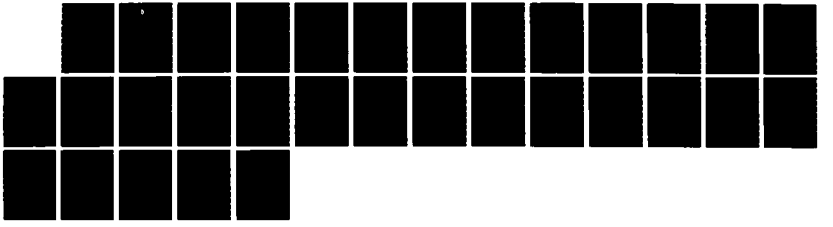
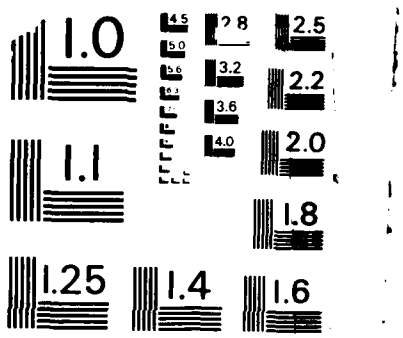
AD-A176 809 THE ALGEBRAIC STRUCTURE OF CONVOLUTIONAL CODES(U) 1/1
UNIVERSITY OF SOUTHERN CALIFORNIA LOS ANGELES DEPT OF
ELECTRICAL ENGINEERING I S REED 10 NOV 86
UNCLASSIFIED AFOSR-TR-87-0124 AFOSR-85-0239 F/G 9/4 NL





(2)

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

AD-A176 889 ... 1987 ... D

	1b. RESTRICTIVE MARKINGS
	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited.
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S) AFOSR-TR- 87-0124
6a. NAME OF PERFORMING ORGANIZATION Univ. of Southern Calif.	6b. OFFICE SYMBOL (If applicable)
	7a. NAME OF MONITORING ORGANIZATION AFOSR
6c. ADDRESS (City, State and ZIP Code) Dept. of EE-Systems University Park Los Angeles, CA 90089-0272	7b. ADDRESS (City, State and ZIP Code) same as 8c
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Dept. of the Air Force	8b. OFFICE SYMBOL (If applicable) NM
	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER AFOSR-85-0259
8c. ADDRESS (City, State and ZIP Code) Air Force Office of Scientific Research (AFSC) Bolling Air Force Base, DC 20332-6448	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. 61102F; PROJECT NO. 2303; TASK NO. A3; WORK UNIT NO. EK2
11. TITLE (Include Security Classification) The Algebraic Structure of ... Convolutional Codes	
12. PERSONAL AUTHOR(S) Irving S. Reed	
13a. TYPE OF REPORT Annual Scientific	13b. TIME COVERED FROM 7/1/84 TO 6/30/85
	14. DATE OF REPORT (Yr., Mo., Day) 1986 November 10
	15. PAGE COUNT
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES		
FIELD	GROUP	SUB. GR

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

A new error-trellis syndrome decoding scheme for convolutional codes is developed. It is demonstrated that the real advantage of error-trellis decoding over both Viterbi and sequential decoding of convolutional codes is the reduction of the number of states and transitions between any two frames. An algebraic syndrome decoder is developed to find the best estimated message sequence for dual-K convolutional codes without finding minimum-error paths in an error-trellis diagram. A LSI chip is developed to realize this algorithm. Another new VLSI architecture is also developed for the Reed-Solomon decoder.

PTR. FILE COPY

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS ☐	21. ABSTRACT SECURITY CLASSIFICATION
22a. NAME OF RESPONSIBLE INDIVIDUAL Irving S. Reed	22b. TELEPHONE NUMBER (Include Area Code) (213) 743-5001
	22c. OFFICE SYMBOL AFOSR/NM

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

SECURITY CLASSIFICATION OF THIS PAGE

THE ALGEBRAIC STRUCTURE OF CONVOLUTIONAL CODES

AFOSR CONTRACT AFOSR-85-0259

Annual Report

July 15, 1985 - July 14, 1986

Irving S. Reed

Annual Technical Progress Report

1. Grant Title and Number: "The Algebraic Structure of Convolutional Codes"

2. Contractor: University of Southern California

3. Period Covered: July 15, 1985 - July 14, 1986

4. Report Prepared By: Prof. Irving S. Reed, Principal Investigator

5. Date Prepared: October 28, 1986

6. A One Year Technical Research Summary:

-"Error-Trellis Syndrome Decoding for Convolutional Codes."

A new error-trellis syndrome decoding scheme for CCs is developed. It is demonstrated that the real advantage of error-trellis decoding over both Viterbi and sequential decoding of CCs is the reduction of the number of states and transitions between any two frames.

-"CSI Architecture for Algebraic Syndrome Decoding of Dual-K Convolutional Codes."

An algebraic syndrome decoder is developed to find the best estimated message sequence for dual-K CCs without finding minimum-error paths in an error-trellis diagram. The advantage of this algebraic syndrome decoder over an error-trellis decoder of the dual-K CCs is that the message sequence can be corrected without a necessity for storing a large number of states or paths in a constraint length of the error trellis diagram. Finally, a LSI chip is developed to realize this algorithm.

-"VLSI Design of a Pipeline Algebraic Syndrome Decoder."

A new VLSI architecture is developed for the Algebraic Syndrome decoder. The advantage of this new architecture is that a substantial reduction in the number of transistors is accomplished.

-"Searching High-Rate Systematic Optimum Distance Convolutional Codes."

Some high-rate systematic optimum distance convolutional codes are being searched with rates up to 7/8 and of constraint length up to 15. These codes can be efficiently decoded using error-trellis syndrome decoding.

-"Decoder Performance Simulation."

Decoder performance simulation is accomplished both for error-trellis decoding of convolutional codes and for algebraic syndrome decoding of dual-K convolutional codes.

7. Published Papers and Abstracts:

-I. S. Reed and T. K. Truong, "Sequential Syndrome Decoding Techniques for Convolutional Codes," submitted to IEE Proceedings, pt. E.

Abstract - This paper reviews previous studies (Refs. 1 and 2) of the algebraic structure of convolutional codes and extends those studies to apply to sequential syndrome decoding. These concepts are then used to realize by example actual sequential decoding, using the stack algorithm.

-J. F. Wang, I. S. Reed, T. K. Truong, J. Sun and J. Y. Lee, "LSI Architecture for Algebraic Syndrome Decoding of Dual-K Convolutional Codes," submitted to IEE Proceedings, pt. E.

Abstract - In this paper, algebraic syndrome decoders are developed which extend the early syndrome decoders of certain convolutional codes such as the Wyner-Ash code. Specifically syndrome decoders are designed to decode both the rate 1/2 and 1/3, dual-k, nonsystematic convolutional codes (CCs). Also the LSI architectures of these decoders are presented. Further, it is demonstrated that such decoders can be realized readily on a single chip with CMOS technology.

The advantage of this algebraic syndrome decoder over error-trellis decoding of dual-k CCs is that the message sequence can be corrected without the necessity for storing a number of states or paths in a constraint length of the error trellis diagram.

-J. M. Jensen and I. S. Reed, "Bounded Distance Coset Decoding of Convolutional Codes," IEE Proceedings, vol. 133, pt. F, no. 5, August 1986.

Abstract - This paper presents a maximum likelihood consistent bounded distance decoding algorithm for convolutional codes. The algorithm correctly decodes all error sequences which fall within the error correcting sphere. A class of codes is defined, in which the decoder exploits the fact that only certain error sequences need to be corrected. For these codes the decoding is based on a reduced encoder state diagram. Thus only a subset of the trellis or tree has to be searched in order to find the error pattern. An exact

characterization of the reduced state diagram is given in this paper along with an example.

-H. M. Shao, T. K. Truong, I. S. Hsu, L. J. Deutsch and I. S. Reed, "A Single Chip VLSI Reed-Solomon Decoder," Proc. Int'l. Conf. on Acoustics, Speech and Signal Processing, Tokyo, Japan, April 7-11, 1986.

