can compute the probabilities of a correct decoding and an incorrect decoding for the u-th section of a segment-array. This is done in the next section.

3. Probabilities Related to the Outer Code Decoding

For $1 \leq u \leq m_1$, let $P_c(u), P_{es}(u)$ and $P_{er}(u)$ be the probabilities of a correct decoding, an erasure and an incorrect decoding for the u-th section of a segment -array. Then

$$P_c(u) + P_{es}(u) + P_{er}(u) = 1 \tag{5}$$

and $P_c(u)$ is given by

$$P_c(u) = \sum_{i=0}^{T_{es}} \binom{n_2}{i} \left[P_{es}^{(1)}\right]^i \sum_{j=0}^{t_2} \binom{n_2 - i}{j} \left[P_{er}^{(1)}(u)\right]^j \left[P_c^{(1)}(u)\right]^{n_2-i-j}. \tag{6}$$

In the following, we will derive an upper bound on the error probability $P_{er}(u)$ for decoding the u-th section of a segment-array.

Let us number the segments in a segment-array from 1 to n_2. Suppose 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 $e_f(u)$ be the error symbol at the u-th symbol position of the f-th decoded segment. Note that $e_f(u)$ is the symbol error at the f-th symbol position of the u-th section of a decoded segment-array. Suppose the u-th section of a segment-array is decoded incorrectly. 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 $\bar{v}$. Clearly if $v_f \neq 0$, there is an error at the f-th symbol position of the decoded word $\bar{v}_c + \bar{v}$. Define the following sets associated to $\bar{v}$.

$$W(\bar{v}) \triangleq \{f: \quad v_f \neq 0 \text{ and } f \notin E_s\}, \tag{7}$$

$$H(\bar{v}) \stackrel{\triangle}{=} \{f: \quad e_f(u) \neq 0, v_f = 0 \text{ and } f \notin E_s\}, \tag{8}$$

and

$$J(\bar{v}) \stackrel{\triangle}{=} \{f: \quad e_f(u) = v_f \neq 0 \text{ and } f \notin E_s\}. \tag{9}$$

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

$$|H(\bar{v})| + |W(\bar{v})| - |J(\bar{v})| \leq t_2 \tag{10}$$

where $|M|$ denotes the number of elements in set M.

For given $1 \leq u \leq m_1, \bar{v} \epsilon C_2, E_s \subseteq \{1, 2, \cdots, n_2\}, H \subseteq \{1, 2, \cdots, n_2\}$ 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 induced by the inner code decoding for which $H(\bar{v}) = H$ and $J(\bar{v}) = J$. Then

$$\begin{aligned} P_e(u, E_s, \bar{v}, H, J) = & \left[P_{es}^{(1)}\right]^i \left[P_{er}^{(1)}(u)\right]^h \left[P_c^{(1)}(u)\right]^{n_2 - i - w - h} \\ & \cdot \prod_{f \epsilon J} p_e(u, v_f) \prod_{f \epsilon W(\bar{v}) - J} (1 - P_{es}^{(1)} - p_e(u, v_f)), \end{aligned} \tag{11}$$

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

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 $h + |W| - j \leq t_2$. Let $C_2(W)$ be defined as the following subset of codewords in C_2:

$$C_2(W) \stackrel{\triangle}{=} \{(v_1, v_2, \cdots, v_{n_2}) \epsilon C_2 \quad : \quad v_f \neq 0 \text{ if and only if } f \epsilon E_s \cup W\} \tag{13}$$

Note that, for $\bar{v} \epsilon C_2(W)$, $W(\bar{v}) = W$. Hence $w = |W(\bar{v})| = W$.

