PERFORMANCE ANALYSIS OF A HYBRID ARQ ERROR CONTROL SCHEME FOR NEAR EARTH SATELLITE COMMUNICATIONS

Technical Report I

to

NASA
Goddard Space Flight Center
Greenbelt, Maryland

Grant Number NAG 5-931

Shu Lin
Principal Investigator
Department of Electrical Engineering
University of Hawaii at Manoa
Honolulu, Hawaii 96822

August 1, 1987

PERFORMANCE ANALYSIS OF A HYBRID ARQ ERROR CONTROL SCHEME FOR NEAR EARTH SATELLITE COMMUNICATIONS

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

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

ABSTRACT

In this report, a robust error control coding scheme is presented. The scheme is a cascaded FEC scheme supported by parity retransmissions for further error correction in the erroneous data words. The error performance and throughput efficiency of the scheme are analyzed. Two specific schemes are proposed for NASA near earth satellite communications. We show that both schemes provide high reliability and throughput efficiency even for high channel bit-error rates in the range of 10^{-2}. The schemes are suitable for high data rate file transfer.

PERFORMANCE ANALYSIS OF A HYBRID ARQ ERROR CONTROL SCHEME FOR NEAR EARTH SATELLITE COMMUNICATIONS

1. Introduction

In an earlier technical report [1], we proposed a hybrid ARQ error control scheme for NASA's near earth satellite communications. The scheme was designed to provide very low error probability and high throughput for high data rate file transfer. In this report, we analyze this error control scheme and show that it indeed performs very well in terms of error probability and throughput efficiency, even for very high bit-error-rates (BER), say in the range 10^{-2}.

In order to make this report self-contained, we re-describe the proposed scheme here. The proposed error control scheme is a FEC (forward-error-correction) scheme supported by parity retransmissions for further error correction [2,3,4], known as a *hybrid ARQ scheme*. The FEC scheme is achieved by cascading two linear codes, the *outer* and *inner* codes. The inner code is either a binary block code or a binary convolutional code. The outer code is a block code with symbols from the Galois field $GF(2^m)$, say a Reed-Solomon (RS) code. The retransmission is designed to provide additional parity-check symbols for further error correction. These additional parity-check symbols are used without decreasing the rate of the overall cascaded code.

The report is organized in the following manner: the FEC scheme is described in Section 2, the retransmission strategy is presented in Section 3, performance analysis of the proposed scheme is given in Sections 4 and 5, specific schemes using NASA standard RS outer code are given in Section 6, and conclusion remarks are given in Section 7. Computation results on error probability and throughput performance are included in tables and figures.

2. The FEC System

The FEC scheme is a cascaded coding scheme [5,6]. In this study, the inner code, denoted C_1, is chosen as a binary (n_1,k_1) linear block code with minimum

distance d_1. C_1 is designed to correct t_1 or fewer errors and simultaneously detect λ_1 (with $\lambda_1 > t_1$) or fewer errors where $t_1+\lambda_1+1 \leq d_1$. The outer code, denoted C_0, is obtained by interleaving a maximum-distance-separable (n_2,k_2) linear code C_2 over $GF(2^\ell)$ with minimum distance d_2 and rate greater than 1/2. Let m_1 be the interleaving degree (or depth). Then the outer code of the scheme is an (m_1n_2,m_1k_2) code with symbols from $GF(2^\ell)$. Note that $d_2 = n_2-k_2+1$ [2]. We call C_2 the *base* outer code which is designed for correcting symbol errors and erasures. In our proposed scheme, we assume that the code parameters satisfy the following conditions:

$$\begin{aligned} k_1 &= m_1\ell \\ n_2 &= m_2(n_2-k_2) = m_2(d_2-1) \ , \end{aligned} \tag{1}$$

with $m_1 \geq 1$ and $m_2 \geq 2$.

There is a *third* code C_r which is used for parity retransmissions. C_r is a half-rate $(2d_2-2,\ d_2-1)$ code obtained by shortening the base outer code C_2. C_r is also a maximum-distance-separable code with the same minimum distance d_2 as C_2. Since C_r is a shortened code obtained from C_2, C_2 and C_r can be encoded and decoded by the same circuits. A very important property of C_r is its *invertible structure* which will be used in data recovery during the parity retransmissions. Let $\bar{u}$ be a sequence of d_2-1 information symbols from $GF(2^\ell)$. Let $R_r(\bar{u})$ denote the sequence of d_2-1 parity-check symbols formed based on the information sequence $\bar{u}$ and the half-rate code C_r. Then the $2(d_2-1)$-symbol word $(\bar{u},R_r(\bar{u}))$ is a codeword in C_r. There is a *one-to-one* correspondence between $\bar{u}$ and $R_r(\bar{u})$. Consequently, knowing only the d_2-1 parity-check symbols of a codeword in C_r, the corresponding d_2-1 information symbols can be uniquely detrmined by an *inversion* operation on the d_2-1 parity-check symbols [see Appendix A]. If C_r is a shortened cyclic code, the inversion from $R_r(\bar{u})$ to $\bar{u}$ can be achieved by a feedback shift register [2]. Let $\bar{v}_i$ be a codeword in C_2. Since $n_2 = m_2(d_2-1)$,

we can divide $\bar{v}_i$ into m_2 subsequences, $\bar{v}_{i1},\bar{v}_{i2},\ldots,\bar{v}_{i,m_2}$; each consists of d_2-1 symbols. For $1 \le j \le m_2$, let $R_r(\bar{v}_{ij})$ be the sequence of d_2-1 parity-check symbols formed based on $\bar{v}_{ij}$ and C_r. Clearly $(\bar{v}_{ij},R_r(\bar{v}_{ij}))$ is a codeword in C_r. Let

$$R(\bar{v}_i) = (R_r(\bar{v}_{i1}),R_r(\bar{v}_{i2}),\ldots,R_r(\bar{v}_{i,m_2})) \tag{2}$$

Then it can be shown that $R(\bar{v}_i)$ is also a codeword in C_2 [see Appendix B]. In fact, $\bar{v}_i$ is a codeword in C_2 if and only if $R(\bar{v}_i)$ is a codeword in C_2. This property will be used in our proposed error control scheme. For convenience, we call $R(\bar{v}_i)$ the parity word of $\bar{v}_i$.

Encoding

A message consists of a string of $k_1 \times k_2$ information bits. This string is divided into k_2 *segments*, each segment consists of k_1 information bits. Each segment is further divided into m_1 ℓ-bit *bytes*. Each ℓ-bit byte is regarded as a symbol in $GF(2^{\ell})$. The encoding operation consists of two stages as shown in Figure 1. For each input message of k_1k_2 bits, the output is an n_1n_2-bit codeword in the cascaded code C. A codeword in two-dimensional format is shown in Figure 2. The transmission is done column by column and from left to right. At the first stage of encoding, each k_1-bit segment is encoded into an n_1-bit codeword in the inner code C_1, which is called a *frame*. At the same time, the m_1 ℓ-bit bytes are multiplexed into m_1 C_2-code encoders to form parity-check symbols for m_1 codewords in C_2. As soon as the k_2 segments of a message have been shifted into the overall encoder, k_2 frames have been formed and transmitted. Also all the parity-check symbols of m_1 codewords in C_2 have been formed and are in the registers of the m_1 C_2-code encoders. Then these parity-check symbols ($m_1(n_2-k_2)$ of them) are multiplexed and shifted into the inner code encoder to form n_2-k_2 more frames (they are parity frames). These n_2-k_2 parity frames and the k_2 data frames formed at the first stage together form a complete codeword array in the cascaded code C.

There is another part of the encoder. This part is for retransmission (if needed). It consists of an encoder for the half-rate code C_r, and a buffer. Let $\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{m_1}$ be codewords in C_2 which are formed by the upper part of the overall encoder. The function of C_r-encoder is to form the m_1 parity codeword in C_2,

$$R(\bar{v}_1),\ R(\bar{v}_2),\ \ldots,\ R(\bar{v}_{m_1})$$

corresponding to the m_1 codewords, $\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{m_1}$, where $R(\bar{v}_i)$ is given by (2). These m_1 parity words are temporarily stored in a buffer for possible retransmission.

There is another encoding arrangement. We can use a single C_2-encoder to form m_1 codewords in C_2 (the first m_1 rows in Figure 2) and store them (in an array form) in a buffer. Then encode the n_2 columns into n_2 frames, and transmit them column by column. This encoding arrangement requires more buffer store.

Corresponding to each message of $k_1 \times k_2$ information bits, the output of the overall encoder shown in Figure 1 is a string of n_2 frames. These n_2 frames are said to form a *data-block*. Consider the data-block shown in Figure 2. The top $k_1 = m_1 \ell$ rows of the array is actually regarded as m_1 ℓ-bit byte rows. Each of these ℓ-bit byte rows is a codeword in C_2 and is called a *data-section* of the code array. The m_1 data-sections form a subarray which is called a *data-segment* array. Each column of a data-segment array is a data-segment. There are k_2 message segments and n_2-k_2 parity segments. Each data section is further divided into m_2 subsections, each subsection consists of d_2-1 symbols (or ℓ-bit bytes) from GF(2^ℓ). The m_1 parity words, $R(\bar{v}_1)$, $R(\bar{v}_2)$, ..., $R(\bar{v}_{m_1})$ form a parity-segment array in the buffer. Each column of this array will be called a parity-segment. Each row is called a parity-section, and consists of m_2 subsections.

Decoding of a Data Block

The decoding of a data-block is basically the same as the one described in our earlier technical report on, "A Cascaded Coding Scheme for Error Control" [5]. It consists of two stages. The first stage of 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 data 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 data-segment is stored in a receiver buffer for the second stage of decoding. A successfully decoded data-segment is called a *decoded segment with no mark*. Note that the 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 deocder will perform one of the following two operations based on a certain criterion:

1. Erasure Operation - The erroneous segment is regarded being erased. In fact this segment is *not really removed* from the buffer, it is still stored there for later use. This segment is called an erased segment. Each ℓ-bit byte of an erased segment is regarded as an *erasure* for the outer code decoding.
2. Leave-it-alone (LIA) Operation - The erroneous segment is stored in the receiver buffer with a *mark*. We call such a segment a marked segment.

Thus, after n_2 frames of a received block have been processed, the receiver buffer may contain three types of segments: decoded segments without marks, erroneous segments with marks, and erased segments.

The above inner code decoding consists of three operations: error-correction, erasure and LIA operations. An inner code decoding which performs only the error-correction and erasure operations is called an *erasure-only decoding*. On the other hand, an inner code decoding which performs only the error-correction and LIA operations is called a *LIA-only decoding*.

When n_2 frames in a received data-block have been processed, the decoder buffer contains a decoded data-segment array with m_1 ℓ-bit byte rows. Each of these ℓ-bit byte rows is regarded as a received codeword from C_2, which may contain erroneous symbols (marked or unmarked) and erasures. The code C_2 and its decoder are designed to correct the combinations of symbol erasures and symbol errors. Maximum-distance-separable codes (or Reed-Solomon codes) with symbol from $GF(2^{\ell})$ are most effective in correcting symbol erasures and errors.

At the second stage of decoding, the C_2-decoder attempts to decode the rows of the data-segment array. Let i and h be the numbers of erased and marked segments respectively. The receiver stops the decoding process and requests a retransmission for the erroneous data-block if either of the following two events occurs:

1. the number i is greater than a certain pre-designed erasure threshold T_{es} with $T_{es} \leq d_2-1$.
2. the number h is greater than a certain pre-designed threshold $T_{e\ell}(i)$ with $T_{e\ell}(i) \leq \lfloor (d_2-1-i)/2 \rfloor$ for a given i.

If none of the above two events occurs, the C_2-decoder starts the error-correction operation on the m_1 erroneous sections (or rows) of the data segment array, one at a time (they can be processed at the same time if we use m_1 C_2-decoders). The i symbol erasures and the symbol errors with or without

marks in each section are corrected based on the code C_2. Let $t_2(i)$ be the error-correction threshold for a given i where

$$t_2(i) \leq \lfloor (d_2-1-i)/2 \rfloor \ . \qquad (3)$$

If the syndrome of a section in the data-segment array corresponds to an error pattern of 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 receiver stops the decoding process and requests a retransmission for the erroneous data-block. If all the m_1 sections of a data segment array are successfully decoded, then the k_2 decoded data-segments are either delivered to the user or saved in the buffer until they are ready to be passed to the user.

3. Retransmission Scheme

When the receiver fails to decode a data-block $\bar{v}$, it saves the erroneous data-segment array of $\bar{v}$ in a buffer and requests a retransmission for $\bar{v}$. The retransmission is not $\bar{v}$ itself but a parity-block $P(\bar{v})$ corresponding to $\bar{v}$. The parity-block $P(\bar{v})$ is formed based on $\bar{v}$. Let $\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{m_1}$ be the m_1 sections of the data segment array of $\bar{v}$. Recall that each section $\bar{v}_i$ is a codeword in C_2. For each section $\bar{v}_i$, the encoder has already constructed a corresponding parity codeword

$$R(\bar{v}_i) = (R_r(\bar{v}_{i1}),\ R_r(\bar{v}_{i2}),\ \ldots,\ R_r(\bar{v}_{i,m_2}))$$

in C_2 where $R_r(\bar{v}_{ij})$ is the parity-check part formed based on the j-th subsection $\bar{v}_{ij}$ of $\bar{v}_i$ and the half-rate $(2d_2-2,\ d_2-1)$ code C_r (i.e., $(\bar{v}_{ij}, R_r(\bar{v}_{ij}))$ is a codeword in C_r). The m_1 parity codewords, $R(\bar{v}_1), R(\bar{v}_2), \ldots, R(\bar{v}_{m_1})$ are stored as a $m_1 \times n_2$ segment array in the transmitter buffer, which is called a parity-segment array. When the transmitter receives a request for a retransmission for

data-block $\bar{v}$, the inner code encoder encodes each segment of the parity-segment array into a frame (a codeword in C_1). Hence a parity-block $P(\bar{v})$ is formed, which is also a codeword in the cascaded code C. The parity-block $P(\bar{v})$ is then transmitted to the receiver.

When a parity-block $P(\bar{v})$ is received, the receiver starts to decode it. The decoding of $P(\bar{v})$ is the same as the decoding of a data-block $\bar{v}$. If the decoding of $P(\bar{v})$ is successful, *inversion* is then performed on the first k_2 decoded segments of the parity-segment array. This inversion gives the k_2 data-segments of $\bar{v}$. These decoded data-segments are then delivered to the user or saved in the receiver buffer until they are ready for delivery. At this time, the erroneous data-segment array which is stored in the receiver buffer is discarded.