Abstract - A new VLSI design of a pipeline Reed-Solomon decoder is presented. The transform decoding technique used in a previous design is replaced by a simple time domain algorithm. A new architecture which realizes such algorithm permits efficient pipeline processing with a minimum of circuits. A systolic array is also developed to perform erasure corrections in the new design. A modified form of Euclid's algorithm is developed with a new architecture which maintains a real-time throughput rate with less transistors. Such improvements result in both an enhanced capability and significant reduction in silicon area, thereby making it possible to build a pipeline (255,223) RS decoder on a single VLSI chip.

-J. F. Wang, I. S. Reed, T. K. Truong and J. Sun, "Algebraic Syndrome Decoding of Dual-K Convolutional Codes," to be submitted for publication soon.

In this paper, algebraic syndrome decoders are developed which extend the early syndrome decoders of high rate convolutional codes such as the Wyner-Ash code. In this paper, syndrome decoders are designed to decode the rate 1/n dual-k nonsystematic convolutional codes. The advantage of the algebraic syndrome decoders over error-trellis decoding of dual-k convolutional codes is that the message sequence can be corrected without the necessity of storing a large number of states or paths in a constraint length of the error trellis diagrams.

-I. S. Reed, I. S. Hsu, J. M. Jensen and T. K. Truong, "The VLSI Design of an Error-Trellis Syndrome Decoding for Certain Convolutional Codes," IEEE Trans. on Computers, vol. C-35, no. 9, pp. 781-789, September 1986.

A recursive algorithm using the error-trellis decoding technique is developed to decode certain convolutional codes, such as dual-k convolutional code. It is demonstrated that such a decoder can be realized readily on a single chip with NMOS technology.

8. List of Professional Personnal Associated with the Research Effort:

-Jaw John Chang received the B.S. degree from National Taiwan University, Taiwan, in 1965, the M.Eng. degree from Asian Institute of Technology, Thailand, in 1970, and the Ph.D. degree from the University of Southern California in 1981.

-Leslie J. Deutsch received the B.S. degree in mathematics from the California Institute of Technology, Pasadena, in 1976, and the M.S. and Ph.D. degrees in theoretical mathematics from the California Institute of Technology in 1979 and 1980, respectively, specializing in harmonic analysis.

-In-Shek Hsu received the B.S. and M.S. degrees in electrical engineering from National Taiwan University, Taipei, Taiwan in 1978 and 1980, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1984.

-J. M. Jensen received the B.Sc. degree in computer sciences in 1980 and the M.Sc. degree in mathematics in 1983, both from Aalborg University Center, Aalborg, Denmark.

-Irving S. Reed received the B.S. and Ph.D. degrees in mathematics from the California Institute of Technology, Pasadena, in 1944 and 1949, respectively.

-Howard M. Shao received the B.S. degree in communication engineering from National Chiao Tung University, Taiwan, in 1975, and the M.S. and Ph.D. degrees in electrical engineering from the University of Southern California, Los Angeles, in 1979 and 1983, respectively.

-Ju Sun received the M.S. degree in electrical engineering from the University of Southern California, Los Angeles, in 1983.

-T. K. Truong received the B.S. degree in electrical engineering from the National Cheng Kung University, Taiwan, China, in 1967, the M.S. Degree in electrical engineering from Washington University, St. Louis, MO, in 1971, and the Ph.D. degree from the University of Southern California, Los Angeles, in 1976.

THE ALGEBRAIC STRUCTURE OF CONVOLUTIONAL CODES

AFOSR Contract AFOSR-85-0259

Scientific Report

July 15, 1985 - July 14, 1986

Irving S. Reed

ABSTRACT

In this report, algebraic syndrome decoders are developed which extend the early syndrome decoders of certain convolutional codes such as the Wyner-Ash code. Specifically syndrome decoders are designed to decode both the rate 1/2 and 1/3, dual-k, nonsystematic convolutional codes (CCs). Also the LSI architectures of these decoders are presented. Further it is demonstrated that such decoders can be realized readily on a single chip with CMOS technology.

The advantage of this algebraic syndrome decoder over error-trellis decoding of dual-k CCs is that the message sequence can be corrected without the necessity for storing a number of states or paths in a constraint length of the error trellis diagram.

I. INTRODUCTION

Recently the authors [1,2,3] developed a new error-trellis syndrome decoding scheme for CCs. This method involved finding minimum-error paths in an error-trellis diagram. It was shown [1,2,3] that the computation of the error trellis could be accomplished by finding the solution of a syndrome equation explicitly in terms of the actual error sequences. The real advantage of error-trellis decoding over Viterbi coding-trellis decoding of CCs is the reduction of the number of states and transitions between any two frames.

It is shown (e.g., see [4]) that a simple logic design for a syndrome decoder can be found for a rate 3/4, one-error-correcting systematic Wyner-Ash code. In this paper, it is shown that these early syndrome decoders such as that used for the Wyner-Ash code can be extended to decode rate $1/n$, dual-k CCs for $n = 2,3$. It is well known, see [5], that a rate $1/n$ dual-k CCs is capable of correcting only t errors in two codeword frames where $t = n-1$. From this fact, it is shown here that an algebraic syndrome decoder can be developed to find the best estimated message sequence $\hat{v}$ for dual-k CCs without finding minimum-error paths in an error-trellis diagram. In other words, if no more than t symbol errors occur in two codeword frames, an algebraic syndrome decoder can be developed which recursively determines the best next corrected message symbol $\hat{v}_i$ from only the current best estimated symbol $\hat{v}_{i-1}$ and the received sequence at time frames i and $i+1$.

Next, an LSI architecture is developed to realize these new algebraic syndrome decoders for both rate 1/2 and 1/2, dual-3 CCs. The designs of these decoders are regular, simple and therefore naturally suitable for LSI implementation.

II. PROPERTIES OF CONVOLUTIONAL CODE

In order to systematically develop an algebraic syndrome decoder, certain properties of a convolutional code are needed.

First let the information of message sequence, the input to the CC, be represented by

$$\underline{x}(D) = [x_1(D), x_2(D) \cdots x_k(D)], \tag{1a}$$

where

$$x_j(D) = \sum_{i=0}^{\infty} x_{ji} D^i \quad 1 \le j \le k \tag{1b}$$

are elements in $F[D]$, the ring of polynomials in the unit delay operator D over $F = GF(q)$, a Galois field, with q, a power of a prime integer. Vector $\underline{x}(D)$ is a generating function in D of the input message sequence $\underline{x} = [\underline{x}_0, \cdots \underline{x}_j, \cdots]$, where $\underline{x}_j = [x_{j1}, \ldots, x_{jk}]$ is a vector belonging to $V_F(k)$, the k-dimensional vector space over F. $\underline{x}(D)$ is sometimes called a D-transform of the message or information sequence $\underline{x}$. The k component vector $\underline{x}_j$ in $\underline{x}$ is called the information frame at stage or frame time j.

In a similar manner, the output sequence is

$$\underline{y}(D) = [y_1(D), \ldots, y_n(D)], \tag{2}$$

where $y_i(D) \in F[D]$, $1 \le i \le n$. Vector $\underline{y}(D)$ is the D-transform of output coded sequence $\underline{y} = [\underline{y}_0, \ldots, \underline{y}_j, \cdots]$, where $\underline{y}_j = [y_{j1}, \ldots, y_{jn}]$ belongs to $V_n(F)$. The n-vector $\underline{y}_j$ is called the j^{th} codeword frame of code sequence $\underline{y}$.

The information and code sequence of an (n,k) convolutional code are linearly related by a $k \times n$, rank k, generator matrix $G(D)$ of polynomial elements in $F[D]$, as follows:

$$\underline{y}(D) = \underline{x}(D) \cdot G(D). \tag{3}$$

The maximum degree m of the polynomial elements of $G(D)$ in D is called the memory, and the *constraint length* L is defined as $L = m+1$.

