FINAL REPORT

to

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
Goddard Space Flight Center
Greenbelt, Maryland 20771

CODING FOR RELIABLE SATELLITE COMMUNICATIONS

Grant No.: NAG 5-407

Period: July 1, 1984 to June 30, 1986

Principal Investigators

N.T. Gaarder
(January 1 - June 30, 1986)

Shu Lin
(July 1, 1984 - December 31, 1985)

Department of Electrical Engineering
University of Hawaii at Manoa
Honolulu, Hawaii 96822
CODING FOR RELIABLE SATELLITE COMMUNICATIONS

ABSTRACT

This research project was set up to investigate several error control coding techniques for reliable satellite communications. During the project period, we investigated the following areas: (1) decoding of Reed-Solomon codes in terms of dual basis; (2) concatenated and cascaded error control coding schemes for satellite and space communications; (3) using hybrid coding schemes (error correction and detection incorporated with retransmission) to improve system reliability and throughput in satellite communications; (4) good codes for simultaneous error correction and error detection; and (5) error control techniques for ring and star networks. Significant results were obtained in all the above areas.
I. A SUMMARY OF RESEARCH RESULTS

This research project was set up to study various kinds of coding techniques for error control in satellite and space communications for NASA Goddard Space Flight Center. During the project period, we investigated the following areas: (1) decoding of Reed-Solomon codes in terms of dual basis; (2) concatenated and cascaded error control coding schemes for satellite and space communications; (3) using hybrid coding schemes (error correction and detection incorporated with retransmission) to improve system reliability and throughput in satellite communications; (4) good codes for simultaneous error correction and error detection; and (5) error control techniques for ring and star networks. Significant results were obtained in all the above areas. In the following, we summarize our research results.

1. Decoding of Reed-Solomon Codes in Dual Basis

Reed-Solomon codes form a class of very powerful cyclic block codes. They are widely used for controlling transmission errors in data communication systems as well as data storage systems. Recently Berlekamp [1] devised a new method for encoding these codes which greatly reduces the encoding-complexity. Berlekamp's encoder is implemented in terms of dual basis using bit-serial multipliers.

During the project period, we investigated decoding of Reed-Solomon codes using the dual basis. The decoding algorithm being used is the Peterson-Berlekamp-Chien algorithm. The algorithm consists of four steps:

1. Compute the syndrome \( \bar{S} = (S_1, S_2, \ldots, S_{2t}) \) from the received polynomial \( \bar{r}(X) \).
2. Determine the error-location polynomial \( Q(X) \) from the syndrome \( \bar{S} \).
3. Determine the error-value evaluator \( Z(X) \) from the syndrome.
4. Evaluate the error-location numbers and error values, and perform error correction.
All the four decoding steps can be carried out in dual basis using bit-serial multiplications or combination of bit-serial multiplications and parallel multiplications. The circuit for the four decoding steps are shown in Figures 1 and 3. An organization for a Reed-Solomon code decoder is shown in Figure 4.

A technical report on the decoding of Reed-Solomon codes in the dual form was written and submitted to NASA Goddard Space Flight Center.

2. A Concatenated Coding Scheme for NASA Telecommand System

During the project period, we also investigated a concatenated coding scheme for error control in data communications. In this scheme, the inner code is used for both error correction and error 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 scheme proposed for NASA Telecommand system is analyzed.

In the scheme proposed for NASA Telecommand system, both inner code and outer code are shortened Hamming codes. The inner code is a distance-4 shortened Hamming code with generator polynomial,

\[ g(X) = (X+1)(X^6+X+1) = X^7+X^6+X^2+1. \]

This code is capable of correcting any single error and detecting any double errors. The outer code is also a distance-4 shortened Hamming code with generator polynomial,

\[ g(X) = X^{16}+X^{12}+X^5+1. \]

This code is the X.25 standard for packet-switched data network [2]. The 16 parity bits of this code is used for error detection only. The reliability performance of the above scheme is analyzed. We have shown that, for bit-error-rate less than $10^{-5}$, the scheme provides extremely high reliability.
A technical report on the performance study of the concatenated coding scheme described above was written and sent to NASA Goddard Space Flight Center.