If the C_2-decoder fails to decode the parity-block $P(\bar{v})$, then the parity-segment array of $P(\bar{v})$ and the data-segment array of $\bar{v}$ (which is stored in the receiver buffer) *together* are used for error correction based on the half-rate code C_r. The receiver puts $\bar{v}_{ij}$ and $R_r(\bar{v}_{ij})$ together to form a subsection pair, $(\bar{v}_{ij}, R_r(\bar{v}_{ij}))$. Then the C_r-decoder decodes $(\bar{v}_{ij}, R_r(\bar{v}_{ij}))$ into an estimate $\bar{v}^*_{ij}$ for $\bar{v}_{ij}$. After $m_1 \times m_2$ such decodings, the receiver contains the following estimated data-segments array:

$$\begin{bmatrix} \bar{v}^*_1 \\ \bar{v}^*_2 \\ . \\ . \\ . \\ \bar{v}^*_{m_1} \end{bmatrix} = \begin{bmatrix} \bar{v}^*_{11} & \bar{v}^*_{12}, & \cdots, & \bar{v}^*_{1,m_2} \\ \bar{v}^*_{21}, & \bar{v}^*_{22}, & \cdots, & \bar{v}^*_{2,m_2} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ \bar{v}^*_{m_1,1} & \bar{v}^*_{m_1,2} & \cdots, & \bar{v}^*_{m_1,m_2} \end{bmatrix}$$

Then the receiver checks whether each $\bar{v}^*_i$, for $1 \le i \le m_1$, is a codeword in C_2. Note that this time C_2 is used only for error detection. If all $\bar{v}^*_1, \bar{v}^*_2, \ldots, \bar{v}^*_{m_1}$

are codewords in C_2, then the decoding is successful and the k_2 estimated data-segments are accepted by the receiver. If any $\bar{v}_i^*$ is not a codeword in C_2, the receiver discards the erroneous data-segment array of $\bar{v}$ (stored in the buffer) and save the parity-segment arragy of $P(\bar{v})$ for later use. At the same time the receiver requests a second retransmission for $\bar{v}$. The second retransmission is the data-block $\bar{v}$ itself. When $\bar{v}$ is received, it is decoded as before. If the C_2-decoder fails to decode $\bar{v}$, then the data-segment array of $\bar{v}$ and the parity-segment array of $P(\bar{v})$ (stored in the buffer) together are used for error correction based on C_r. If the correction process is not successful, then the receiver discards the parity-segment array of $P(\bar{v})$ and saves the data-segment array of $\bar{v}$. At the same time, the receiver reqeusts a third retransmission for $\bar{v}$. The third retransmission for $\bar{v}$ is the parity block $P(\bar{v})$. When $P(\bar{v})$ is received, the receiver starts the decoding process again. Therefore, the retransmissions are *alternate repetitions* of the parity block $P(\bar{v})$ and the data-block $\bar{v}$ as shown in Figure 3. The retransmissions continue until the message in $\bar{v}$ is finally recovered by the receiver.

The major advantage of this error control scheme is that extra parity symbols for error correction are transmitted only when they are needed. These extra parity symbols are used without decreasing the rate of the cascaded code C. If the half-rate code C_r is powerful enough, *at most* one retransmission is needed to recover a message. When the channel is not very noisy, the error correcting capability of the cascaded code C should be able to recover the message in its first transmission. In this situation, the system throughput is equal to the rate of C which is R_1R_2. When the channel is noisy, the first retransmission provides us the parity symbols of C_r for extra error correction capability. Since C_r is used for correcting errors *only in a subsection of a codeword in* C_2, and since C_r has the same error correcting capability as C_2, errors in the entire data-segment array should be corrected by C_r. In this

situation, the throughput of the system should be $R_1R_2/2$. If the noisy situation is rare, then the proposed error control schemes provides maximum throughput R_1R_2 most of the time.

Since C_r is a shortened code obtained from C_2, the decoder for C_2 can be used for decoding C_r. Therefore, only decoders for C_1 and C_2 are needed. Since the inner code C_1 is binary and shorter, its decoder is much simpler than the decoder for C_2.

In our earlier report [5], we showed that a cascaded coding scheme provides extremely high reliability. We expect the proposed scheme in this report will also provide extremely high reliability. Analysis of the scheme will be given in sections 4 and 5.

A special case for the above error control scheme is that $n_1 = k_1 = \ell$. In this case, no inner code is used, the outer code is simply C_2 which is used for both error correction and detection. The code C_r is used for error correction only.

Retransmissions can be carried out in any of the three modes: the stop-and-wait, the go-back-N and the selective-repeat [2]. Selective-repeat scheme is the most efficient retransmission scheme and provides the highest throughput efficiency. For high data rate file transfer over satellite links, only selective-repeat ARQ scheme provides satisfactory throughput for high channel bit-error rate. Of course, selective-repeat ARQ scheme is more complicated to implement than the other two ARQ schemes. Various selective-repeat ARQ protocols have been proposed and studied [2,7-10]. A practical and efficient selective-repeat ARQ protocol, particularly designed for satellite communications, is the Yu-Lin's selective-repeat ARQ protocol [2,7]. The basic Yu-Lin's protocol requires a storage buffer at the receiver which is capable of storing N blocks (data or parity) that can be transmitted during a round-trip delay

period. This basic Yu-Lin's protocol has been proved to provide very good throughput performance for satellite links. Better throughput performance can be achieved by doubling the size of buffer store [7].

4. Performance Analysis - A Special Case

In this section, we analyze a special case of the proposed error control scheme for which $n_1 = k_1 = \ell$ and $m_1 = 1$. That is, in this special, there is no inner code C_1 and the base outer code C_2 is not interleaved. Hence every data (or parity) block consists of a single codeword from C_2. Since there is no inner code, there is no erasure operation. The outer code C_2 is used to correct up to $t_2 \leq \lfloor (d_2-1)/2 \rfloor$ symbol errors. The half-rate code C_r is used to correct up to $t_r = \lfloor (d_2-1)/2 \rfloor$ symbol errors in each data-parity subsection pair when retransmission occurs. To evaluate the overall error performance of the scheme, we need to know the error performance of the C_2-decoder and C_r-decoder.

Error Performance of C_2-decoder

Let ϵ be the channel bit error rate. Let P_{er} and P_{es} denote the probabilities of an incorrect decoding and a decoding failure respectively for a received data (or parity) block by the C_2-decoder. Then

$$P_{er} + P_{es} = \sum_{j=t_2+1}^{n_2} \binom{n_2}{j} [\tilde{p}_e]^j [1-\tilde{p}_e]^{n_2-j}, \tag{4}$$

and

$$P_{er} \leq \sum_{w=d_2}^{n_2} \binom{n_2}{w} \sum_{h=0}^{\min\{t_2, n_2-w\}} \binom{n_2-w}{j} \sum_{j=w+h-t_2}^{w} \binom{w}{j} \bar{P}(w,h,j), \tag{5}$$

where

$$\tilde{p}_e = 1 - (1-\epsilon)^{\ell}, \tag{6}$$

$$\bar{P}(w,h,j) = [\tilde{p}_e]^{w+h-d_2} [1-\tilde{p}_e]^{n_2-w-h} \sum_{i=0}^{\ell} \binom{\ell}{j} \left[\epsilon^i (1-\epsilon)^{\ell-i}\right]^{j+d_2-w} \tag{7}$$

The derivations of (4) and (5) are given in [5,6].

Let $\bar{P}_{er}$ denote the right-hand side of (5). Then $\bar{P}_{er}$ is an upperbound on the probability of a decoding error of C_2-decoder. In the first specific scheme proposed for NASA near earth satellite communications, the (256,224) RS code over GF(2^8) is chosen as the C_2 code. The code is capable of correcting a maximum of 16 symbol errors. For several values of $t_2 \leq 16$, $\bar{P}_{er}$ and $P_{er}+P_{es}$ are given in Table 1 and Figures 4 and 5.

Error Performance of C_r-decoder

Let $\bar{v}$ and $R(\bar{v})$ be a *received* data-block and its corresponding parity-block respectively. For $1 \leq j \leq m_2$, let $\bar{v}_j$ and $R_r(\bar{v}_j)$ be the subsections of $\bar{v}$ and $R(\bar{v})$ respectively. If $\bar{v}_j$ and $R_r(\bar{v}_j)$ are error-free, the word $(\bar{v}_j, R_r(\bar{v}_j))$ is a codeword in C_r. In a retransmission, when the C_2-decoder fails to decode $R(\bar{v})$ (or $\bar{v}$), the C_r-decoder starts to decode the m_2 subsection pairs, $(\bar{v}_j, R_r(\bar{v}_j))$ for $1 \leq j \leq m_2$. The C_r-decoder decodes $(\bar{v}_j, R_r(\bar{v}_j))$ into an estimate $\bar{v}_j^*$ if the syndrome of $(\bar{v}_j, R_r(\bar{v}_j))$ corresponds to $\lfloor (d_2-1)/2 \rfloor$ or fewer errors. If the C_r-decoding is successful for every subsection pair and the decoded block

$$\bar{v}^* = (\bar{v}_1^*, \bar{v}_2^*, \ldots, \bar{v}_{m_2}^*)$$

is a codeword in C_2, then $\bar{v}^*$ is delivered to the user. In this case we say that the C_r-decoding is successful for the data-block $\bar{v}$. Otherwise, a decoding failure is declared, and another retransmission is requested. To achieve high reliability, the base outer code C_2 should be a rather powerful code (like the NASA standard (255,223) RS code over GF(2^8)). As a result, C_r is extremely powerful because it is used only to correct errors in a subsection of $\bar{v}$. We can imagine that the probability of a decoding failure of C_r-decoder is very small even for a high bit-error rate. Therefore, for practical applications, we may assume that at most one retransmission is needed.

Assume that a data-block $\bar{v}$ and its parity-block $P(\bar{v})$ are sent and the received pair is decoded by the C_r-decoder. Let $P_{er}^{(r)}$ and $P_{df}^{(r)}$ be the

probabilities of a decoding error and a decoding failure of the C_r-decoder respectively for a subsection pair $(\bar{v}_j, R_r(\bar{v}_j))$ from $\bar{v}$ and $P(\bar{v})$. Then

$$P_{er}^{(r)} + P_{df}^{(r)} = \sum_{j=t_r+1}^{n_r} \binom{n_r}{j} \left[\tilde{p}_e\right]^j \left[1-\tilde{p}_e\right]^{n_r-j}, \tag{8}$$

$$P_{er}^{(r)} \le \bar{P}_{er}^{(r)} \triangleq \sum_{w=d_2}^{n_r} \binom{n_r}{w} \sum_{h=0}^{\min\{t_r, n_r-w\}} \binom{n_r-w}{h} \sum_{j=w+h-t_r}^{w} \binom{w}{j} \bar{P}(w,h,j) , \tag{9}$$

where $n_2 = 2(d_2-1)$ and $t_r = \lfloor (d_2-1)/2 \rfloor$. Let $P_{er}^{(all)}$ and $P_{df}^{(all)}$ be the probabilities of a decoding error and a decoding failure of the C_r-decoder respectively for the data block $\bar{v}$. Then

$$P_{er}^{(all)} + P_{df}^{(all)} = 1 - \left[1 - P_{er}^{(r)} - P_{df}^{(r)}\right]^{m_2} . \tag{10}$$

Note that, for any combination of symbol errors introduced by the C_r-decoder in the first m_2-1 subsections of $\bar{v}$, there is exactly one symbol error pattern introduced by the C_r-decoder in the last subsection of $\bar{v}$ (which consists of all the check symbols) such that the resulting block $\bar{v}^*$ is a codeword in C_2. The probability that a given nonzero error pattern is introduced by the C_r-decoder in a specific subsection of a data-block is upper bounded by

$$\bar{P}_{ep}^{(max)} \triangleq \sum_{h=0}^{d_2-2} \binom{d_2-2}{h} \sum_{j=\lfloor (d_2+1)/2 \rfloor}^{d_2} \binom{d_2}{j} \left[\tilde{p}_e\right]^h \left[1-\tilde{p}_e\right]^{d_2-2-h} \epsilon^j (1-\epsilon)^{j(\ell-1)} . \tag{11}$$

[see Appendix C for proof]. Then we have

$$P_{er}^{(all)} \le \bar{P}_{ep}^{(max)} \sum_{i=1}^{m_2-1} \binom{m_2-1}{i} \left[\bar{P}_{er}^{(r)}\right]^i \left[1-P_{er}^{(r)}-P_{df}^{(r)}\right]^{m_2-i-1} . \tag{12}$$

Overall Error Performance and Throughput Efficiency

As we pointed out earlier, since C_r is very powerful, at most one retransmission is needed. Therefore, the performance with at most one retransmission

will give us a good indication of the overall performance of the system. Let $P_{er}^{(2)}$ and $P_{df}^{(2)}$ be the probabilities of a decoding error and a decoding failure for the system. Let $\bar{P}_{er}^{(all)}$ denote the right-hand side of (12). Then we obtain the following upper bounds on the error performance of the system:

$$P_{er}^{(2)} \leq P_{er} + P_{es}P_{er} + P_{er}^{(all)} \leq \bar{P}_{er} + (P_{er}+P_{es})\bar{P}_{er} + \bar{P}_{er}^{(all)} \triangleq \bar{P}_{er}^{(2)} , \quad (13)$$

$$P_{df}^{(2)} \leq P_{df}^{(all)} \leq P_{er}^{(all)} + P_{df}^{(all)} \triangleq \bar{P}_{df}^{(2)} . \quad (14)$$

Define $\eta^{(2)}$ as follows:

$$\eta^{(2)} \triangleq \frac{k_2}{n_2(1+P_{es})} \quad (15)$$

Then $\eta^{(2)}$ is a measure of the system throughput efficiency. Obviously $\eta^{(2)}$ is lowerbounded by

$$\eta^{(2)} \geq \frac{n_2-d_2+1}{n_2(1+P_{er}+P_{es})} . \quad (16)$$

5. Performance Analysis - General Case with Erasure-only Decoding

In this section, we analyze the performance of the proposed scheme in which the inner code decoder performs only the error-correction and erasure operations (no LIA operation).

Error Performance of the Combined C_1 and C_2 Decoders

In each transmission (or retransmission), a data (or parity) block is first decoded by the C_1-decoder and then by the C_2-decoder. The C_1-decoder may result in erased segments, each erased segment contains m_1 erasure symbols. The C_2-decoder then attempts to correct the erasures and symbol errors in each section of the received data (or parity) segment array. Again let P_{er} and P_{es} denote the probabilities of a decoding error and a decoding failure for a block respectively by the combined C_1 and C_2 decodings. An upper bound on P_{er} and an expression for the sum $P_{er}+P_{es}$ have been derived and can be found in one of our earlier technical reports [5].

Error Performance of the C_r-decoder

Let $\bar{v}$ and $P(\bar{v})$ be a received data-block and its corresponding parity block respectively. When the C_2-decoder fail to decode $\bar{v}$ and $P(\bar{v})$ in two separate transmissions, the C_r-decoder starts to decode. At this time, the receiver buffer contains two segment arrays, one obtained from $\bar{v}$ and the other obtained from $P(\bar{v})$. Both segments are obtained after the inner code decoding, and hence both contain erased segments. For $1 \le i \le m_1$ and $1 \le j \le m_2$, let $\bar{v}_{ij}$ and $R_r(\bar{v}_{ij})$ be the j-th subsections of the i-th sections of the data-segment array and its corresponding parity-segment array respectively. Let s_j and s'_j be the number of erasures in $\bar{v}_{ij}$ and $R_r(\bar{v}_{ij})$ respectively. For each subsection pair $(\bar{v}_{ij}, R_r(\bar{v}_{ij}))$, the C_r-decoder decodes it into an estimate $\bar{v}^*_{ij}$, if its syndrome correspond to $s_j+s'_j$ symbol erasures and $\lfloor (d_2-1-s_j-s'_j)/2 \rfloor$ or fewer symbol errors. If the C_r-decoder successfully decodes every subsection pair, and $\bar{v}^*_i = (\bar{v}^*_{i1}, \bar{v}^*_{i2}, \ldots, \bar{v}^*_{i,m_2})$ is a codeword in C_2 for every i with $1 \le i \le m_1$. Then the decoded words, $\bar{v}^*_1, \bar{v}^*_2, \ldots, \bar{v}^*_{m_1}$, with their parity symbols removed are delivered to the user, and the C_r-decoding is said to be successful. Otherwise, a decoding failure is declared and another retransmission is requested.

