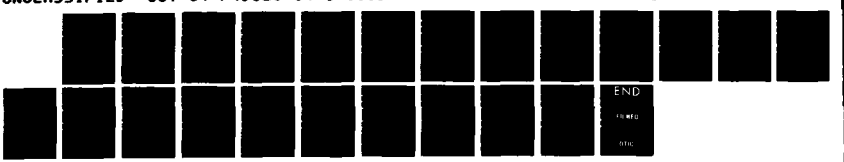
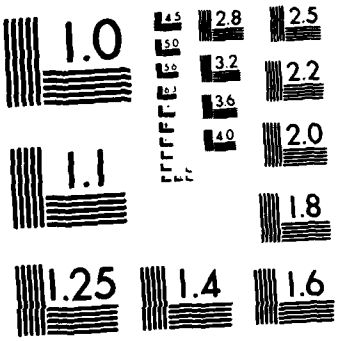
AD-A148 770 THE ALGEBRAIC STRUCTURE OF CONVOLUTIONAL CODES WITH APPLICATION TO CODE C.. (U) UNIVERSITY OF SOUTHERN CALIFORNIA LOS ANGELES DEPT OF ELECTRI.. I S REED

1/1

UNCLASSIFIED OCT 84 F49620-84-C-0069 F/G 12/1 NL





UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION: UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT: Approved for public release; distribution unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S): AFOSR-TR- 84-1082
6a. NAME OF PERFORMING ORGANIZATION: University of Southern California (6b. OFFICE SYMBOL (If applicable))	7a. NAME OF MONITORING ORGANIZATION: Air Force Office of Scientific Research
6c. ADDRESS (City, State and ZIP Code): Electrical Engineering Department, Los Angeles CA 90089-0272	7b. ADDRESS (City, State and ZIP Code): Directorate of Mathematical & Information Sciences, Bolling AFB DC 20332-6448
8a. NAME OF FUNDING/SPONSORING ORGANIZATION: AFOSR (8b. OFFICE SYMBOL (If applicable): NM)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER: F49620-84-C-0069
8c. ADDRESS (City, State and ZIP Code): Bldg 410 AFB DC 20332-6448	10. SOURCE OF FUNDING NOS: PROGRAM ELEMENT NO 61102F; PROJECT NO 2304; TASK NO A6; WORK UNIT NO
11. TITLE (Include Security Classification): [illegible] STRUCTURE OF CONVOLUTIONAL CODES WITH APPLICATION TO CODE CONSTRUCTION [illegible]	
12. PERSONAL AUTHOR(S): [illegible] C. Reed	
13a. TYPE OF REPORT: Interim (Quarterly)	13b. TIME COVERED: FROM 1/7/84 TO 30/9/84
14. DATE OF REPORT (Yr., Mo., Day): OCT 84	15. PAGE COUNT: 21
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)

During this quarter, the error trellis syndrome decoding techniques for convolutional codes [illegible] developed. This algorithm is specialized then to the entire class of systematic convolutional codes. Finally, this algorithm is applied to the high rate Wyner-Ash convolutional codes. A special example of the one-error-correcting Wyner-Ash code, a 3/4 rate code is treated in this report.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT: UNCLASSIFIED UNLIMITED Σ SAME AS RPT ☐ DTIC USERS ☐	21. ABSTRACT SECURITY CLASSIFICATION: UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL: Maj Brian W. Woodruff	22b. TELEPHONE NUMBER (Include Area Code): (202) 767-5027 / 22c. OFFICE SYMBOL: NM

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

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

AD-A148 770

AFOSR-TR- 84-1082

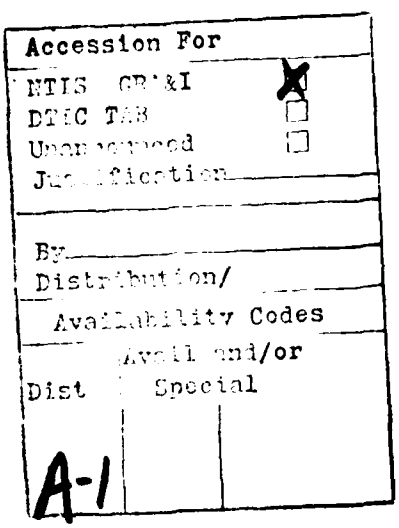
QUARTERLY TECHNICAL REPORT #1

1. Grant Title and Number

THE ALGEBRAIC STRUCTURE OF CONVOLUTIONAL CODES WITH APPLICATION TO CODE CONSTRUCTION AND DECODING. #F49620-84-C-0069.

2. Period Covered

July 1, 1984 to September 30, 1984.



3. Report Prepared by

Professor Irving S. Reed

Principal Investigator

4. Date of This Report

September 30, 1984.

5. Research Summary

During this quarter, the error trellis syndrome decoding techniques for convolutional codes is developed. This algorithm is specialized then to the entire class of systematic convolutional codes. Finally, this algorithm is applied to the high rate Wyner-Ash convolutional codes. A special example of the one-error-correcting Wyner-Ash code, a 3/4 rate code is treated in this report.