The free distance of a CC is defined by

$$d_{\text{free}} = \min_{\underline{y}(D) \neq 0} W_H(\underline{y}(D)), \tag{4}$$

where $W_H(\underline{y}(D))$ is the cumulative Hamming weight of the coefficients $\underline{y}_j$ of D^j for all $j \geq 0$, where $\underline{y}_j$ is the j^{th} codeword frame. Note that the computation of d_{free} requires at least L codeword frames for all codes of practical interest.

To avoid catastrophic error propagation, $G(D)$ is assumed to be in a format of a basic encoder [6]. The Smith normal form of a basic encoder [2] is

$$G(D) = A(D)[I_k, 0]B(D), \tag{5}$$

where $A(D)$ and $B(D)$ are, respectively, $k \times k$ and $n \times n$ invertible matrices over $F[D]$ and I_k is a $k \times k$ identify matrix.

In Eq. (5), let matrix $B[D]$ be partitioned as

$$B(D) = \begin{bmatrix} B_1(D) \\ B_2(D) \end{bmatrix}$$

where $B_1(D)$ consists of the first k rows of $B(D)$ and $B_2(D)$ consists of the last $n-k$ rows of $B(D)$. Similarly, let

$$B(D)^{-1} = [\overline{B}_1(D), \overline{B}_2(D)],$$

where $\overline{B}_1(D)$ consists of the first k columns of $B(D)^{-1}$ and $\overline{B}_2(D)$ consists of the last $n-k$ columns of $B(D)^{-1}$. Since $B(D) \cdot B(D)^{-1} = I_n$, the following identities evidently hold:

$$\begin{aligned} &B_1(D) \cdot \overline{B}_1(D) = I_k, \quad B_1(D) \cdot \overline{B}_2(D) = 0 \\ &B_2(D) \cdot \overline{B}_1(D) = 0, \quad B_2(D) \cdot \overline{B}_2(D) = I_{n-k} \end{aligned} \tag{6}$$

A parity-check matrix $H(D)$ is defined to be an $(n-k) \times n$ matrix of rank $(n-k)$, satisfying

$$G(D) \cdot H^T(D) = 0, \tag{7}$$

From Eqs. (5), (6), and (7), it is seen next that

$$H(D) = B_2^{-T}(D) \tag{8}$$

has the properties of a parity-check matrix $H(D)$ associated with $G(D)$.

By Eq. (3), the CC generated by $G(D)$ is the set

$$C = \{\underline{y}(D) = [y_1(D), \ldots, y_n(D)] \,|\, \underline{y}(D) = \underline{x}(D)G(D)\}. \tag{9}$$

It is now shown also that

$$C = \{\underline{y}(D) = [y_1(D), \ldots, y_n(D)] \,|\, \underline{y}(D)H^T(D) = 0\}, \tag{10}$$

where $H(D)$ is given in Eq. (8). To see this, denote the right side of Eq. (10) by C_H. Clearly an element of C, as given in Eq. (9), belongs to C_H and hence $C \subseteq C_H$.

Next suppose $\underline{y}_1(D)$ is an element of C_H, i.e. by Eqs. (8) and (10),

$$\underline{y}_1(D)H^T(D) = \underline{y}_1(D)\overline{B}_2(D) = 0.$$

But, by definition, $\overline{B}_2(D)$ consists of the last $(n-k)$ columns of $B^{-1}(D)$, so that

$$\overline{B}_2(D) = B^{-1}(D) \cdot \begin{bmatrix} 0 \\ I_{n-k} \end{bmatrix} \tag{11}$$

where "0" denotes a block of k rows of zeroes and I_{n-k} is the $(n-k)$ row identity matrix. Thus, $\underline{y}_1(D)$ satisfies the equation

$$\underline{y}_1(D)B^{-1}(D) \cdot \begin{bmatrix} 0 \\ I_{n-k} \end{bmatrix} = 0.$$

The most general solution of this equation for $\underline{y}_1(D)B^{-1}(D)$ is

$$\underline{y}_1(D)B^{-1}(D) = [\tau_1(D), \ldots, \tau_k(D), 0 \cdots 0] = [\underline{\tau}(D), 0]$$

where $\tau_j(D)$ for $1 \le j \le k$ can be chosen to be any arbitrary elements of $F[D]$. Solving for $\underline{y}_1(D)$

yields, finally, by Eq. (5),

$$\underline{y}_1(D) = \underline{\tau}(D)[I_k,0]B(D) = \underline{\tau}(D)A^{-1}(D)G(D),$$

which belongs to C, as given in Eq. (9). Thus $C_H \subseteq C$ and Eq. (10) is proved.

The fact that the CCs given by the set C in Eq. (9) can be characterized by Eq. (10) is used in the following section to find the coset of solutions to the syndrome equation.

III. METHOD OF ALGEBRAIC SYNDROME DECODING

Let $\underline{y}(D)$ in Eq. (3) be transmitted and $\underline{z}(D)$ be received. Then,

$$\underline{z}(D) = \underline{y}(D) + \underline{e}(D), \tag{12}$$

where $\underline{e}(D)$ is the D-transform of the error sequence. By Eqs. (12) and (7), the syndrome of the received sequence is

$$\begin{aligned}\underline{s}(D) &= \underline{z}(D)\cdot H^{T(D)} = [\underline{y}(D) + \underline{e}(D)]\cdot H^T(D) \\ &= \underline{e}(D)\cdot H^T(D),\end{aligned} \tag{13}$$

or its equivalent,

$$(\underline{e}(D) - \underline{z}(D))H^T(D) = 0, \tag{14}$$

for all solutions $\underline{e}(D)$.

By Eqs. (10) and (9), the term $(\underline{e}(D) - \underline{z}(D))$ in Eq. (14) must be some code sequence $\underline{v}(D)G(D)$. Hence, the most general solution of the syndrome equation, Eq. (14), is

$$\underline{e}(D) = \underline{z}(D) + \underline{v}(D)G(D). \tag{15}$$

where $\underline{v}(D)$ is the D-transform of an arbitrary message-like sequence $\underline{v} = [\underline{v}_0, \ldots, \underline{v}_j, \cdots]$ of k-vectors $\underline{v}_j \in v_k(F)$.

Equation (15) shows that the most general solution of the syndrome equation, Eq. (13), for $\underline{e}(D)$ is the coset

$$C_z = \{\underline{e}(D) = \underline{z}(D) + \underline{v}(D)G(D) \mid \underline{v}(D) = [v_1(D), \ldots, v_k(D)]\}$$

of code C, defined by either Eq. (9) or Eq. (10). A minimization of the Hamming weights over all elements of coset C_z yields the standard minimum-error solution for message $\underline{v}(D)$. Efficient methods for achieving this minimization include the Viterbi algorithm and all sequential decoding methods for convolutional codes.

The difficulty with the standard decoding methods of CCs, i.e., Viterbi or sequential decoding, is the need to consider a sometimes prohibitively large number of states and paths in the decoding trellis. Such minimum-weight, path-finding decoding method does not take the advantage of the limited error-correcting capability which one might expect could reduce complexity of the decoder. It is shown in the next section that such reduced complexity is possible by using Eq. (15) to systematically develop algebraic syndrome decoders.

IV. ALGEBRAIC DECODING OF DUAL-K CCs

Dual-k convolutional codes are of rate $1/n$ of memory $m = 1$, and with symbols in the finite or Galois field $GF(2^k)$ (see Odenwalder's paper [5]). The generating matrix G has the following form, namely,

$$G = \begin{bmatrix} G_0 & G_1 & & \\ & G_0 & G_1 & \\ & & \ddots & \ddots \end{bmatrix} \tag{16a}$$

where $G_0 = [1,1,1, \ldots, 1]$ and $G_1 = [g_{11}, g_{12}, \ldots, g_{1n}]$ with $g_{1j} \neq 0$ and $g_{1j} \in GF(2^k)$ and the g_{1j}'s are all distinct, for $1 \leq j \leq n$. Thus by (3)

$$G(D) = G_0 + G_1 D \tag{16b}$$

where D is the unit delay operator.

