Simplified Syndrome Decoding of (n, 1) Convolutional Codes

I. S. Reed
Department of Electrical Engineering
University of Southern California

T. K. Truong
Communication System Research

This paper presents a new syndrome decoding algorithm for the (n, 1) convolutional codes (CC) that is different and simpler than the previous syndrome decoding algorithm of Schalkwijk and Vinck. The new algorithm uses the general solution of the polynomial linear Diophantine equation for the error polynomial vector E(D). This set of Diophantine solutions is a coset of the CC space. A recursive or Viterbi-like algorithm is developed to find the minimum weight error vector $\hat{E}(D)$ in this error coset. An example illustrating the new decoding algorithm is given for the binary nonsymmetric (2, 1) CC.

I. Introduction

In this paper the syndrome decoding algorithm invented in 1976 by Schalkwijk and Vinck (Ref. 1) is simplified and generalized to all (n, 1) convolutional codes (CC), both systematic and nonsystematic. Indications are given also of how the techniques used here can be further extended to apply to any (n, k) CC for which a parity check polynomial matrix can be found.

Following Refs. 2 and 3, the input $X(D)$ and output sequences $Y_1(D), \cdots, Y_n(D)$ of an $(n, 1)$ CC are formal power series of finite length over a finite field $GF(q)$ in the unit delay operator D. The input $X(D)$ and the output $Y(D) = [Y_1(D), \cdots, Y_n(D)]$, as a vector, are connected by a $1 \times n$ polynomial generator matrix $G(D)$ of form

$$G(D) = [G_1(D), \cdots, G_n(D)], \tag{1}$$

where $G_k(D)$ are monic polynomials of finite degree in D over $GF(q)$. This relationship is

$$Y(D) = X(D)G(D) \tag{2}$$

The maximum degree M of the polynomials in $G(D)$ is called the memory and the constraint of the code is $L = M + 1$.

To avoid the possibility of catastrophic error propagation the important criterion of Massey and Sain (Ref. 4) is a necessity. In this paper attention is restricted to coder inverses without delay. Hence one must have

$$GCD[G_1(D), \cdots, G_n(D)] = 1$$

where GCD denotes "greatest common divisor" and $G_k(D)$ is the kth component polynomial of $G(D)$ in (1).

The parity-check matrix $H(D)$, associated with a general $k \times n$ generator matrix $G(D)$, is a $k \times (n-k)$, maximum rank matrix of polynomials over $GF(q)$ with the property

$$G(D)H^T(D) = 0 \tag{3}$$

where T denotes matrix transpose. If $G(D)$ is the generator matrix of a systematic (n, k) CC, $G(D)$ has the form $[I_k, P(D)]$ where I_k is the $k \times k$ identity matrix and $P(D)$ is a $k \times (n-k)$ matrix of polynomials in D over $GF(q)$. In this case it is easily shown (Ref. 5) that

$$H(D) = [-P^T(D), I_{n-k}] \tag{4}$$

is the appropriate parity check matrix.

The parity check matrix $H(D)$ for the general nonsystematic (n, k) CC is considerably more difficult to find. Forney in Ref. 3 develops a general procedure to find $H(D)$. However, for the $(n, 1)$ CC considered in this paper the powerful machinery of Forney is not needed. For the nonsystematic $(n, 1)$ CC with the generator matrix $G(D)$, given in (1), it is easily verified that

$$H(D) = \begin{bmatrix} G_2(D), & G_1(D), & 0 & \cdots & 0 \\ G_3(D), & 0, & G_1(D) & \cdots & 0 \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ G_n(D), & 0, & 0 & \cdots & G_1(D) \end{bmatrix} \tag{5}$$

satisfies (3) and is a parity check matrix.