Now we analyze the error performance of the C_r-decoder. Assume that a data-block and its corresponding parity-block are sent and the received pair is decoded by the C_r-decoder. For $1 \le u \le m_1$, let $P^{(r)}_{er}(u)$ and $P^{(r)}_{df}(u)$ be the probabilities of a decoding error and a decoding failure respectively for a subsection pair of the u-th section of a data-parity block pair by the C_r-decoder. Let $P^{(1)}_{es}$ denote the probability of a frame erasure. For any element α in $GF(2^\ell)$ and $1 \le u \le m_1$, 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. For $1 \le u \le m_1$, let $\tilde{p}_e(u)$ be the probability that the u-th symbol of a decoded segment is erroneous. Then

$$\tilde{p}_e(u) = \sum_{\substack{\alpha \in GF(2^\ell) \\ \alpha \neq 0}} p_e(u,\alpha) \tag{17}$$

A procedure for evaluating $p_e(u,\alpha)$ is given in [6]. Using the same argument as in [6], we can show that

$$P_{er}^{(r)}(u) + P_{df}^{(r)}(u) = \sum_{i=0}^{d_2-1} \binom{n_r}{i} \left[P_{es}^{(1)}\right]^i \sum_{j=\lfloor n_r-1-i)/2\rfloor+1}^{n_r-i} \binom{n_r-i}{j}$$

$$\cdot \left[\tilde{p}_e(u)\right]^j \left[1-P_{es}^{(1)}-\tilde{p}_e(u)\right]^{n_r-i-j}$$

$$+ \sum_{i=d_2}^{n_r} \binom{n_r}{i} \left[P_{es}^{(1)}\right]^i \left[1-P_{es}^{(1)}\right]^{n_r-i} \tag{18}$$

$$P_{er}^{(r)}(u) \leq \bar{P}_{er}^{(r)}(u) \triangleq \sum_{i=0}^{d_2-1} \binom{n_r}{i} \sum_{w=d_2-i}^{n_r-i} \binom{n_r-i}{w} \sum_{h=0}^{\min\{\lfloor (n_r-1-i)/2\rfloor, n_r-i-w\}}$$

$$\binom{n_r-i-w}{h} \sum_{j=w+h-\lfloor (n_r-1-i)/2\rfloor}^{w} \binom{w}{j} \bar{P}(u,i.w.h,j) \tag{19}$$

where $n_r = 2(d_2-1)$ and

$$\bar{P}(u,i.w,h,j) = \left[P_{es}^{(1)}\right]^i \left[\tilde{p}_e(u)\right]^{i+w+h-d_2} \left[p_e(u,0)\right]^{n_r-i-w-h}$$

$$\cdot \left[1-P_{es}^{(1)}\right]^{w-j} \sum_{q=0}^{2^\ell-2} \left[p_e(u,\gamma^q)\right]^{j+d_2-i-w}, \tag{20}$$

and γ is a primitive element in $GF(2^\ell)$. Let $P_{er}^{(all)}$ and $P_{df}^{(all)}$ be the probabilities of a decoding error and a decoding failure for the data block $\bar{v}$. Then

$$P_{er}^{(all)}+P_{df}^{(all)} \leq \max\left\{ \sum_{u=1}^{m_1} \left(1 - \left[1-P_{er}^{(r)}(u)-P_{df}^{(r)}(u)\right]^{m_2}\right), 1 \right\} \tag{21}$$

Note that, for any combination of symbol errors introduced by the C_r-decoder in the m_2-1 subsections of the u-th section of a data-block $\bar{v}$, there

is exactly one symbol error pattern introduced by the C_r-decoder in the last subsection such that the decoded u-th section is a codeword in C_2. The probability that a given nonzero error pattern is introduced by the C_r-decoder in a specific subsection of the u-th section for $1 \le u \le m_1$ is upper bounded by the following expression:

$$\bar{P}_{ep}^{(max)}(u) \triangleq \sum_{i_1=0}^{d_2-1} \binom{d_2}{i_1} \sum_{i_2=0}^{d_2-1-i_1} \binom{n_r-d_2}{i_2} \left[P_{es}^{(1)}\right]^{i_1+i_2}$$

$$\cdot \sum_{h=0}^{\min\{\lfloor d_2-i_1-i_2-1)/2 \rfloor, n_r-i_2-d_2\}} \binom{n_r-i_2-d_2}{h}$$

$$\cdot \left[\tilde{p}_e(u)\right]^h \left[p_e(u,0)\right]^{n_r-d_2-i_2-h} \sum_{j=d_2-i_1+h-\lfloor (d_2-i_1-i_2-1)/2 \rfloor}^{d_2-i_1} \binom{d_2-i_1}{j}$$

$$\cdot \left[\max_{\alpha \neq 0}\{p_e(u,\alpha)\}\right]^j \left[1-P_{es}^{(1)}\right]^{d_2-i_1-j}. \qquad (22)$$

It follows from (22) that

$$P_{er}^{(all)} \le \sum_{u=1}^{m_1} \left\{ \bar{P}_{ep}^{(max)} \sum_{i=1}^{m_2-1} \binom{m_2-1}{i} \left[\bar{P}_{er}^{(r)}(u)\right]^i \right.$$

$$\left. \cdot \left[1-P_{er}^{(r)}(u) - P_{df}^{(r)}(u)\right]^{m_2-i-1} \right\}. \qquad (23)$$

Let $\bar{P}_{er}^{(all)}$ denote the right-hand side of (23). Then $\bar{P}_{er}^{(all)}$ serves as an upper bound on the probability of an incorrect decoding for a data block $\bar{v}$.

Overall Error Performance and Throughput Efficiency

Again we assume that the code C_r is very powerful so that at most one retransmission is needed to recover a data-block. Let $P_{er}^{(2)}$ and $P_{df}^{(2)}$ be the probabilities of a decoding error and a decoding failure for the system respectively. Then we have the following bounds on $P_{er}^{(2)}$ and $P_{df}^{(2)}$:

$$P_{er}^{(2)} \le P_{er}+P_{es}P_{er}+P_{er}^{(all)} \le \bar{P}_{er} + (P_{es}+P_{er})\bar{P}_{er}+\bar{P}_{er}^{(all)} \triangleq \bar{P}_{er}^{(2)} , \qquad (24)$$

$$P_{df}^{(2)} \le P_{df}^{(all)} \le P_{er}^{(all)} + P_{df}^{(all)} \triangleq \bar{P}_{df}^{(2)} . \qquad (25)$$

The system throughput is measured by

$$\eta^{(2)} \triangleq \frac{k_1k_2}{n_1n_2(1+P_{es})} \ge \frac{(n_2-d_2+1)k_1}{n_1n_2(1+P_{er}+P_{es})} . \qquad (26)$$

6. Specific Schemes for NASA Near Earth Satellite Communications

For NASA near earth satellite communications, we propose two specific schemes. For the first scheme, we choose $n_1=k_1=\ell=8$. No inner code is used. The outer code C_2 is the extended (256,224) Reed-Solomon (RS) code over $GF(2^8)$ (or a shortened version of this code). The (256,224) RS code is actually the NASA standard code for TDRS Systems with an additional information symbol. This code has 32 parity-check symbols and is capable of correcting any combination of t or fewer symbol errors and e or fewer symbol erasures provided that $2t+e \le 32$. Note that the length of this code, 256, is a multiple of 32. The code C_r is the shortened (64,32) RS code obtained from shortening C_2. C_r is capable of correcting 16 symbol errors and is extremely powerful. Therefore, even in a very noisy situation, a transmitted data block should be recovered at most with one retransmission.

The error performance of C_2-decoder, C_r-decoder and the overall system is given in Table 1 and Figures 4-8 for various values of t_2 (the designed error correcting capability of C_2). For channel bit-error rate $\epsilon=10^{-2}$, we see from Table 1 and Figure 8 that the probability of a decoding failure of the system with at most one retransmission is upper bounded by 4×10^{-5}. The probability of a decoding error (from Table 1 and Figure 7) of the system with $t_2=7$ is upper bounded by 2×10^{-11}. The system throughput is shown in Figure 9. For bit-error rate $\epsilon=10^{-2}$, the system throughput efficiency is about 50%. For channel bit-error rate $\epsilon=10^{-3}$, the probability of a system decoding failure is upper bounded

1.64×10^{-20}! The system throughput efficiency is simply the system code rate, 95%, and the probability of a decoding error is upper bounded by 10^{-30}! Therefore, for $\epsilon \leq 10^{-3}$, the system is practically error-free and the system throughput is nearly 100% of the overall code rate R_1R_2.

For the second specific scheme, we choose ℓ=8 and m_1=6. The inner code C_1 is a distance-4 shortened (55,48) Hamming code which is used for correcting single error and detecting double errors in a frame. The base outer code C_2 is again the (256,224) extended RS code over the Galois field $GF(2^8)$. C_2 is interleaved by a depth of 6. The code C_r is again the (64,32) shortened RS code over $Gf(2^8)$.

The error performance of the combined C_1 and C_2 decoders is given in Figures 10 and 11. The error performance of the C_r-decoder is shown in Figure 12. The overall error performance of the system is given in Figures 13 and 14. Throughput efficiency of the system is shown in Figure 15. From these figures, we see that the second specific scheme also performs extremely well for channel bit error rate $\epsilon \leq 10^{-2}$.

Since the second scheme uses an inner code and the base outer code is interleaved, it provides better performance than the first scheme. From Figures 7 and 13, we see that the second scheme gives smaller error probability for the same channel bit-error rate ϵ. Figures 16 and 17 gives a comparison of two schemes in probability of decoding failure and throughput efficiency. For bit-error rate ϵ less than 2×10^{-2}, the probability of a decoding failure of the second scheme is much smaller than that of the first scheme. As a result, the second scheme provides higher throughput efficiency than the first scheme (see Figure 17) for a certain range of bit-error rates. However, for $\epsilon \leq 10^{-3}$, the first scheme gives higher throughput efficiency because, for this error rate, the probability of decoding failure of the first scheme is also extremely small and it uses less parity-check bits. The second scheme is more complicated

to implement and requires more buffer storage at both transmitter and receiver due to interleaving.

7. Conclusion

In this report, a robust error control coding scheme has been presented and analyzed. The scheme is a cascaded FEC scheme supported by parity retransmissions for further error corrections in parts (or subsections). The extra parity-check symbols for further error correction are transmitted only when they are needed. When the channel is quiet or not so noisy, the scheme behaves like a conventional FEC scheme with throughput efficiency equal to the overall code rate. When the channel is noisy, parity retransmission is requested and extra parity symbols for correcting errors in subsections of a codeword are transmitted. The parity symbols sent in a retransmission are formed based on the data in the original transmission and a half-rate invertible code C_r. These parity symbols contain the *same amount* of information as the original data. As a result, they can be used to recover the original data either by inversion or by decoding based on C_r. If C_r is powerful enough, at most one retransmission is needed to recover the erroneous data. If selective-repeat ARQ is used for retransmissions, the system throughput efficiency would remain high, say 50% of the system code rate, even for very high bit-error rate, say in the range of 10^{-2}. The proposed error control scheme is particularly suitable for satellite links with long propagation delay and *nonstationary* bit-error rate. The scheme uses the same amount of buffer store at the transmitter and receiver as a corresponding conventional hybrid ARQ scheme [2,3].

Two specific schemes are proposed for NASA's near earth satellite communications. The first scheme does not use an inner code and the outer code is not interleaved. The outer code is the NASA standard (256,224) RS code over $GF(2^8)$. The half-rate code used for correcting errors in subsections during parity retransmission is the shortened (64,32) RS code obtained from the (256,224) RS

code. The (64,32) code is used for correcting 16 symbol errors over a subsection pair of 64 symbols. Therefore, it is a very powerful code. As a result, an erroneous data would be recovered with at most one retransmission even for a bit-error rate as high as 10^{-2}. The scheme provides very high reliability (i.e. very low error probability) for channel bit-error rate up to 10^{-2}. If this scheme is used in cooperation with Yu-Lin's selective-repeat ARQ retransmission protocol, a buffer with size equal to the number of codewords transmitted in one round-trip delay is needed at the receiver. This buffer size is the same as the buffer used in a corresponding conventional selective-repeat ARQ scheme.

The second specific scheme proposed for NASA uses the same (256,224) RS code as the base outer code C_2 except that it is interleaved to a depth of 6. The half-rate code C_r for parity retransmission is again the (64,32) shortened RS code. The scheme uses an inner code which is the distance-4 (55,48) shortened cyclic Hamming code. The inner code is used for correcting single error and detecting double errors in a frame. The decoding of this code is very simple, it can be implemented with a ROM using table-look-up. The second scheme provides better performance than the first scheme, however it requires a buffer with a size which is six times larger than that of the first scheme. For channel bit-error rate less than 5×10^{-3}, both schemes practically provide error-free communication and have the same throughput performance. However for bit-error rate in the range 5×10^{-3} to 10^{-2} or higher, the second scheme gives much higher throughput efficiency. If NASA's satellite links for high rate file transfer operate with error rates less than 5×10^{-3}, we recommend that the first scheme be used. If 50% throughput efficiency at bit-error rate $\epsilon=10^{-2}$ is acceptable, the first scheme is still a better choice. The second scheme is recommended when extremely high reliability and high throughput are needed for bit-error rate in the range from 5×10^{-3} to 10^{-2}.

REFERENCES

1. Shu Lin and Tadao Kasami, "Two Hybrid ARQ Error Control Schemes for Near Earth Satellite Communications," *NASA-GSFC Technical Report*, Grant Number NAG 5-778, August 4, 1986.

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

3. Shu Lin and P.S. Yu, "A Hybrid ARQ Scheme with Parity Retransmission for Error Control of Satellite Channels," *IEEE Transactions on Communications*, Vol. COM-30, No. 7, July 1982.

4. Y.M. Wang and Shu Lin, "A Modified Selective-Repeat Type-II Hybrid ARQ System and Its Performance Analysis, *IEEE Transactions on Communications*, Vol. COM-31, No. 5, pp. 593-608, May 1983.

5. T. Kasami and Shu Lin, "A Cascaded Coding Scheme for Error Control," *NASA-GSFC Technical Report*, Grant Number NAG 5-407, December 10, 1985.

6. T. Kasami, T. Fujiwara and T. Takata and Shu Lin, "A Cascaded Coding Scheme for Error Control and Its Performance Analysis," accepted for publication in *IEEE Transactions on Information Theory*, 1987.

7. P.S. Yu and Shu Lin, "An Efficient Selective-Repeat ARQ Scheme for Satellite Channels and Its Performance Analysis," *IEEE Transactions on Communications*, Vol. COM-29, No. 3, pp. 353-363, March 1981.

8. M.J. Miller and Shu Lin, "The Analysis of Some Selective-Repeat ARQ Schemes with Finite Receiver Buffer," *IEEE Transactions on Communications*, Vol. COM-29, No. 9, pp. 1307-1315, Sept. 1981.

9. J.J. Metzner, "A Study of an Efficient Retransmission Strategy for Data Links," *NTC '77 Conference Record*, pp. 3B:1-1-3B:1-5, November, 1987.

10. E.J. Weldon, Jr., "An Improved Selective Repeat ARQ Strategy," *IEEE Transactions on Communications*, Vol. COM-30, No. 3, pp. 480-486, March 1982.

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

APPENDIX A

Invertible Property of the C_r Code

Since C_2 is a maximum-distance-separable code, C_r is also a maximum-distance-separable code [11]. The generator matrix in systematic form of C_r is a $(d_2-1)\times(2d_2-2)$ matrix of the following form:

$$G_r = [I\ P]$$

where I is a (d_2-1)-dimensional identity matrix and P is a $(d_2-1)\times(d_2-1)$ square matrix over $GF(2^\ell)$. The parity-check matrix of C_r in systematic form is then

$$H_r = \left[P^T I\right] ,$$

where P^T is the transpose of P. Since the minimum distance of C_r is d_2, the d_2-1 columns of P^T must be linearly independent. This implies that the d_2-1 rows of P are linearly independent. As a result, P is a nonsingular square matrix over $GF(2^\ell)$. Let P^{-1} be the inverse of P. Then $PP^{-1} = I$.

