Syndrome Decoding of Binary Rate *k/n* Convolutional Codes

J. PIETER M. SCHALKWIJK, SENIOR MEMBER, IEEE, A. J. VINCK, MEMBER, IEEE, AND KAREL A. POST, MEMBER, IEEE

***Abstract*—A state-space approach to the syndrome decoding of binary rate k/n convolutional codes is described. State-space symmetries of a certain class of codes can be exploited to obtain a reduction in the exponent of growth of the decoder hardware. Aside from these savings it is felt that the state-space formalism developed has some unique intrinsic value.**

I. Introduction

This paper is concerned with a state-space approach to the syndrome decoding of binary rate k/n convolutional codes. It extends and generalizes earlier work [1]–[3] on syndrome decoding of binary rate $\frac{1}{2}$ convolutional codes. In Sections II and III, we develop a concise mathematical formulation of the problem. Section IV introduces a special class of binary rate $(n-1)/n$ convolutional codes. It is shown that the state-space symmetries of this class of codes allow an exponential reduction of decoder hardware. Section V extends the results of the previous section to rate k/n codes. Table II lists the free distance of some short constraint length codes that exhibit the required symmetries.

Fig. 1 shows a conventional [4] binary rate 2/3 convolutional encoder with two memory elements. The inputs to this encoder are two binary message sequences

$$\langle m_i \rangle = \cdots, m_{i,-1}, m_{i0}, m_{i1}, \cdots, \qquad i=1,2.$$

The outputs are three binary codeword sequences $\langle c_1 \rangle$, $\langle c_2 \rangle$, and $\langle c_3 \rangle$ (hence the rate is 2/3). The elements of the three output sequences $\langle c_1 \rangle$, $\langle c_2 \rangle$, and $\langle c_3 \rangle$ are, respectively,

$$\begin{aligned} c_{1,t} &= m_{1,t} \oplus m_{1,t-1} \oplus m_{2,t} \\ c_{2,t} &= m_{1,t-1} \oplus m_{2,t} \\ c_{3,t} &= m_{1,t} \oplus m_{1,t-1} \oplus m_{2,t-1} \end{aligned}$$

where $\oplus$ denotes modulo-2 addition.

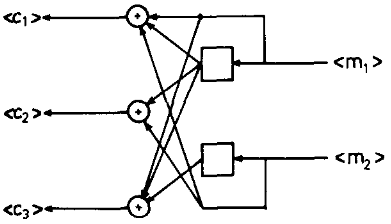

Fig. 1. Rate 2/3 convolutional encoder.

We express the input and output sequences in terms of the delay operator D:

$$m_i(D) = \cdots + m_{i,-1}D^{-1} + m_{i0} + m_{i1}D + m_{i2}D^2 + \cdots, \qquad i=1,2$$

$$c_j(D) = \cdots + c_{j,-1}D^{-1} + c_{j0} + c_{j1}D + c_{j2}D^2 + \cdots, \qquad j=1,2,3.$$

For notational convenience we shall generally suppress the parenthetical D in subsequent references to sequences; thus m_i means $m_i(D)$, $c_j = c_j(D)$, and so forth, where the fact that a letter represents a sequence (transform) should be clear from the context. The input/output relationships are expressed concisely as

$$\boldsymbol{c} = \boldsymbol{m}G, \tag{1}$$

where $\boldsymbol{m} = (m_1, m_2)$, $\boldsymbol{c} = (c_1, c_2, c_3)$, and the generator matrix $G = [g_{ij}(D)]$ is

$$G = \begin{bmatrix} 1+D & D & 1+D \\ 1 & 1 & D \end{bmatrix},$$

and formal power series multiplication with coefficient operations modulo-2 is applied. In general, there are k inputs and n outputs. If we define the constraint length for the ith input as

$$\nu_i = \max_{1 \leq j \leq n} [\deg g_{ij}(D)],$$

then the overall constraint length

$$\nu = \sum_{i=1}^{k} \nu_i$$

($\nu = 2$ for the encoder of Fig. 1) equals the number of memory elements for what Forney [4] calls the obvious realization of the encoder.