From the above definition of a dual-k CC, it is known in [5] or can be verified that the minimum distance of the code is $d_{\min} = (2n-1)$ and the free distance is $d_{\text{free}} = 2n$. Hence if no more than t symbol errors occur in the first 2 codeword frames and $2t+1 \le d_{\min} = 2n-1$ or $t \le n-1$, then those errors which occur in the first frame can be corrected. In other words, the dual-k CC is a t-error-per-blocklength-correcting CC, where $t = [(d_{\min}-1)/2]$ and $[x]$ denotes the greatest integer less than x. Note that blocklength is equal to $n(m+1) = nL$ symbols where m is the memory and L is the constraint length.

The following sections present the algebraic syndrome decoding algorithm for the rate 1/2 and 1/3 dual-k convolutional codes.

V. ALGEBRAIC SYNDROME DECODING OF A RATE 1/2, DUAL-K CC

Let the Galois field $GF(2^3)$ be generated by the 3rd degree irreducible polynomial $p(x) = x^3+x^2+1$, over $GF(2)$. If α is a root of $p(x)$, then α, α^2, $\alpha^3 = 1+\alpha^2$, $\alpha^4 = 1+\alpha+\alpha^2$, $\alpha^5 = 1+\alpha$, $\alpha^6 = \alpha+\alpha^2$, $\alpha^7 = 1$ and 0 are the eight elements of $GF(2^3)$. The generating matrix of type (16b) for a rate 1/2, dual-3 CC is given by

$$G(D) = [1, a_1] + [1, a_2]D = [1+a_1 D, 1+a_2 D].$$

where $a_1 \neq a_2$, $a_2 \neq 0$. In Eq. (15), let

$$\underline{v}(D) = \sum_{i=0}^{\infty} v_i D^i \tag{17}$$

$$\underline{e}(D) = \sum_{i=0}^{\infty} [e_{1i}, e_{2i}] D^i \tag{18}$$

and

$$\underline{z}(D) = \sum_{i=0}^{\infty} [z_{1i}, z_{2i}]D^i \tag{19}$$

A substitution of Eqs. (17), (18), (19) into Eq. (15) yields

$$\sum_{i=0}^{\infty} [e_{1i}, e_{2i}]D^i = \sum_{i=0}^{\infty} v_i D^i \cdot G(D) + \sum_{i=0}^{\infty} [z_{1i}, z_{2i}]D^i$$

or

$$\sum_{i=0}^{\infty} [e_{1i}, e_{2i}]D^i = \sum_{i=0}^{\infty} [v_i + a_1 v_{i-1},\ v_i + a_2 v_{i-1}]D^i + \sum_{i=0}^{\infty} [z_{1i}, z_{2i}]D^i \tag{20}$$

Thus,

$$v_i + a_1 v_{i-1} = z_{1i} + e_{1i} \tag{21}$$

$$v_i + a_2 v_{i-1} = z_{2i} + e_{2i} \tag{22}$$

Solve v_i and v_{i-1} in terms of z_{1i}, z_{2i}, e_{1i} and e_{2i}, one obtains,

$$v_{i-1} = (a_1 + a_2)^{-1}[(z_{1i} + z_{2i}) + (e_{1i} + e_{2i})] \tag{23}$$

$$v_i = (a_1 + a_2)^{-1}[(a_2 z_{1i} + a_1 z_{2i}) + (a_2 e_{1i} + a_1 e_{2i})] \tag{24}$$

where v_{i-1} and v_i constitute the current message symbol and next message symbol in the input information sequence.

In the above notation, the following results can be established.

Result 1:

Let the error correcting capacity be $t = 1$ for one blocklength CCs. Then,

(i) $v_{i-1} = (a_1 + a_2)^{-1}(z_{1i} + z_{2i})$ iff $(e_{1i}, e_{2i}) = (0,0)$.

(ii) If no error occurs at the i^{th} frame time, i.e., $(e_{1i}, e_{2i}) = (0,0)$, then

$$v_{i-1} = (a_1 + a_2)^{-1}(z_{1i} + z_{2i}) \tag{25}$$

$$v_i = (a_1 + a_2)^{-1}[(1+a_2)z_{1i} + (1+a_1)z_{2i}] + (a_1 + a_2)^{-1}[z_{1i} + z_{2i}] \tag{26}$$

Proof:

(i) For part (i), if $(e_{1i},e_{2i}) = (0,0)$, then by (23) and (24), one obtains $v_{i-1} = (z_{1i} + z_{2i})(a_1 + a_2)^{-1}$ and

$$\begin{aligned} v_i &= (a_1 + a_2)^{-1}(a_2 z_{1i} + a_1 z_{2i}) \\ &= (a_1 + a_2)^{-1}[(1+a_2)z_{1i} + z_{1i} + (1+a_1)z_{2i} + z_{1i}] \\ &= (a_1 + a_2)^{-1}[(1+a_2)z_{1i} + (1+a_1)z_{1i}] + (a_1 + a_2)^{-1}[z_{1i} + z_{2i}] \end{aligned}$$

If $v_{i-1} = (a_1 + a_2)^{-1}(z_{1i} + z_{2i})$ then by (25) $e_{1i} + e_{2i} = 0$. Now since $t = 1$, e_{1i} and e_{2i} cannot be simultaneously both nonzero. In other words, (e_{1i},e_{2i}) must be one of the following forms: $(0,0)$, $(0,a)$, $(a,0)$ where $a \in GF(2^k)$. Therefore, it can be readily verified that $(e_{1i},e_{2i}) = (0,0)$.

(ii) If $(e_{1i},e_{2i}) = (0,0)$ then from part (i), it is known that $v_{i-1} = (a_1 + a_2)^{-1}(z_{1i} + z_{2i})$ and hence the result.

Note that from (i) of Result 1, it follows that if $(e_{1i},e_{2i}) = (0,0)$ then

$$v_i = v_{i-1} + (a_1 + a_2)^{-1}[(1+a_2)z_{1i} + (1+a_1)z_{2i}]$$

Based on Result 1, a flow chart for the decoding algorithm is shown in Figure 1.

Example 1:

A specific rate 1/2 dual-3 CC with $G(D) = (1+D, 1+\alpha D)$ is given, i.e. $a_1 = 1$, $a_2 = \alpha$.

Solving v_i and v_{i-1} in Eqs. (21) and (22), one has

$$\begin{cases} v_{i-1} = (z_{1i} + z_{2i})\alpha^2 + (e_{1i} + e_{2i})\alpha^2 \\ v_i = z_{1i} + (z_{1i} + z_{2i})\alpha^2 + (e_{1i} + e_{2i})\alpha^2 + e_{1i} \end{cases}$$

Then from Result 1:

$$v_{i-1} = (z_{1i} + z_{2i})\alpha^2 \quad \text{iff} \quad (e_{1i} + e_{2i}) = (0,0)$$

