

## General Disclaimer

### One or more of the Following Statements may affect this Document

- This document has been reproduced from the best copy furnished by the organizational source. It is being released in the interest of making available as much information as possible.
- This document may contain data, which exceeds the sheet parameters. It was furnished in this condition by the organizational source and is the best copy available.
- This document may contain tone-on-tone or color graphs, charts and/or pictures, which have been reproduced in black and white.
- This document is paginated as submitted by the original source.
- Portions of this document are not fully legible due to the historical nature of some of the material. However, it is the best reproduction available from the original submission.

PROBABILITY OF UNDETECTED ERROR AFTER DECODING  
FOR A CONCATENATED CODING SCHEME

Technical Report

to

NASA  
Goddard Space Flight Center  
Greenbelt, Maryland

(NASA-CR-173837) PROBABILITY OF UNDETECTED  
ERROR AFTER DECODING FOR A CONCATENATED  
CODING SCHEME (Illinois Univ.) 25 p  
HC A02/MF A01

N84-31992

CSCL 12A

Unclass

G3/64 20154

Grant Number NAG 5-234

Principal Investigators

Daniel J. Costello, Jr.  
Department of Electrical Engineering  
Illinois Institute of Technology  
Chicago, Illinois 60616

Shu Lin  
Department of Electrical Engineering  
University of Hawaii at Manoa  
2540 Dole Street  
Honolulu, Hawaii 96822

July 23, 1984



PROBABILITY OF UNDETECTED ERROR AFTER DECODING  
FOR A CONCATENATED CODING SCHEME

Tadao Kasami  
Osaka University  
Toyonaka, Osaka, Japan

Shu Lin  
University of Hawaii at Manoa  
Honolulu, Hawaii 96822

ABSTRACT

In this paper, a concatenated coding scheme for error control in data communications is analyzed. In this scheme, the inner code is used for both error correction and detection, however the outer code is used only for error detection. A retransmission is requested if the outer code detects the presence of errors after the inner code decoding. Probability of undetected error is derived and bounded. A particular example, proposed for NASA telecommand system is analyzed.

## 1. Introduction

Consider a concatenated coding scheme for error control for a binary symmetric channel with bit-error-rate  $\epsilon < 1/2$  as shown in Figure 1. Two linear block codes,  $C_f$  and  $C_b$ , are used. The inner code  $C_f$ , called frame code, is an  $(n, k)$  code with minimum distance  $d_f$ . The frame code is designed to correct  $t$  or fewer errors and simultaneously detect  $\lambda$  ( $\lambda > t$ ) or fewer errors where  $t + \lambda + 1 \leq d_f$ . The outer code  $C_b$  is an  $(n_b, k_b)$  code with minimum distance  $d_b$  and

$$n_b = mk ,$$

where  $m$  is a positive integer. The outer code is designed for error detection only.

The encoding is done in two stages. A message of  $k_b$  bits is first encoded into a codeword of  $n_b$  bits in the outer code  $C_b$ . Then the  $n_b$ -bit word is divided into  $m$   $k$ -bit segments. Each  $k$ -bit segment is encoded into an  $n$ -bit word in the frame code  $C_f$ . This  $n$ -bit word is called a frame. Thus, corresponding to each  $k_b$ -bit message at the input of the outer code encoder, the output of the frame code encoder is a sequence of  $m$  frames. This sequence of  $m$  frames is called a block. A two dimensional block format is depicted in Figure 2.

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

be error free and are accepted (with the  $n_b - k_b$  parity bits removed) by the receiver. If the presence of errors is detected, the  $m$  decoded segments are discarded and the receiver requests a retransmission of the rejected block. Retransmission and decoding process continues until a transmitted block is successfully received. Note that a successfully received block may be either error free or contains undetectable errors.

The error control scheme described above is actually a combination of forward-error-correction (FEC) and automatic-repeat-request (ARQ), called a hybrid ARQ scheme [1]. The retransmission strategy determines the system throughput, it may be one of the three basic modes namely, stop-and-wait, go-back-N or selective-repeat. In this paper, we are only concerned with the reliability of the proposed error control scheme. The reliability is measured in terms of the probability of undetected error after decoding. The probability of undetected error is derived and bounded.

An example scheme, proposed for NASA telecommand operation, is analyzed.

## 2. Probability of Undetected Error for the Frame Code

For a codeword  $\bar{v}$  in the frame code  $C_f$ , let  $w(\bar{v})$ ,  $w^{(1)}(\bar{v})$  and  $w^{(2)}(\bar{v})$  denote the weight of  $\bar{v}$ , the weight of the information-part of  $\bar{v}$  and the weight of parity-part of  $\bar{v}$  respectively. Clearly  $w(\bar{v}) = w^{(1)}(\bar{v}) + w^{(2)}(\bar{v})$ . If a decoded frame contains an undetectable error pattern, this error pattern must be a nonzero codeword in  $C_f$  [1-3]. Let  $\bar{e}_0$  be a nonzero error pattern after decoding. Since  $\bar{e}_0$  is a word in  $C_f$ , we have

$$w^{(1)}(\bar{e}_0) + w^{(2)}(\bar{e}_0) \geq d_f, \quad (1)$$

and

$$w^{(1)}(e_0) \geq 1. \quad (2)$$

The probability  $P_f(\bar{e}_0, \epsilon)$  that a decoded frame contains a nonzero error vector  $\bar{e}_0$  after decoding is given by [2,4,5],

$$P_f(\bar{e}_0, \epsilon) = \sum_{i=0}^t \sum_{j=0}^{\min(t-i, n-w)} \binom{w}{i} \binom{n-w}{j} \epsilon^{w-i+j} (1-\epsilon)^{n-w+i-j}, \quad (3)$$

where  $w = w(\bar{e}_0)$ .

In the following we will derive an upper bound on  $P_f(\bar{e}_0, \epsilon)$ . Let  $Q_t(w, \epsilon)$  denote the right-hand side of (3). For  $w \leq n-1-j$ ,

$$\frac{\binom{w+1}{i} \binom{n-w-1}{j} \epsilon^{w+1-i+j} (1-\epsilon)^{n-w-1+i-j}}{\binom{w}{i} \binom{n-w}{j} \epsilon^{w-i+j} (1-\epsilon)^{n-w+i-j}} = \frac{(w+1)(n-w-j)\epsilon}{(w+1-i)(n-w)(1-\epsilon)} \leq \frac{(w+1)\epsilon}{(w+1-t)(1-\epsilon)}. \quad (4)$$

Since  $w \geq 2t+1$ , we have that

$$\frac{w+1}{w+1-t} \leq \frac{2t+2}{t+2}. \quad (5)$$

It follows from (4) and (5) that, for  $\epsilon \leq \frac{t+2}{3t+4}$ ,

$$Q_t(w+1, \epsilon) \leq Q_t(w, \epsilon). \quad (6)$$

For a positive integer  $i$ , define  $\beta(i)$  as follows:

(1) If the frame code  $C_f$  is an even-weight code, then

$$\beta(i) = \begin{cases} d_f, & \text{for } i \leq d_f \\ i, & \text{for even } i \text{ and } i > d_f \\ i+1, & \text{otherwise.} \end{cases}$$

(2) If  $C_f$  is not an even-weight code, then

$$\beta(i) = \max(d_f, i).$$

For a nonzero error pattern  $\bar{e}_0$  which is a codeword in  $C_f$ , we see that

$$w(\bar{e}_0) \geq \beta(w^{(1)}(\bar{e}_0)). \quad (7)$$

It follows from (3), (6) and (7) that, for  $0 \leq \epsilon \leq (t+2)/(3t+4)$ ,

$$Q_t(w(\bar{e}_0), \epsilon) \leq Q_t(\beta(w^{(1)}(\bar{e}_0)), \epsilon). \quad (8)$$