6. Results

The inputs and outputs of an (n,k) convolutional code (CC) can be represented, respectively, as D-transforms

$$x(D) = \sum_{j=0}^{\infty} x_j \cdot D^j \tag{1}$$

and

$$y(D) = \sum_{j=0}^{\infty} y_j \cdot D^j \tag{2}$$

of the input sequence of k-vectors of form $x_j = [x_{1j}, x_{2j}, \ldots, x_{kj}]$ and the output sequence of n-vectors of form $y_j = [y_{1j}, y_{2j}, \ldots, y_{nj}]$, where x_{ij} and y_{ij} belong to a finite Galois field F = GF(q) usually restricted to the binary field GF(2) of two elements, and D is the delay operator. The input x(D) and the output y(D) are linearly related by means of a k×n generator matrix G(D) as follows:

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

where the elements of G(D) are assumed usually to be polynomials over the finite field GF(q), where q is the power of a prime number. The maximum degree M of the polynomial elements of G(D) is called the memory delay of the code, and the constraint length of the code is K = M+1.

In order to avoid catastrophic error propagation, the encoder matrix G(D) is assumed to be basic. For the basic encoder, the Smith normal form of G(D) is

$$G = A \cdot [I_k, D] \cdot B \tag{4}$$

where A = A(D) is a k×k invertible matrix with elements in F[D], the ring of polynomials in D over F, and B = B(D) is an n×n invertible matrix with elements in F[D]. The elements of the inverses A^{-1} and B^{-1} of matrices A and B, respectively,

are polynomials in F[D].

By definition,

$$G(D)\cdot H^T(D) = 0 \tag{5}$$

where H(D) is the parity check matrix. Let

$$B = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} \tag{6}$$

and

$$B^{-1} = [\bar{B}_1, \bar{B}_2], \tag{7}$$

where the first k rows of B constitute submatrix B_1 and the remaining (n-k) rows are matrix B_2, and where, likewise, the first k columns of B^{-1} constitute submatrix $\bar{B}_1$ and the remaining (n-k) columns are matrix $\bar{B}_2$. Since

$$B\cdot B^{-1} = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} \cdot [\bar{B}_1, \bar{B}_2]$$

$$= \begin{bmatrix} B_1\bar{B}_1, & B_1\bar{B}_2 \\ B_2\bar{B}_1, & B_2\bar{B}_2 \end{bmatrix}$$

$$= I_n$$

we get

$$\begin{aligned} B_1\bar{B}_1 &= I_k, & B_1\bar{B}_2 &= 0 \\ B_2\bar{B}_1 &= 0, & B_2\bar{B}_2 &= I_{n-k} \end{aligned} \tag{8}$$

In terms of partition, Eq. (7), the parity check matrix is defined by

$$H = \bar{B}_2^T \tag{9}$$

It should be noted that the parity-check matrix is not unique. For example, it can be shown that $H = CB_2^T$ is a parity-check matrix where C is any $(n-k)\times(n-k)$ invertible matrix with elements in F[D].

Let the received codes be

$$z(D) = y(D)+e(D), \tag{10}$$

where e(D) is the D-transform of the error sequence. The syndrome of the received code z(D) Is

$$\begin{aligned} s(D) &= z(D)\cdot H^T(D) \\ &= (y+e)\cdot H^T \\ &= (xG+e)\cdot H^T \end{aligned} \tag{11}$$

Since $G\cdot H^T = D$, we get

$$s = e\cdot H^T \tag{12}$$

It has been shown [1] that the set of solutions is a coset of the set of all codewords.

To explicitly solve the syndrome equation, Eq. (12), substitute H as given by Eq. (9) in Eq. (12), thereby obtaining

$$s = e\bar{B}_2 = eB^{-1}\begin{bmatrix} 0 \\ I_{n-k} \end{bmatrix}, \tag{13}$$

In Eq. (13), let

$$\varepsilon = eB^{-1}, \tag{14}$$

So that Eq. (13) becomes the simple equation

$$s = \varepsilon \begin{bmatrix} 0 \\ I_{n-k} \end{bmatrix}, \tag{15}$$

where $s = [s_1, s_2, \ldots, s_{n-k}]$ and $\varepsilon = [\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n]$. The general solutions of Eq. (15) over the ring F[D] is given evidently by

$$\begin{aligned} [\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{10}] &= [\tau_1, \tau_2, \ldots, \tau_k] = \tau, \\ [\varepsilon_{k+1}, \varepsilon_{k+2}, \ldots, \varepsilon_n] &= [s_1, s_2, \ldots, s_{n-k}] = s \end{aligned} \tag{16}$$

where $\tau_j = \tau_j(D)$ are arbitrary elements in F[d]. Thus, more compactly, the general solution of Eq. (14) is

$$\varepsilon = [\tau, S] = eB^{-1} \tag{17}$$

where τ, as in Eq. (16), is an arbitary k-vector of elements in ring F[D]. Finally, a multiplication of both sides of Eq. (17) by B yields

$$e = \varepsilon B = [\tau, s] \cdot \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} = \tau B_1 + s B_2 \tag{18}$$