Let $\bar{a}$ be a (d_2-1)-tuple over $GF(2^\ell)$. Then the $(2d_2-2)$-tuple,

$$\bar{v} = (\bar{a},\bar{b}) = \bar{a}\cdot G_r , \tag{A-1}$$

is a codeword in C_r where

$$\bar{b} = \bar{a}\cdot P \tag{A-2}$$

is the parity part of $\bar{v}$.

Let $\bar{a}'$ be another (d_2-1)-tuple over $GF(2^\ell)$ such that $\bar{a}'\neq\bar{a}$. The codeword in C_r corresponding to $\bar{a}'$ is

$$\bar{v}' = (\bar{a}',\bar{b}') = \bar{a}'\cdot G_r$$

where

$$\bar{b}' = \bar{a}'\cdot P . \tag{A-3}$$

Now we want to show that $\bar{b} \neq \bar{b}'$. Suppose that $\bar{b}=\bar{b}'$. Then, from (A-2) and (A-3), we have

$$\bar{0} = \bar{b}-\bar{b}' = (\bar{a}-\bar{a}')\cdot P . \tag{A-4}$$

Since $\bar{a} \neq \bar{a}'$, $\bar{a}\text{-}\bar{a}' \neq \bar{0}$. Equation (A-4) implies that the rows of P are *not* linearly independent. This is a contradiction. Hence $\bar{b} \neq \bar{b}'$. This says that there is a one-to-one correspondence between $\bar{a}$ and $\bar{b}$. Multiplying both sides of (A-2) by P^{-1}, we have

$$\bar{b} \cdot P^{-1} = a \cdot P \cdot P^{-1} = \bar{a} \ .$$

Hence the data $\bar{a}$ can be recovered uniquely from its corresponding parity part $\bar{b}$ by taking an inversion.

APPENDIX B

Most commonly used maximum-distance-separable codes are RS codes. Let C_2 be a RS (or shortened or extended) code over $GF(2^{\ell})$. Let $\bar{g}_2(X)$ be the generator polynomial of C_2. The degree of $\bar{g}_2(X)$ is $n_2-k_2 = d_2-1$. Let $\bar{v}(X)$ be a code polynomial in C_2. Let $\bar{v}_1(X),\bar{v}_2(X),\ldots,\bar{v}_{m_2}(X)$ be the m_2 subsections of $\bar{v}(X)$. Then

$$\bar{v}(X) = \bar{v}_1(X) + \bar{v}_2(X)X^{n_2-k_2} + \ldots + \bar{v}_{m_2}(X)X^{(m_2-1)(n_2-k_2)} \tag{B-1}$$

where

$$\bar{v}_i(X) = v_{i0} + v_{i1}X + \ldots + v_{i,n_2-k_2-1}X^{n_2-k_2-1} . \tag{B-2}$$

Since C_r is obtained by shortening C_2, the generator polynomial of C_r is also $\bar{g}_2(X)$. If we encode the i-th section $\bar{v}_i(X)$ of $\bar{v}(X)$ based on C_r, the parity check part of the code polynomial is the remainder $R_r[\bar{v}_i(X)]$ obtained by dividing $X^{n_2-k_2}\,\bar{v}_i(X)$ by $\bar{g}_2(X)$, i.e.,

$$X^{n_2-k_2}\,\bar{v}_i(X) = \bar{a}_i(X)\bar{g}_2(X) + R_r[\bar{v}_i(X)] . \tag{B-3}$$

where the degree of $R_r[\bar{v}_i(X)]$ is n_2-k_2-1 or less. Consider the polynomial,

$$R[\bar{v}(X)] = R_r[\bar{v}_1(X)] + R_r[\bar{v}_2(X)]\,X^{n_2-k_2} + \ldots + R_r[\bar{v}_{m_2}(X)]X^{(m_2-1)(n_2-k_2)} . \tag{B-4}$$

From (B-1), (B-3) and (B-4), we have

$$R[\bar{v}(X)] = \left\{a_1(X) + a_2(X)X^{n_2-k_2} + \ldots + a_{m_2}(X)X^{(m_2-1)(n_2-k_2)}\right\}\bar{g}_2(X) + \bar{v}(X)X^{n_2-k_2} . \tag{B-5}$$

Since $\bar{v}(X)$ is code polynomial in C_2, $\bar{v}(X)$ is divisible by $\bar{g}_2(X)$. From (B-5), we see that $R[\bar{v}(X)]$ is divisible by $\bar{g}_2(X)$. Since $R[\bar{v}(X)]$ is a polynomial of degree $m_2(n_2-k_2)-1 = n_2-1$ or less, $R[\bar{v}(X)]$ is a code polynomial in C_2.

APPENDIX C

Derivation of $\bar{P}_{ep}^{(max)}$

Let $P_{er}(w)$ be the probability of occurrence of an error pattern of weight w in a subsection after C_r-decoding. It is shown in [5,6] that this probability is upper bounded by

$$P_{er}(w) \le \bar{P}_{er}(w) \triangleq \sum_{h=0}^{\min\{t_r, n_r-w\}} \binom{n_r-w}{h} \sum_{j=w+h-t_r}^{w} \binom{w}{j} \cdot \left[\tilde{p}_e\right]^{w+h-d_2} \left[1-\tilde{p}_e\right]^{n_r-w-h} \left[\max_{\alpha \neq 0}\{p_e(\alpha)\}\right]^j \quad \text{(C-1)}$$

where $n_r = 2(d_2-1)$, $t_r = \lfloor (d_2-1)/2 \rfloor$ and

$$\max_{\alpha \neq 0}\{p_e(\alpha)\} = \epsilon(1-\epsilon)^{\ell-1} .$$

Next we want to show that, if

$$\frac{[1-(1-\epsilon)^{\ell}]\epsilon}{1-\epsilon} \le \frac{d_2+3}{4(d_2-1)} , \quad \text{(C-2)}$$

then

$$\bar{P}_{er}(d_2) \ge \bar{P}_{er}(w) \quad \text{(C-3)}$$

for $d_2 \le w < n_r$. From (C-1), we have

$$\bar{P}_{er}(w+1) = \sum_{h=0}^{\min\{t_r, n_r-w-1\}} \binom{n_r-w-1}{h} \sum_{j=w+h-t_r}^{w} \binom{w+1}{j+1} \cdot \left[\tilde{p}_e\right]^{w+1+h-d_2} \left[1-\tilde{p}_e\right]^{n_r-w-1-h} \left[\max_{\alpha \neq 0}\{p_e(\alpha)\}\right]^{j+1} \quad \text{(C-4)}$$

By comparing each term in the right-hand sides of (C-1) and (C-4), we see that, if

$$\frac{\binom{n_r-w-1}{h}\binom{w+1}{j+1}\tilde{p}_e\left[\max_{\alpha\neq 0}\{p_e(\alpha)\}\right]^k}{\binom{n_r-w}{h}\binom{w}{j}\left[1-\tilde{p}_e\right]} \leq 1 , \qquad \text{(C-5)}$$

for $d_2 \leq w \leq n_r$, $0 \leq h \leq \min\{t_r, n_r-w\}$ and

$$w + h - t_r \leq j \leq w ,$$

then (C-3) holds. The inequality of (C-5) can be rewritten as follows:

$$\frac{\tilde{p}_e\left[\max_{\alpha\neq 0}\{p_e(\alpha)\}\right]}{(1-\tilde{p}_e)} \leq \frac{(n_r-w)(j-1)}{(n_r-w-h)(w+1)} \qquad \text{(C-6)}$$

for $d_2 \leq w \leq n_2$, $0 \leq h \leq \min\{t_r, n_r-w\}$ and $w+h-t_r \leq j \leq w$. The inequality of (C-6) holds if

$$\frac{[1-(1-\epsilon)^{\ell}]\epsilon}{(1-\epsilon)} \leq \frac{d_2-t_r+1}{n_r} = \frac{d_2-\lfloor (d_2-1)/2 \rfloor+1}{2(d_2-1)} \leq \frac{d_2+3}{4(d_2-1)} . \qquad \text{(C-7)}$$

It follows from (C-5) to (C-7) that we obtain the inequality of (C-3) under the condition of (C-2). Equation (C-2) holds if $\epsilon \leq 0.2$. From (C-1) and (C-3), we obtain the upper bound given by (11).

Table 1 Error performance and throughput efficiency of the first specific scheme

Bit-Error-Rate (%)	$\bar{P}_{er}$ $t_2=7$	$P_{er}+P_{es}$ $t_2=7$	Per(all)	Per(2)	Pdf(2)	Throughput $\eta^{(2)}$
0.05	7.79E-38	1.10E-05	5.51E-75	7.79E-38	1.54E-25	8.75E-01
0.10	2.03E-30	1.17E-03	6.61E-65	2.03E-30	1.64E-20	8.74E-01
0.15	2.98E-26	1.26E-02	4.48E-59	3.01E-26	1.32E-17	8.64E-01
0.20	2.05E-23	5.38E-02	5.54E-55	2.16E-23	1.42E-15	8.30E-01
0.25	2.63E-21	1.39E-01	7.63E-52	3.00E-21	5.13E-14	7.68E-01
0.30	1.17E-19	2.66E-01	2.62E-49	1.48E-19	9.26E-13	6.91E-01
0.35	2.52E-18	4.14E-01	3.46E-47	3.56E-18	1.04E-11	6.19E-01
0.40	3.16E-17	5.60E-01	2.27E-45	4.93E-17	8.15E-11	5.61E-01
0.45	2.64E-16	6.89E-01	8.69E-44	4.46E-16	4.91E-10	5.18E-01
0.50	1.60E-15	7.91E-01	2.18E-42	2.87E-15	2.39E-09	4.89E-01
0.60	2.83E-14	9.17E-01	5.25E-40	5.43E-14	3.51E-08	4.56E-01
0.70	2.43E-13	9.72E-01	4.85E-38	4.79E-13	3.20E-07	4.44E-01
0.80	1.23E-12	9.91E-01	2.22E-36	2.46E-12	2.01E-06	4.39E-01
0.90	4.21E-12	9.98E-01	5.96E-35	8.41E-12	1.01E-05	4.38E-01
1.00	1.06E-11	9.99E-01	1.05E-33	2.12E-11	3.99E-05	4.38E-01
1.10	2.09E-11	1.00E00	1.31E-32	4.19E-11	1.34E-04	4.38E-01
1.20	3.42E-11	1.00E00	1.24E-31	6.83E-11	3.90E-04	4.38E-01
1.30	4.78E-11	1.00E00	9.21E-31	9.56E-11	1.01E-03	4.38E-01
1.40	5.94E-11	1.00E00	5.60E-30	1.19E-10	2.36E-03	4.38E-01
1.50	6.71E-11	1.00E00	2.86E-29	1.34E-10	5.06E-03	4.38E-01
1.60	7.07E-11	1.00E00	1.26E-28	1.41E-10	1.01E-02	4.38E-01
1.70	7.08E-11	1.00E00	4.81E-28	1.42E-10	1.87E-02	4.38E-01
1.80	6.84E-11	1.00E00	1.63E-27	1.37E-10	3.28E-02	4.38E-01
1.90	6.45E-11	1.00E00	4.95E-27	1.29E-10	5.42E-02	4.38E-01
2.00	6.00E-11	1.00E00	1.36E-26	1.20E-10	8.54E-02	4.38E-01
2.10	5.53E-11	1.00E00	3.39E-26	1.11E-10	1.28E-01	4.38E-01
2.20	5.07E-11	1.00E00	7.71E-26	1.01E-10	1.84E-01	4.38E-01
2.30	4.64E-11	1.00E00	1.61E-25	9.27E-11	2.53E-01	4.38E-01
2.40	4.23E-11	1.00E00	3.10E-25	8.47E-11	3.34E-01	4.38E-01
2.50	3.86E-11	1.00E00	5.49E-25	7.72E-11	4.23E-01	4.38E-01
2.60	3.52E-11	1.00E00	9.00E-25	7.04E-11	5.18E-01	4.38E-01
2.70	3.21E-11	1.00E00	1.36E-24	6.42E-11	6.12E-01	4.38E-01
2.80	2.93E-11	1.00E00	1.92E-24	5.85E-11	7.00E-01	4.38E-01
2.90	2.67E-11	1.00E00	2.50E-24	5.33E-11	7.78E-01	4.38E-01
3.00	2.43E-11	1.00E00	3.03E-24	4.85E-11	8.43E-01	4.38E-01
3.50	1.51E-11	1.00E00	2.79E-24	3.03E-11	9.87E-01	4.38E-01
4.00	9.35E-12	1.00E00	5.42E-25	1.87E-11	1.00E00	4.38E-01
4.50	5.73E-12	1.00E00	3.18E-26	1.15E-11	1.00E00	4.38E-01
5.00	3.49E-12	1.00E00	9.79E-28	6.98E-12	1.00E00	4.38E-01