For  $\epsilon \ll 1/n$ , we can see from (3) and (8) that

$$P_f(\bar{e}_0, \epsilon) \leq \binom{\beta(w^{(1)}(\bar{e}_0))}{t} \epsilon^{\beta(w^{(1)}(\bar{e}_0)) - t} (1 - \epsilon)^{n - \beta(w^{(1)}(\bar{e}_0)) + t} . \quad (9)$$

### 3. Probability of Undetected Error for the Outer Code

Recall that a codeword in the outer code  $C_b$  consists of  $m$   $k$ -bit segments. At the receiver, error detection is performed on every  $m$  decoded segments based on  $C_b$ . Let  $P_b(\bar{e}, \epsilon)$  denote the probability that the decoded word contains an undetectable error pattern  $\bar{e}$  (a nonzero codeword in  $C_b$ ). For a codeword  $\bar{v}$  in  $C_b$ , let  $\bar{v}^{(j)}$  denote the  $j$ -th segment of  $\bar{v}$ , and let  $w_j(\bar{v})$  be the weight of the codeword in frame code  $C_f$  into which  $\bar{v}^{(j)}$  is encoded. Then it follows from (3) that for an undetectable error pattern  $\bar{e}$  in a block

$$P_b(\bar{e}, \epsilon) = \prod_{j=1}^m Q_t(w_j(\bar{e}), \epsilon) . \quad (10)$$

Let  $P_{ud}^{(b)}(\epsilon)$  be the probability of undetected error for the outer code  $C_b$ . Then

$$P_{ud}^{(b)}(\epsilon) = \sum_{\bar{e} \in C_b - \{\bar{0}\}} P_b(\bar{e}, \epsilon) . \quad (11)$$

For  $1 \leq j_1 < j_2 < \dots < j_h \leq m$ , consider the set of codewords in  $C_b$  where nonzero bits are confined in the  $j_1$ -th segment, the  $j_2$ -th segment, ..., and the  $j_h$ -th segment. This set of codewords forms a subcode of  $C_b$ , call a  $(j_1, j_2, \dots, j_h)$ -subcode of  $C_b$  and denoted by  $C_b(j_1, j_2, \dots, j_h)$ . If  $C_b$  is a cyclic or shortened cyclic code, then

- (1) for  $h=1$ , all  $(j_1)$ -subcodes of  $C_b$  are equivalent;
- (2) for  $h \geq 2$ , all  $(j_1, j_2, \dots, j_h)$ -subcodes of  $C_b$  with the same  $j_2 - j_1, j_3 - j_2, \dots, j_h - j_{h-1}$  are equivalent codes and are called  $h$ -segment  $(j_2 - j_1, j_3 - j_2, \dots, j_h - j_{h-1})$  subcodes of  $C_b$ .

Consider a  $(j_1, j_2, \dots, j_h)$ -subcode of  $C_b$ . Let  $i_1, i_2, \dots, i_h, r_1, r_2, \dots, r_h$  be a set of integers for which  $0 \leq i_q \leq k$  and  $0 \leq r_q \leq n - k$  with  $1 \leq q \leq h$ . Let  $A_{(i_1, r_1), (i_2, r_2), \dots, (i_h, r_h)}^{j_1, j_2, \dots, j_h}$  denote the number of codewords  $\bar{v}$  in  $C_b(j_1, j_2, \dots, j_h)$

such that, for  $1 \leq q \leq h$ , the  $j_q$ -th segment  $\bar{v}^{(j_q)}$  of  $\bar{v}$  has weight  $i_q$  and  $w_{j_q}(\bar{v}) = i_q + r_q$ . Then it follows from (10), (11) and the definition of

$A^{j_1, j_2, \dots, j_h}(i_1, r_1), (i_2, r_2), \dots, (i_h, r_h)$  that

$$P_{ud}^{(b)}(\epsilon) = \sum_{h=1}^m Q_t(0, \epsilon)^{m-h} \left\{ \sum_{1 \leq j_1 < j_2 < \dots < j_h \leq m} \sum_{IR_h}^{j_1, j_2, \dots, j_h} A^{j_1, j_2, \dots, j_h}(i_1, r_1), (i_2, r_2), \dots, (i_h, r_h) \prod_{q=1}^h Q_t(i_q + r_q, \epsilon) \right\}, \quad (12)$$

where

$$IR_h = \left\{ ((i_1, r_1), (i_2, r_2), \dots, (i_h, r_h)) : \begin{array}{l} 1 \leq i_q \leq k, \\ 0 \leq r_q \leq n-k, d_f \leq i_q + r_q (1 \leq q \leq h) \text{ and } d_b \leq \sum_{q=1}^h i_q \leq n_b \end{array} \right\}.$$

If  $C_b$  is a cyclic or shortened cyclic code, then Eq. (12) can be simplified as follows:

$$P_{ud}^{(b)}(\epsilon) = \sum_{h=1}^m Q_t(0, \epsilon)^{m-h} \left\{ \sum_{1 \leq j_1 < j_2 < \dots < j_h \leq m} \binom{m-j_h+1}{m-j_h+1} \cdot \sum_{IR_h}^{j_1, j_2, \dots, j_h} A^{j_1, j_2, \dots, j_h}(i_1, r_1), (i_2, r_2), \dots, (i_h, r_h) \prod_{q=1}^h Q_t(i_q + r_q, \epsilon) \right\}. \quad (13)$$

From (12) we see that, if we know the detail weight structure of  $C_b(j_1, j_2, \dots, j_h)$ , the error probability  $P_{ud}^{(b)}(\epsilon)$  can be computed. However, for a given  $C_b$ , it is not easy to find  $A^{j_1, j_2, \dots, j_h}(i_1, r_1), (i_2, r_2), \dots, (i_h, r_h)$ . To overcome this difficulty, we will drive upper bounds on the terms on the right-hand side of (13). We assume that  $\epsilon \leq (t+2)/(3t+4)$ . It follows from (8) that

$$\begin{aligned} & \sum_{r_1=0}^{n-k} \sum_{r_2=0}^{n-k} \dots \sum_{r_h=0}^{n-k} A^{j_1, j_2, \dots, j_h}(i_1, r_1), (i_2, r_2), \dots, (i_h, r_h) \prod_{q=1}^h Q_t(i_q + r_q, \epsilon) \\ & \leq A^{j_1, j_2, \dots, j_h}(i_1, i_2, \dots, i_h) \prod_{q=1}^h Q_t(\beta(i_q), \epsilon), \end{aligned} \quad (14)$$



where

$$A_{i_1, i_2, \dots, i_h}^{j_1, j_2, \dots, j_h} = \sum_{r_1=0}^{n-k} \sum_{r_2=0}^{n-k} \dots \sum_{r_h=0}^{n-k} A^{j_1, j_2, \dots, j_h}(i_1, r_1), (i_2, r_2), \dots, (i_h, r_h)$$

Since the check bits are uniquely determined by the information bits,

$A_{i_1, i_2, \dots, i_h}^{j_1, j_2, \dots, j_h}$  is the number of codewords in  $C_b(j_1, j_2, \dots, j_h)$  whose weight in the  $j_q$ -th segment is  $i_q$  for  $1 \leq q \leq h$ .