From the identity in Eq. (8) and (9) that B_2^T is the left inverse, denoted by H^{-1}, of parity-check matrix. Hence,

$$B_2 = (H^{-1})^T, \tag{19}$$

where H^{-1} is the left inverse of H. From the Smith normal form in Eq. (4) of a basic encoder that

$$A^{-1}G = [I_k, 0] \cdot B = B_1 \tag{20}$$

A substittuion of B_1 in Eq. (20) and B_2 in Eq. (19) into Eq. (18) obtains

$$e = \tau A^{-1} G + s(H^{-1})^T. \tag{21}$$

Since τ is an arbitrary k-vector of elements in F[D],

$$t = \tau A^{-1} \tag{22}$$

is also an arbitrary vector of polynomials in F[D]. Substituting t in Eq. (22) into Eq. (21) yields,

$$e = tG+s(H^{-1})^T \tag{23}$$

as the general solution of syndrome equation, Eq. (12).

Towards this end, substitute Eq. (19) into Eq. (23) and, by Eq. (9) and (11), the quantity $z\cdot\overline{B}_2$ for syndrome s. These substitutions yield

$$e = (t)G+z\cdot(\overline{B}_2\cdot B_2) \tag{24}$$

Let $R = \overline{B}_2\ B_2$, since B_2 and $\overline{B}_2$ have rank (n-k), it can be shown that matrix $R = \overline{B}_2\ B_2$ also has rank (n-k). A substitution of R into Eq. (24) yields

$$e = tG+zR \tag{25}$$

By the maximum likelihood principle, the most likely error sequence is the one with minimum Hamming weight. Given z(D), the sequence e(D) with minimum Hamming weight is found by minimizing the weight of the right side of Eq. (25) over all polynomials t(D) in F[D]. That is,

$$\min||e|| = \min_{t\epsilon F[D]} ||tG+zR||, \tag{27}$$

what one attempts to do in Eq. (27) is to find that sequence $\hat{t}$ which, when encoded as $\hat{t}G$ and subtracted from $z\cdot R$, yields the sequence $\hat{e}$ of minimum Hamming weight. That is,

$$\hat{e} = \hat{t}G+zR \tag{28}$$

is the D-transform of the minimum weight possible error sequence.

By Eq. (4), the right inverse G^{-1} of the generating matrix G is

$$G^{-1} = B^{-1} \cdot \begin{bmatrix} I_k \\ 0 \end{bmatrix} \cdot A^{-1} \tag{29}$$

From Eq. (28) and Eq. (29), one obtains

$$\begin{aligned} \hat{e} \cdot G^{-1} &= [\hat{t}G + z\bar{B}_2 \; B_2] \cdot G^{-1} \\ &= \hat{t} + z \cdot \bar{B}_2 \cdot B_2 [\bar{B}_1, \bar{B}_2] \cdot \begin{bmatrix} I_k \\ 0 \end{bmatrix} \cdot A^{-1} \\ &= \hat{t} + z\bar{B}_2 \cdot [0, I_{n-k}] \cdot \begin{bmatrix} I_k \\ 0 \end{bmatrix} \cdot A^{-1} \\ &= \hat{t}. \end{aligned} \tag{30}$$

By Eq. (10), the subtraction of $\hat{e}$ from z produces a best estimate $\hat{y}$ of the transmitted code, i.e.,

$$\hat{y} = z - \hat{e}. \tag{31}$$

If multiplied on the right by G, yields

$$\hat{x} = \hat{y} \cdot G^{-1}, \tag{32}$$

the best estimate of the original message. Hence, substituting Eq. (31) in Eq. (32) and using Eq. (30) produces

$$\begin{aligned} \hat{x} &= (z - \hat{e}) \cdot G^{-1} \\ &= z \cdot G^{-1} - \hat{t} \end{aligned} \tag{33}$$

This important identity shows that $\hat{t} = \hat{t}(D)$, obtained by the minimization in Eq. (27), is a correction factor to the standard method of recovering the message from $z = z(D)$ if z were noise-free.

The above results are now applied to systematic convolutional codes. The generator matrix for a systematic CC has form

$$G(D) = [I_k, P(D)] \tag{34}$$

where I_k is the $k \times k$ identity matrix and $P(D)$ is a $k \times (n-k)$ of polynomials over GF(q) in the delayed operator D. A parity check matrix associated with $G(D)$ in Eq. (34) is the $(n-k) \times n$ matrix,

$$H(D) = [-P^T(D), I_{n-k}] \tag{35}$$

The Smith normal form of Eq. (34) is, by Eq. (14),

$$\begin{aligned} G &= A[I_k, 0]B \\ &= [I_k, 0] \begin{bmatrix} I_k, & P \\ 0, & I_{n-k} \end{bmatrix} \end{aligned} \tag{36}$$

Hence, for a systematic code, $A = I_k$ and

$$B = \begin{bmatrix} I_k, & P \\ 0, & I_{n-k} \end{bmatrix} \tag{37}$$

the inverse of B is found to be

$$B^{-1} = \begin{bmatrix} I_k, & -P \\ 0, & I_{n-k} \end{bmatrix}, \tag{38}$$

The partitions, given in Eqs. (6) and (7), of B and B^{-1}, respectively, are, for a systematic CC,

$$B = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} .$$

where

$$B_1 = [I_k, P(D)] \text{ and } B_2 = [0, I_{n-k}] \tag{39}$$

and

$$B^{-1} = [\bar{B}_1, \bar{B}_2],$$

where

$$\bar{B}_1 = \begin{bmatrix} I_k \\ 0 \end{bmatrix} \quad \text{and} \quad \bar{B}_2 = \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix} . \tag{40}$$