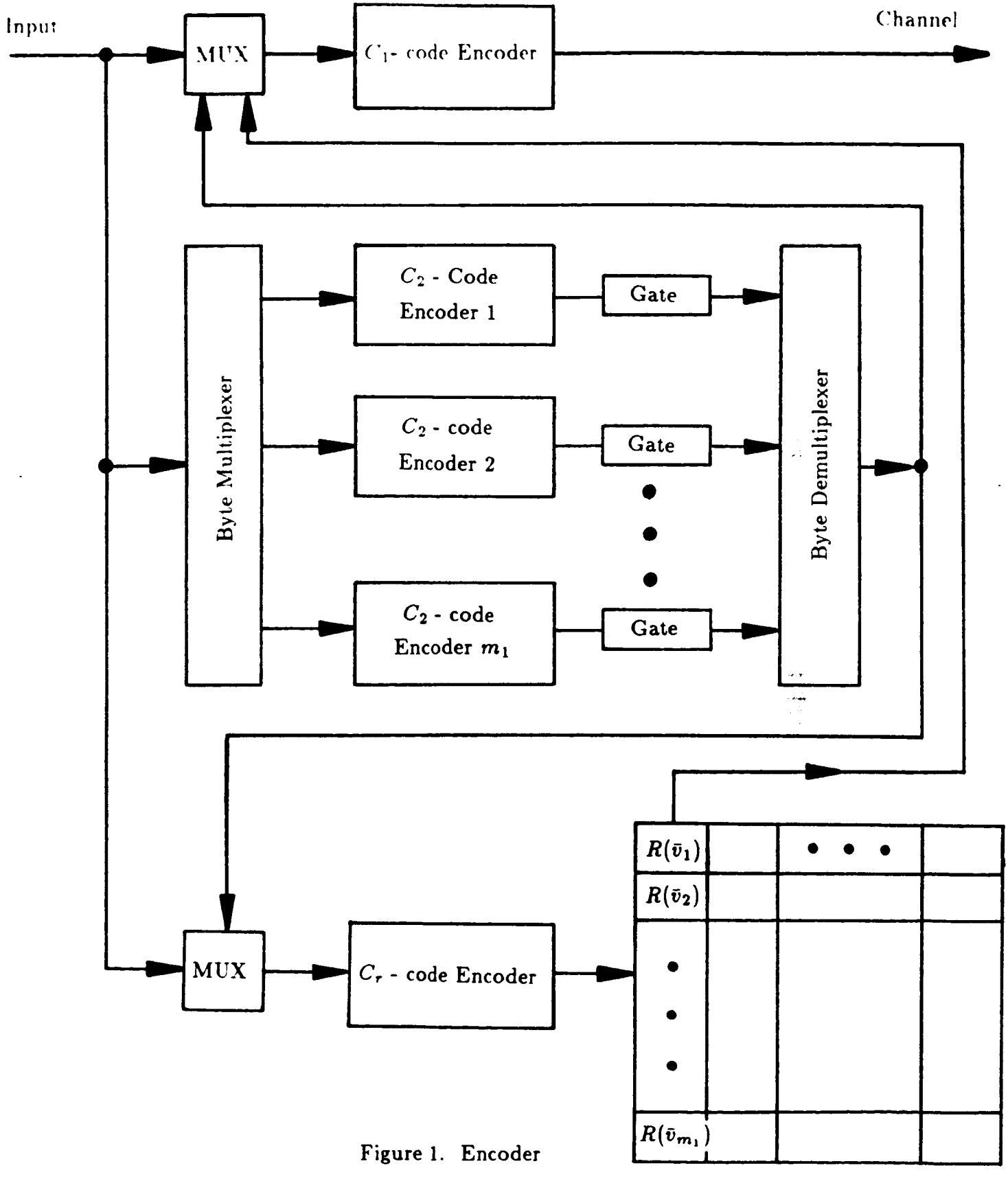

Figure 1. Encoder

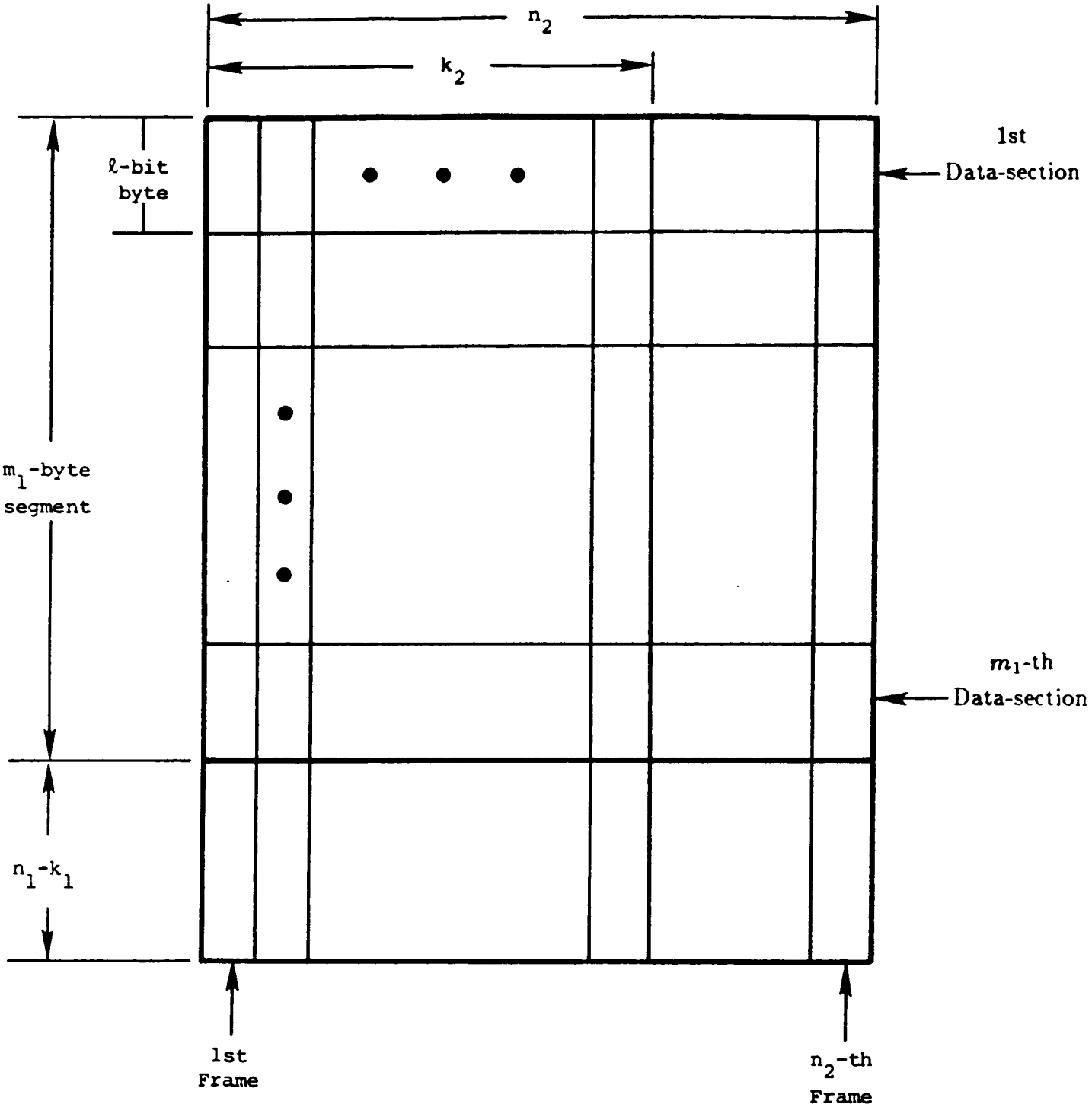

Figure 2. Block format

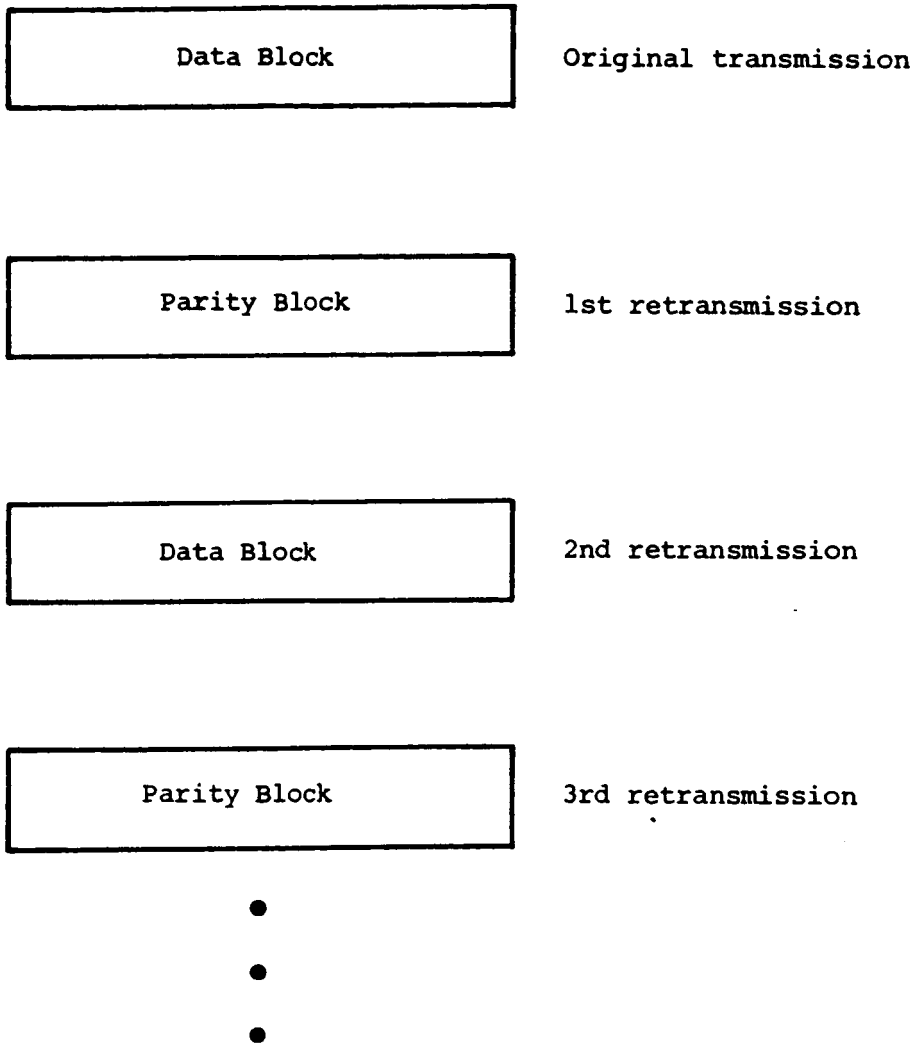

Figure 3. Alternate data-parity retransmission strategy

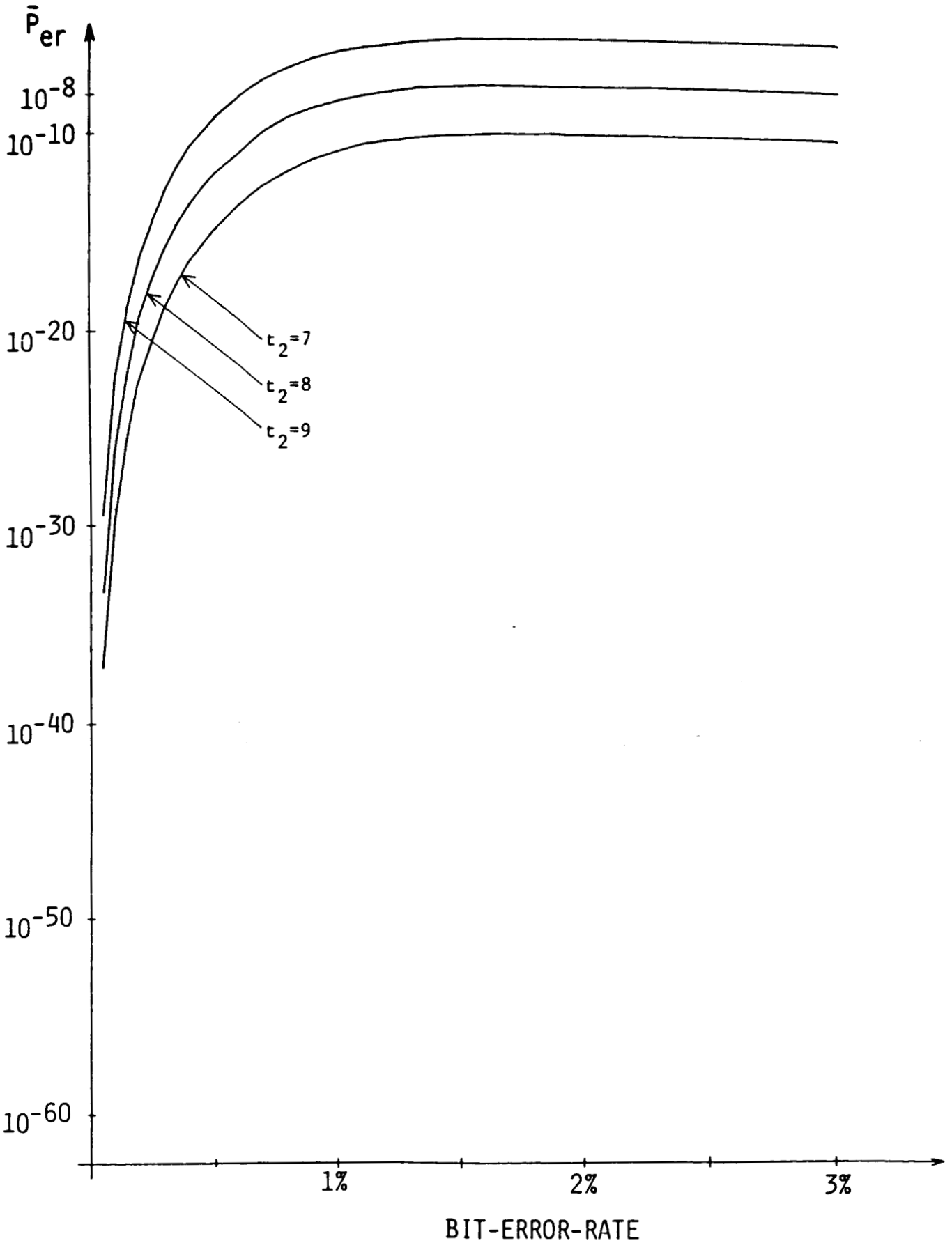

Figure 4 Upper bounds on the probability of a decoding error of the C_2-decoder for a received data-block or parity block.

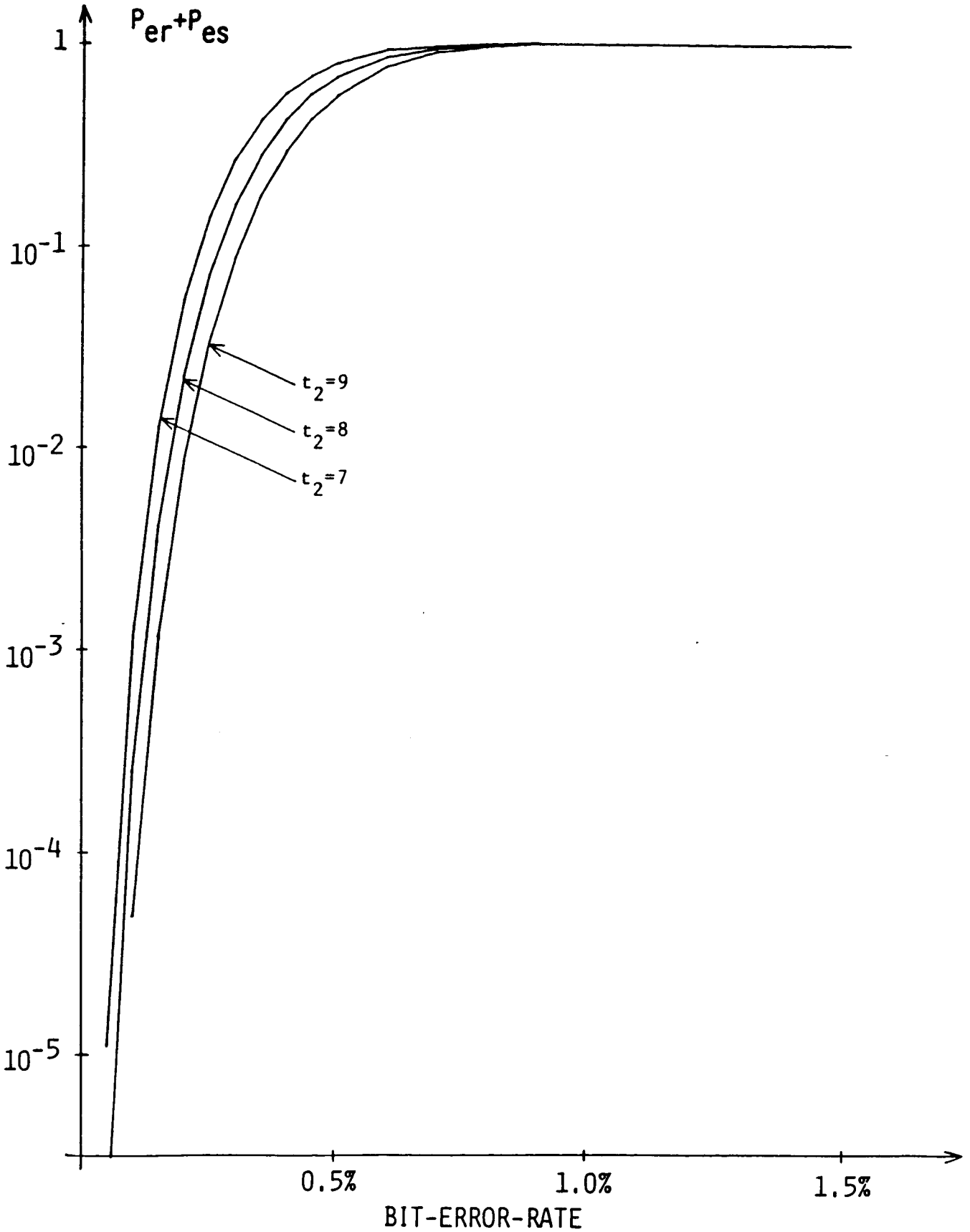

Figure 5 The sum of probabilities of a decoding failure and a decoding error of the C_2-decoder for a received data-block or parity-block.