Next we want to estimate the following sum:

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

Since $i \leq T_{es}$, it follows from (1) that

$$d_2 \geq i + 2t_2 + 1. \tag{13}$$

Since $d_2 \leq w + i$ and $h + w - j \leq t_2$, we have that

$$j \geq i + w - d_2 \geq 0. \tag{14}$$

Let J' be a subset of J such that

$$|J'| = i + w - d_2. \tag{15}$$

For any $a_f \epsilon GF(2^\ell) - \{0\}$ with $f \epsilon J'$, 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 $C_2(W)$ such that $v_f = v'_f = a_f$ for $f \epsilon J'$. Since the weight of $\bar{v} - \bar{v}'$ is at least d_2, we have that

$$v_f \neq v'_f, \quad \text{for } f \epsilon W \cup E_s - J'. \tag{16}$$

It follows from Schwarz's inequality that

$$\sum_{\bar{v} \epsilon \{\bar{v} \epsilon C_2(W):\ v_f = a_f \text{ for } f \epsilon J'\}} \prod_{f \epsilon J} p_e(u, v_f) \leq \prod_{f \epsilon J'} p_e(u, a_f) \sum_{q=0}^{2^\ell - 2} [p_e(u, \gamma^q)]^{j + d_2 - i - w}, \tag{17}$$

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

$$\sum_{\bar{v} \epsilon C_2(W)} \prod_{f \epsilon J} p_e(u, v_f) \leq \left[P_{er}^{(1)}(u)\right]^{i + w - d_2} \sum_{q=0}^{2^\ell - 2} [p_e(u, \gamma^q)]^{j + d_2 - i - w} \tag{18}$$

Thus we have that

$$\sum_{\bar{v} \epsilon C_2(W)} P_e(u, E_s, \bar{v}, H, J) \leq \left[P_{es}^{(1)}\right]^i \left[P_{er}^{(1)}(u)\right]^{h + i + w - d_2} \left[P_c^{(1)}(u)\right]^{n_2 - i - w - h}$$

$$\cdot \left[1 - P_{es}^{(1)}\right]^{w - j} \sum_{q=0}^{2^\ell - 2} [p_e(u, \gamma^q)]^{j + d_2 - i - w}. \tag{19}$$

Let $\bar{P}(u,i,w,h,j)$ denote the right-hand side of (19). Since $P_{er}(u)$ is the sum of $\sum_{\bar{v}\epsilon C_2(W)} P_e(u,E_s,\bar{v},H,J)$ taken over all possible E_s, W, H and J, we have that

$$P_{er}(u) \leq \sum_{i=0}^{T_{es}} \binom{n_2}{i} \sum_{w=d_2-i}^{n_2-i} \binom{n_2-i}{w} \sum_{h=0}^{\min\{t_2,n_2-i-w\}} \binom{n_2-i-w}{h} \cdot \sum_{j=w+h-t_2}^{w} \binom{w}{j} \bar{P}(u,i,w,h,j). \tag{20}$$

4. Probabilities Related to the Decoding of a Code Block

Let $\bar{P}_c$ be the probability of a correct decoding of the m_1 sections in a segment-array after the inner decoding. Clearly P_c is the probability of a correct block decoding. For a binary m_1-tuple $(a_1, a_2, \cdots, a_{m_1})$, let $P^{(1)}_{e,a_1,\cdots,a_{m_1}}$ denoted the probability that a segment during the inner code decoding is not erased and the u-th symbol of the decoded segment is error-free if and only if $a_u = 0$. A procedure for computing $P^{(1)}_{e,a_1,\cdots,a_{m_1}}$ is given in Appendix-II. 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

$$\left[\sum_{(a_1,a_2,\cdots,a_{m_1})\epsilon\{0,1\}^{m_1}} P^{(1)}_{e,a_1,a_2,\cdots a_{m_1}} X_1^{a_1} X_2^{a_2} \cdots X_{m_1}^{a_{m_1}}\right]^n =$$

$$\sum_{j_1=0}^{n} \sum_{j_2=0}^{n} \cdots \sum_{j_{m_1}=0}^{n} P_{e,j_1,j_2,\cdots,j_{m_1}}(n) X_1^{j_1} X_2^{j_2} \cdots X_{m_1}^{j_{m_1}}. \tag{21}$$