Let $Z(D) = Y(D) + E(D)$ be the received code sequence in powers of the delay operator D, possibly corrupted by an error or noise sequence $E(D)$. The *syndrome* $S(D)$ of $Z(D)$ is defined by

$$S(D) = Z(D)H^T(D) \tag{6}$$

By (2) and (3) the syndrome reduces to

$$S(D) = [(Y(D) + E(D)]\,H^T(D) = E(D)H^T(D) \tag{7}$$

in terms of the noise sequence $E(D)$, only. For example by (5) and (7) the syndrome for the 1/2 rate code, (2, 1) CC, is

$$S(D) = E_1(D)G_2(D) + E_2(D)G_1(D) \tag{8}$$

For the 1/3 rate code, (3, 1) CC,

$$\begin{aligned} S(D) &= [S_1(D), S_2(D)] \\ &= [E_1(D)G_2(D) + E_2(D)G_1(D), E_1(D)G_3(D) \\ &\quad + E_3(D)G_1(D)] \end{aligned} \tag{9}$$

In Ref. 1 Schalkwijk and Vinck showed how the states of the syndrome processor of $S(D)$ in (8) could be used to form a trellis diagram for implementing a recursive algorithm similar to the Viterbi algorithm (Ref. 5). In the present paper this idea is extended in a manner which is simpler and more easily applied. The departure point for the new simplified syndrome decoding is to first find the solution of the syndrome equation (7) for the error vector $E(D)$.

This technique for finding the solution of (7) for error vector $E(D)$ is illustrated by finding solutions for $E_k(D)$ in the special cases (8) and (9). The total set in which the solutions $E_k(D)$ are to be found is the set $F[D]$ of all polynomials in operator D over $F = GF(q)$. It is well known (Ref. 6) that $F[D]$ is an integral domain (a commutative ring without zero divisors) and as a consequence satisfies many of the properties of the integers. In particular (8), (9) and more generally (7) are linear Diophantine equations over polynomials in D instead of the integers.

Using techniques precisely similar to those used for the integers, e.g., see Ref. 6, the general solution of (8) is readily found. Since $GCD\,[G_1(D), G_2(D)] = 1$, the Euclidean algorithm can be used to find polynomials $\alpha_1(D)$ and $\alpha_2(D)$ such that

$$\alpha_1(D)G_2(D) + \alpha_2(D)G_1(D) = 1.$$

In terms of $\alpha_k(D)$ the general solution of (8) is

$$\begin{aligned} E_1(D) &= \alpha_1(D)S(D) + G_1(D)t(D) \\ E_2(D) &= \alpha_2(D)S(D) + G_2(D)t(D) \end{aligned} \tag{10}$$

where $t(D)$ is an arbitrary polynomial in $F[D]$.

To find the Diophantine solution of (9), first eliminate $E_1(D)$ from the two components $S_k(D)$ for $(k = 1, 2)$ by multiplying the first component by $G_3(D)$ and the second by $G_2(D)$. The resulting equation after subtraction is

$$\begin{aligned} [E_2(D)G_3(D) - E_3(D)G_2(D)]\,G_1(D) &= G_3(D)S_1(D) \\ &\quad - G_2(D)S_2(D) \end{aligned} \tag{11}$$

Observe that in terms of the original computation of $S(D)$ in (6),

$$\begin{aligned} G_3(D)S_1(D) - G_2(D)S_2(D) &= G_3(D)[Z_1(D)G_2(D) \\ &\quad + Z_2(D)G_1(D)] \\ &\quad - G_2(D)[Z_1(D)G_3(D) \\ &\quad + Z_3(D)G_1(D)] \\ &= [Z_2(D)G_3(D) \\ &\quad - Z_3(D)G_2(D)]\, G_1(D) \end{aligned}$$

so that the right side of (11) is always divisible by $G_1(D)$. Dividing (11) by $G_1(D)$ yields