For a nonzero codeword  $\bar{v}$  in  $C_b$ , we define the weight configuration of  $\bar{v}$  as the sequence of nonzero weights of component segments of  $\bar{v}$ , arranged in ascending order. For an undetectable error pattern  $\bar{e}$  with weight configuration  $(i_1, i_2, \dots, i_h)$ , it follows from (8) and (10) that

$$P_b(\bar{e}, \epsilon) \leq \prod_{q=1}^h Q_t(\beta(i_q), \epsilon) \quad (15)$$

Consequently we have the following upper bound on  $P_{ud}^{(b)}(\epsilon)$ ,

$$P_{ud}^{(b)}(\epsilon) \leq \sum_{\bar{e} \in C_b - \{0\}} \prod_{q=1}^h Q_t(\beta(i_q), \epsilon) .$$

#### 4. Example

Consider the concatenated coding scheme proposed for NASA telecommand system in which both inner (frame) code and outer code are shortened Hamming codes. The frame code  $C_f$  is a distance-4 Hamming code with generator polynomial,

$$\bar{g}(X) = (X+1)(X^6+X+1) = X^7+X^6+X^2+1 ,$$

where  $X^6+X+1$  is a primitive polynomial of degree 6. The maximum length of this code is 63. This code is used for single error correction. The code is capable of detecting all the error patterns of double and odd number errors. The outer code is also a distance-4 shortened Hamming code with generator polynomial,

$$\begin{aligned}\bar{g}(X) &= (X+1)(X^{15}+X^{14}+X^{13}+X^{12}+X^4+X^3+X^2+X+1) \\ &= X^{16}+X^{12}+X^5+1,\end{aligned}$$

where  $X^{15}+X^{14}+X^{13}+X^{12}+X^4+X^3+X^2+X+1$  is a primitive polynomial of degree 15. This code is the X.25 standard for packet-switched data networks [6]. The natural length of this code is  $2^{15}-1 = 32,767$ . But the maximum length of  $n_b$  being considered is 3,584 bits. We assume that the number of frames in a block is greater than 3 and less than 65. The 16 parity bits of this code is used for error detection only.

It follows from (9) and (15) that the smallest power of  $\epsilon$  in the right-hand side of (15), denoted  $O_\epsilon(\bar{e})$  is

$$O_\epsilon(\bar{e}) = \sum_{q=1}^h \beta(i_q) - th, \quad (16)$$

which is called the order of  $\bar{e}$ .

To evaluate  $P_{ud}^{(b)}(\epsilon)$ , we need to know those error patterns  $\bar{e}$  for which  $O_\epsilon(\bar{e})$  is small. The weight configurations of error patterns for which  $O_\epsilon(\bar{e})$  is less than 10 are listed in Table 1. The order of an error pattern  $\bar{e}$ ,  $O_\epsilon(\bar{e})$ , is at least

$$w(\bar{e}) - \lfloor w(\bar{e})/4 \rfloor, \quad (17)$$

which occurs for the weight configuration

$$(4, 4, \dots, 4, w(\bar{e}) - 4\lfloor w(\bar{e})/4 \rfloor + 4),$$

where  $\lfloor x \rfloor$  denotes the largest integer no greater than  $x$ .

Suppose that  $n \geq 7$  and

$$\epsilon \leq 1/2n. \quad (18)$$

Then  $(1-\epsilon)^n \geq 1/2$  and  $(1-\epsilon)/\epsilon \geq 13$ . Note that

$$Q_1(w, \epsilon)^{1/w} = \frac{\epsilon}{1-\epsilon} \left[ \frac{w(1-\epsilon)^{n+1}}{\epsilon} \right]^{1/w} \left[ 1 + \frac{\epsilon}{w(1-\epsilon)} + \frac{n-w}{w} \left( \frac{\epsilon}{1-\epsilon} \right)^2 \right]^{1/w}, \quad (19)$$

which decreases monotonically as  $w$  increases for  $4 \leq w \leq n$ . Hence

$$Q_1(w', \epsilon)^{1/w'} \leq Q_1(w, \epsilon)^{1/w}, \quad (20)$$

for  $4 \leq w \leq w' \leq n$ . It is easy to check that

$$Q_1(4, \epsilon) \leq Q_1(6, \epsilon)^{1/2}. \quad (21)$$

and that

$$Q_1(4, \epsilon)Q_1(8, \epsilon) \leq Q_1(6, \epsilon)^2. \quad (22)$$

It follows from (15), (20), (21) and (22) that

1) for an error pattern  $\bar{e}$  in an  $h$ -segment subcode with  $h \geq 3$ ,

$$P_b(\bar{e}, \epsilon) \leq Q_1(4, \epsilon)^3; \quad (23)$$

2) for an error pattern  $\bar{e}$  of weight 12 whose weight configuration is not (4,4,4),

$$P_b(\bar{e}, \epsilon) \leq Q_1(6, \epsilon)^2; \quad (24)$$

3) for any nonzero error pattern  $\bar{e}$ ,

$$P_b(\bar{e}, \epsilon) \leq \begin{cases} Q_1(4, \epsilon)^{w(\bar{e})/4}, & \text{if } w(\bar{e}) \text{ is a multiple of } 4, \\ Q_1(4, \epsilon)^{\lfloor w(\bar{e})/4 \rfloor - 1} Q_1(6, \epsilon), & \text{otherwise.} \end{cases} \quad (25)$$

Now we will consider how to evaluate  $P_{ud}^{(b)}(\epsilon)$  of (13). For  $4 \leq i \leq n-4$  and  $0 \leq r \leq n-i$ ,  $A_{(i,r)}^1$  can be computed as is shown in Appendix. We found that for  $n \leq 63$

$$A_{(4,0)}^1 = A_{(6,0)}^1 = 0, \quad (26)$$

and that for  $n \leq 39$

$$A_{(8,0)}^1 = 0. \quad (27)$$

On the other hand, it is time-consuming to obtain  $A_{(i_1, r_1), (i_2, r_2), \dots, (i_h, r_h)}^{1, j_2, \dots, j_h}$  for  $i_i \geq 2$ . However it is not difficult to compute  $A_{i_1, i_2}^{1, j_2}$  for  $2 \leq j_2 \leq m$  as is shown in the Appendix. The weight  $A_{i_1, i_2}^{1, j_2}$  can be computed from the weights of the dual

ORIGINAL PAGE IS  
OF POOR QUALITY

code of the 2 segment ( $j_2-1$ ) subcode of  $C_b$ . Since it is time-consuming to obtain  $A_{i_1, i_2, \dots, i_h}^{1, j_2, \dots, j_h}$  for  $h \geq 3$ , we will use some upper bounds on  $P_b(\bar{e}, \epsilon)$ .

Let  $\{A_i^{(b)}\}$  be the weight distribution of the outer code  $C_b$ .  $\{A_i^{(b)}\}$  can be computed from the weight distribution of the dual code of  $C_b$  (see Appendix).

Then it follows from (13), (14) and (23) that we have the following bounds:

$$\sum_{\substack{w(\bar{e}) \leq 10 \\ \bar{e} \text{ is in a} \\ \text{one segment subcode}}} P_b(\bar{e}, \epsilon) \leq m \sum_{i=4}^{10} \sum_{r=0}^6 A_{(i,r)}^1 Q_1(i+r, \epsilon), \quad (28)$$

$$\sum_{\substack{w(\bar{e}) \leq 10 \\ \bar{e} \text{ is in a} \\ \text{2-segment subcode}}} P_b(\bar{e}, \epsilon) \leq \sum_{2 \leq j \leq m} (m-j+1) \sum_{\substack{i_1+i_2 \leq 10 \\ i_1, i_2 \geq 1}} A_{i_1, i_2}^{1, j} \prod_{p=1}^2 Q_1(\beta(i_p), \epsilon), \quad (29)$$

$$\sum_{\substack{w(\bar{e}) \leq 10 \\ \bar{e} \text{ is in an} \\ \text{h-segment subcode} \\ \text{with } h \geq 3}} P_b(\bar{e}, \epsilon) \leq \left( \sum_{i=2} (A_{2i}^{(b)} - mA_i^1) - \sum_{j=2}^m (m-j+1) \sum_{1 \leq i_1, i_2 \leq 10} A_{i_1, i_2}^{1, j} \right) Q_1(4, \epsilon)^3. \quad (30)$$

It can be shown that the following inequalities hold:

$$A_{4,4,4}^{1, j_1, j_2} \leq \binom{k}{3} \binom{k}{4}^2, \quad (31)$$

$$A_i^{(b)} \leq \binom{n_b}{i}, \quad (32)$$

$$\sum_{i=25}^{n_b} \binom{n_b}{i} Q_1(4, \epsilon)^{i/4} \leq (26/n_b)^{-26} (1-26/n_b)^{-(n_b-26)} Q_1(4, \epsilon)^{26/4}, \quad (33)$$

(the third inequality is obtained by using Chernoff inequality [7]).