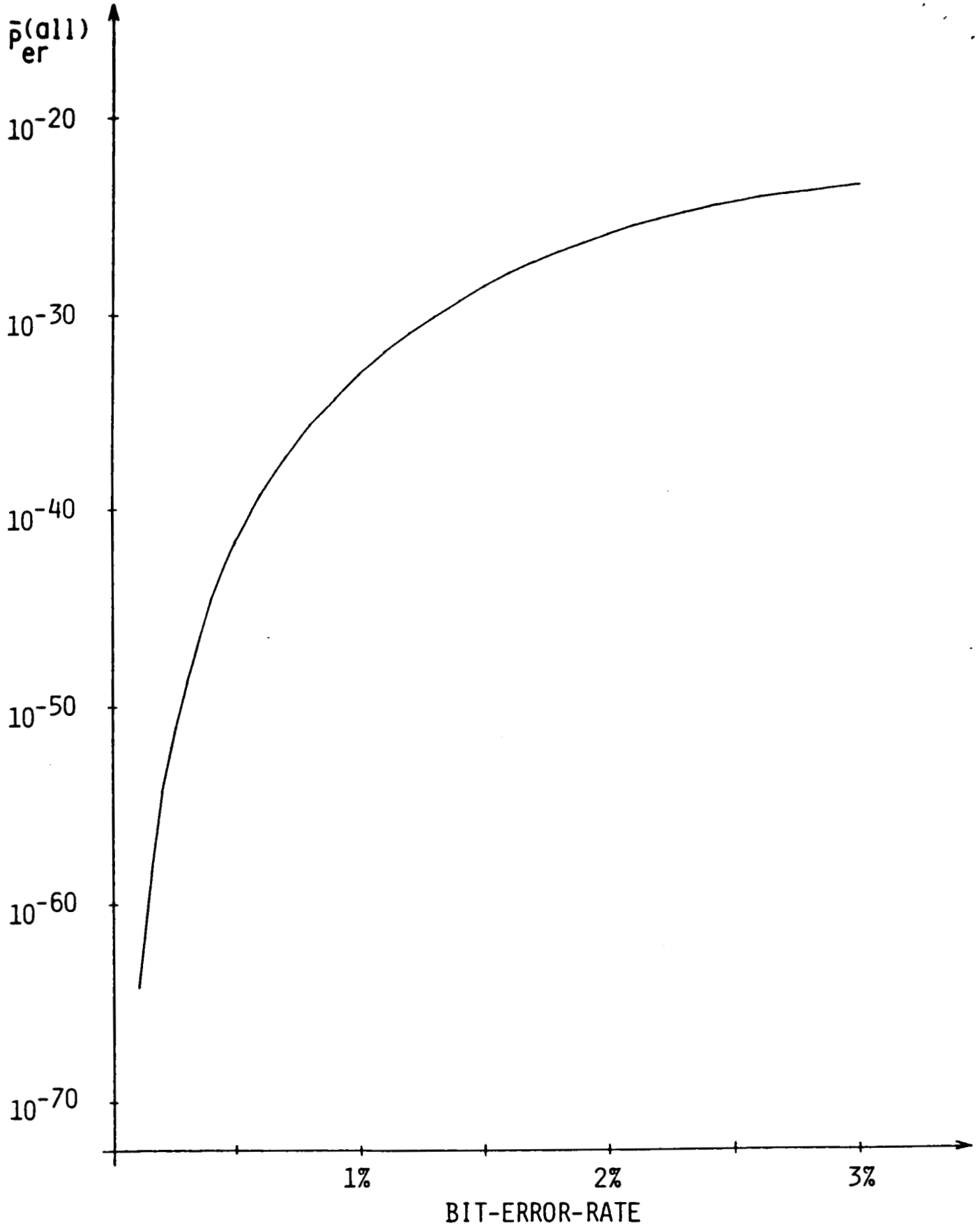

Figure 6 Upper bounds on the probability of incorrect decoding for a block when each subsection pair is decoded by the C_r-decoder.

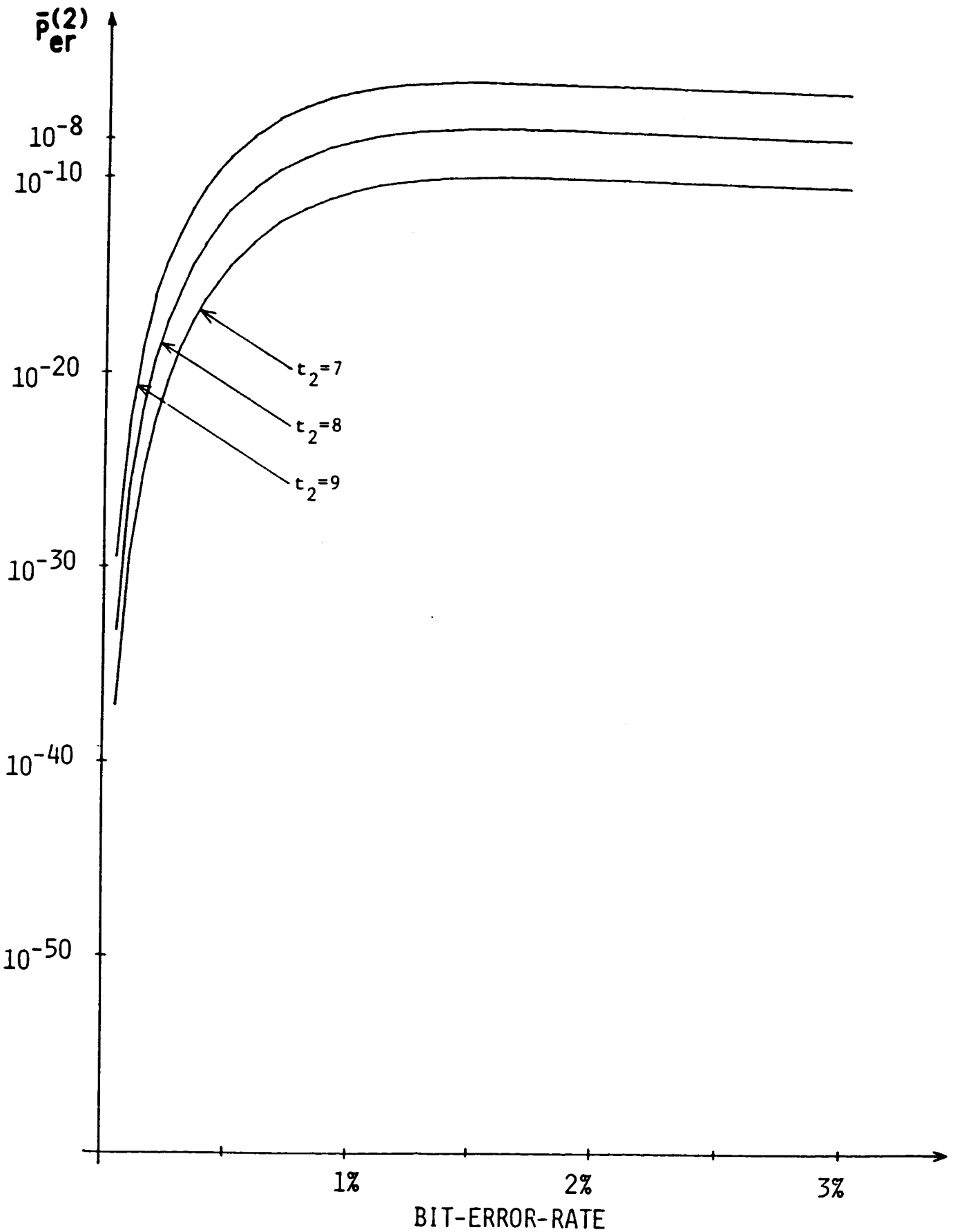

Figure 7 Upper bounds on the probability of a decoding error of the first specific scheme.

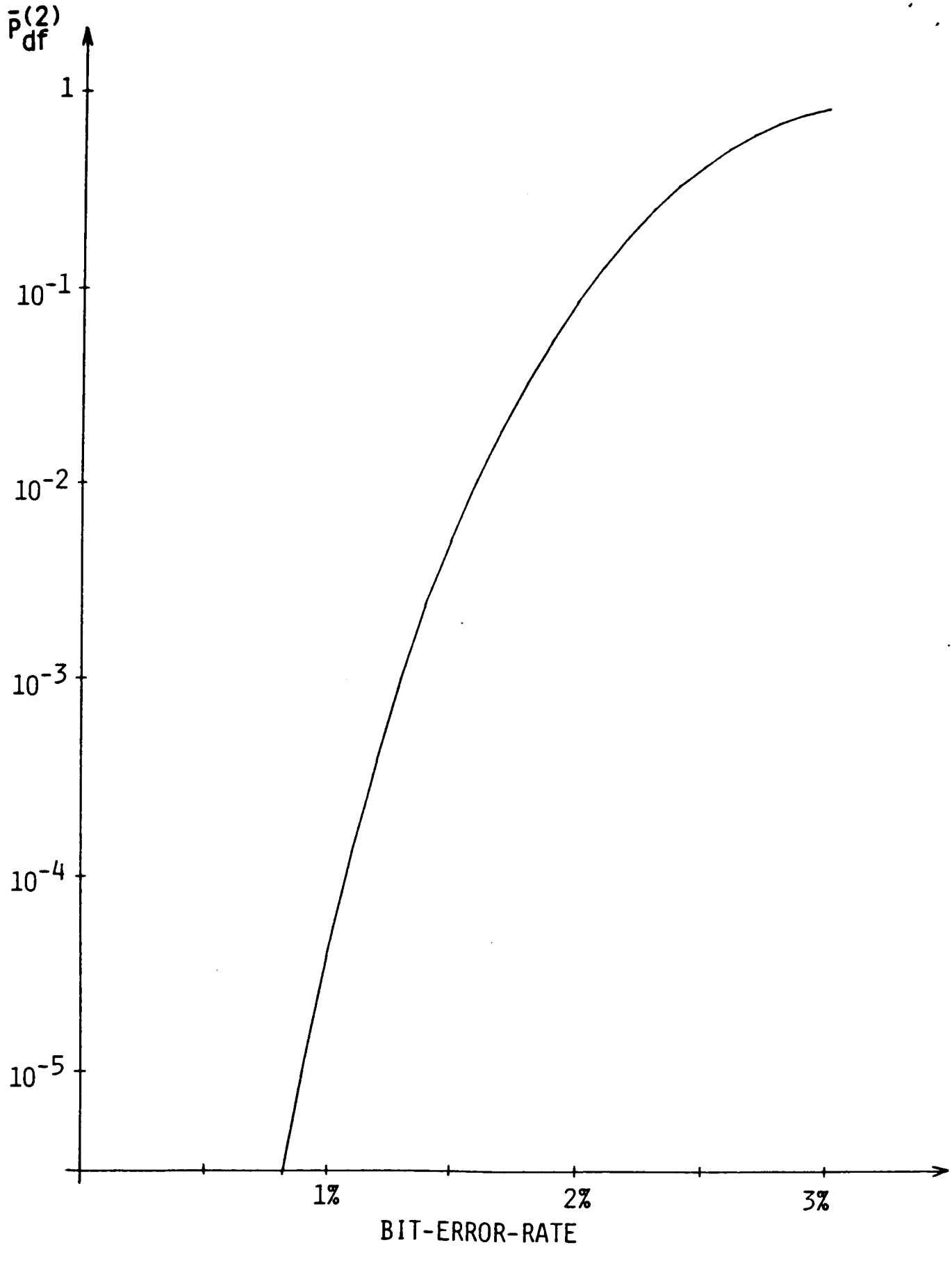

Figure 8 Upper bounds on the probability of a decoding failure of the first specific scheme.

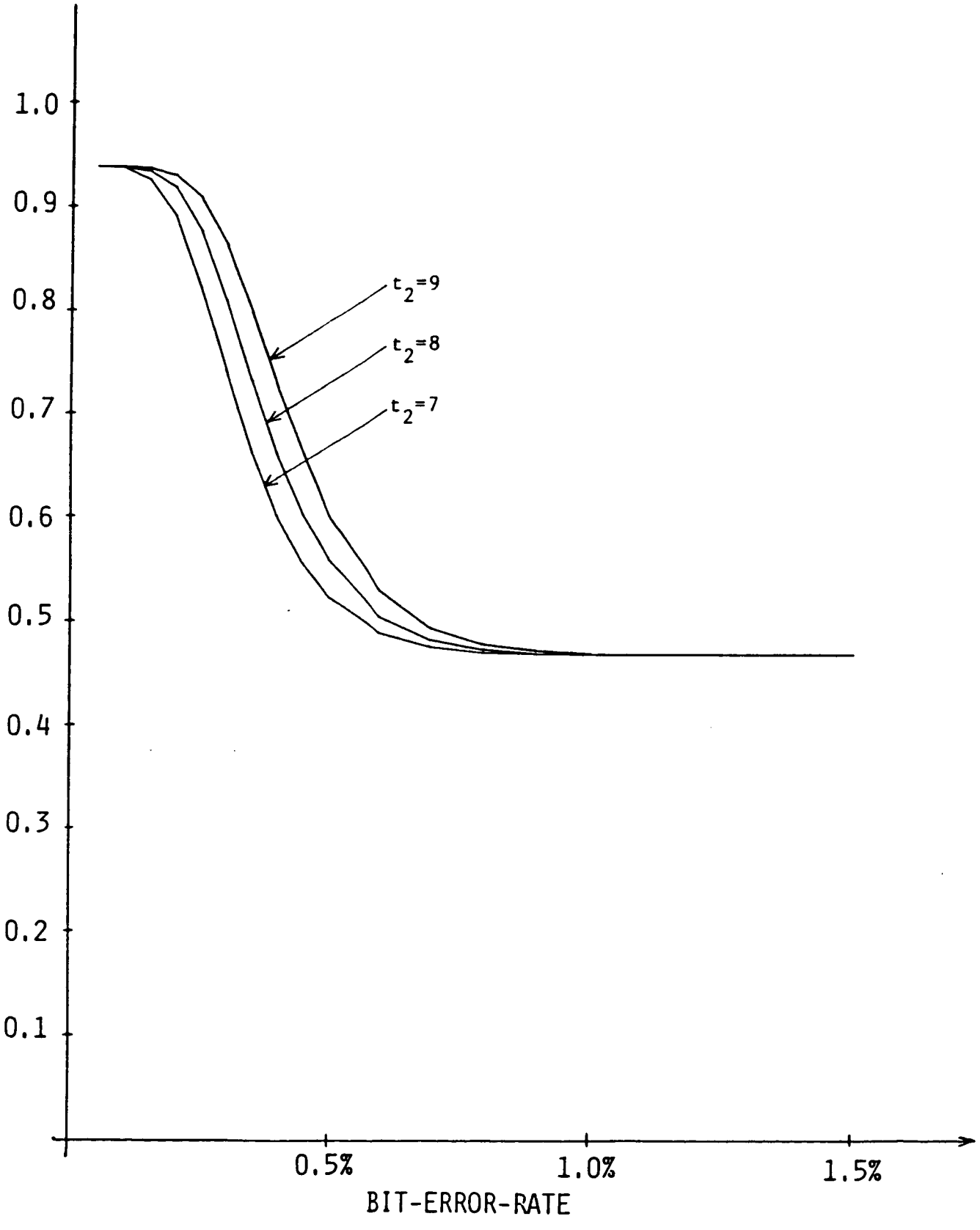

Figure 9 Lower bounds on a measure of the throughput efficiency of the first specific scheme.