$$E_2(D)G_3(D) - E_3(D)G_2(D) = R(D) \tag{12}$$

where

$$R(D) = \frac{[G_3(D)S_1(D) - G_2(D)S_2(D)]}{G_1(D)}, \tag{13}$$

a polynomial in D over $GF(q)$. The greatest common divisor of the $G_k(D)$'s must equal one by the Massey and Sain criterion. This criterion is achieved for this case by assuming $GCD\,[G_2(D), G_3(D)] = 1$. Thus (12) has a solution similar to (10), namely,

$$\begin{aligned} E_2(D) &= \beta_3(D)R(D) + G_2(D)t(D) \\ E_3(D) &= -\beta_2(D)R(D) + G_3(D)t(D) \end{aligned} \tag{14}$$

where $\beta_2(D)$ and $\beta_3(D)$ are a particular solution to

$$\beta_2(D)G_2(D) + \beta_3(D)G_3(D) = 1 \tag{15}$$

and $t(D)$ is an arbitrary polynomial in D over $GF(q)$. Finally to find $E_1(D)$ substitute (14) into the components of $S(D)$ in (9) and solve for $E_1(D)$ by multiplying the first equation by $\beta_2(D)$ and the second by $\beta_3(D)$. This yields

$$E_1(D) = S_1(D)\beta_2(D) + S_2(D)\beta_3(D) - G_1(D)t(D) \tag{16}$$

where $\beta_2(D)$ and $\beta_3(D)$ satisfies (15). Equations (14) and (16) with (15) where $t(D) \in F[D]$ constitute the general solution of (7) for $E(D)$ of the (3, 1) CC. The above Diophantine techniques extend to yield solutions to all $(n, 1)$ CC. In fact it is readily demonstrated that the general solution of (7) for $E(D)$ is the linear function

$$E(D) = L\,[t(D)] = L_0(D) + L_1(D)t(D). \tag{17}$$

for all $t(D)$ in $F[D]$. The set of all $L\,[t(D)]$ is a coset of the $(n, 1)$ CC code space $\{L_1(D)t(D) \mid t(D) \in F[D]\}$.

In order to use syndrome decoding to find a maximum likelihood estimate (MLE) $\hat{E}(D)$ of the actual error sequence, both the weight of the sequence and the channel need to be defined. For an $(n, 1)$ CC a possible error sequence is of form $E(D) = [E_1(D), E_2(D), \cdots, E_n(D)]$ where $E_k(D)$ are finite degree polynomials over $GF(q)$. The Hamming weight of $E(D)$ is

$$W_H[E(D)] = \sum_{k=1}^{n} W_H[E_k(D)]$$

where $W_H[E_k(D)]$, the Hamming of polynomial $E_k(D)$, is the number of nonzero coefficients of $E_k(D)$. Assume the channel over which $Y(D)$ is sent is approximated by a q-ary channel (see Ref. 2, Sec. 7.2).

If $\deg[X(D)] \leqslant L - 1$, the codeward $Y(D) = [Y_1(D), \cdots, Y_n(D)]$ is the Lth truncation of an $(n, 1)$ CC (Ref. 2, p. 203). Each component $Y_k(D)$ has degree $\leqslant M + L - 1$ where M is memory of code. For a truncated $(n, 1)$ CC transmitted over a q-ary symmetric channel it is evident that the MLE of an error vector is $\hat{E}(D)$ such that

$$W_H(\hat{E}) = \operatorname*{Min}_{t(D)} \{L\,[t(D)]\} \tag{18}$$

where $L\,[t(D)]$ is the linear Diophantine solution (17) for $E(D)$ of syndrome equation (7)

The above procedure for finding the MLE $\hat{E}(D)$ is equivalent to the standard syndrome decoding technique used for block codes, e.g., see Ref. 7. In the next section a recursive or Viterbi-like algorithm is developed to efficiently find $\hat{E}(D)$, the estimate of the error sequence.