Consequently, the syndrome s in Eq. (12) is

$$\begin{aligned} s = z \cdot H^T &= Z \cdot \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix} \\ &= [z_m, z_p] \cdot \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix} \\ &= -z_m(D) \cdot P(D) + z_p(D), \end{aligned} \tag{41}$$

where $z_m(D)$ is the message code vector of k components, possibly corrupted by noise, and $z_p(D)$ is an (n-k) component vector of parity symbols, also possibly changed by channel noise.

Next, by Eqs. (39) and (40), the matrix R in Eq. (26) is given by

$$R = \overline{B}_2\, B_2 = \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix} \cdot [0,\ I_{n-k}]$$

$$= \begin{bmatrix} 0, & -P \\ 0, & I_{n-k} \end{bmatrix} . \tag{42}$$

Thus,

$$e = tG+zR = t[I_k, P]+z\begin{bmatrix} 0, & -P \\ 0, & I_{n-k} \end{bmatrix}$$

$$= [tI_k,\ tP(D)] + \left[0,\ z\begin{bmatrix} -P \\ I_{n-k} \end{bmatrix}\right]$$

$$= [t(D),\ (t(D)-z_m(D))P(D)+z_p(D)], \tag{43}$$

where $z_m(D)$ is the received message sequence "in the clear", $z_p(D)$ is the received parity sequence of CC, and $t(D)$ is an element of $F[D]$. By Eq. (41), the above general solution, Eq. (43), of the syndrome equation for a systematic CC can be expressed in an alternate form

$$e(D) = [t(D),\ t(D)P(D)+s(D)], \tag{44}$$

Let $\hat{e}$ denote the error sequence of the solution, Eq. (44), of minimum Hamming weight, and let $\hat{t}$ be element $t(D) \in F[D]$, for which the Hamming weight of $e(D)$ in Eq. (43) or Eq. (44) is a minimum. Then, by Eqs. (43) and (44), as in Eq. (28), $\hat{e}$ and $\hat{t}$ are related by

$$\hat{e} = [\hat{t},\ (\hat{t}-z_m)\cdot P+z_p]$$

$$= [\hat{t},\ \hat{t}P+s]. \tag{45}$$

By Eqs. (29), (36), and (38), the right inverse of the generator matrix G in Eq. (34) is

$$G^{-1} = B^{-1}\begin{bmatrix} I_k \\ 0 \end{bmatrix} = \begin{bmatrix} I_k, & -P \\ 0, & I_{n-k} \end{bmatrix}\begin{bmatrix} I_k \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} I_k \\ 0 \end{bmatrix}. \tag{46}$$

Again, the subtraction of e from z produces

$$\hat{y} = z - \hat{e}$$

as the best estimate at transmitted code, so that

$$\hat{x} = \hat{y}G^{-1} = (z-\hat{e})\cdot G^{-1} = zG^{-1} - \hat{t}$$

$$= [z_m, z_p]\begin{bmatrix} I_k \\ 0 \end{bmatrix}\cdot\hat{t} = z_m - \hat{t} \tag{47}$$

as the best estimate of the received message in terms of z_m, the received message in the clear, and the correction factor, $\hat{t}$.

Next, we are going to give an example on the error trellis syndrome decoding of Wyner-Ash convolutional code.

If

$$G(D) = G_0 + G_1 D + \ldots + G_m D^m \tag{48}$$

is a generator matrix of a CC of memory M = m, as defined in Eq. (3), then evidently

$$G = \begin{bmatrix} G_0 & G_1 & G_2 & \cdots & G_m & 0 & 0 & 0 & \cdots \\ 0 & G_0 & G_1 & G_2 & \cdots & G_m & 0 & 0 & \cdots \\ 0 & 0 & G_0 & G_1 & G_2 & \cdots & G_m & 0 & \cdots \end{bmatrix} \tag{49}$$

is the infinite generator matrix associated with G(D). Thus, a systematic code with generator matrix $G(D) = [I_k, P(D)]$ has

$$G = \begin{bmatrix} I_k & P_0 & 0 & P_1 & 0 & P_2 & \cdots & 0 & P_m & & \\ & I_k & P_0 & 0 & P_1 & 0 & \cdots & 0 & P_m & & \\ & & I_k & P_0 & 0 & P_1 & \cdots & 0 & P_m & & \\ & & & & & & \cdots & & & & \end{bmatrix} \tag{50}$$

as its companion infinite generator matrix, where

$$P(D) = P_0+P_1D+P_2D^2+\ldots+P_mD^m \tag{51}$$

where 0 is the k×k all zero matrix and P_i is the k×(n-k) matrix. By Eq. (35), the associated parity-check matrix is

$$H = \begin{bmatrix} P_0^T & I & & & \\ P_1^T & 0 & P_0^T & I & \\ P_2^T & 0 & P_1^T & 0 & I \\ P_m^T & 0 & & & \cdots \\ & & P_m^T & 0 & \\ & & & & \ddots \end{bmatrix} \tag{52}$$