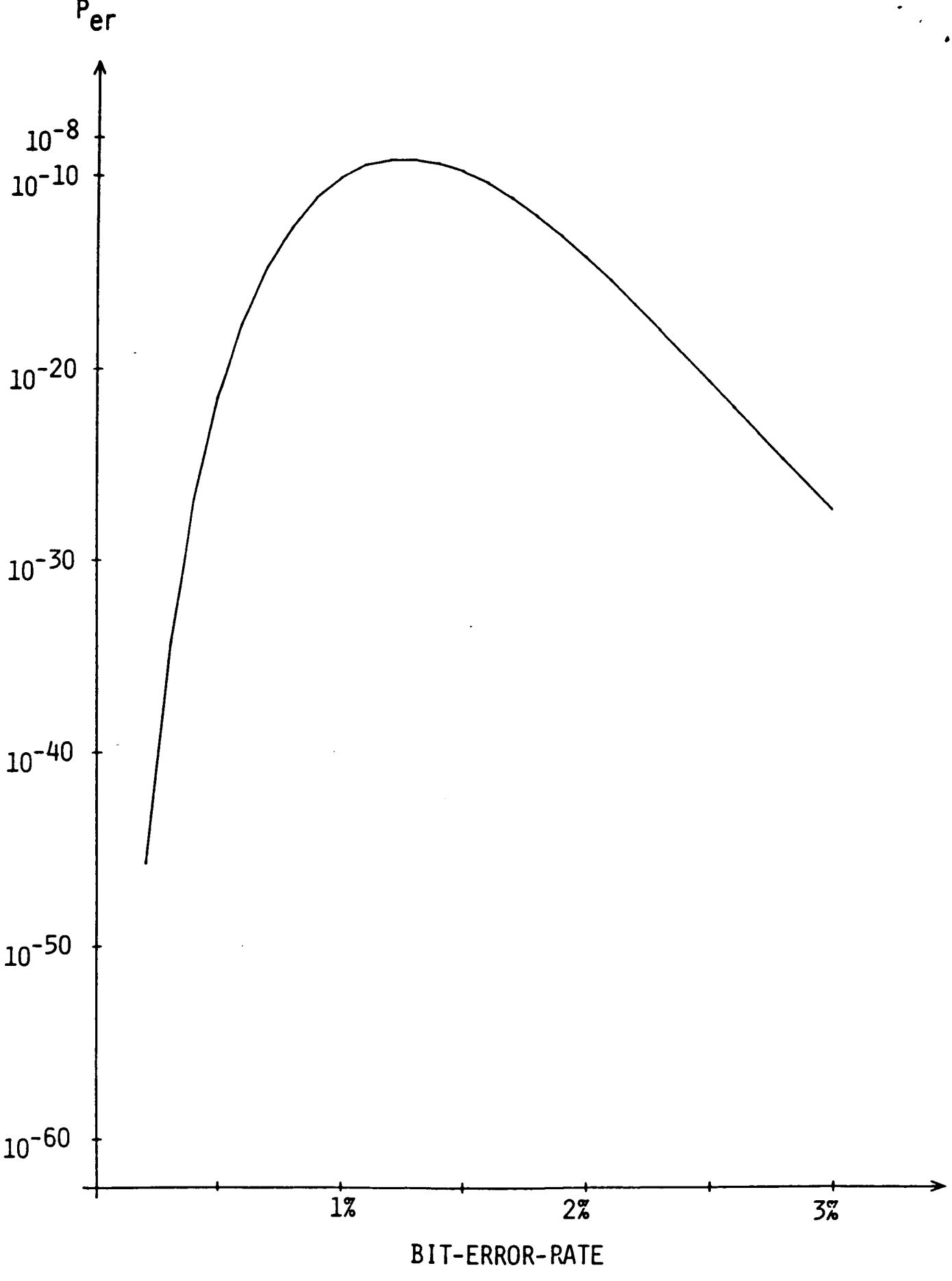

Figure 10 Upper bounds on the probability of a decoding error for a received data-block or parity-block by C_1 and C_2-decoders.

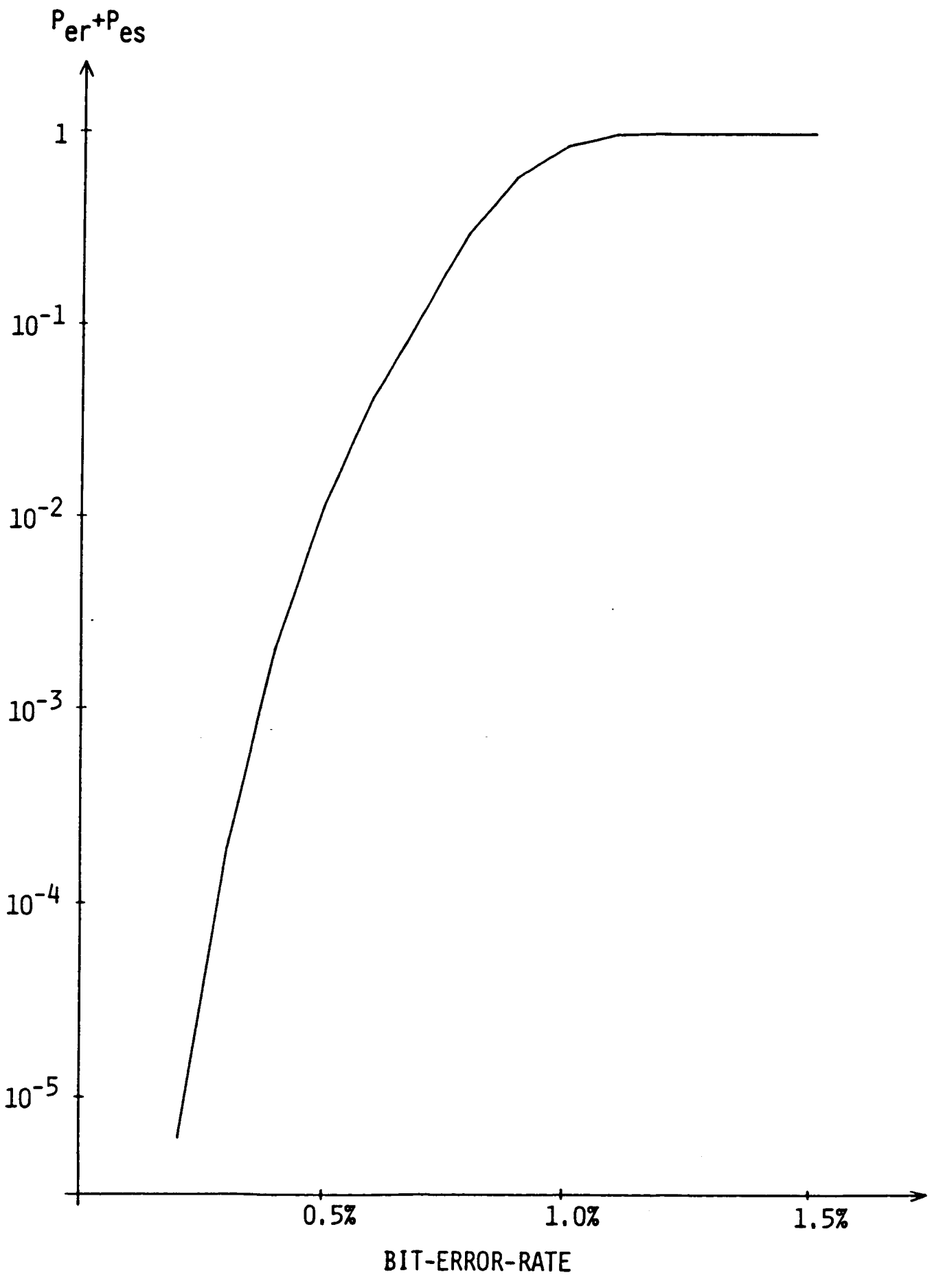

Figure 11 The sum of probabilities of a decoding failure and a decoding error for a received data-block or parity-block by the C_1 and C_2-decoder.

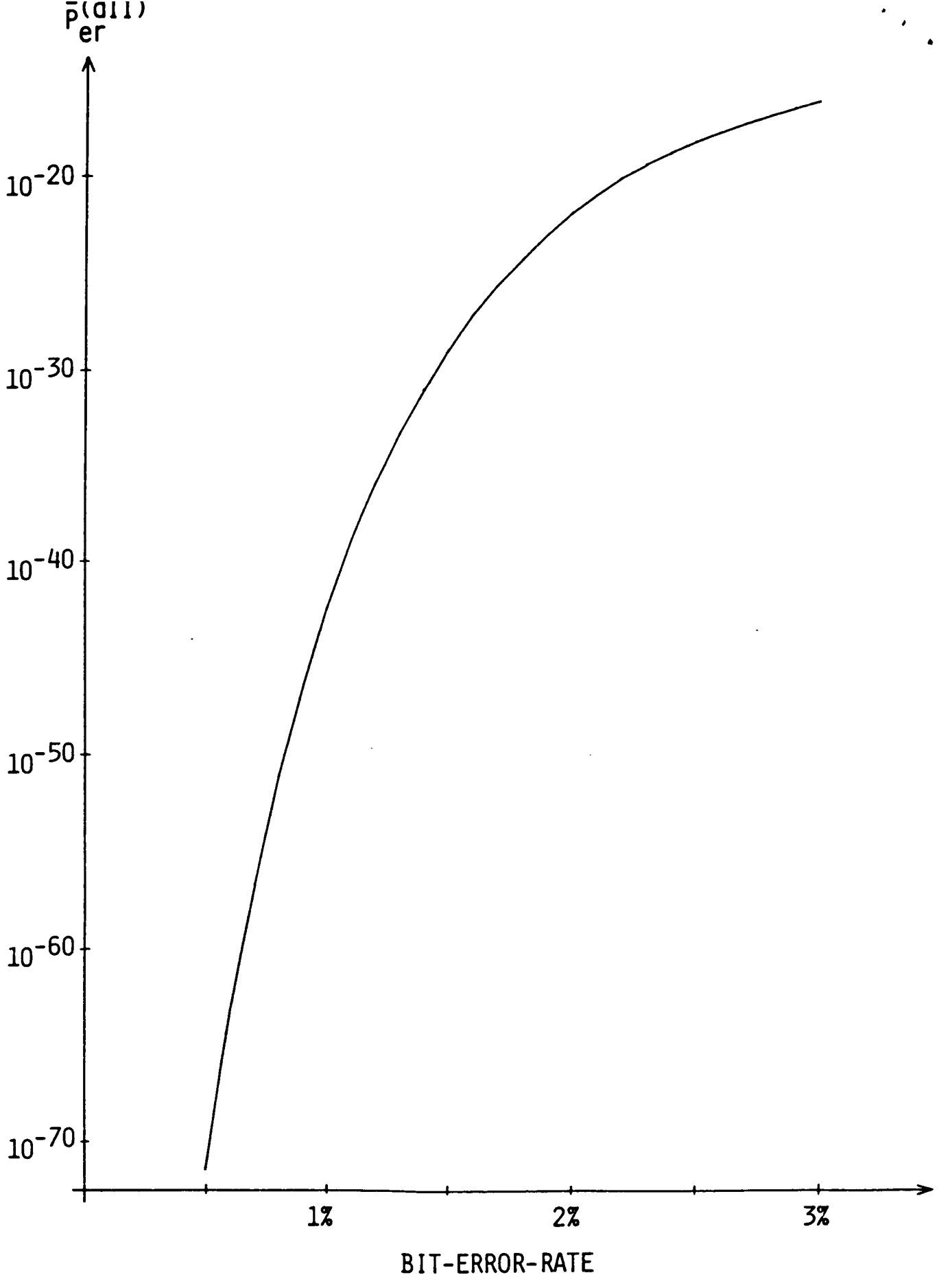

Figure 12 Upper bounds on the probability of a decoding error for a block when each frame is decoded by C_l-decoder at the first stage and then each received subsection pair is decoded by C_r-decoder at the second stage.

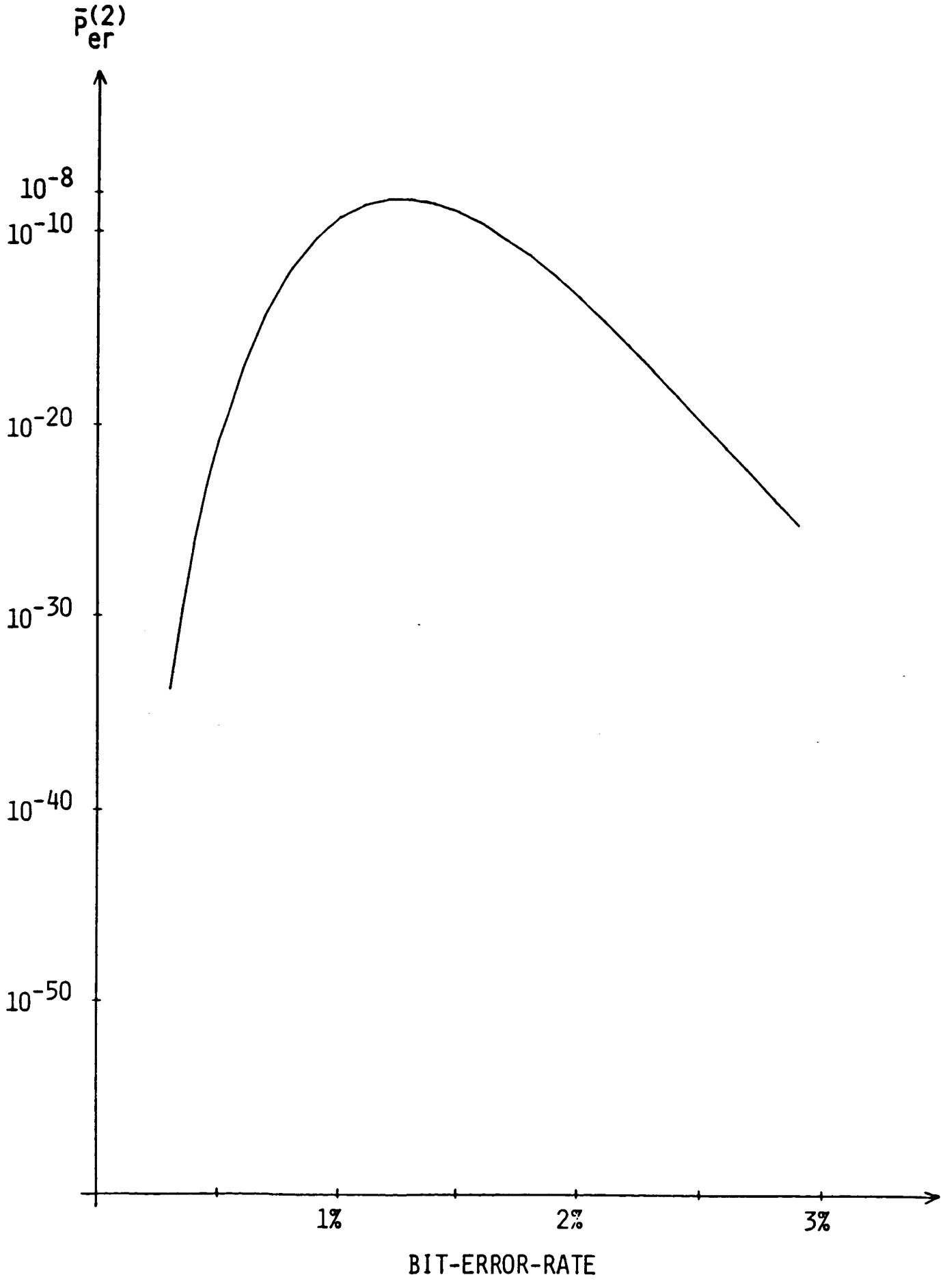

Figure 13 Upper bound on the probability of a decoding error for the the second specific scheme.