II. Recursive Syndrome Decoding

The new technique of recursive syndrome decoding is presented by example, with the same nonsystematic (2, 1) CC used in Ref. 1. For this code,

$$G(D) = [G_1(D), G_2(D)] = [1 + D^2, 1 + D + D^2]$$

and

$$H(D) = [G_2(D), G_1(D)] = [1 + D + D^2, 1 + D^2]$$

are the generating and parity-check matrices, respectively. By (8) the syndrome is

$$\begin{aligned} S(D) &= Z_1(D)(1 + D + D^2) + Z_2(D)(1 + D^2) \\ &= Z_1(D) + Z_1^{(1)}(D) + Z_1^{(2)}(D) + Z_2(D) + Z_2^{(2)}(D) \end{aligned} \tag{19}$$

Note that terms such as $Z_1^{(1)}(D)$ in this expression can be regarded either as a delayed version of $Z_1(D)$ or a right shift of sequence $Z_1(D)$ when viewed as a sequence proceeding from left to right. Finally the Diophantine solutions (10) of the syndrome equation (8) for error sequences $E_1(D)$ and $E_2(D)$ are

$$\begin{aligned} E_1(D) &= DS(D) + (1 + D^2)t(D) \\ &= S^{(1)}(D) + t(D) + t^{(2)}(D) \end{aligned}$$

and

$$\begin{aligned} E_2(D) &= (1 + D)S(D) + (1 + D + D^2)t(D) \\ &= S(D) + S^{(1)}(D) + t(D) + t^{(1)}(D) + t^{(2)}(D) \end{aligned} \tag{20}$$

since

$$\alpha_1(D) = D \quad \text{and} \quad \alpha_2(D) = 1 + D$$

constitute a particular solution of

$$\alpha_1(D)G_1(D) + \alpha_2(D)G_2(D) = 1.$$

Schalkwijk and Vinck (Ref. 1) used the states of the sequential circuit, used to form the syndrome $S(D)$, for the states of their trellis diagram. Here the states of the trellis diagram are obtained from the states of the shift register needed in (20) to obtain $t^{(1)}(D)$ and $t^{(2)}(D)$ from $t(D)$. A block diagram of a shift register to produce the delayed versions, $t^{(1)}(D)$ and $t^{(2)}(D)$, from $t(D)$ is shown in Fig. 1. The state table of this shift register, when regarded as a sequential circuit, is given in Fig. 2. Finally in Fig. 3 the trellis diagram, associated with this state table is presented. A solid-line transition in Fig. 3 corresponds to the input $t(D) = 0$; a dashed-line transition corresponds to the input $t(D) = 1$.

The new Viterbi-like syndrome decoding algorithm is illustrated by example in Fig. 4. For this example assume that the message to be transmitted is the six-bit message

$$X(D) = [0\ 1\ 0\ 0\ 1\ 0]$$

so that the truncation length is $L = 6$. By (2)

$$Y_1(D) = [0\ 1\ 0\ 1\ 1\ 0\ 1\ 0]$$

and

$$Y_2(D) = [0\ 1\ 1\ 1\ 1\ 1\ 1\ 0]$$

are the two components of $Y(D)$. Thus the scalar representation of the code word is

$$C = [0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0]$$

of overall code length $n(L + M) = 2(6 + 2) = 16$ (see Ref. 2, pp. 201–203).

Let the received codeward be

$$R = [1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0]$$

Then

$$Z_1(D) = [1\ 1\ 0\ 1\ 1\ 1\ 1\ 0]$$

and

$$Z_2(D) = [0\ 1\ 0\ 1\ 1\ 1\ 1\ 0]$$

are the two components of received message $Z(D)$. Using (19) this syndrome sequence is

$$\begin{aligned} S(D) &= 1 + D + D^4 + D^5 + D^6 + D^7 \\ &= [1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0] \end{aligned}$$

both as a polynomial in D over $GF(2)$ and as a simple finite sequence. The latter representation of $S(D)$ is shown in Fig. 4 with its digits placed over the transition paths of the trellis.