It follows from (24), (25) and (31) that

$$\sum_{w(\bar{e})=12} P_b(\bar{e}, \epsilon) \leq A_{12}^{(b)} Q_1(6, \epsilon)^2 + \min \left\{ \binom{m}{3} \binom{k}{4}^2 \binom{k}{3}, A_{12}^{(b)} \right\} Q_1(4, \epsilon)^3 \quad (34)$$

Using the inequalities of (25), (32) and (33), we have

$$\sum_{w(\bar{e}) \geq 14} P_b(\bar{e}, \epsilon) \leq \sum_{i=4}^6 A_{4i}^{(b)} Q_1(4, \epsilon)^i + \sum_{i=3}^5 A_{4i+2}^{(b)} Q_1(4, \epsilon)^{i-1} Q_1(6, \epsilon) + (26/n_b)^{-26} (1-26/n_b)^{-(n_b-26)} Q_1(4, \epsilon)^5 Q_1(6, \epsilon) \quad (35)$$

It follows from (28), (29), (30), (34) and (35) that we obtain the following bound on  $P_{ud}^{(b)}(\epsilon)$ :

$$\begin{aligned} P_{ud}^{(b)}(\epsilon) \leq & m \sum_{i=8}^{10} \sum_{r=0}^5 A_{(i,r)}^1 Q_1(i+r, \epsilon) \\ & + \sum_{2 \leq j \leq m} (m-j+1) \sum_{\substack{i_1+i_2 \leq 10 \\ 1 \leq i_1, i_2}} A_{i_1, i_2}^{1,j} \prod_{p=1}^2 Q_1(8(i_p), \epsilon) \\ & + \left\{ \sum_{i=2}^5 (A_{2i}^{(b)} - mA_{2i}^1) - \sum_{j=2}^m (m-j+1) \sum_{\substack{i_1+i_2 \leq 10 \\ i \leq i_1, i_2}} A_{i_1, i_2}^{1,j} \right\} Q_1(4, \epsilon)^3 \\ & + \min \left\{ \binom{m}{3} \binom{k}{4}^2 \binom{k}{3}, A_{12}^{(b)} \right\} Q_1(4, \epsilon)^3 + A_{12}^{(b)} Q_1(6, \epsilon)^2 \\ & + \sum_{i=4}^6 A_{4i}^{(b)} Q_1(4, \epsilon)^i + \sum_{i=3}^5 A_{4i+2}^{(b)} Q_1(4, \epsilon)^{i-1} Q_1(6, \epsilon) \\ & + (26/n_b)^{-26} (1-26/n_b)^{n_b-26} Q_1(4, \epsilon)^5 Q_1(6, \epsilon) \quad (36) \end{aligned}$$

On the other hand, it follows from (13) that

$$P_{ud}^{(b)}(\epsilon) \geq m Q_1(0, \epsilon)^{m-1} \sum_{i=4}^{10} \sum_{r=0}^6 A_{(i,r)}^1 Q_1(i+r, \epsilon) \quad (37)$$

For various  $\epsilon$ ,  $k$  and  $m$ , the bound on  $P_{ud}^{(b)}(\epsilon)$  given by (36) is evaluated and plotted in Figures 3 through 6. Numerical data is given in Tables 2, 3 and 4, where "upper bound" is the value of the righthand side of (36) and "lower bound" is the value of the righthand side of (37). We see that, for  $\epsilon \leq 10^{-5}$ , the coding scheme provides very high reliability.

ORIGINAL PAGE IS  
OF POOR QUALITY

## 5. Conclusion

In this paper a concatenated coding scheme for error control is presented. The reliability performance of this scheme is analyzed for a binary symmetric channel. Particularly, the scheme considered by NASA for possible adoption in telecommand operations is analyzed. It is shown that, for  $\epsilon \leq 10^{-5}$ , the scheme provides very high reliability.

APPENDIX

Let  $C_{bf}$  denote the  $(n, k+k_b-n_b)$  linear subcode of frame code  $C_f$  consisting of those codewords of  $C_f$  whose information-part (the first  $k$  components) is a codeword of the first single segment subcode of outer code  $C_b$ , and let  $C_{bf}^\perp$  denote the dual code of  $C_{bf}$ .  $C_{bf}^\perp$  has a codeword  $\bar{u}_1$  (or  $\bar{u}_2$ ) whose first  $k$  bits are all ones (or zeros) and whose last  $n-k$  bits are all zeros (or ones). Let  $C_{bf}^{\perp'}$  be the  $(n, n-k+n_b-k_b-2)$  linear subcode of  $C_{bf}^\perp$  which does not contain  $\bar{u}_1$  and  $\bar{u}_2$ . For  $0 \leq i \leq k$  and  $0 \leq r \leq n-k$ , let  $B_{(i,r)}$  (or  $B'_{(i,r)}$ ) be the number of codewords of  $C_{bf}^\perp$  (or  $C_{bf}^{\perp'}$ ) whose weights in the first  $k$  bits and in the last  $n-k$  bits are  $i$  and  $r$ , respectively. Then we have that

$$B_{(i,r)} = B'_{(i,r)} + B'_{(k-i,r)} + B'_{(i,n-k-r)} + B'_{(k-i,n-k-r)}. \quad (A1)$$

$C_{bf}^{\perp'}$ , has  $2^{21}$  codewords. We obtained  $B'_{(i,r)}$  with  $1 \leq i \leq k$  and  $1 \leq r \leq n-k$  by generating all codewords in an efficient way [8]. Then we computed  $B_{(i,r)}$  by (A1) and found  $A_{(i,r)}^1$  from  $B_{(i,r)}$ 's by the MacWilliams' identity [3]:

$$A_{(i,r)}^1 = 2^{-(n-k+n_b-k_b)} \left\{ \sum_{i'=0}^k \sum_{r'=0}^{n-k} B_{(i',r')} P_i(i';k) P_r(r';n-k) \right\},$$

where  $P_k(x;j)$  is a Krawtchouk polynomial.

Let  $C_b^\perp$  be the dual code of outer code  $C_b$ , and  $C_{b,j}^\perp$  be the dual code of the 2-segment  $(j-1)$  subcode of  $C_b$  with  $1 \leq j \leq m$ . For  $0 \leq i \leq n_b$ , let  $B_i$  denote the number of codewords of weight  $i$  in  $C_b^\perp$ ; and for  $1 \leq j \leq m$ ,  $0 \leq i_1 \leq k$  and  $0 \leq i_2 \leq k$ , let  $B_{i_1, i_2}^{1,j}$  be the number of codewords in  $C_{b,j}^\perp$  whose weights in the first half and in the last half are  $i_1$  and  $i_2$ , respectively. Both  $C_b^\perp$  and  $C_{b,j}^\perp$  have  $2^{16}$  codewords. By using the fact that the dual code of the Hamming code is a maximum-length-sequence code, we obtained  $B_i$  with  $0 \leq i \leq n_b$  and  $B_{i_1, i_2}^{1,j}$  with  $1 \leq j \leq m$ ,  $0 \leq i_1 \leq k$  and  $0 \leq i_2 \leq k$  by computer [8]. Then we computed  $A_i^{(b)}$  from  $B_i$ 's and  $A_{i_1, i_2}^{1,j}$  from  $B_{i_1, i_2}^{1,j}$ 's, respectively, by the MacWilliams' identity.