3. A Cascaded Error Control Coding Scheme for Satellite and Space Communications

In this scheme, two linear block codes, $C_1$ and $C_2$, are used. The inner code $C_1$ is a binary $(n_1, k_1)$ code with minimum distance $d_1$. The inner code is designed to correct $t_1$ or fewer errors and simultaneously detect $t_1 + 1$ or fewer errors where $t_1 + 1 \leq d_1 [3]$. The outer code $C_2$ is an $(n_2, k_2)$ code with symbols from the Galois Field $GF(2^\ell)$ and minimum distance $d_2$. If each code symbol of the outer code is represented by binary $\ell$-tuple based on certain basis of $GF(2^\ell)$, then the outer code becomes an $(n_2^\ell, k_2^\ell)$ linear binary code. For the proposed coding scheme, we assume that the following conditions hold:

$$k_1 = m_1 \ell,$$

and

$$n_2 = m_1 m_2,$$

where $m_1$ and $m_2$ are positive integers.

The encoding is performed in two stages as shown in Figure 5. First, a message of $k_2^\ell$ binary information digits is divided into $k_2$ bytes of information bits each. Each $\ell$-bit byte (or binary $\ell$-tuple) is regarded as a symbol in $GF(2^\ell)$. These $k_2$ bytes are encoded according to the outer code $C_2$ to form an $n_2$-byte ($n_2^\ell$ bits) codeword in $C$. At the second stage of encoding, the $n_2$-byte codeword at the output of the outer code encoder is divided into $m_2$ segments of $m$ bytes (or $m_2^\ell$ bits) each. Each $m_1$-byte segment is then encoded according to the inner code $C_1$ to form an $n_1$-bit codeword. This $n_1$-bit codeword in $C_1$ is called a frame. Thus, corresponding to a message of $k_2^\ell$-bit at the input of the outer code encoder, the output of the inner code encoder is a sequence of $m_2$ frames of $n_1$ bits each. This
sequence of $m_2$ frames is called a block. A block format is depicted in Figure 6.

The decoding of the scheme also consists of two stages as shown in Figure 5. The first stage of decoding is the inner code decoding. Depending on the number of errors in a received frame, the inner code decoder performs one of the three following operations: error-correction, erasure and leave-it-alone (LIA) operations. When a frame in a block is received, its syndrome is computed based on the inner code $C_{n_1-k_1}$. If the syndrome corresponds to an error pattern $e$ of $t_1$ or fewer errors, error correction is performed by adding $e$ to the received frame. The $n_1-k_1$ parity bits are removed from the decoded frame, and the decoded $m_1$-byte segment is stored in a receiver buffer for the second stage of decoding. A successfully decoded segment is called a decoded segment with no mark. Note that 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 $t_1$, the errors may result in a syndrome which corresponds to a correctable error pattern with $t_1$ or fewer errors. In this case, the decoding will be successful, but the decoded frame (or segment) contains undetected errors. If an uncorrectable error pattern is detected in a received frame, the inner code decoder will perform one of the following two operations based on a certain criterion:

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

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 $m_2$ 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.

As soon as $m_2$ frames in a received block have been processed, the second stage of decoding begins and the outer code decoder starts to decode the $m_2$ segments stored in the buffer. Note that an erased segment creates $m_1$ symbol erasures (or $m_1$ 8-bit-byte erasures). Symbol errors are contained in the segments with or without marks. The outer code $C_2$ and its decoder are designed to correct the combinations of symbol erasures and symbol errors. Maximum-distance-separable codes with symbol from $GF(2^8)$ are most effective in correcting symbol erasures and errors.