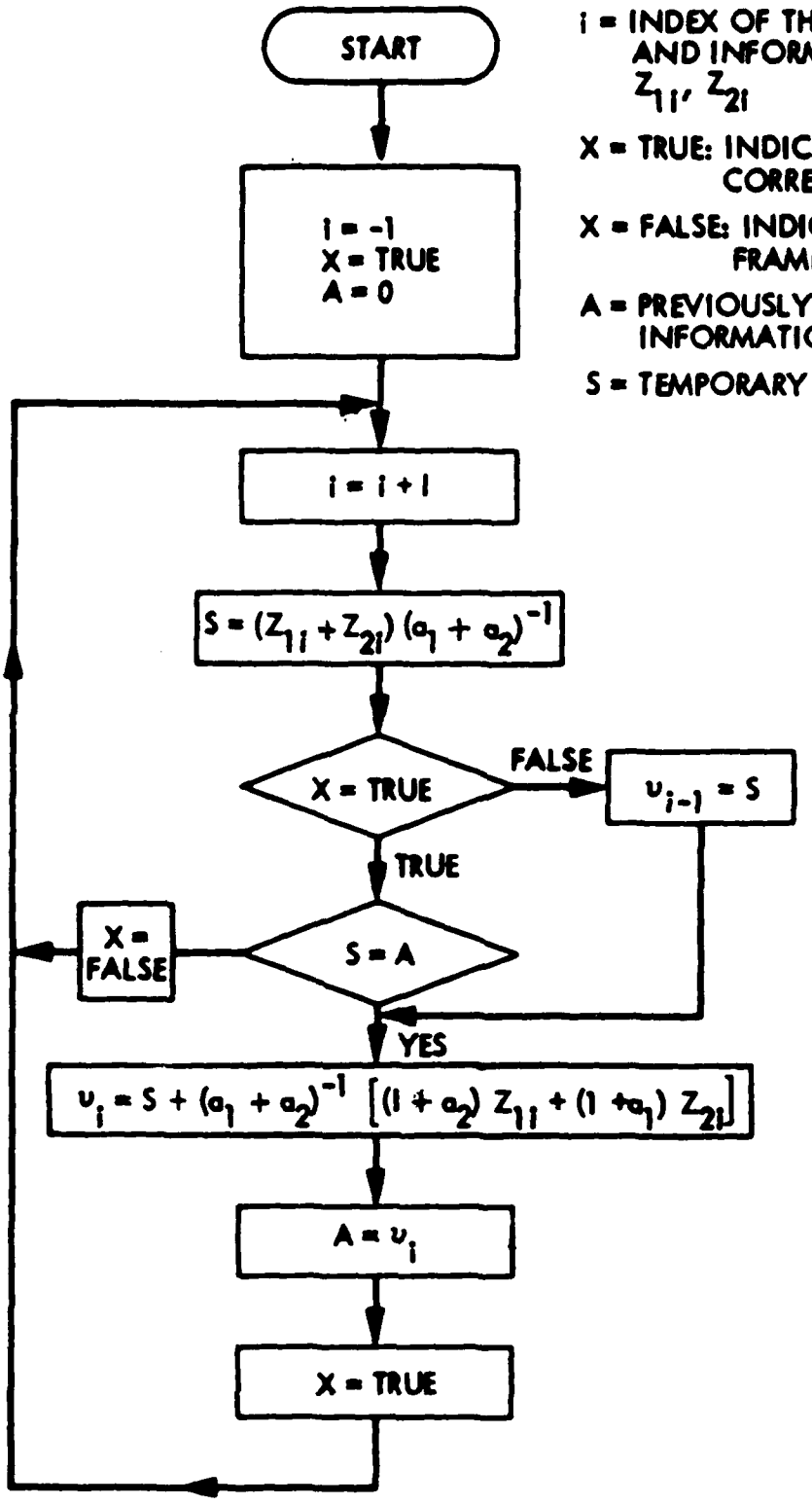

START
i = -1
X = TRUE
A = 0
i = i + 1
$S = (Z_{1i} + Z_{2i})(a_1 + a_2)^{-1}$
X = TRUE
FALSE
$v_{i-1} = S$
TRUE
S = A
X = FALSE
YES
$v_i = S + (a_1 + a_2)^{-1}[(1 + a_2) Z_{1i} + (1 + a_1) Z_{2i}]$
$A = v_i$
X = TRUE
i = INDEX OF THE RECEIVED AND INFORMATION SEQ.: Z_{1i}, Z_{2i}
X = TRUE: INDICATING PREVIOUSLY CORRECTED FRAME
X = FALSE: INDICATING PREVIOUS FRAME INCORRECT
A = PREVIOUSLY CORRECTED INFORMATION SYMBOL
S = TEMPORARY VARBLE

Figure 1

and if no error occurs at the i^{th} frame time, then

$$v_{i-1} = (z_{1i} + z_{2i})\alpha^2$$
$$v_i = z_{1i} + (z_{1i} + z_{2i})\alpha^2$$

The detailed steps of the algorithm shown by the flow chart now are described and explained as follows:

Assume initially that the message symbol is 0.

Step 0: Set $i = -1$, x = true and $A = 0$ (the initial message symbol 0).

Step 1: Set $i = i+1$, compute $S = (z_{1i} + z_{2i})\alpha^2$.

Step 2: If the previous time had an error, i.e., x = false then since only one error is allowed for two continuous time frames, the current time frame must be error free. Therefore, by Result 1, part (ii), get $v_{i-1} = S = (z_{1i} + z_{2i})\alpha^2$ and get $v_i = (z_{1i} + S)$. Next set x = true and $A = v_i$. Go to Step 1.

If the previous time frame had no error, i.e., x = true, then go to Step 3 to check if any error occurs at the current time frame i or not.

Step 3: If $S = A$ then by Result 1, part (i), $[e_{1i},e_{2i}] = [0,0]$.

Thus v_i can be computed by Eq. (24) $v_i = z_{1i} + S$; set $A = v_i$ and x = time. Go to Step 1.

If $S \neq A$ again by Result 1, part (i), an error occurs at time frame i; set x = false. Go to Step 1.

To illustrate the decoding algorithm works, let the D-transform of input sequence be $\underline{x}(D) = 1+\alpha D$. Then

$$\underline{y}(D) = \underline{x}(D)G(D) = [1,1] + [\alpha^5,0]D + [\alpha,\alpha^2]D^2$$

Next let the error sequence be $\underline{e}(D) = [0,\alpha] + [1,0]D^2$. So that $\underline{z}(D) = \underline{y}(D) + \underline{e}(D) = [1,\alpha^5] + [\alpha^5,0]D + [\alpha^5,\alpha^2]D^2$ is the received sequence. The decoding algorithm can be checked as follows:

Step 0: Set $i = -1$, x = true and $A = 0$.

Step 1: Set $i = i+1 = 0$ and $S = (z_{10} + z_{20})\alpha^2 = (1+\alpha^5)\alpha^2 = \alpha^3$.

Step 2: Initially it is assumed that there is no error. Hence go to Step 3.

Step 3: Since $S = \alpha^3 \neq 0 = A$, one concludes that an error occurred at frame time 0. Set x = false. Go to Step 1.

Step 1: $i = i+1 = 1$ and $S = (z_{11} + z_{21})\alpha^2 = (\alpha^5+0)\alpha^2 = 1$.

Step 2: Since an error occurred at the previous time frame (x = false), set $v_{i-1} = v_0 = S = 1$ and $v_i = v_1 = z_1 + S = \alpha^5 + 1 = \alpha$, x = true, $A = v_i = v_1 = \alpha$ and go to Step 1.

Step 1: $i = i+1 = 2$ and $S = (z_{12} + z_{22})\alpha^2 = (\alpha^5 + \alpha^2)\alpha^2 = \alpha^6$.

Step 2: Since x = true, go to Step 3.

Step 3: Since $\alpha^6 \neq \alpha = A$, set x = false to indicate an error occurred at time frame 2. Go to Step 1.

Step 1: $i = i+1 = 3$ and $S = (z_{13} + z_{23})\alpha^2 = (0,0)\alpha^2 = 0$.

Step 2: Since x = false, $v_{i-1} = v_2 = S = 0$ and $v_3 = S + z_{13} = 0$.

Finally, $v(D) = v_0 + v_1\alpha + v_2\alpha^2 + v_3\alpha^3 + 1 + \alpha D$ which equals the original information sequence.

A program to simulate this algorithm has been written in Pascal. The LSI design of decoder using this algorithm is given in Appendix A. This type of decoding algorithm is very efficient and

much simpler than Viterbi decoding. In fact, less than 30 gates are needed to implement this decoder.