Then P_c is given by

$$P_c = \sum_{i=0}^{T_{es}} \binom{n_2}{i} \sum_{j_1=0}^{t_2} \sum_{j_2=0}^{t_2} \cdots \sum_{j_{m_1}=0}^{t_2} P_{e,j_1,j_2,\cdots,j_{m_1}}(n_2-i). \tag{22}$$

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

Note that an incorrect block decoding occurs if one or more of the m_1 interleaved sections in a segment-array are decoded incorrectly. Hence the probability of an incorrect

block decoding, denoted P_{er}, is bounded above by

$$P_{er} \leq \sum_{u=1}^{m_1} P_{er}(u). \tag{23}$$

It follows from (20) and (23) that we have the following bound on P_{er}:

$$P_{er} \leq \sum_{i=0}^{T_{es}} \binom{n_2}{i} \sum_{w=d_2-i}^{n_2-i} \binom{n_2-i}{w} \cdot \sum_{h=0}^{\min\{t_2, n_2-i-w\}} \binom{n_2-i-w}{h} \sum_{j=w+h-t_2}^{w} \binom{w}{j} \sum_{u=1}^{m_1} \bar{P}(u,i,w,h,j). \tag{24}$$

Let P_{es} denote the probability of a block erasure (decoding failure). Then

$$P_c + P_{er} + P_{es} = 1. \tag{25}$$

From (22) and (25), we can compute

$$P_{er} + P_{es} = 1 - P_c.$$

5. Example Schemes

In this section, fifteen example schemes are considered and their error probabilities are evaluated. In these example schemes, the inner codes range from high rates to very low rates, and the outer codes are Reed-Solomon (RS) (or shortened RS) codes. The inner codes are listed in Table 1 in descending order of the rates. The first five inner codes, $C_1(1)$ to $C_1(5)$ are shortened distance-4 Hamming codes. The next three codes, $C_1(6)$ to $C_1(8)$ are obtained by shortening the even subcodes of primitive BCH codes of length 63. The sixth and seventh codes, $C_1(6)$ and $C_1(7)$, can be decoded with a table look-up decoding. The eighth code $C_1(8)$ is majority-logic decodabe in two steps [2], and its decoder can be implemented easily. $C_1(9)$ is a quadruple-error correcting Goppa code. The tenth code is an extended primitive BCH code. In fact, it is also a Reed-Muller code and is majority-logic decodabe. $C_1(11)$ is the extended (24,12) Golay code which is widely used for satellite and deep space communications. $C_1(12)$, $C_1(14)$ and $C_1(15)$ are low-rate biorthogonal codes (or first-order Reed-Muller codes). $C_1(13)$ is a quadruple-error correcting one-step majority-logic decodabe code [2].

The parameters of the outer codes are given in Tables 2, 3 and 4. The first 10 example schemes and the twelveth example scheme use the same outer code which is the NASA standard (255, 223) Reed-Solomon code with symbols from $GF(2^8)$ and minimum distance 33. However, various erasure and error-correcting threholds are used. Consider the third example scheme (third row of Table 2). The outer code is designed for correcting 22 or fewer symbol erasures and two or fewer symbol errors. The inner code is $C_1(3)$. The total code rate for this scheme is 0.744. The rates of example schemes shown in Table 3 are less than 0.6 and greater than 0.4, and example schemes with lower rates are shown in Table 4. Consider the fifteenth example scheme (the third row of Table 4). The inner code $C_1(14)$ is the (16,5) biorthogonal code which is designed to correct three or fewer bit-errors. The outer code is the (31,15) Reed-Solomon code with symbols from $GF(2^5)$ and minimum distance 17 which is designed for correcting seven or fewer erasures and two or fewer symbol errors. The code rate of this example scheme is 0.151. Let $\bar{P}_{er}$ denote the upper bound on the error probability given by the right-hand side of (24). The bound $\bar{P}_{er}$ for each of the example schemes is computed for various high bit-error rates between 0.5×10^{-2} to 3×10^{-1}. We see that all the example schemes provide extremely high reliability. For example, consider the 3rd example scheme (see Table 2). For bit-error rate $\epsilon = 0.5 \times 10^{-2}$, the scheme has an error probability upper bounded by 3.82×10^{-24}! The probability of a decoding failure (or erasure) is 2.35×10^{-3} i.e., there are less than 3 erasures in a thousand transmitted code blocks. If the 5-th example scheme (see Table 2) is used, the error probability is less than 1.72×10^{-39} for bit-error rate $\epsilon = 0.5 \times 10^{-2}$, and the decoding failure is 1.50×10^{-4}! The high-rate example schemes are suitable for high date rate near earth satellite communications for large file transfer.