In terms of Eq. (51) and (52), Blahut defines an $(n,k) = (2^m, 2^m-1)$ Wyner-Ash code as follows: Let H^1 be the parity-check matrix of the binary $(2^m-1, 2^m-1-m)$ Hamming one-error-correcting block code. Choose matrices $P_1^T, P_2^T, \ldots, P_m^T$ to be the m rows of the parity-check matrix H^1, i.e.,

$$H^1 = \begin{bmatrix} P_1^T \\ P_2^T \\ \vdots \\ P_m^T \end{bmatrix} = [P_1, P_2, \ldots, P_m]^T \tag{53}$$

Finally, let P_0^T be a vector of 2^m-1 ones, i.e.,

$$P_0^T = \underbrace{[1,1,\ldots,1]}_{2^m-1} \tag{54}$$

Blahut shows [6, Theorem 12.5.1] that the minimum free distance of the Wyner-Ash code is 3 and, as a consequence, it will correct at least one error.

Example: For m = 2, the parity-check matrix of the Hamming code is

$$H^1 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

so that by Eqs. (53) and (54), $P_0^T = [1\ 1\ 1]$, $P_1^T = [1\ 1\ 0]$, and $P_2^T = [1\ 0\ 1]$. Thus by Eqs. (51)

$$P(D) = \begin{bmatrix} 1+D+D^2 \\ 1+D \\ 1 \quad +D^2 \end{bmatrix}$$

and, by Eqs. (34) and (35),

$$G(D) = \begin{bmatrix} 1\ 0\ 0, & 1+D+D^2 \\ 0\ 1\ 0, & 1+D \\ 0\ 0\ 1, & 1 \quad +D^2 \end{bmatrix}$$

and

$$H(D) = [1+D+D^2,\ 1+D,\ 1+D^2,\ 1] \tag{55}$$

are the generator and parity-check matrices of the (4,3) Wyner-Ash CC, respectively. Also by Eqs. (37) and (38)

$$B = B^{-1} = \begin{bmatrix} I_k, & P(D) \\ 0, & I_{n-k} \end{bmatrix} = \begin{bmatrix} 1\ 0\ 0, & 1+D+D^2 \\ 0\ 1\ 0, & 1+D \\ 0\ 0\ 1, & 1\ \ +D^2 \\ 0\ 0\ 0, & 1 \end{bmatrix}$$

So that, by Eqs. (39) and (40), $B_2 = [0\ 0\ 0\ 1]$ and $\overline{B}_2 = H^T$ and, finally, by Eq. (42),

$$R = \overline{B}_2 B_2 = \begin{bmatrix} 1+D+D^2 \\ 1+D \\ 1\ \ +D^2 \\ 1 \end{bmatrix} [0\ 0\ 0\ 1] = \begin{bmatrix} 0\ 0\ 0, & 1+D+D^2 \\ 0\ 0\ 0, & 1+D \\ 0\ 0\ 0, & 1\ \ +D^2 \\ 0\ 0\ 0, & 1 \end{bmatrix} \tag{56}$$

Substituting Eqs. (55) and (56) into Eq. (25) or directly from Eq. (43). The result is

$$\begin{aligned} e(D) \equiv e &= [e_1, e_2, e_3, e_4] \\ &= [t, (t_1+z_1)(1+D+D^2)+(t_2+z_2)(1+D)+(t_3+z_3)(1+D^2)+z_4], \end{aligned} \tag{57}$$

where

$$t(D) \equiv t = [t_1, t_2, t_3]. \tag{58}$$

By Eqs. (41) and (44), e in Eq. (57) can also be expressed as

$$e = [t, r+s] \tag{59}$$

where s is the syndrome,

$$s(D) \equiv s = z_1(1+D+D^2)+z_2(1+D)+z_3(1+D^2)+z_4 \tag{60}$$

and

$$r(D) \equiv r = t_1(1+D+D^2)+t_2(1+D)+t_3(1+D^2) \tag{61}$$

Define the truncation of e(D) at stage or frame time N as

$$[e(D)]_N = \sum_{j=0}^{N} [e_{1j}, e_{2j}, \ldots, e_{nj}]D^j \tag{62}$$

Thus the Hamming weight of the sequence of possible errors in N frames is

$$\begin{aligned} ||[e(D)]_N|| &= \sum_{j=0}^{N} ||[e_{1j}, e_{2j}, \ldots, e_{nj}]|| \\ &= \sum_{j=0}^{N} ||\underset{D^j}{\text{coef}}[e(D)]||. \end{aligned} \tag{63}$$

By Eqs. (57) and (63) for this particular example of a convolutional code,

$$\underset{D^j}{\text{coef}}[e(D)] = [t_{1j}, t_{2j}, t_{3j}, r_j + s_j]. \tag{64}$$

where

$$\begin{aligned} r_j = {} & t_{1,j} + t_{1,j-1} + t_{1,j-2} + \\ & t_{2,j} + t_{2,j-1} + \\ & t_{3,j} \qquad + t_{3,j-2} \end{aligned} \tag{65}$$

and

$$\begin{aligned} s_j = {} & z_{1j} + z_{1,j-1} + z_{1,j-2} + \\ & z_{2j} + z_{2,j-1} + \\ & z_{3j} \qquad + z_{3,j-2} + \\ & z_{4j} \end{aligned} \tag{66}$$