## 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. F.J. MacWilliams and N.J.A. Sloane, Theory of Error-Correcting Codes, North Holland, Amsterdam, 1977.
4. J. MacWilliams, "A Theorem on the Distribution of Weights in a Systematic Code," Bell System Technical Journal, Vol. 42, pp. 79-94, 1963.
5. Z. McHuntoon and A.M. Michelson, "On the Computation of the Probability of Post-Decoding Error Events for Block Codes," IEEE Trans. on Information Theory, vol. IT-23, No. 3, May 1977, pp. 399-403.
6. CCITT: Recommendation X.25, "Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment for Terminals Operating in Packet Mode on Public Data Networks," with Plenary Assembly, Doc. No. 7, Geneva, 1980.
7. W.W. Peterson and E.J. Weldon, Jr., Error-Correcting Codes, Second Edition, Cambridge, Mass., The MIT Press, 1972.
8. A. Kitai, "A Method for Computing Probability of Undetectable Error of Error Correcting Codes," Thesis for M.E. degree, Dept. of Information and Computer Sciences, Osaka University, 1984.



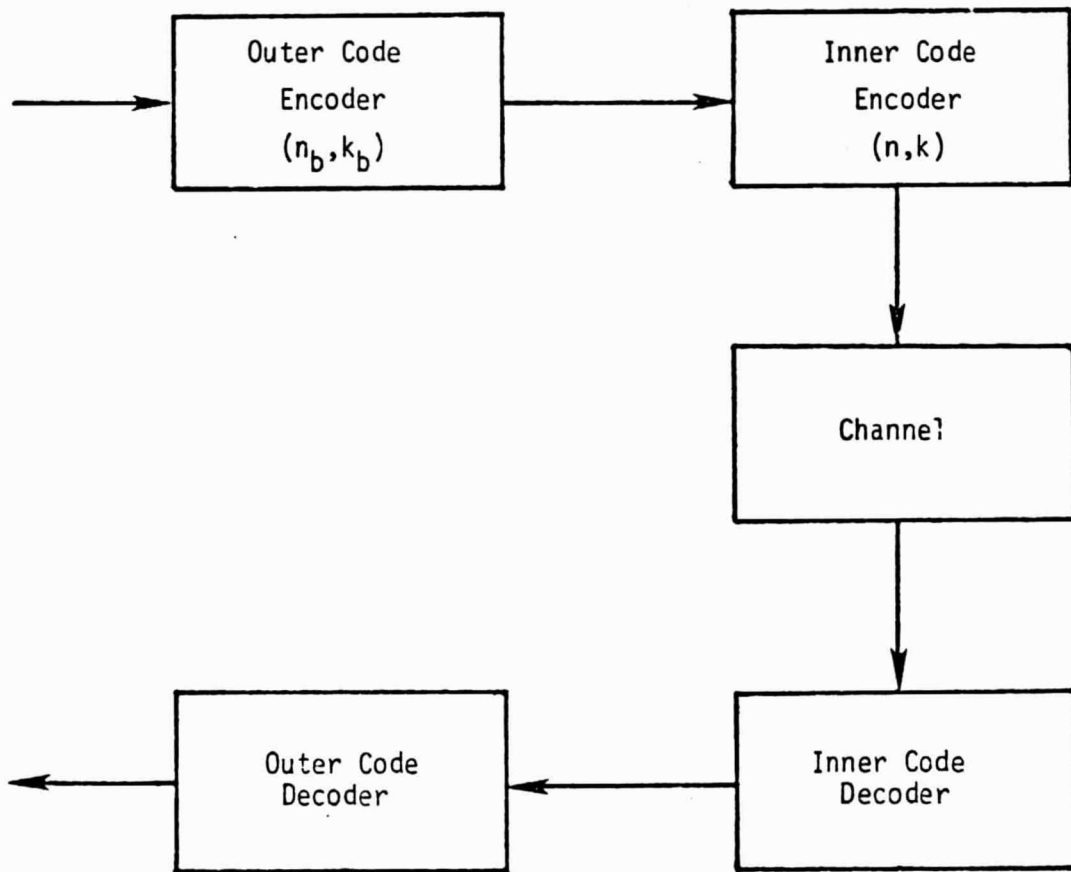


Figure 1 A concatenated coding system

ORDER OF BITS  
OF POOR QUALITY

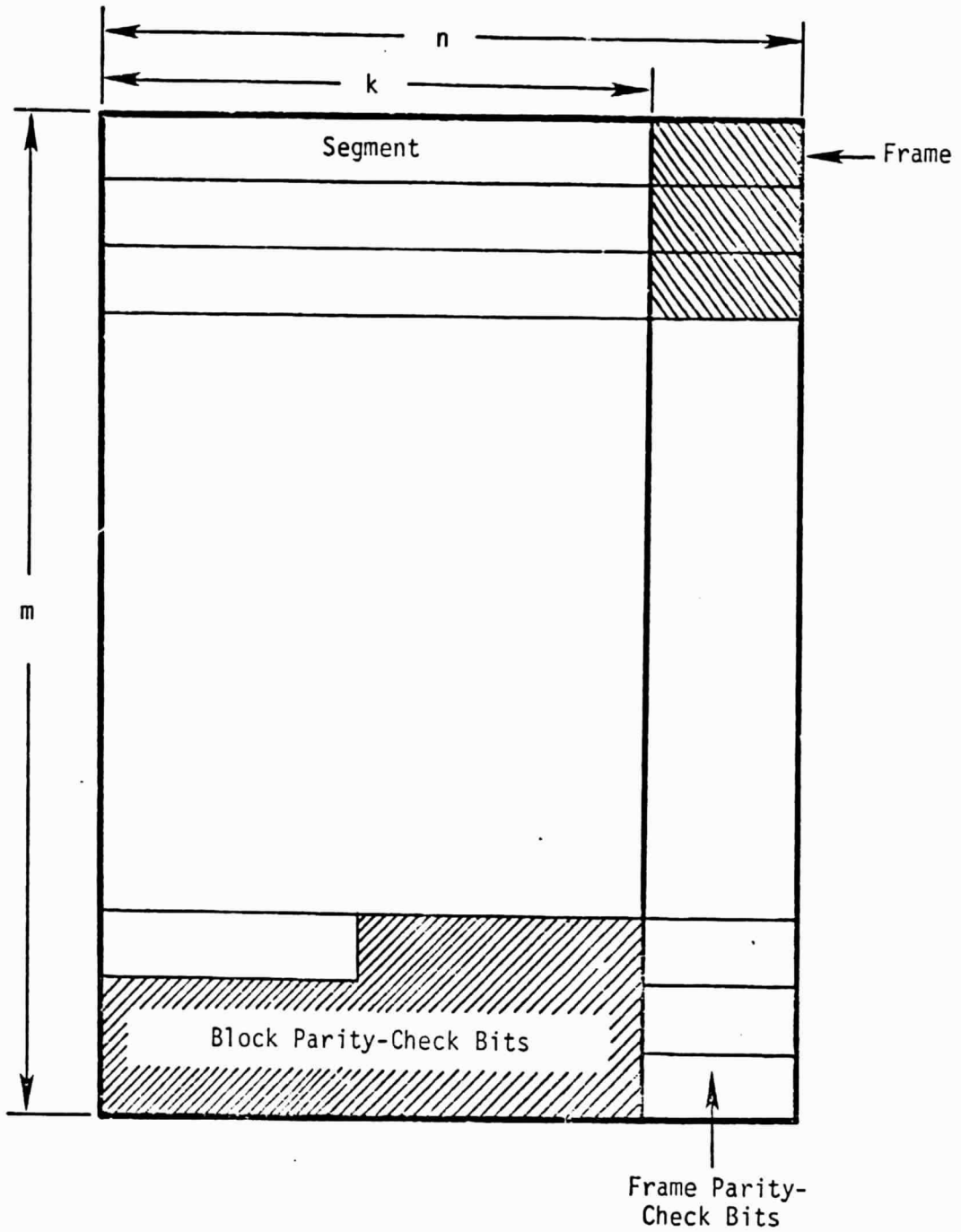


Figure 2 Block format

ORIGINAL PAGE IS  
OF POOR QUALITY

Probability of undetected error

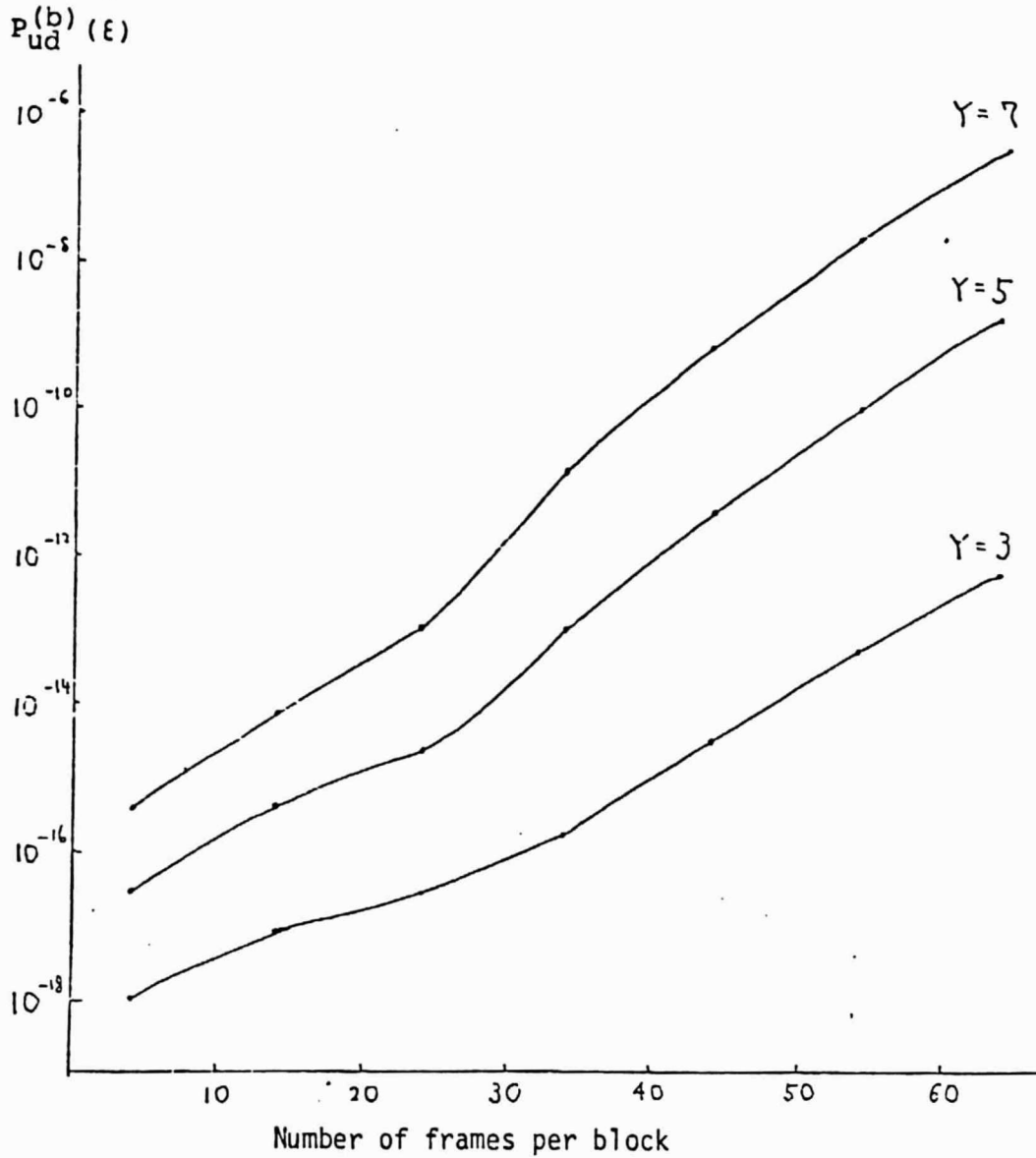


Figure 3 Upper bounds on the probability of undetected error for bit error rate  $\epsilon = 10^{-4}$ .