The low-rate example schemes are suitable for low-data rate deep space communications. For example, consider the 16-th example scheme (see Table 4). For bit-error rate ϵ as high as 10^{-1}, the error probability is less than 2.23×10^{-42}, and the probability of a block erasure is 1.87×10^{-8} (less than 2 erasures in one hundred million transmitted code blocks). For bit-error rate $\epsilon = 0.5 \times 10^{-1}$, the error probability is less than 8.30×10^{-92}, and the probability of a block erasure is 3.76×10^{-15}! Suppose the data rate is 100 kps.

With a bit-error rate $\epsilon = 0.5 \times 10^{-1}$, it will take many million years to have a block erasure!

APPENDIX-I

A Procedure for Computing $p_e(u,\alpha)$

For $1 \leq u \leq m_1, 0 \leq i \leq n_1 - \ell$ and $\alpha \epsilon GF(2^\ell)$ let $A_i^{(1)}(u,\alpha)$ be the number of codewords in C_1 whose u-th symbol (or ℓ-bit byte) is α and whose binary weight excluding the u-th symbol is i. Let $C_1^\perp$ denote the dual code of C_1. Similarly, let $B_i^{(1)}(u,\alpha)$ be the number of codewords in $C_1^\perp$ whose u-th symbol is α and whose binary wieght 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 representation of α.

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 $W_{j,s}^{(i)}(n)$ is

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

It follows from the definition of $p_e(u,\alpha)$ that

$$\begin{aligned} p_e(u,\alpha) = \sum_{i=0}^{n_1-\ell} A_i^{(1)}(u,\alpha) \sum_{j=0}^{n_1-\ell} \sum_{j'=0}^{\ell} \\ \cdot \sum_{s=0}^{t_1} \sum_{s'=0}^{t_1-s} W_{j,s}^{(i)}(n_1-\ell) \\ \cdot W_{j',s'}^{(|\alpha|)}(\ell) \epsilon^{s+s'}(1-\epsilon)^{n_1-s-s'}. \end{aligned} \qquad (I-2)$$

For relatively small k_1, say less than 25, the weight distribution

$$\{A_i^{(1)}(u,\alpha) \quad : \quad 0 \leq i \leq n_1 - \ell\}$$

for an α in $GF(2^\ell)$ can be computed by generating $2^{k_1-\ell}$ codewords of C_1.

For $k_1 > n_1 - k_1$, it is easier to compute $p_e(u,\alpha)$ by generating the weight distribution

$$\{B_h^{(1)}(u,\alpha) \quad : \quad 0 \leq h \leq n_1 - \ell\}.$$

Using the generalized MacMillians' identity [3, p 147], we have

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

$$\cdot P_i(h, n_1-\ell) \prod_{f=1}^{\ell} P_{\alpha_f}(\beta_f, 1). \qquad (I-3)$$

where $P_i(\cdot,\cdot)$ is a Krawtchouk polynomial [3, p. 129] whose generating function is

$$\sum_{s=0}^{n} P_s(i,n) Y^s = (1+Y)^{n-i}(1-Y)^i \qquad (I-4)$$

From this identity, we have

$$\prod_{f=1}^{\ell} P_{\alpha_f}(\beta_f, 1) = (-1)^{(|\alpha|+|\beta|-|\alpha+\beta|)/2} \qquad (I-5)$$