The dual code [5] to a convolutional code C, denoted by $C^{\perp}$, is the linear space generated by the set of all

Manuscript received March 19, 1977; revised March 23, 1978. This work was supported in part by the U.S. Navy under Contract N00123-76-0842.

J. P. M. Schalkwijk and A. J. Vinck are with the Department of Electrical Engineering, Eindhoven University of Technology, Eindhoven, The Netherlands.

K. A. Post is with the Department of Applied Physics and Information Science, University of California at San Diego, La Jolla, on leave from the Department of Mathematics, Eindhoven University of Technology, Eindhoven, The Netherlands.

0018-9448/78/0900-0553$00.75 ©1978 IEEE

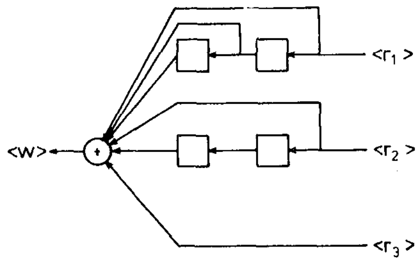

Fig. 2. Syndrome former for rate 2/3 convolutional code.

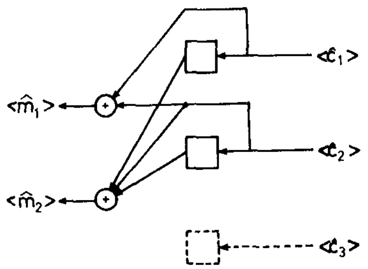

Fig. 3. Inverse encoder for rate 2/3 convolutional code of Fig. 1.

n-tuples of finite (for infinite sequences the inner product may not be defined) sequences $\boldsymbol{d}$ such that the inner product $(\boldsymbol{c},\boldsymbol{d}) \triangleq \boldsymbol{c}\cdot\boldsymbol{d}^T$ (where T means transpose) is zero for all $\boldsymbol{c}$ in C. The dual code of a rate k/n convolutional code, generated by an encoder G, is a rate $(n-k)/n$ code that can be generated by a suitable encoder H, such that $GH^T=0$. The matrix H^T can be obtained from the inverse of the B matrix in an invariant factor decomposition [4], [5] $G=A\Gamma B$ of the encoder matrix G by taking the last $n-k$ columns of B^{-1}. The n-input, $(n-k)$-output linear sequential circuit whose transfer function matrix is H^T is called the syndrome former and has the property that $\boldsymbol{c}H^T=0$ if and only if $\boldsymbol{c}\in C$.

For the encoder G of Fig. 1 we have an H^T matrix

$$H^T=\begin{bmatrix} 1+D+D^2 \\ 1+D^2 \\ 1 \end{bmatrix}.$$

Fig. 2 gives the obvious realization of the syndrome former. Two comments are in order. First, note that for rate $(n-1)/n$ codes the syndrome former has n inputs but a single output as in Fig. 2. This single output is the reason that we first concentrate on rate $(n-1)/n$ codes (Sections II–IV). In Table III of Section V we list codes in terms of their syndrome formers. The invariant factor theorem can now be used on the matrix H, i.e., $H=C\Gamma D$, to find a suitable encoder G from the D^{-1} matrix. This encoder is conventional (i.e., it has no feedback), but it is not necessarily minimal [4], i.e., the obvious realization does not necessarily have the smallest possible number of memory elements.