VI. ALGEBRAIC SYNDROME DECODING OF A RATE 1/3, DUAL-K, CC

Let $G(D) = (1+a_1D, 1+a_2D, 1+a_3D)$ where $\alpha \in GF(2^3)$ is a root of $p(x)$ as defined in Section V. Again in Eq. (15), let

$$\underline{v}(D) = \sum_{i=0}^{\infty} v_i D^i \tag{27}$$

$$\underline{z}(D) = \sum_{i=0}^{\infty} [z_{1i}, z_{2i}, z_{3i}] D^i \tag{28}$$

$$\underline{e}(D) = \sum_{i=0}^{\infty} [e_{1i}, e_{2i}, e_{3i}] D^i \tag{29}$$

Substituting these equations and $G(D)$ into Eq. (15) and equating the coefficients yield,

$$a_1 v_{i-1} + v_i = z_{1i} + e_{1i} \tag{30}$$

$$a_2 v_{i-1} + v_i = z_{2i} + e_{2i} \tag{31}$$

$$a_3 v_{i-1} + v_i = z_{3i} + e_{3i} \tag{32}$$

The solutions for v_{i-1} and v_i are given as follows:

For v_{i-1} one has the two solutions,

$$v_{i-1} = (z_{1i} + z_{3i} + e_{1i} + e_{3i})(a_1 + a_3)^{-1} \tag{33a}$$

$$v_{i-1} = (z_{1i} + z_{2i} + e_{1i} + e_{2i})(a_1 + a_2)^{-1} \tag{33b}$$

For v_i one also has the solutions

$$v_i = a_1 v_{i-1} + z_{1i} + e_{1i} \tag{34a}$$

$$v_i = a_2 v_{i-1} + z_{2i} + e_{2i} \tag{34b}$$

where v_{i-1} is given in either (33a) or (33b). By (33a) and (33b), one obtains

$$[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}](z_{1i} + e_{1i}) + (a_1 + a_2)^{-1}(z_{2i} + e_{2i}) = (a_1 + a_3)^{-1}(z_{3i} + e_{3i}) \tag{35}$$

Result 2:

Let a rate 1/3, dual-3 CC be generated by $G(D) = (1+a_1D, 1+a_2D, 1+a_3D)$. Assume that no more than $t = 2$ errors can occur in one constraint length, $W_H(e_{1i}, e_{2i}, e_{3i}) + W_H(e_{1,i+1}, e_{2,i+1}, e_{3,i+1}) \leq 2$, where W_H denotes Hamming weight.

(i) If $[e_{1i}, e_{2i}, e_{3i}] = [0,0,0]$, then

$$[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]z_{1i} + (a_1 + a_2)^{-1}z_{2i} = (a_1 + a_3)^{-1}z_{3i} \tag{36}$$

$$v_{i-1} = (z_{1i} + z_{2i})(a_1 + a_2)^{-1} \tag{37}$$

$$v_i = v_{i-1} + z_{1i} \tag{38}$$

(ii) If $[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]z_{1i} + (a_1 + a_2)^{-1}z_{2i} = (a_1 + a_3)^{-1}z_{3i}$, then at least one error occurs at frame i, i.e., $W_H(e_{1i}, e_{2i}, e_{3i}) \geq 1$.

(iii) If $[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]z_{1i} + (a_1 + a_2)^{-1}z_{2i} = (a_1 + a_3)^{-1}z_{3i}$, then either 0 or 2 errors occur at frame i, i.e., $W_H(e_{1i}, e_{2i}, e_{3i}) = 0$ or 2.

(iv)

$$v_{i-1} = (z_{1i} + z_{2i})(a_1 + a_2)^{-1} \tag{39}$$

and

$$[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]z_{1i} + (a_1 + a_2)^{-1}z_{2i} = (a_1 + a_3)^{-1}z_{3i} \tag{40}$$

iff $[e_{1i}, e_{2i}, e_{3i}] = [0,0,0]$.

(v) Suppose $[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]z_{1i} + (a_1 + a_2)^{-1}z_{2i} \neq (a_1 + a_3)^{-1}z_{3i}$ and $W_H(e_{1i}, e_{2i}, e_{3i}) = 1$.

(a) If $$\frac{a_1 + a_2}{a_2 + a_3} z_{2i} + \frac{a_1 + a_2}{a_2 + a_3} z_{3i}(a_1 + a_2)v_{i-1} = 0, \tag{41}$$

then $e_{1i} = z_{1i} + \frac{a_1 + a_3}{a_2 + a_3} z_{2i} + \frac{a_1 + a_2}{a_2 + a_3} z_{3i} \neq 0$, $e_{2i} = e_{3i} = 0$.

(b) If $\frac{a_1 + a_2}{a_2 + a_3} z_{2i} + \frac{a_1 + a_2}{a_2 + a_3} z_{3i} + (a_1 + a_2)v_{i-1} \neq 0$ then $e_{1i} = 0$.

Proof:

(i) Follows immediately from Eqs. (33), (34) and (35).

(ii) Follows immediately from part (i).

(iii) If $[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]z_{1i} + (a_1 + a_2)^{-1}z_{2i} = (a_1 + a_3)^{-1}z_{3i}$, then by (35) one obtains

$$[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]e_{1i} + (a_1 + a_2)^{-1}e_{2i} = (a_1 + a_3)^{-1}e_{3i} \tag{42}$$

Now if $W_H(e_{1i},e_{2i},e_{3i}) = 1$, then it can be readily verified that (42) cannot be satisfied. Moreover, since for dual-k of rate 1/3 CC, the correcting capacity $t = 2$, one concludes that $W_H(e_{1i},e_{2i},e_{3i}) = 0$ or 2.

(iv) If $v_{i-1} = (z_{1i} + z_{2i})(a_1 + a_2)^{-1}$ and $[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]z_{1i} + (a_1 + a_2)^{-1}z_{2i} = (a_1 + a_3)^{-1}z_{3i}$, then by (33), (35), (38) and (40), one obtains

$$e_{1i} + e_{2i} = 0 \tag{43}$$

$$[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]e_{1i} + (a_1 + a_2)^{-1}e_{2i} = (a_1 + a_3)^{-1}e_{3i} \tag{44}$$

A substitution of (43) into (44) gives $e_{1i} = e_{3i}$. This implies $e_{1i} = e_{2i} = e_{3i}$. Since $t = 2$, three errors are not allowed. Thus, $(e_{1i},e_{2i},e_{3i}) = (0,0,0)$. The converse follows immediately from part (i).

(v)

(a): A substitution of (41) into (33b) yields

$$(a_1 + a_2)(a_2 + a_3)^{-1}(z_{2i} + z_{3i}) = z_{1i} + z_{2i} + e_{1i} + e_{2i} \tag{45}$$

Solving (45) and (35), one obtains

$$e_{2i} = e_{3i} \tag{46}$$

$$e_{1i} = z_{1i} + \frac{a_1 + a_3}{a_2 + a_3} z_{2i} + \frac{a_1 + a_2}{a_2 + a_3} z_{3i} + e_{3i} \tag{47}$$

Since $W_H(e_{1i},e_{2i},e_{3i}) = 1$, e_{2i} and e_{3i} cannot both be nonzero thus, $e_{2i} = e_{3i} = 0$ and $e_{1i} = z_{1i} + \frac{a_1 + a_3}{a_2 + a_3} z_{2i} + \frac{a_1 + a_2}{a_2 + a_3} z_{3i} \neq 0$.

(v)

(b): Eliminating v_1 in Eqs. (30) and (31) gives

$$e_{1i} + e_{2i} + z_{1i} + z_{2i} + a_1 + a_2 v_{i-1} = 0. \tag{48}$$

Similarly, eliminating v_1 in Eqs. (31) and (32) gives

$$e_{1i} + e_{3i} + z_{1i} + z_{3i} + a_1 + a_3 v_{i-1} = 0. \tag{49}$$

Adding Eqs. (48) and (49) yields

$$e_{2i} + 3ei + z_{2i} + z_{3i} + a_2 + a_3 v_{i-1} = 0$$

or

$$\frac{a_1 + a_2}{a_2 + a_3} (e_{2i} + e_{3i}) = \frac{a_1 + a_2}{a_2 + a_3} (z_{2i} + z_{3i}) + a_1 + a_2 v_{i-1} \neq 0.$$

Thus $e_{2i} \neq e_{3i}$. Since $W_H(e_{1i},e_{2i},e_{3i}) = 1$, one obtains $e_{1i} = 0$.

The flow chart for decoding a rate 1/3, dual-3 CC is shown in Fig. 2. Initially, $i = -1$ and $A = 0$, where i is the index for both received and information sequence and A is used to store the previously corrected message symbol. For any two contiguous time frames (time frame i and $i+1$), four Boolean variables $BOLN[j]$, $1 \leq j \leq 4$ are defined as follows:

If $[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]z_{1i} + (a_1 + a_2)^{-1}]z_{2i} = (a_1 + a_3)z_{3i}$ then $BOLN[1]$ = true, else $BOLN[1]$ = false.