and

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

$$= (1+X)^{n_1-\ell-h}(1-X)^h(1+Y)^{n_1-\ell-h}(1-Y)^h. \qquad (I-6)$$

It follows from (I-1), (I-3), (I-5) and (I-6) that

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

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

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

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

$$\cdot(1+X)^{n_1-\ell-h}(1-X)^h \sum_{s=0}^{n_1} Q'_s(h, n_1-\ell, |\alpha|, \ell, X) Y^s, \qquad (I-7)$$

where

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

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

Taking the terms on both sides of (I-7) for which the degree of Y is t_1 or less, substituting $\epsilon/(1-\epsilon)$ for X and 1 for Y and multiplying both sides by $(1-\epsilon)^{n_1}$, we obtain the following formula from (I-2):

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

$$\cdot \sum_{s=0}^{t_1} Q'_s(h, n_1-\ell, |\alpha|, \ell, \epsilon/(1-\epsilon))$$

$$\cdot \sum_{\beta \epsilon GF(2^\ell)} B_h^{(1)}(u,\beta)(-1)^{(|\alpha|+|\beta|-|\alpha+\beta|)/2}.$$

If C_1 is a shortened cyclic code, $\min\{\ell, n_1-k_1\}$ columns of a generator matrix corresponding to the u-th symbol position are linearly independent, and for a symbol β,

$$\{B_h^{(1)}(u,\beta) \quad : \quad 0 \le h \le n_1-\ell\}$$

can be found by generating $2^{n_1-k_1-\ell}$ codewords of the dual code $C_1^{\perp}$ of C_1.

APPENDIX II

A Procedure for Computing $P^{(1)}_{e,a_1,\cdots,a_{m_1}}$

Let H be a subset of $\{1,2,\cdots,m_1\}$. Let $P_e^{(1)}(H)$ be the probability that a segment is not erased and for $h \epsilon H$, the h-th ℓ-bit byte of the decoded segment is error free. In [1], a formula for computing $P^{(1)}(H)$ was derived. $P^{(1)}(H)$ can be computed if $\min\{k_1, n_1 - k_1\}$ is relatively samll, say less than 25. For small m_1, say less than 11,

$$\{P^{(1)}(H) \quad : \quad H \subseteq \{1,2,\cdots,m_1\}\}$$

can be found. Then it follows from the principle of inclusion and exclusion that

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

where

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

REFERENCES

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

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

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

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	$(1+X)(1+X^3+X^7)$
$C_1(3)$	shortened Hamming code	(47,40)	0.851	8	5	4	1	$(1+X)\phi_1(X)$
$C_1(4)$	shortened Hamming code	(48,40)	0.833	8	5	4	1	$(1+X)(1+X^3+X^7)$
$C_1(5)$	shortened Hamming code	(30,24)	0.800	8	3	4	1	$(1+X)(1+X^2+X^5)$
$C_1(6)$	shortened BCH code	(61,48)	0.787	8	6	6	2	$(1+X)\phi_1(X)\phi_3(X)$
$C_1(7)$	shortened BCH code	(53,40)	0.755	8	5	6	2	$(1+X)\phi_1(X)\phi_3(X)$
$C_1(8)$	shortened BCH code	(59,40)	0.678	8	5	8	3	$(1+X)\phi_1(X)\phi_3(X)\phi_5(X)$
$C_1(9)$	Goppa code	(64,40)	0.625	8	5	9	4	
$C_1(10)$	extended BCH code	(32,16)	0.500	8	2	4	3	
$C_1(11)$	extended Golay code	(24,12)	0.500	6	2	8	3	
$C_1(12)$	biorthogonal code	(8, 4)	0.500	4	1	4	1	
$C_1(13)$	shortened Type 0 DTI code	(51,24)	0.471	8	3	10	4	$(1+X)\phi_1(X)\phi_3(X)\phi_5(X)$ $\cdot\phi_7(X)\phi_{21}(X)$
$C_1(14)$	biorthogonal code	(16, 5)	0.313	5	1	8	3	
$C_1(15)$	biorthogonal code	(32, 6)	0.188	6	1	16	7	