If the values of r_j at frame time j are imagined to be generated by a sequential circuit, then the pair

$$\sigma_j = (\underline{t}_{j-1}, \underline{t}_{j-2}) \tag{67}$$

where

$$\underline{t}_{j-1} = [t_{1,j-1}, t_{2,j-1}, t_{3,j-1}]$$

and

$$\underline{t}_{j-2} = [t_{1,j-2}, t_{2,t-2}, t_{3,j-2}]$$

constitutes the values of the internal states of the circuit and vector $\underline{t}_j$ is the j-th input to the circuit.

Let the sequential circuit with output

$$u_j = [t_j, r(\underline{t}_j, \sigma_j)] \tag{68}$$

then by Eq. (59), the error trellis of the code is, for all path generated,

$$v_j = [\underline{t}_j, s_j + r(\underline{t}_j, \sigma_j)]. \tag{69}$$

To illustrate the above concepts, let the input to the present example of the CC be

$$x = [1\ 1\ 1,\ 0\ 0\ 0,\ 1\ 1\ 1,\ 0\ 0\ 0,\ 1\ 1\ 1],$$

i.e., $x_1 = [1\ 0\ 1\ 0\ 1] = x_2 = x_3$. By the generating matrix given in Eq. (55), the output $y = [y_1, y_2, y_3, y_4]$ are obtained as follows:

$$y_1 = y_2 = y_3 = x_1 = [1\ 0\ 1\ 0\ 1] \text{ and}$$

$$y_4 = (1+D+D^2)x_1 + (1+D)x_2 + (1+D^2)x_3.$$

Explicitly,

$$y_4 = [1\ 0\ 1\ 0\ 1\ 0\ 0].$$

Thus, the output of the encoder is

$$y = [1\ 1\ 1\ 1,\ 0\ 0\ 0\ 0,\ 1\ 1\ 1\ 1,\ 0\ 0\ 0\ 0,\ 1\ 1\ 1\ 1] \tag{70}$$

Assume y, given in Eq. (70) is transmitted over a binary symmetric channel (BSC) with probability of error somewhat less than $\frac{1}{12} = 0.0833$. Then, the received code sequence is likely

$$z = [1\ 1\ 0\ 1,\ 0\ 0\ 0\ 0,\ 1\ 1\ 1\ 1,\ 0\ 0\ 0\ 0,\ 0\ 1\ 1\ 1] \tag{71}$$

i.e.

$$z_1 = [1\ 0\ 1\ 0\ 0], \qquad z_2 = [1\ 0\ 1\ 0\ 1],$$

$$z_3 = [0\ 0\ 1\ 0\ 1], \qquad z_4 = [1\ 0\ 1\ 0\ 1].$$

By Eq. (60), the syndrome sequence for this value of received sequence is

$$s = [1\ 0\ 1\ 0\ 1\ 1\ 1] \tag{72}$$

It is shown in Ref. 6, p. 366, that the present 3/4 rate code of this example can correct one error in every 3 frame times or code length of 12. As a consequence, one needs only to correct one error every 3 frames. This limits the number of $t = [t_1, t_2, t_3]$ to 4, namely the values

$$\begin{aligned} [0\ 0\ 0] &\equiv 0, & [1\ 0\ 0] &\equiv 1 \\ [0\ 1\ 0] &\equiv 2, & [0\ 0\ 1] &\equiv 3 \end{aligned} \tag{73}$$

Figure 1 shows a constrained regulator trellis with outputs [t,r]. In Fig. 1, note that, because of the limited error-correction capability of the code, the number of internal states $\sigma = (Dt, D^2t)$ of the circuit can be limited to 7 out of possible 64. Moreover, the number of state transitors can be limited to those shown in Fig. 1 for the regulator trellis diagram. The branches of the trellis are labeled with the value [t,r]. For example, the branch from state $\sigma = [0\ 0]$ to $\sigma = [3\ 0]$ is labeled by $[t,r] = [3,1] \equiv [0,0,1,1]$, which