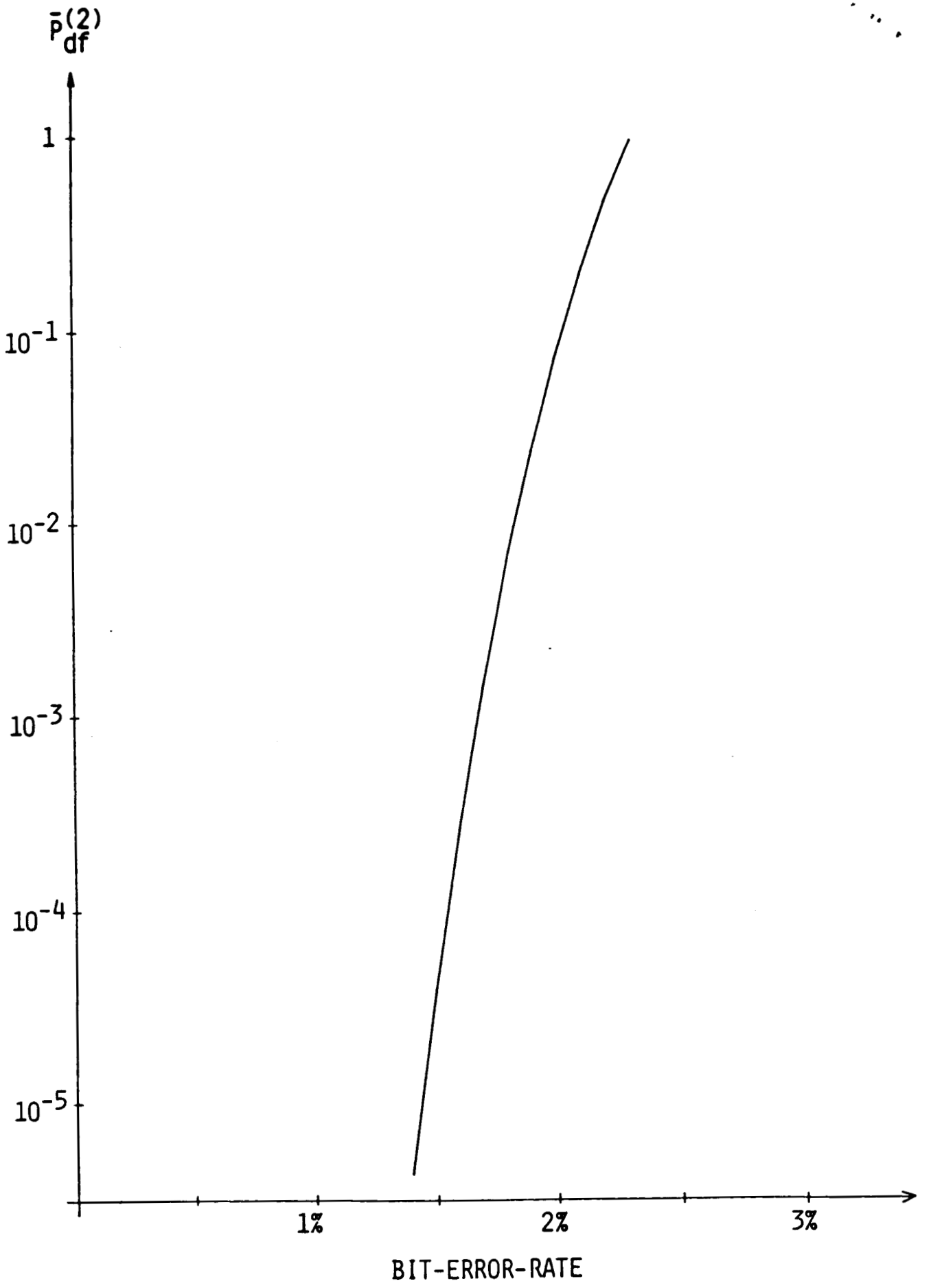

Figure 14 Upper bound on the probability of a decoding failure for the second specific scheme.

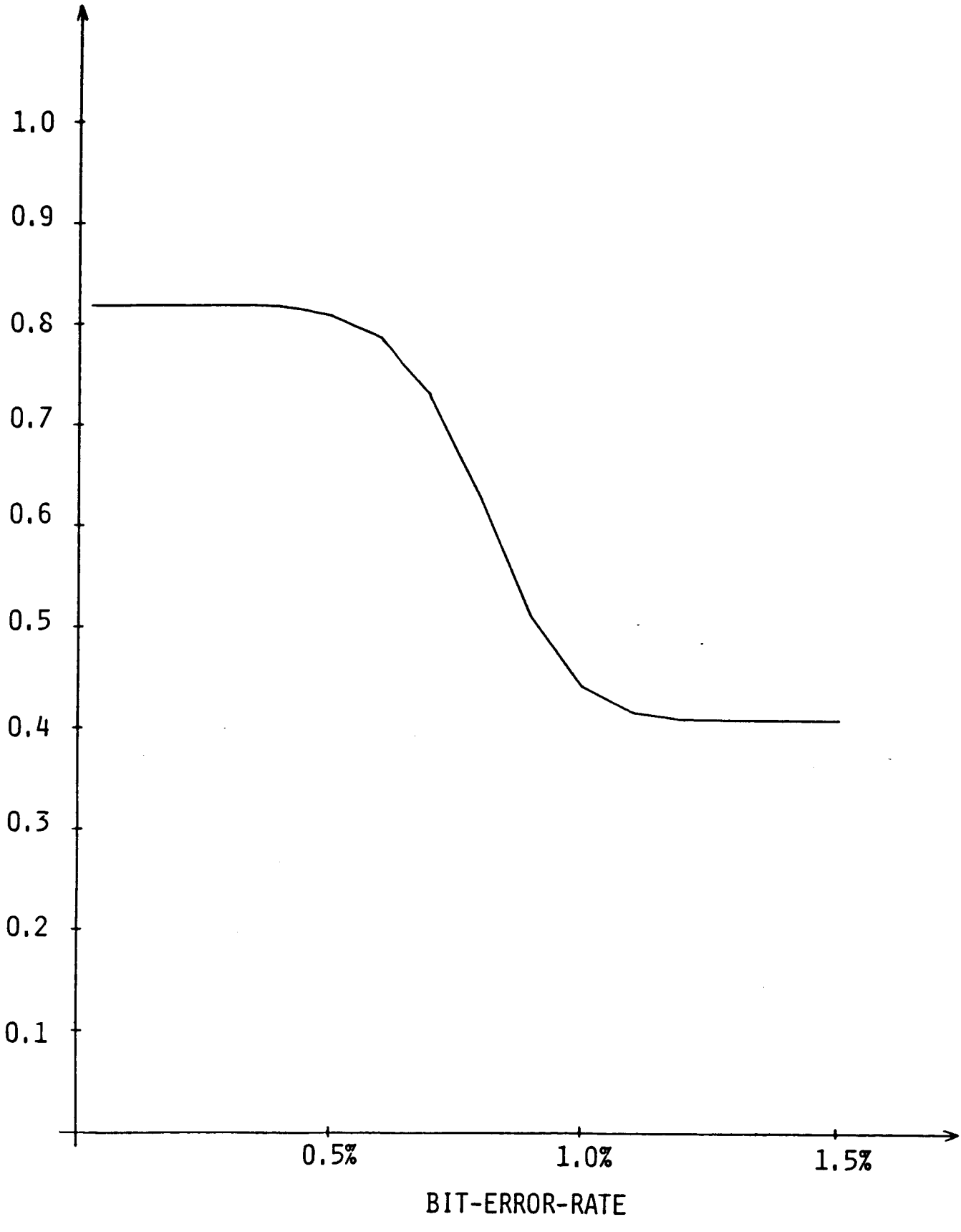

Figure 15 Lower bound on a measure of the throughput efficiency for the second specific scheme.

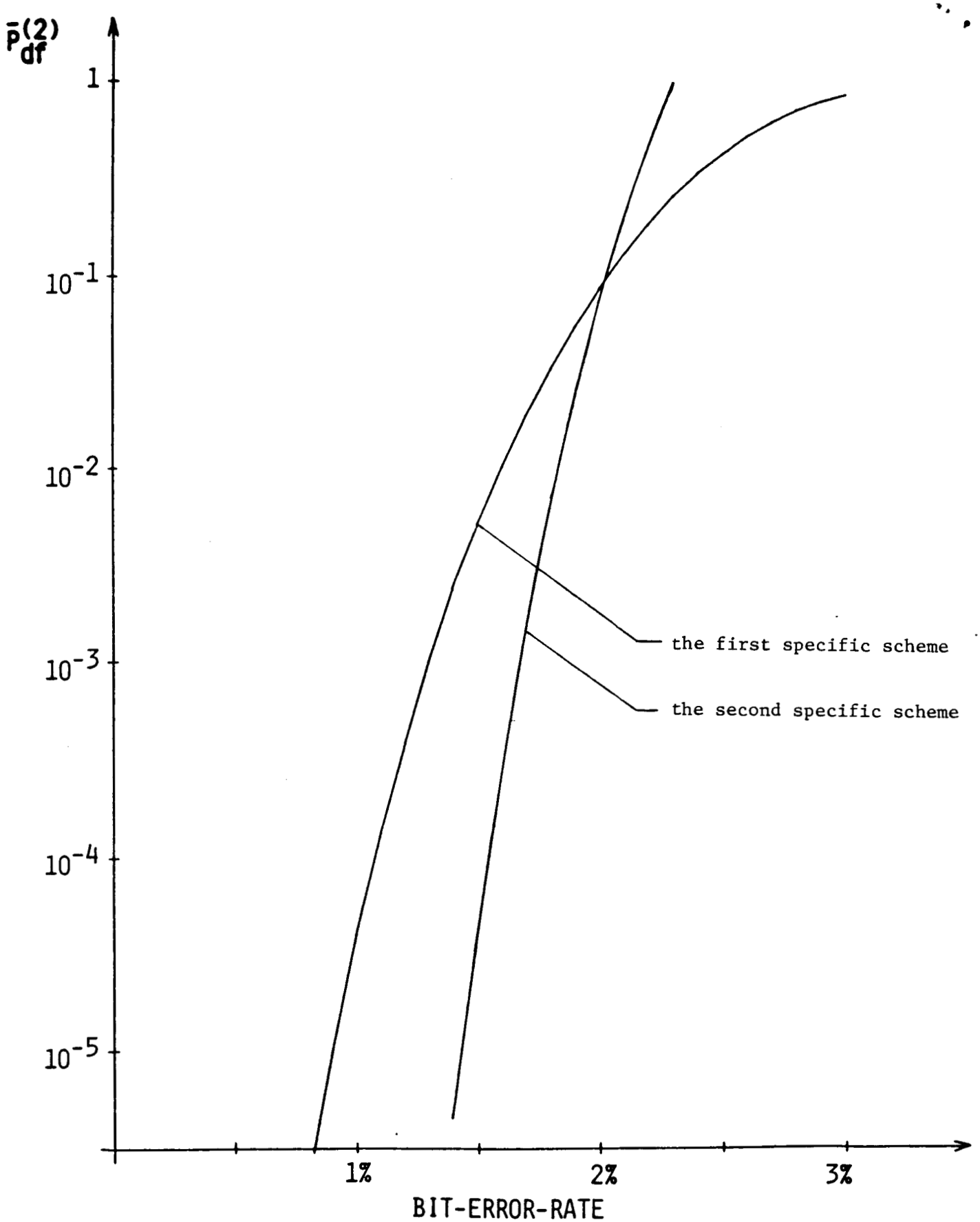

Figure 16 Upper bounds on the probability of a decoding failure for two schemes.

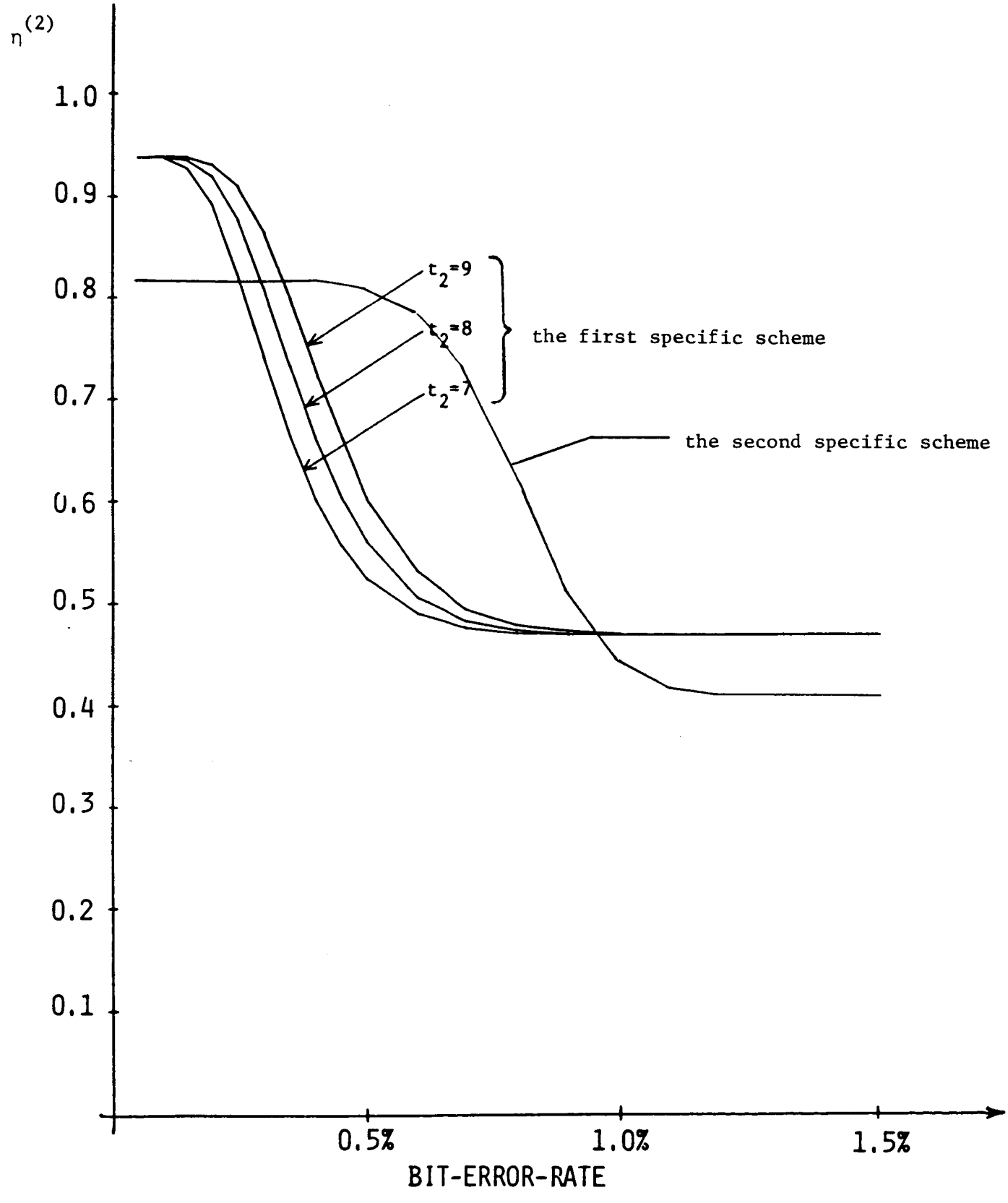

Figure 17 Lower bounds on a measure of the throughput efficiency for the two schemes.