$Y$ : the number of information bytes in a frame

ORIGINAL PAGE IS  
OF POOR QUALITY

Probability of undetected error

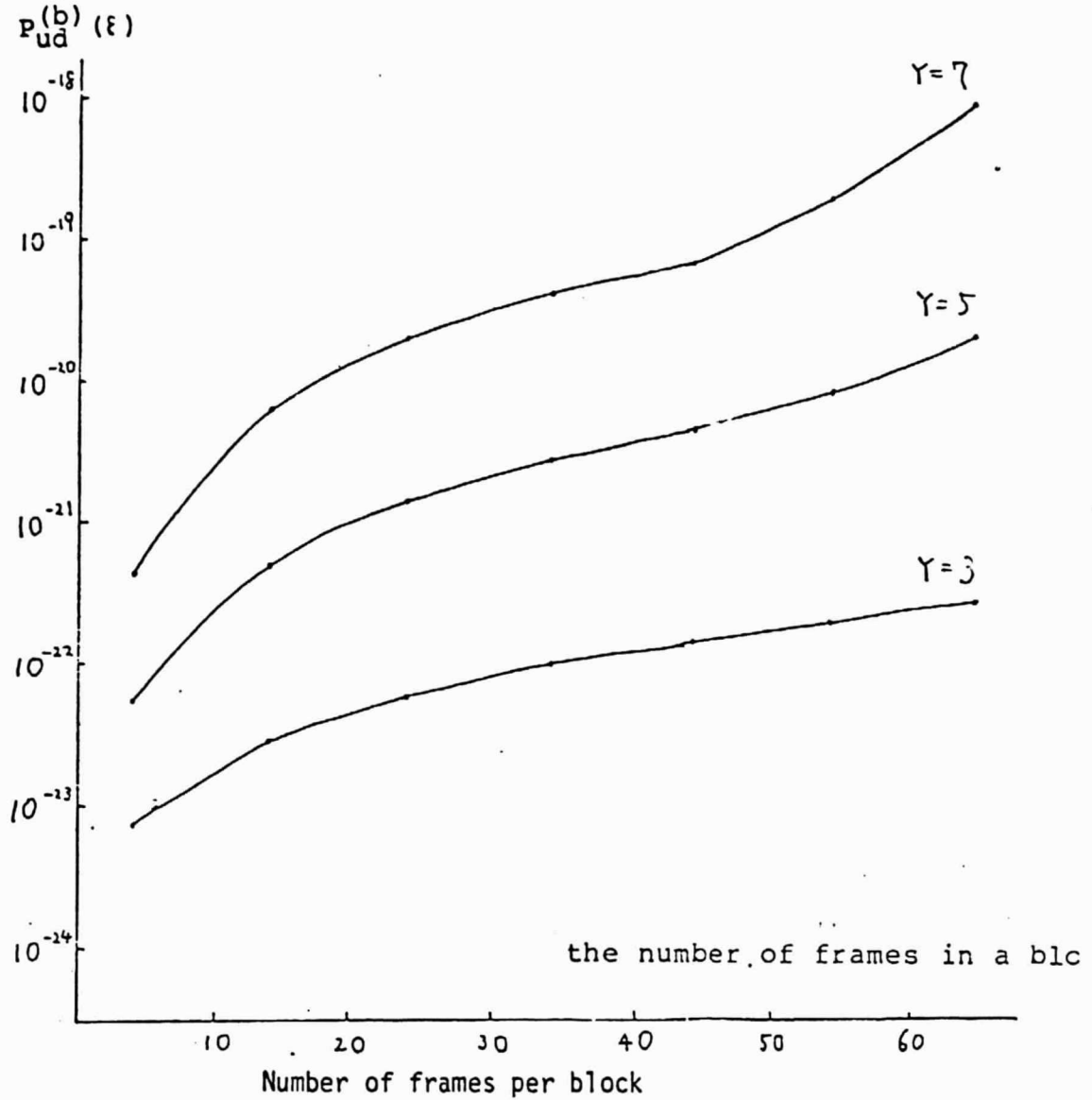


Figure 4 Upper bounds on the probability of undetected error for bit error rate  $\epsilon = 10^{-5}$ .

Y: the number of information bytes in a frame

ORIGINAL PAGE IS  
OF POOR QUALITY

Probability of undetected error

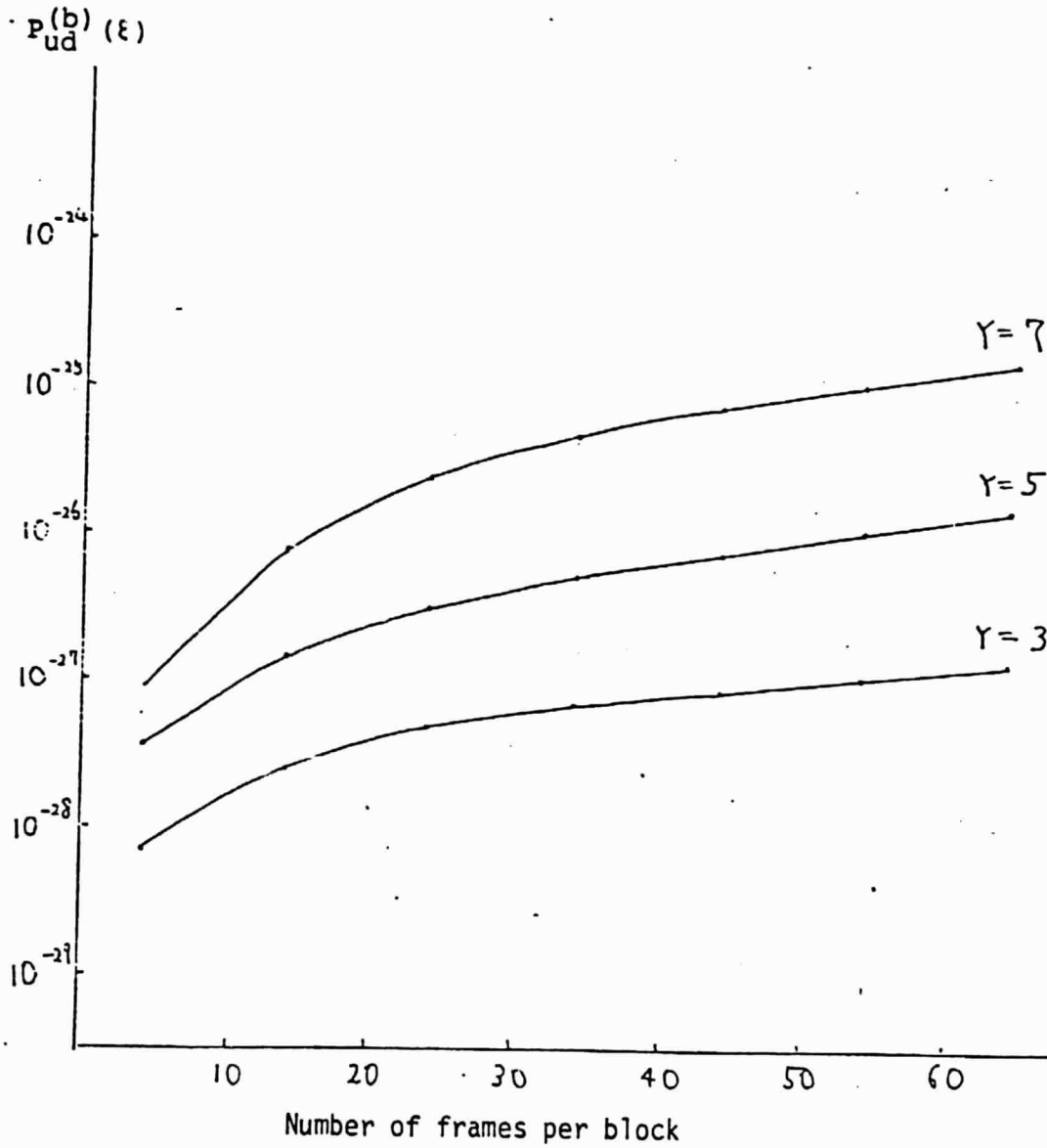


Figure 5 Upper bounds on the probability of undetected error for bit error rate  $\epsilon = 10^{-6}$ .  
Y: the number of information bytes in a frame