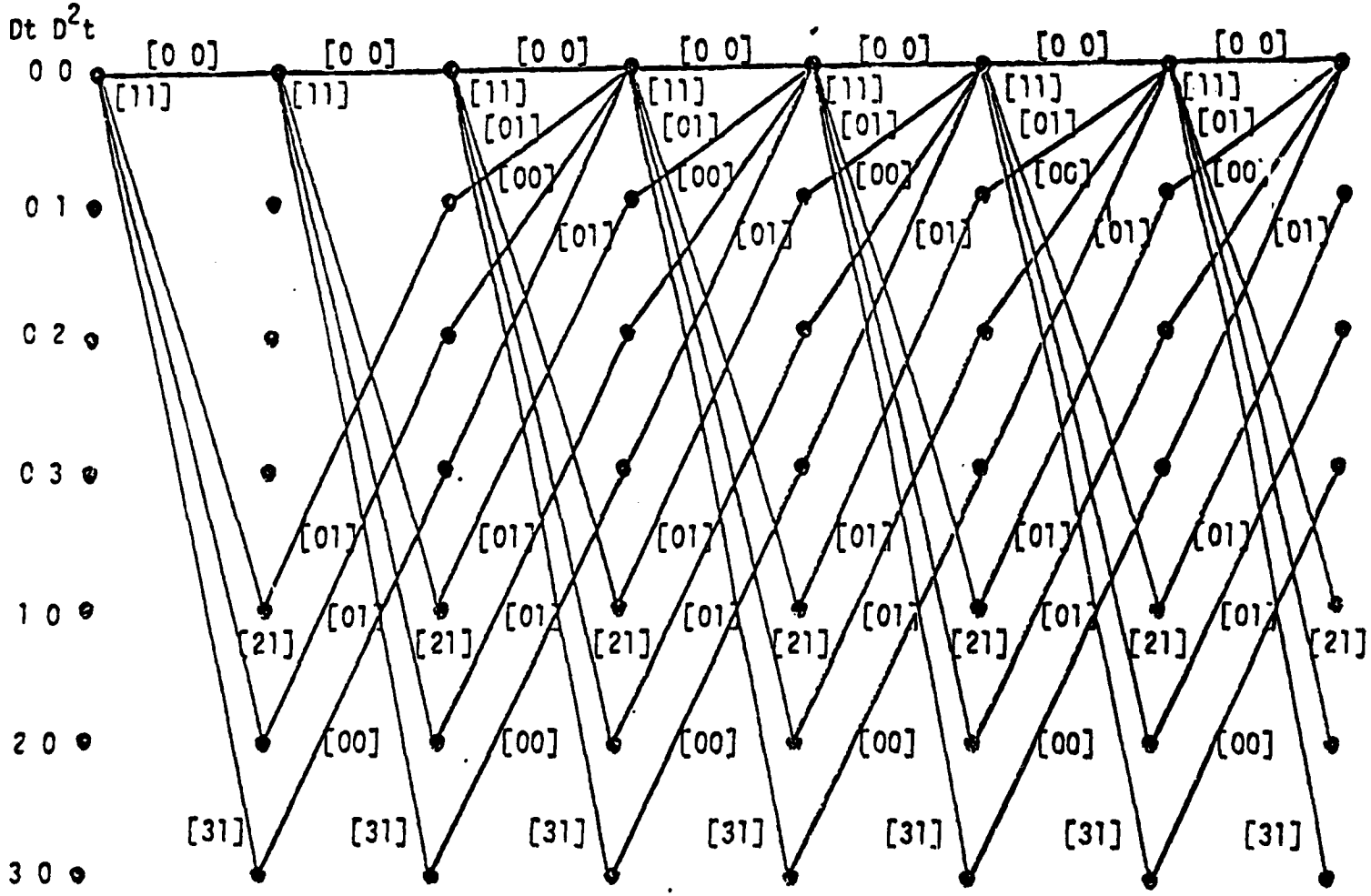


Fig. 1 — Constrained regulator trellis with outputs [t, r],

where $r = t_1(1 + D + D^2) + t_2(1 + D) + t_3(1 + D^2) \equiv r(t, \sigma)$ and where $t = [t_1, t_2, t_3] = [0\ 0\ 0] \equiv 0$,

$t = [1\ 0\ 0] \equiv 1$, $t = [0\ 1\ 0] \equiv 2$, and $t = [0\ 0\ 1] \equiv 3$.

means $t_1 = 0$, $t_2 = 0$, $t_3 = 1$, and $r = 1$.

To decode the message in Eq. (71), by Eq. (68) an error trellis is created by adding the vector [0,s] to all labels in the regulator trellis where, s is the syndrome value. Thus, in Fig. 2, the value of [0,s], where s is the syndrome value in Eq. (72), appear on all possible transitions $\sigma = [0\ 0]$ to $\sigma = [0\ 0]$ on the top line of the error trellis. At each node, the cumulative Hamming weight of the path, passing through that node, is written. The Hamming weight at each node, plus the weight of a possible branching from that to the next node, is used to eliminate branches. To illustrate, in Fig. 2 there are four branches at frame z which could go to state or node $\sigma = [0\ 0]$. The transition is chosen in the branch from $\sigma = [0\ 3]$ to $\sigma = [0\ 0]$. Since the node weight 2 plus branch weight 0 is 2, the minimum 4 possible transitions.

The minimum overall path weight of the error trellis in Fig. 2 is

$$[0\ 0,\ 3\ 0,\ 0\ 3,\ 0\ 0,\ 0\ 0,\ 1\ 0,\ 0\ 1,\ 0\ 0,\ 0\ 0]$$

in terms of state values $\sigma = [Dt,\ D^2t]$. Hence, based on the criterion of Eq. (27), the best estimates of t is

$$\hat{t} = [3,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0]$$

$$= [0\ 0\ 1,\ 0\ 0\ 0,\ 0\ 0\ 0,\ 0\ 0\ 0,\ 1\ 0\ 0,\ 0\ 0\ 0].$$

If this vector is added component-wise to z in Eq. (71), the message is corrected to yield $\hat{x} = x$, the original message.