Let $i$ and $h$ be the numbers of erased segments and marked segments respectively. The outer code decoder declares an erasure (or raises a flag) for the entire block of $m_2$ segments if either of the following two events occurs:

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

2. The number $h$ is greater than a certain threshold $T_{el}(i)$ with
   
   \[ T_{el}(i) \leq \frac{(d_2-1-m_1)i}{2} \text{ for a given } i. \]

If none of the above two events occurs, the outer code decoder starts the error-correction operation on the $m_2$ decoded segments. The $m_1i$ symbol erasures and the symbol errors in the marked or unmarked segments are corrected based on the outer code $C_2$. Let $t_2(i)$ be the error-correction threshold for a given $i$ where

\[ t_2(i) \leq \frac{(d_2-1-m_1)i}{2}. \]

If the syndrome of $m_2$ decoded segments in the buffer corresponds to an error pattern of $m_1i$ erasures and $t_2(i)$ or fewer symbol errors, error-correction is performed. The values of the erased symbols, and the values and the
locations of symbol errors are determined based on a certain algorithm. If more than \( t_2(i) \) symbol errors are detected, then the outer code decoder again declares an erasure (or raises a flag) for the entire block of \( m_2 \) decoded segments.

The error performance of the proposed cascaded coding scheme where the outer code is used for both error correction and detection was analyzed. We showed that, if proper inner and outer codes are chosen, the scheme provides extremely good reliability even for high-bit-error-rate \( \varepsilon=10^{-2} \). The scheme is particularly suitable for downlink error control in satellite communications. A number of specific schemes using various inner and outer codes were proposed to NASA-GSFC for possible applications in satellite communications.

A technical report on this scheme was submitted to NASA-GSFC.

4. Error Detecting Capabilities of IEEE standard 802.3 Codes

During the project period, we investigated the error detecting capabilities of the shortened Hamming codes which are adopted for error detection in IEEE Standard 802.3 CSMA/CD. These codes are also used for error detection in the data link layer of the Ethernet, a local network. The generator polynomial of these codes is

\[
X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^{8} + X^{7} + X^{5} + X^{4} + X^{2} + X + 1,
\]

a primitive polynomial of degree 32. Let \( C_n \) denote the shortened code of length \( n \). In the Ethernet the code length \( n \) is a multiple of 8 greater than 511 and less than 12145.

We first compute the weight distribution of the dual code of \( C_n \) for \( n=2^p \) with \( 9<p<13 \) and \( n=12144 \) by the Method II in [4]. Using MacWilliams' identity we compute the number of codewords in \( C_n \) whose weight is \( i \) for these \( n \) and \( 3<i<30 \). From the results we notice that the minimum-distance of
\( C_n \), denoted as \( d_n \), is 4 or 5 for \( 512 < n < 12144 \). By finding the \( n_0 \) such that \( d_{n_0} = 5 \) and \( d_{n_0+1} = 4 \), we show that \( d_n = 5 \) for \( 512 < n < 3006 \), and \( d = 4 \) for \( 3007 < n < 12144 \).

Let \( p_e(C_n, \varepsilon) \) and \( p_d(C_n, \varepsilon) \) be the probability of undetectable error and that of detectable error, respectively, when code \( C_n \) is used for error detection on a binary symmetric channel with bit-error-rate \( \varepsilon \). From the weight distributions of the dual codes, we compute \( p_e(C_n, \varepsilon) \) and \( p_d(C_n, \varepsilon) \) for \( n = 2^p \) with \( 9 < p < 13 \) and \( n = 12144 \), and \( 10^{-5} \leq \varepsilon \leq 1/2 \). The results are plotted in Figures 7 and 8. From the computation we see that the maximum value of \( p_e(C_{512}, \varepsilon) \) for \( \varepsilon < 1/2 \) is \( 2.6544E-10 \) which occurs for \( \varepsilon = 1.3918E-2 \) and the maximum value of \( p_e(C_{1024}, \varepsilon) \) for \( \varepsilon < 1/2 \) is \( 2.3286E-10 \) which occurs for \( \varepsilon = 1.4383E-2 \). Note that these peak values are greater than \( 2^{-32} \). For the larger values \( n = 2^p \) with \( 11 \leq p \leq 13 \) and \( n = 12444 \), no peak is detected within accuracy in computation.

We also analyze the double-burst-detecting capability. Using the algorithm in [5] we compute the maximum code length \( n_\beta \) such that \( C_{n_\beta} \) has the capability of correcting any burst error of length \( \beta \) or less. We show that \( n_\beta = 38 \) for \( 14 \leq \beta \leq 16 \), \( n_{13} = 730 \), \( n_{12} = 1729 \), \( n_{11} = 5680 \), \( n_{10} = 11933 \) and \( n < 13000 \).