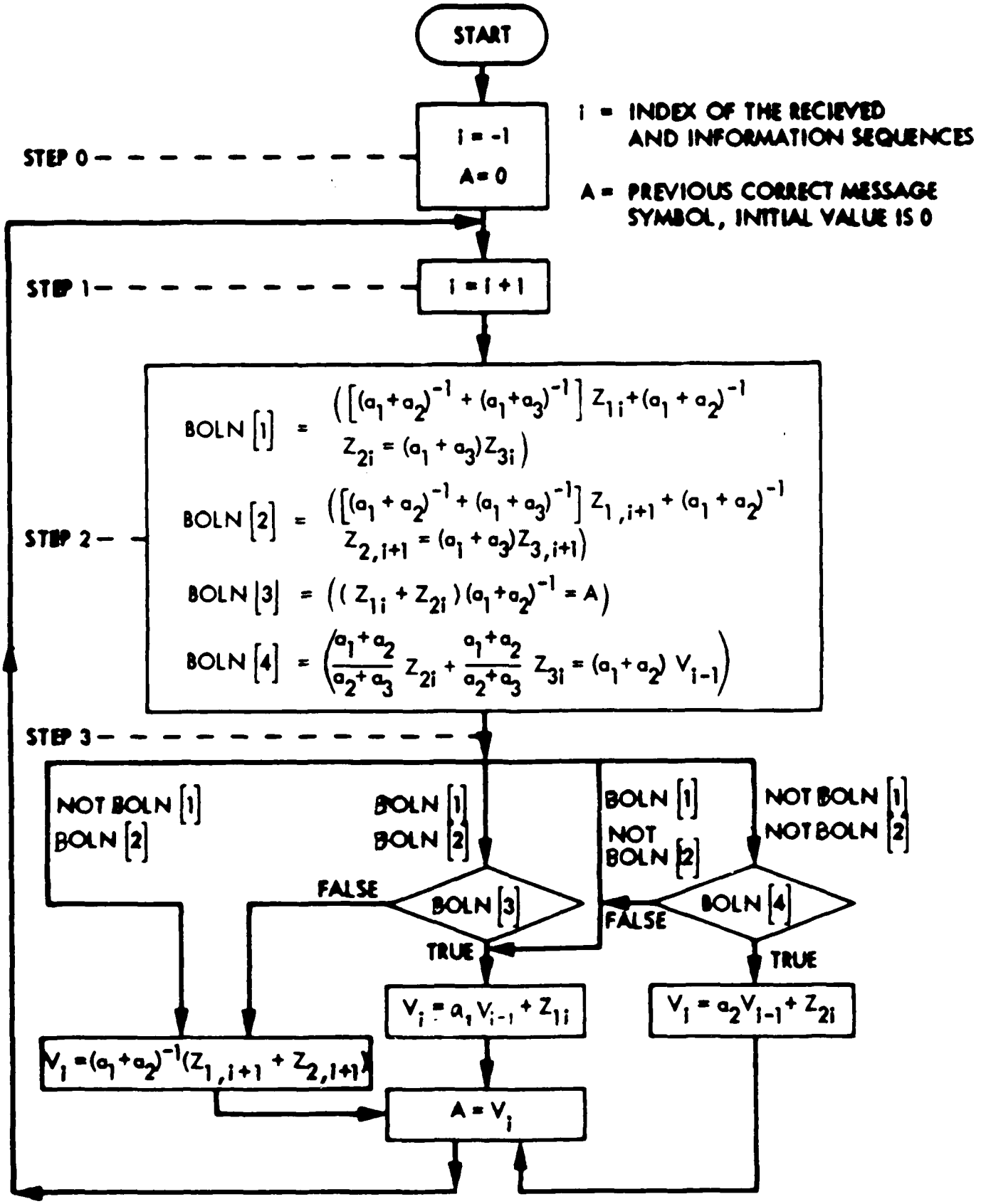

START
STEP 0
I = -1
A = 0
I = INDEX OF THE RECIEVED AND INFORMATION SEQUENCES
A = PREVIOUS CORRECT MESSAGE SYMBOL, INITIAL VALUE IS 0
STEP 1
I = I + 1
STEP 2
BOLN [1] = $\left(\left[(a_1+a_2)^{-1}+(a_1+a_3)^{-1}\right]Z_{1i}+(a_1+a_2)^{-1}\right.$ $\left.Z_{2i}=(a_1+a_3)Z_{3i}\right)$
BOLN [2] = $\left(\left[(a_1+a_2)^{-1}+(a_1+a_3)^{-1}\right]Z_{1,i+1}+(a_1+a_2)^{-1}\right.$ $\left.Z_{2,i+1}=(a_1+a_3)Z_{3,i+1}\right)$
BOLN [3] = $\left((Z_{1i}+Z_{2i})(a_1+a_2)^{-1}=A\right)$
BOLN [4] = $\left(\frac{a_1+a_2}{a_2+a_3}Z_{2i}+\frac{a_1+a_2}{a_2+a_3}Z_{3i}=(a_1+a_2)V_{i-1}\right)$
STEP 3
NOT BOLN [1]
BOLN [2]
BOLN [1]
BOLN [2]
BOLN [1]
NOT BOLN [2]
NOT BOLN [1]
NOT BOLN [2]
FALSE
BOLN [3]
FALSE
BOLN [4]
TRUE
TRUE
$V_i = a_1 V_{i-1} + Z_{1i}$
$V_i = a_2 V_{i-1} + Z_{2i}$
$V_i = (a_1+a_2)^{-1}(Z_{1,i+1} + Z_{2,i+1})$
A = V_i

Figure 2

If $[(a_1 + a_2)^{-1} + (a_1 + a_3)^{-1}]z_{1,i+1} + (a_1 + a_2)^{-1}]z_{2,i+1} = (a_1 + a_3)z_{3,i+1}$ then $BOLN[2]$ = true, else $BOLN[2]$ = false.

If $(z_{1i} + z_{2i})(a_1 + a_2)^{-1} = A$, then $BOLN[3]$ = true, else $BOLN[3]$ = false.

If $\frac{a_1 + a_2}{a_2 + a_3} z_{2i} + \frac{a_1 + a_2}{a_2 + a_3} z_{3i} = (a_1 + a_2)v_{i-1}$ then $BOLN[4]$ = true, else $BOLN[4]$ = false.

Four cases are discussed according to the Boolean values of $BOLN[1]$ and $BOLN[2]$.

Case 1: $BOLN[1]$ and $BOLN[2]$ are both true.

By Result 2, part (iii), there are 0 or two errors for both time frames i and $i+1$, i.e., $W_H(e_{1i},e_{2i},e_{3i}) = 0$ or 2, $W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) = 0$ or 2.

If $BOLN[3]$ is true, then by Result 2, part (iv), $(e_{1i},e_{2i},e_{3i}) = (0,0,0)$, and thus by Result 2, part (i), v_i can be determined by Eq. (38).

If $BOLN[3]$ is false, then by Result 2, part (iv), $W_H(e_{1i},e_{2i},e_{3i}) \geq 1$, and since $W_H(e_{1i},e_{2i},e_{3i}) = 0$ or 2, as discussed, one concludes that $W_H(e_{1i},e_{2i},e_{3i}) = 2$. Thus $W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) = (0,0,0)$ for the reason that no more than 2 errors can occur in two contiguous time frames. Therefore v_i can be determined by Eq. (37) $v_i = (z_{1,i+1} + z_{2,i+1})(a_1 + a_2)^{-1}$.

Case 2: $BOLN[1]$ false, $BOLN[2]$ true.

By Result 2, part (ii), $W_H(e_{1i},e_{2i},e_{3i}) \geq 1$. By Result 2, part (iii), $W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) = 0$ or 2. Also by the assumption that $W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) + W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) \leq 2$. Thus, $W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) = 0$, i.e. $(e_{1,i+1},e_{2,i+1},e_{3,i+1}) = (0,0,0)$, and so v_i again can be determined by Eq. (37).

Case 3: $BOLN[1]$ true, $BOLN[2]$ false.