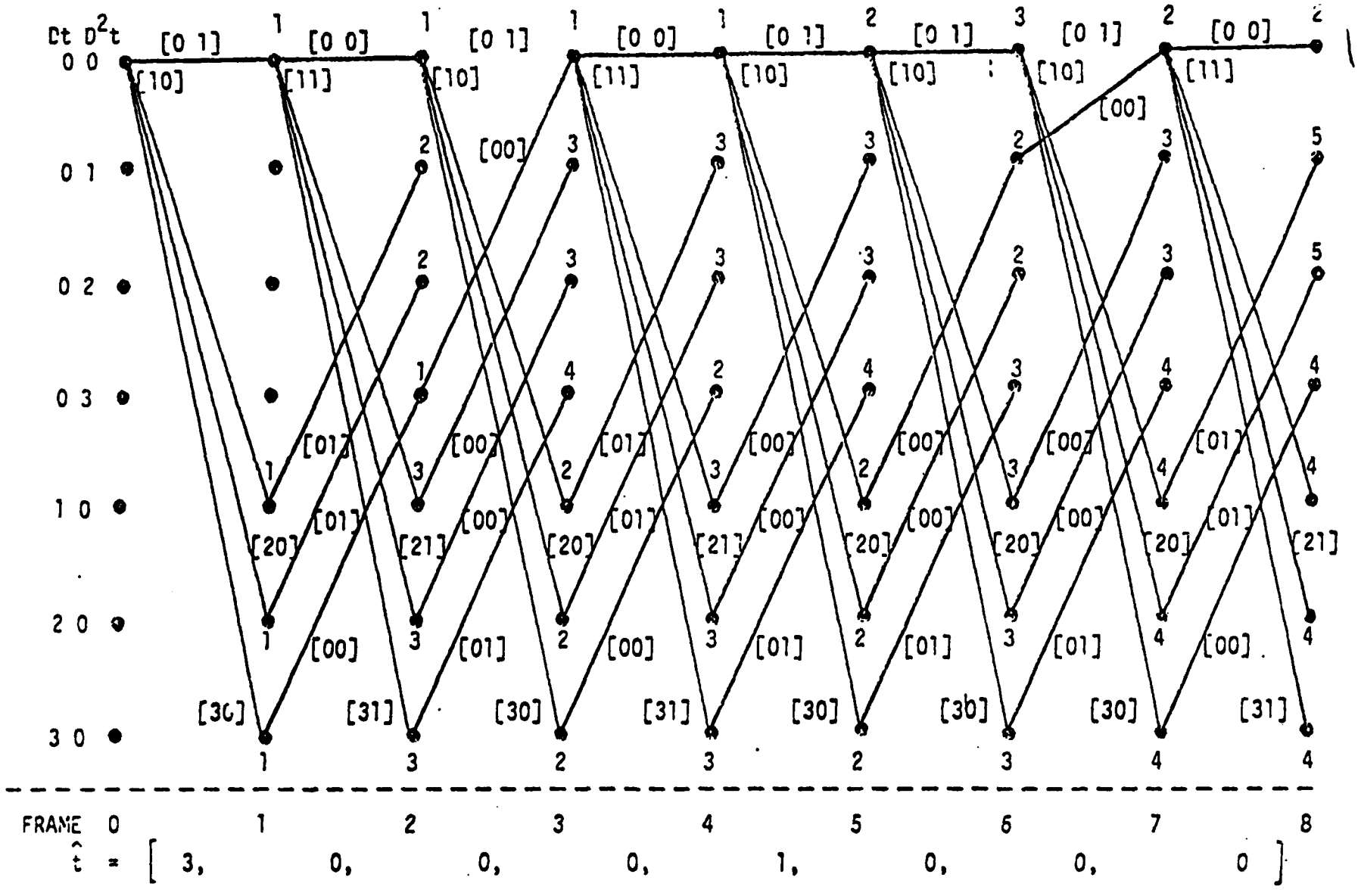


Fig. 2 — Error trellis with input and state-transition constraints for one-error-correcting Wyner-Ash convolutional code.

REFERENCES

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

2. I.S. Reed and T.K. Truong, "New Syndrome Decoding Techniques for Convolutional Codes Over GF(q)," to be published in Proceedings IEE.

3. C.D. Forney, Jr., "Convolutional Codes I: Algebraic Structure," IEEE Trans. Info. Theor. IT-9, 1963, pp. 64-74.

4. A.J. Vinck, A.J.P. de Paepe, and J.P.M. Schalkwijk, "A Class of Binary Rate On-Half Convolutional Codes that Allows an Improved Stack Decoder," IEEE Trans. Info. Theor. IT-26, No. 4, 1980, pp. 389-392.

5. A.D. Wyner and R.B. Ash, "Analysis of Recurrent Codes," IEEE Trans. Info. Theor. IT-9, 1963, pp. 143-156.

6. R.E. Blahut, Theory and Practice of Error Control Codes, Addison-Wesley, 1983.

END

FILMED

1-85

DTIC