Let us proceed briefly through the trellis. The syndrome is set to 0 prior to stage 0 so that at stage 0, $S^{(1)}(D) = 0$, and

$S(D) = 1$. Likewise it is assumed initially that the shift register in Fig. 1 is cleared so that $t^{(1)}(D) = t^{(2)}(D) = 0$. This puts the algorithm at stage 0 at stage $a = [0, 0]$. The label on branch $t(D) = 0$ is found by substituting these values in (20). That is,

$$E_1(D) = S^{(1)}(D) + t(D) + t^{(2)}(D) = 0 + 0 + 0 = 0$$

$$E_2(D) = S(D) + S^{(1)}(D) + t(D) + t^{(1)}(D) + t^{(2)}(D)$$

$$= 1 + 0 + 0 + 0 + 0 = 1$$

Hence the label on branch $t(D) = 0$ at stage zero in $[E_1(D) E_2(D)] = [0, 1]$. By the same substitution but with $t(D) = 1$, the label on the alternate branch is $[E_1(D), E_2(D)] = [1, 0]$, the componentwise complement of the previous branch. The Hamming weight of $[E_1(D), E_2(D)]$ for both these branches is 1. Note that this weight of 1 is placed immediately above states a and c at stage 1.

To illustrate the Viterbi or dynamic-programming technique for computing survivors in the trellis suppose that the algorithm is either at state a or state b at stage 2. Note from Fig. 3 that there are only two ways to state a, by a transition from b to a or a transition from a to a. At state a or b at stage 2, $S(D) = 0$ and $S^{(1)}(D) = 1$. At stage 2 at state a, $t^{(1)}(D) = 0$ and $t^{(2)}(D) = 0$ so that at branch $t(D) = 0$,

$$E_1(D) = S^{(1)}(D) + t(D) + t^{(2)}(D) = 1 + 0 + 0 = 1$$

$$E_2(D) = S(D) + S^{(1)}(D) + t(D) + t^{(1)}(D) + t^{(2)}(D)$$

$$= 0 + 1 + 0 + 0 + 0 = 1$$

The total weight of $[E_1(D), E_2(D)]$ for the minimum weight path, going through state a at stage 2, is thus $2 + 2 = 4$. However, at stage 2 at state b, $t^{(1)}(D) = 0$ and $t^{(2)}(D) = 1$, so that at branch $t(D) = 0$,

$$E_1(D) = S^{(1)}(D) + t(D) + t^{(2)}(D) = 1 + 0 + 1 = 0$$

$$E_2(D) = S(D) + S^{(1)}(D) + t(D) + t^{(1)}(D) + t^{(2)}(D)$$

$$= 0 + 1 + 0 + 0 + 1 = 0$$

Thus the total weight of $[E_1(D), E_2(D)]$ for the minimum weight path, going through state b at stage 2 is thus $3 + 0 = 3$. Since this weight is smaller than the previous weight, only the path going through state b to a at stage 2 survives. The segment of path from state a to a is deleted as shown in Fig. 4. Similarly in Fig. 4 some paths lead to equal weights or a "tie." In such a case either segment can be chosen as part of the survivor path.

The entire trellis diagram shown in Fig. 4 is completed by the rules illustrated above. At stage 9 the minimum weight path in the trellis diagram of Fig. 4 is $a\ c\ d\ b\ c\ b\ c\ d\ b\ a$. The branches of this path yield

$$\hat{E}(D) = [1\ 0\ 0\ 0\ 0\ 1\ 0\ 0, 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0]$$

$$= [1 + D^5, D^2] = [\hat{E}_1(D), \hat{E}_2(D)]$$

as the estimate of the error vector. Subtracting these estimates of the error from $Z(D)$ produces

$$\hat{Y}_1(D) = [0\ 1\ 0\ 1\ 1\ 0\ 1\ 0]$$

and

$$\hat{Y}_2(D) = [0\ 1\ 1\ 1\ 1\ 1\ 1\ 0]$$

as estimates of the transmitted coded message. Finally the inverse linear sequential circuit of Massey and Sain (Ref. 4), with equation

$$\hat{X}(D) = (1 + D)\hat{Y}_1(D) + D\hat{Y}_2(D)$$

is used to find $\hat{X}(D) = [0\ 1\ 0\ 0\ 1\ 0]$ as an estimate of the original message.