ORIGINAL PAGE IS  
OF POOR QUALITY

Probability of undetected error

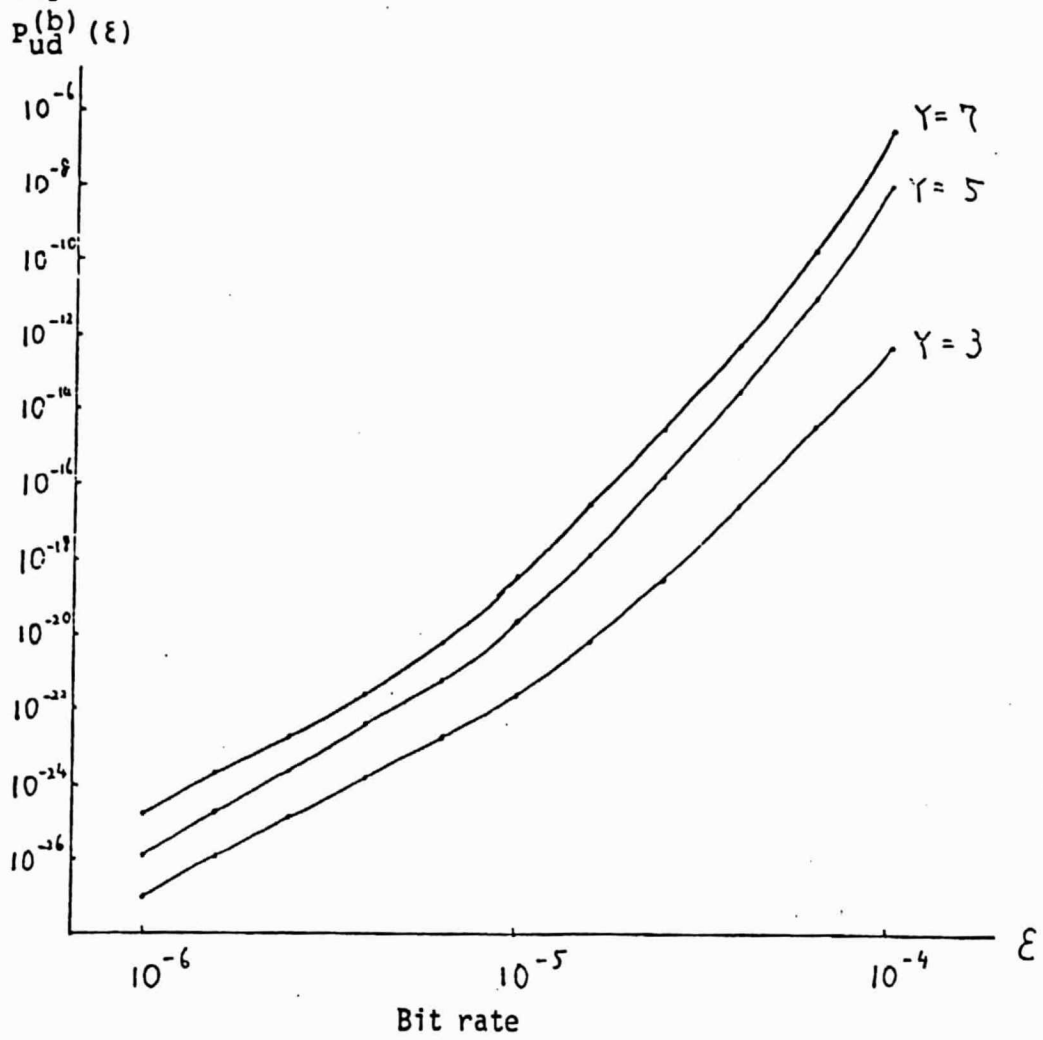


Figure 6 Upper bounds on the probability of undetected error for the case where the number of frames is 64.

Y: the number of information bytes in a frame

Table 1 Weight configuration of error patterns  $\bar{e}$ 's with  $O_{\epsilon}(\bar{e}) < 10$ .

weight	weight configuration	h	$O_{\epsilon}(\bar{e})$
4	( 1, 3 )	2	6
	( 2, 2 )	2	6
	( 1, 1, 2 )	3	9
6	( 1, 5 )	2	8
	( 2, 4 )	2	6
	( 3, 3 )	2	6
	( 1, 1, 4 )	3	9
	( 1, 2, 3 )	3	9
	( 2, 2, 2 )	3	9
8	( 2, 6 )	2	8
	( 3, 5 )	2	8
	( 4, 4 )	2	6
	( 1, 3, 4 )	3	9
	( 2, 2, 4 )	3	9
	( 2, 3, 3 )	3	9
10	( 4, 6 )	2	8
	( 2, 4, 4 )	3	9
	( 3, 3, 3 )	3	9
12	( 4, 4, 4 )	3	9

h: the number of nonzero segments

Table 2 Upper bounds and lower bounds on the probability of undetected error for bit error rate  $\epsilon = 10^{-4}$

m \ IB		3	4	5	6	7
4	upper bound	1.07E-18	6.05E-18	2.86E-17	1.18E-16	4.14E-16
	lower bound	7.18E-19	2.15E-18	3.34E-18	4.05E-18	5.01E-18
14	upper bound	7.97E-18	6.85E-17	4.11E-16	1.90E-15	7.23E-15
	lower bound	2.51E-18	7.53E-18	1.17E-17	1.42E-17	1.75E-17
24	upper bound	2.35E-17	2.57E-16	2.08E-15	1.48E-14	9.90E-14
	lower bound	4.30E-18	1.29E-17	2.00E-17	2.43E-17	3.00E-17
34	upper bound	1.55E-16	4.45E-15	9.14E-14	1.32E-12	1.37E-11
	lower bound	6.10E-18	1.82E-17	2.84E-17	3.45E-17	4.25E-17
44	upper bound	2.81E-15	1.48E-13	4.12E-12	6.80E-11	7.54E-10
	lower bound	7.89E-18	2.36E-17	3.67E-17	4.46E-17	5.50E-17
54	upper bound	4.49E-14	3.12E-12	9.67E-11	1.68E-9	1.91E-8
	lower bound	9.69E-18	2.90E-17	4.51E-17	5.47E-17	6.75E-17
64	upper bound	5.32E-13	4.24E-11	1.39E-9	2.46E-8	2.83E-7
	lower bound	1.14E-17	3.44E-17	5.34E-17	6.48E-17	8.00E-17

m: The number of frames in a block

IB: The number of information bytes in a frame



Table 3 Upper bounds and lower bounds on the probability of undetected error for bit error rate  $\epsilon = 10^{-5}$

m \ IB		3	4	5	6	7
4	upper bound	7.55E-24	2.56E-23	5.88E-23	1.54E-22	4.51E-22
	lower bound	7.19E-24	2.15E-23	3.35E-23	4.07E-23	5.03E-23
14	upper bound	3.07E-23	1.36E-22	5.01E-22	1.86E-21	6.25E-21
	lower bound	2.51E-23	7.55E-23	1.17E-22	1.42E-22	1.76E-22
24	upper bound	5.98E-23	3.12E-22	1.37E-21	5.46E-21	1.88E-20
	lower bound	4.31E-23	1.29E-22	2.01E-22	2.44E-22	3.02E-22
34	upper bound	9.51E-23	5.56E-22	2.66E-21	1.11E-20	3.83E-20
	lower bound	6.11E-23	1.83E-22	2.85E-22	3.46E-22	4.28E-22
44	upper bound	1.38E-22	8.81E-22	4.52E-21	1.96E-20	7.09E-20
	lower bound	7.91E-23	2.37E-22	3.69E-22	4.48E-22	5.54E-22
54	upper bound	1.92E-22	1.39E-21	8.09E-21	4.03E-20	1.79E-19
	lower bound	9.71E-23	2.91E-22	4.53E-22	5.50E-22	6.79E-22
64	upper bound	2.81E-22	2.59E-21	2.01E-20	1.39E-19	8.78E-19
	lower bound	1.15E-22	3.45E-22	5.37E-22	6.52E-22	8.05E-22

m: The number of frames in a block

IB: The number of information bytes in a frame

Table 4 Upper bounds and lower bounds on the probability of undetected error for bit error rate  $\epsilon = 10^{-6}$

m \ IB	3	4	5	6	7	
4	upper bound	7.24E-29	2.20E-28	3.62E-28	5.22E-28	9.05E-28
	lower bound	7.19E-29	2.15E-28	3.35E-28	4.07E-28	5.03E-28
14	upper bound	2.58E-28	8.17E-28	1.56E-27	3.15E-27	7.85E-27
	lower bound	2.51E-28	7.55E-28	1.17E-27	1.42E-27	1.76E-27
24	upper bound	4.49E-28	1.48E-27	3.18E-27	7.66E-27	2.15E-26
	lower bound	4.31E-28	1.29E-27	2.01E-27	2.44E-27	3.02E-27
34	upper bound	6.46E-28	2.21E-27	5.22E-27	1.41E-26	4.18E-26
	lower bound	6.11E-28	1.83E-27	2.85E-27	3.46E-27	4.28E-27
44	upper bound	8.50E-28	3.01E-27	7.67E-27	2.24E-26	6.88E-26
	lower bound	7.91E-28	2.37E-27	3.69E-27	4.48E-27	5.54E-27
54	upper bound	1.06E-27	3.87E-27	1.06E-26	3.26E-26	1.03E-25
	lower bound	9.71E-28	2.91E-27	4.53E-27	5.50E-27	6.80E-27
64	upper bound	1.28E-27	4.80E-27	1.39E-26	4.46E-26	1.43E-25
	lower bound	1.15E-27	3.45E-27	5.37E-27	6.52E-27	8.06E-27

m: The number of frames in a block

IB: The number of information bytes in a frame