Let $\boldsymbol{e}$ be the error vector sequence, and let $\boldsymbol{r}=\boldsymbol{c}+\boldsymbol{e}$ be the received data vector sequence. We then define the syndrome vector sequence $\boldsymbol{w}$ as

$$\boldsymbol{w} \triangleq \boldsymbol{r}H^T=(\boldsymbol{c}+\boldsymbol{e})H^T=\boldsymbol{e}H^T.$$

The task of the codeword estimator [4] is now to find an error vector sequence estimate $\hat{\boldsymbol{e}}$ of minimum Hamming weight that may be a possible cause of the syndrome vector sequence $\boldsymbol{w}$. The codeword vector sequence estimate $\hat{\boldsymbol{c}}$ is then given by

$$\hat{\boldsymbol{c}}=\boldsymbol{r}+\hat{\boldsymbol{e}}.$$

Using the codeword vector sequence estimate $\hat{\boldsymbol{c}}$, the inverse encoder G^{-1} now forms an estimate $\hat{\boldsymbol{m}}$ of the message vector sequence $\boldsymbol{m}$, i.e., $\hat{\boldsymbol{m}}=\hat{\boldsymbol{c}}G^{-1}$ where G^{-1} is a right inverse of G, i.e., $GG^{-1}=I$. This inverse encoder G^{-1} can also (i.e., like the syndrome former) be obtained from the invariant factor decomposition $G=A\Gamma B$ of the encoder G. For the encoder G of Fig. 1, we have

$$G^{-1}=B^{-1}\Gamma^{-1}A^{-1}=\begin{bmatrix} 1 & D \\ 1 & 1+D \\ 0 & 0 \end{bmatrix}.$$

Fig. 3 gives the obvious realization of the inverse encoder G^{-1}.

Note that both G and G^{-1} represent one-to-one (and in fact linear) maps that can be realized with simple circuitry; compare Figs. 1 and 3. The codeword estimator determines both the complexity and the performance of the system. Section II deals with the state space of the syndrome former of a binary rate $(n-1)/n$ convolutional code. Section III gives a description of the codeword estimator in terms of the state-space framework developed in Section II. As it turns out, certain symmetries in the syndrome former state space can be exploited to greatly reduce the complexity of the codeword estimator.

Before embarking on our state-space approach (which is the core of this paper) towards the codeword estimator, one final comment is in order. The estimate $\hat{\boldsymbol{m}}$ of the message vector sequence $\boldsymbol{m}$ can also be written as

$$\hat{\boldsymbol{m}}=\hat{\boldsymbol{c}}G^{-1}=\boldsymbol{r}G^{-1}+\hat{\boldsymbol{e}}G^{-1}.$$

The first term $\boldsymbol{r}G^{-1}$ on the right side of the above equation can be easily obtained from the received data vector sequence $\boldsymbol{r}$ using the simple circuitry of Fig. 3. As in [1]–[3], it turns out that the overall decoder requires less hardware if we let the estimator determine the second term $\hat{\boldsymbol{e}}G^{-1}$ directly. Hence we define the message (as opposed to the codeword) correction vector sequence $\hat{\boldsymbol{e}}_m$ as

$$\hat{\boldsymbol{e}}_m \triangleq \hat{\boldsymbol{e}}G^{-1}. \tag{2}$$

II. State Space

For a state-space analysis, it is convenient to represent the syndrome former of a rate $(n-1)/n$ code by an n-tuple $(A,B,C,\cdots,D)$ of binary polynomials (see Fig. 4). In order to avoid accumulation of indices, we denote the present noise by the n-vector $[x,y,z,\cdots,t]$.

Obviously one single-noise vector can at most influence $h+1$ successive syndrome digits where h is the maximum

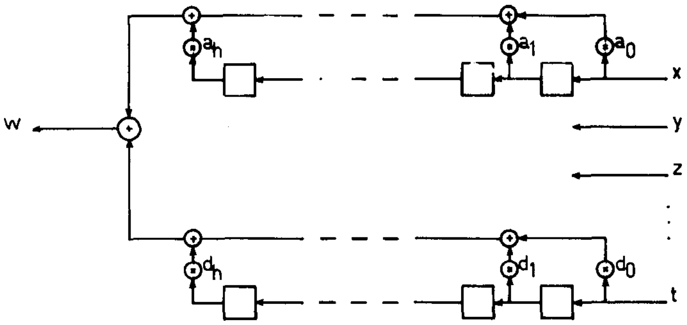

Fig. 4. Syndrome former for rate $(n-1)/n$ convolutional code.

degree of the syndrome polynomials $A,B,C,\cdots,D$. We define the "physical state" of the system to be the nh-dimensional binary vector representing the contents of all shift register stages in Fig. 4. Every noise vector that enters the system causes a transition of its physical state and gives rise to a binary-syndrome digit. The phenomenon occurs that two different initial physical states are syndrome-indistinguishable, i.e., that under every noise vector sequence their syndrome sequences are equal. This natural concept [3], [4] of syndrome-indistinguishability is exactly the same as the following equivalence relation.