For the above example, this new syndrome decoding algorithm yields the original message. However, if the number of errors exceeds the capability of the code, at the end of the decoding period there may exist two or more paths with the same minimum error weight. In such a circumstance a decoding failure and an erasure should be declared.

III. Conclusions

In this paper a new simplified syndrome decoding algorithm for $(n, 1)$ CC is developed which utilizes the general Diophantine solution for the error vector $E(D)$ in the syndrome equation. The least weight error vector $\hat{E}(D)$ is found by a recursive Viterbi-like algorithm, similar to an algorithm conceived previously by Schalkwijk and Vinck (Ref. 1)

This new syndrome decoder appears to be comparable in complexity to the Viterbi decoder except that in the new decoder fewer comparisons are required and the control logic is considerably simpler. Another possible advantage of the new algorithm is its ability to detect decoding failures more readily than the classical Viterbi approach. A more detailed comparison of these decoders is a topic for further study.

Acknowledgment

The authors wish to thank Charles Wang of JPL for his helpful suggestions made during the preparation of this paper.

References

1. Schalkwijk, J. P. M., and Vinck, A. J., "Syndrome decoding of binary rate–1/2 convolutional codes," *IEEE Trans. Comm.*, COM–24, pp. 977–985, 1976.
2. McEliece, R. J., *The Theory of Information and Coding*, Addison-Wesley Publishing Co., Reading, Mass., 1974.
3. Forney, G. D., "Convolutional Codes I: algebraic structure," *IEEE Trans. Inform.*, IT–16, pp. 720–738, 1970.
4. Massey, J. L., and Sain, M. K., "Inverses of linear circuits," *IEEE Trans. Comput.*, C–17, pp. 330–337, 1968.
5. Viterbi, A., and Omura, J., *Digital Communication and Coding*, McGraw-Hill Book Co., New York, 1978.
6. Nagell, T., *Introduction to Number Theory*, John Wiley and Sons, New York, 1951.
7. Peterson, W. W., and Weldon, E. J., Jr., *Error-Correcting Codes*, 2nd ed., M.I.T. Press, Cambridge, Mass., 1972.

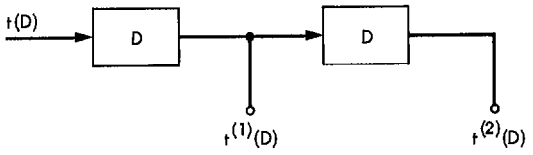


Fig. 1. Shift register to generate delayed versions of *t(D)*

$t^{(1)}(D), t^{(2)}(D)$		t(D) = 0	t(D) = 1
a = 0	0	0 0	1 0
b = 0	1	0 0	1 0
c = 0	0	0 1	1 1
d = 1	1	0 1	1 1