By Result 2, part (iii), $W_H(e_{1i},e_{2i},e_{3i}) = 0$ or 2. By Result 2, part (ii), $W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) \geq 1$. Also by the assumption that $W_H(e_{1i},e_{2i},e_{3i}) + W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) \leq 2$. Thus, $W_H(e_{1i},e_{2i},e_{3i}) = 0$ and so by Result 2, part (i), v_i can be computed by Eq. (38).

Case 4: *BOLN*[1] false, *BOLN*[2] false.

By Result 2, part (ii), $W_H(e_{1i},e_{2i},e_{3i}) \geq 1$ and $W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) \leq 1$ and since $W_H(e_{1i},e_{2i},e_{3i}) + W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) \leq 2$, it follows that $W_H(e_{1i},e_{2i},e_{3i}) = 1$ and $W_H(e_{1,i+1},e_{2,i+1},e_{3,i+1}) = 1$. Therefore by Result 2, part (v), if *BOLN*[4] is true then $e_{2i} = 0$, otherwise $e_{1i} = 0$. And so v_i can be computed by Eq. (34b) or (34a) depending on $e_{2i} = 0$ or $e_{1i} = 0$.

After v_i is determined, then v_i is substituted for A and the recursive process is repeated to determine v_{i+1}. Finally the entire estimated information sequence is obtained. The estimated information sequence is exactly the original input information sequence as long as there is no more than 2 errors for each constraint length.

To illustrate the above algorithm, an example is given as follows:

Example 2:

Consider a special 1/2 rate dual-3 CC with $G(D) = (1+D, 1+\alpha D, 1+\alpha^6 D)$, i.e., $A_1 = 1$, $A_2 = \alpha$, $A_3 = \alpha^6$ then the four Boolean functions are as follows:

$$Bolu[1] = (\alpha^4 z_{1i} + \alpha^6 z_{2i} = z_{3i})$$
$$Bolu[2] = (\alpha^4 z_{1,i+1} + \alpha^6 z_{2,i+1} = z_{3,i+1})$$
$$Bolu[3] = ((z_{1i} + z_{2i})\alpha^2 = A)$$
$$Bolu[4] = (\alpha^3 z_{1i} + \alpha^3 z_{3i} = v_{i-1}\alpha^5)$$

Let the input be $x(D) = 1 + \alpha D^2$. Then the encoder output is

$$\underline{y}(D) = \underline{x}(D)G(D) = [1,1,1] + [1,\alpha,\alpha^6]D + [\alpha,\alpha,\alpha]D^2 + [\alpha,\alpha^2,1]D^3$$

Next let $\underline{e}(D) = [\alpha^5,0,0] + [0,0,\alpha]D + [\alpha,\alpha^2,0]D^3$, so that the received sequence $\underline{z}(D) = [\alpha,1,1] + [1,\alpha,\alpha^2]D + [\alpha,\alpha,\alpha]D^2 + [0,0,1]D^3$.

The decoding algorithm then can be checked as follows:

Step 0: $i = -1$, $A = 0$.

Step 1: $i = i+1 = 0$.

Step 2: $\alpha^4 z_{10} + \alpha^6 z_{20} = \alpha^3 \neq 1 = z_{30} \rightarrow BOLN[1]$ is false.

$\alpha^4 z_{11} + \alpha^6 z_{21} = \alpha^6 \neq \alpha^2 = z_{31} \rightarrow BOLN[2]$ is false.

$\alpha^3 z_{20} + \alpha^3 z_{30} = 0 = v_{-1} \rightarrow BOLN[4]$ is true.

Step 3: $e_{10} = z_{10} + \alpha^2 z_{20} + \alpha^3 z_{20} = \alpha^5$, $v_0 = z_{10} + v_{-1} + e_{10} = \alpha + 0 + \alpha^5 = 1$ and $A = v_0 = 1$.

Step 1: $i = i+1 = 1$.

Step 2: $\alpha^4 z_{11} + \alpha^6 z_{21} = \alpha^6 \neq \alpha^2 = z_{31} \rightarrow BOLN[1]$ is false.

$\alpha^4 z_{12} + \alpha^6 z_{22} = \alpha = z_{32} \rightarrow BOLN[2]$ is true.

Step 3: $v_1 = (z_{1,i+1} + z_{2,i+1})\alpha^2 = (z_{1,2} + z_{2,2})\alpha^2 = 0$, $A + v_1 = 0$.

Step 1: $i = i+1 = 2$.

Step 2: $\alpha^4 z_{12} + \alpha^6 z_{22} = \alpha = z_{32} \rightarrow BOLN[1]$ is true.

$\alpha^4 z_{13} + \alpha^6 z_{23} = 0 \neq 1 = z_{33} \rightarrow BOLN[2]$ is false.

Step 3: $v_2 = v_1 + z_{12} = 0 + \alpha = \alpha$

Step 1: $i = i+1 = 3$.

Step 2: $\alpha^4 z_{13} + \alpha^6 z_{23} = 0 \neq 1 = z_{33} \rightarrow BOLN[1]$ is false.

$\alpha^4 z_{14} + \alpha^6 z_{24} = 0 = z_{34} \rightarrow BOLN[2]$ is true.

Step 3: $v_3 = (z_{1,4} + z_{2,4})\alpha^2 = 0$, $A = v_3 = 0$.

Step 1: $i = i+1 = 4$.

Step 2: $\alpha^4 z_{14} + \alpha^6 z_{24} = 0 = z_{34} \rightarrow BOLN[1]$ is true.

$\alpha^4 z_{15} + \alpha^6 z_{25} = 0 = z_{35} \rightarrow BOLN[2]$ is true.

$(z_{14} + z_{24})\alpha^2 = 0 = A \rightarrow BOLN[3]$ is true.

Step 3: $v_4 = v_3 + z_{14} = 0$.

Finally, $v_0 = 1$, $v_1 = 0$, $v_2 = \alpha$, $v_3 = 0$ and $v_4 = 0$ or $\underline{v}(D) = 1 + \alpha D^2$, which is the same as the original input sequence. A simulation program for the algorithm was written in Pascal. An LSI design of the algorithm is given in Appendix B.

The implementation of this decoder is much simpler than Viterbi decoding, thus, this decoder can be applied to telephony and HF radio, where a moderate error correction is desired at a relatively low cost, see [7].

V. CONCLUSION

In this report, algebraic syndrome decoders of both rate 1/2 and 1/3, dual-k, nonsystematic convolution codes are developed in detail, including an efficient method for finding the corrected message sequence. This is achieved without the necessity of storing a number of states or paths in a constraint length of the error trellis diagram. Currently, the problem of algebraic syndrome decoding of a rate $1/n$, dual-k, CCs for $n > 3$ is being investigated. Finally, a single VLSI chip with CMOS technology for the rate 1/2, dual-2 algebraic syndrome decoder is being developed.

REFERENCES

[1] I.S. Reed and T.K. Truong, "New Syndrome Decoding for (n,1) Convolutional Codes," *Electronic Letters*, Vol. 19, No. 9, April 1983, pp. 344-346.

[2] I.S. Reed and T.K. Truong, "Error-Trellis Syndrome Decoding Techniques for Convolutional Codes," *IEEE Proceedings*, Vol. 132, Pt. F., No. 2, April 1985.

[3] I.S. Reed, T.K. Truong, J.M. Jensen and I.S. Hsu, "The VLSI Design Error-Trellis Syndrome Decoding for Convolutional Codes," *IEEE Trans. on Computers*, Vol. C-35, No. 9, September 1986, pp. 781-789.

[4] R.E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley, 1983.

[5] V.P. Odenwalder, "Dual-K Convolutional Codes for Non-Coherently Demodulated Channels," *Proceedings of the International Telemetering Conference (ITC)*, Vol. 12, 1978, pp. 165-174.

[6] G.D. Forney, "Convolutional Codes: Algebraic Structure," *IEEE Trans. on Information Theory*, Vol. IT-16, 1970, pp. 720-738.

[7] S. Lin and D.T. Cosello, Jr., *Error Control Coding*, Prentice Hall, New Jersey, 1983.

END

3-87

DTIC