Definition: Two physical states are called equivalent if their difference has a sequence of syndrome digits identically zero in response to a sequence of all zero-noise vectors. In fact, we may restrict ourselves in this definition to sequences of zero-noise vectors of length h, since all subsequent zero-noise vectors must yield zero-syndrome digits.

Example: The contents

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

in Fig. 2 are equivalent physical states.

The equivalence classes [6] of the above equivalence relation will be called "abstract states," or briefly "states" of the system. There are several equivalent state descriptions. In [3], Schalkwijk and Vinck use the contents of the bottom register D of the syndrome former (Fig. 4) as a description of the state. Forney [4] uses the zero-noise syndrome sequence to label the state. In the present paper we opt for this latter description.

We are now ready to introduce some convenient notation: *states*, as opposed to noise *vectors* (given by their zero-noise syndrome sequence), are denoted by lower case Greek letters with a subscript, e.g.,

$$\sigma_1 \triangleq [s_1,s_2,s_3,\cdots,s_{h-2},s_{h-1},s_h],$$

and its left shifts

$$\sigma_2 \triangleq [s_2,s_3,s_4,\cdots,s_{h-1},s_h,0] \qquad \sigma_3 \triangleq [s_3,s_4,s_5,\cdots,s_h,0,0]$$

and so on. Occasionally, i.e., if $s_h=0$, we also write the right shift, e.g.,

$$\sigma_0 = [0,s_1,s_2,\cdots,s_{h-3},s_{h-2},s_{h-1}].$$

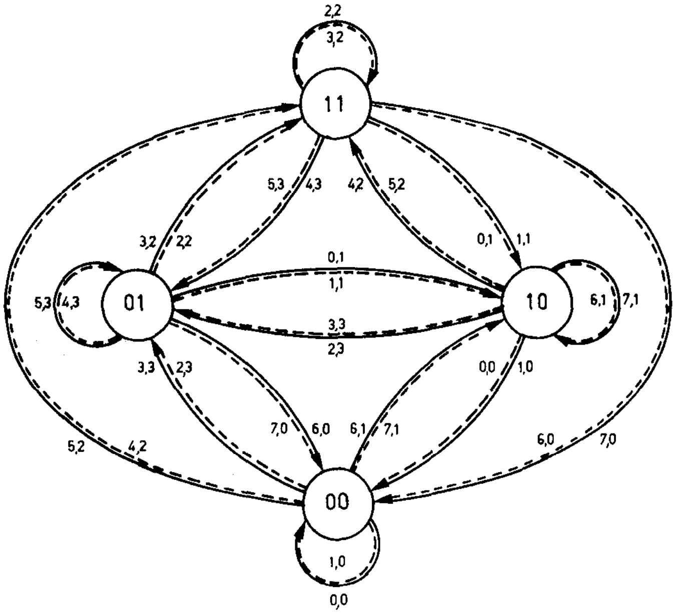

Fig. 5. State diagram of syndrome former.

Finally, we introduce the symbols $\alpha_1,\beta_1,\gamma_1,\cdots,\delta_1$ to denote the states generated by the system, i.e.,

$$\alpha_1 \triangleq [a_1,a_2,\cdots,a_h], \beta_1 \triangleq [b_1,b_2,\cdots,b_h],$$
$$\gamma_1 \triangleq [c_1,c_2,\cdots,c_h],\cdots,\delta_1 \triangleq [d_1,d_2,\cdots,d_h].$$

Without loss of generality we assume $a_h=1$. This assumption is justified by the definition of h and implies that the state space has dimension h.