The generator polynomials are shown only for the shortened cyclic codes, and $\phi_1(X)$ 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 Cascades Codes with (255,223) RS Outer Codes

Rate	n_2	k_2	d_2	I_d	E/L	T_{es}	t_2	Inner code		bit-error rate $\epsilon = 0.2 \times 10^{-2}$	$\epsilon = 0.5 \times 10^{-2}$	$\epsilon = 1 \times 10^{-2}$	$\epsilon = 2 \times 10^{-2}$	$\epsilon = 3 \times 10^{-2}$
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	21	2	$C_1(2)$	$P_{es} + P_{er}$	8.35E-7	1.75E-3	8.50E-1	1.00E0	——
									$\bar{P}_{er}$	6.22E-49	1.11E-24	1.45E-13	5.09E-20	——
0.744	255	223	33	5	E	22	2	$C_1(3)$	$P_{es} + P_{er}$		2.35E-3	3.72E-1	1.00E0	1.00E0
									$\bar{P}_{er}$		3.82E-24	6.87E-11	9.67E-11	8.15E-22
0.729	255	223	33	5	E			$C_1(4)$	$P_{es} + P_{er}$					
									$\bar{P}_{er}$					
0.700	255	233	33	3	E	20	2	$C_1(5)$	$P_{es} + P_{er}$	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	233	33	6	E	21	2	$C_1(6)$	$P_{es} + P_{er}$	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	$C_1(7)$	$P_{es} + P_{er}$	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 3 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 $\epsilon = 1 \times 10^{-2}$	$\epsilon = 2 \times 10^{-2}$	$\epsilon = 3 \times 10^{-2}$	$\epsilon = 4 \times 10^{-2}$	$\epsilon = 5 \times 10^{-2}$
0.593	255	223	33	5	E	21	3	$C_1(8)$	$P_{es} + P_{er}$	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	$C_1(9)$	$P_{es} + P_{er}$	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	$C_1(10)$	$P_{es} + P_{er}$	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	$C_1(13$	$P_{es} + P_{er}$	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	1.59-17	3.02E-13
0.333	63	42	22	2	E	16	2	$C_1(11)$	$P_{es} + P_{er}$	1.72E-12	3.22E-8	7.89E-6	3.17E-4	4.49E-3
									$\bar{P}_{er}$	5.51E-69	2.00E-45	2.05E-32	8.77E-24	1.29E-17

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 $\epsilon = 0.2 \times 10^{-1}$	$\epsilon = 0.5 \times 10^{-1}$	$\epsilon = 1 \times 10^{-1}$	$\epsilon = 2 \times 10^{-1}$	$\epsilon = 3 \times 10^{-1}$
0.246	63	31	33	2	E	21	2	$C_1(11)$	$P_{es} + P_{er}$	3.22E-8	4.49E-3	7.98E-1	1.00E0	1.00E0
									$\bar{P}_{er}$	4.79E-87	5.81E-42	2.89E-17	2.92E-11	2.84E-12
0.233	15	7	9	1	E	2	0	$C_1(12)$	$P_{es} + P_{er}$	6.50E-3	1.17E-1	6.63E-1	9.99E-1	1.00E0
									$\bar{P}_{er}$	4.12E-30	6.92E-21	9.50E-15	1.88E-10	1.51E-9
0.151	31	15	17	1	E	7	2	$C_1(14)$	$P_{es} + P_{er}$	3.72E-13	1.34E-7	1.30E-3	9.28E-1	1.00E0
									$\bar{P}_{er}$	5.56E-65	4.88E-40	1.80E-23	7.00E-13	6.68E-13
0.110	63	37	27	1	E	20	2	$C_1(15)$	$P_{es} + P_{er}$		3.76E-15	1.87E-8	3.09E-1	1.00E0
									$\bar{P}_{er}$		8.30E-92	2.23E-42	5.59E-11	2.68E-18