Fig. 2. State table of shift register for *t(D)*

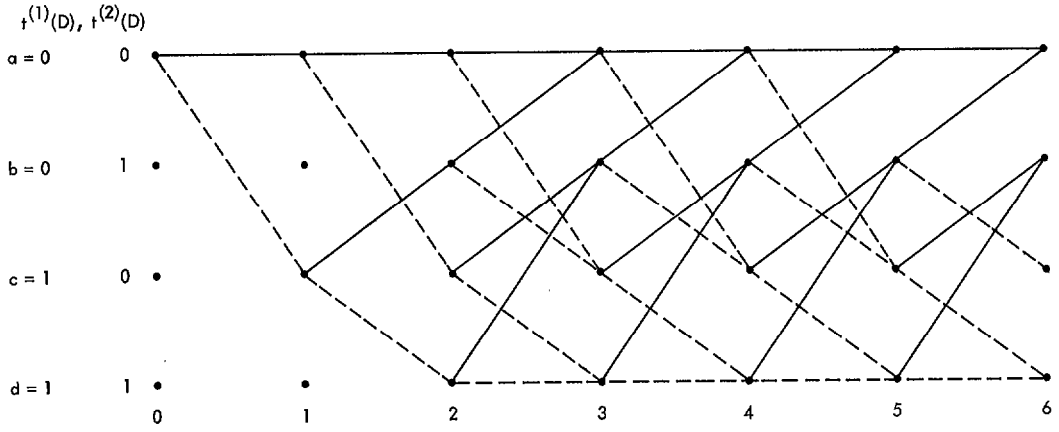
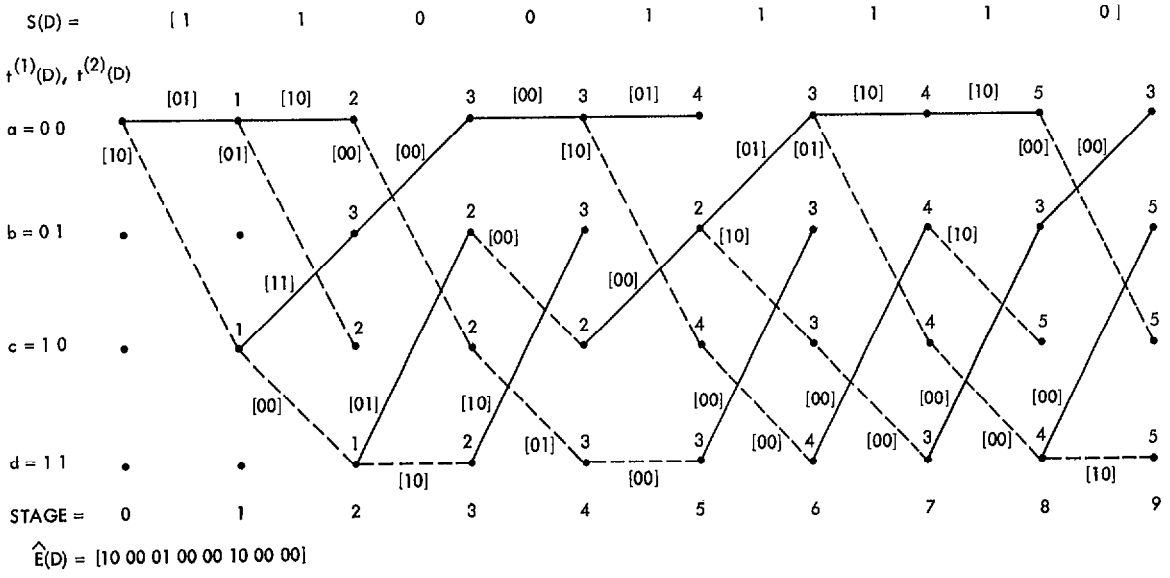


Fig. 3. Trellis diagram of shift register for *t(D)*. Input *t(D)* = 0 is represented by a solid line. *t(D)* = 1 is represented by a dashed line



$\hat{E}(D)$ = [10 00 01 00 00 10 00 00]

Fig. 4. New Viterbi-like syndrome decoding algorithm. Each branch of trellis is labeled with $[E_1(D), E_2(D)]$ where $E_1(D) = S^{(1)}(D)+t(D)+t^{(2)}(D)$ and $E_2(D) = S(D)+S^{(1)}(D)+t^{(1)}(D)+t^{(2)}(D)$. Each node at k is labeled with $W_H[E_1(D), E_2(D)]$ up to time k