A technical report is in preparation and will be submitted to NASA-GSFC.

5. An ARQ Scheme for Broadcast Communication Systems

Consider a point-to-multipoint communication system consisting of \( (R+1) \) stations, where a single transmitter broadcasts data frames to \( R \) receivers, each of which has a finite buffer capacity to store data frames for processing. During the project period, we investigated an ARQ scheme for error control in such system. In our proposed scheme, each data frame consists of \( k \) message bits and \((n-k)\) parity bits which are formed based on an \((n,k)\) linear block code for error detection. When a data frame is received by a receiver, parity checking is performed. If no error is detected, the received data frame (with \( n-k \) parity bits removed) is either delivered to the user or stored in the receiver buffer until it is ready to be delivered to the receiver.
user. If a received frame is detected in errors, it is discarded and the receiver requests a retransmission of that frame. In our proposed retransmission strategy, we use a constraint in the transmitter to prevent any buffer overflow at the receivers. Retransmissions continue until positive acknowledgements are received from all R receivers. All the receivers that have received a frame successfully, continue to positively acknowledge the retransmissions, whether or not the new copies of data frame are error free. Hence the scheme makes full use of the outcomes of previous transmissions. The proposed scheme can also handle data and/or acknowledgement loss.

The throughput performance of the proposed scheme is analyzed and simulated. Results obtained from analysis and simulation agree reasonably well. The results also show that the proposed scheme outperforms the full-memory go-back-N scheme proposed by Gopal, et al. [6].

A technical report on this ARQ scheme has been submitted to NASA-GSFC.

REFERENCES


II. PERSONNEL

Principal Investigators:

Dr. Shu Lin (July 1, 1984 - December 31, 1985; Dr. Lin is currently on leave)

Dr. N.T. Gaarder (January 1 - June 30, 1986)

Consultant: Professor Tadao Kasami

Graduate Students:

Ram Chandran
Mao-chao Lin

III. RESEARCH ACTIVITIES

Journal Publications


Technical Reports


Conference Presentations

1. "Encoding and Decoding of Reed-Solomon Codes in Dual Basis," Seminar, Osaka University, October 31, 1984.


Consultation with NASA Officers

During the project period, Dr. Lin made three visits (November 3, 1984; March 29, 1985 and April 1, 1986) to NASA Goddard Space Flight Center, and discussed with Dr. James C. Morakis and Mr. Warner H. Miller on various project problems.
Figure 1 A circuit for computing the syndrome component $S_i$ with a bit-serial multiplier.
Figure 2 Circuit for finding $\sigma(X)$ and $Z(X)$
Input

Receiver Buffer Register $T(X)$ (dual form)

$T(X)$ (dual form)

Adder $C$

$Z(\alpha^e)$ (dual form)

Adder $C$

$Z(\alpha^e)$ (dual form)

Gate

Look-up Table

$[\alpha^e \sigma'(\alpha^e)]^{-1}$ (conventional form)

$\alpha^e \sigma'(\alpha^e)$

Adder

$B$

Adder

$\sum_{i \text{ even}} \sigma_i \alpha^{i\ell}$ (dual)

$\sum_{i \text{ odd}} \sigma_i \alpha^{i\ell}$ (dual)

Figure 3 Error-correction circuit
Figure 4 An organization of a RS decoder
Figure 5 A cascaded coding system
Figure 6. Block format
The probability of undetectable error

\[ P_e(C_n, \epsilon) \]

Bit-error-rate \( \epsilon \)

Figure 7 The probability \( P_e(C_n, \epsilon) \) that a received vector contains an undetected error pattern for a binary symmetric channel with bit-error-rate \( \epsilon \).
The probability of detectable error

\[ P_d(C_n, \epsilon) \]

Figure 8 The probability \( P_d(C_n, \epsilon) \) that a received vector contains a detectable error pattern for a binary symmetric channel with bit-error-rate \( \epsilon \).