The syndrome digit w, and the new state τ_1 (see Fig. 4) are completely determined by the present state σ_1 and the noise vector $[x,y,z,\cdots,t]$,

$$\begin{array}{ll} [x,y,z,\cdots,t] & \\ \downarrow & \\ \sigma_1 \mapsto & \tau_1 = \sigma_2 + x\alpha_1 + y\beta_1 + z\gamma_1 + \cdots + t\delta_1 \qquad (3) \\ \searrow & \\ & w = s_1 + xa_0 + yb_0 + zc_0 + \cdots + td_0. \end{array}$$

Fig. 5 gives the state diagram of the syndrome former of Fig. 2. Solid lines correspond to a syndrome digit $w=0$, and dashed lines correspond to a syndrome digit $w=1$. The decimal values indicated along the edges are the noise vector and the message correction vector, respectively, to be interpreted as binary numbers.

The fact that the message correction vector is solely determined by the next state [3] of the syndrome former (see Fig. 5) follows from Forney [5]. Let G and H be dual encoders, and let G be minimal. Then according to Forney the state spaces of G and H^T, and hence of G^{-1} and H^T, are isomorphic. As we can equate the state of the inverse encoder G^{-1} to its most recent output, the

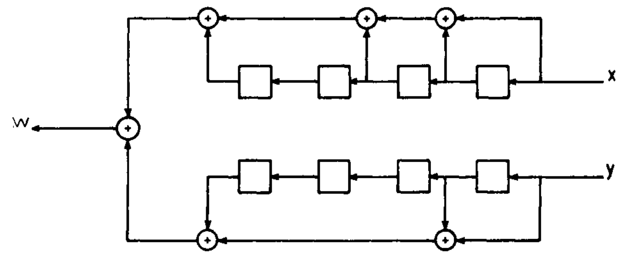

Fig. 6. Syndrome former for rate 1/2 convolutional code.

message correction vector is uniquely determined by the next state of the syndrome former.

Now consider the linear subspace $L[\alpha_1,\beta_1,\gamma_1,\cdots,\delta_1]$ spanned by the generators $\alpha_1,\beta_1,\gamma_1,\cdots,\delta_1$. If this subspace has dimension q, then according to (3), each state σ_1 has exactly 2^q state transition images. Again by (3), these images form a coset of $L[\alpha_1,\beta_1,\gamma_1,\cdots,\delta_1]$. This coset will be called the "sink-tuple" of σ_1.

The linear subspace $L[\alpha_1,\beta_1,\gamma_1,\cdots,\delta_1]$ is identical to the linear subspace $L[\alpha_1,\beta_1+b_h\alpha_1,\gamma_1+c_h\alpha_1,\cdots,\delta_1+d_h\alpha_1]$. However, as $a_h=1$, the vectors $\beta_1+b_h\alpha_1,\gamma_1+c_h\alpha_1,\cdots,\delta_1+d_h\alpha_1$ have a rightmost coordinate equal to zero. Thus these vectors have a right shift. Furthermore,

$$\operatorname{rank}\begin{bmatrix} a_1 & ,\cdots, & a_{h-1} & , & 1\\ b_1+b_ha_1 & ,\cdots, & b_{h-1}+b_ha_{h-1} & , & 0\\ \vdots & & & & \vdots\\ d_1+d_ha_1 & ,\cdots, & d_{h-1}+d_ha_{h-1} & , & 0\end{bmatrix}$$

$$=\operatorname{rank}\begin{bmatrix} 1, & 0 & ,\cdots, & 0\\ 0, & b_1+b_ha_1 & ,\cdots, & b_{h-1}+b_ha_{h-1}\\ \vdots & & & \\ 0, & d_1+d_ha_1 & ,\cdots, & d_{h-1}+d_ha_{h-1}\end{bmatrix}.$$

If we define $\epsilon_1 \triangleq [1,0,0,\cdots,0]$ as a row vector of length h, then

$$\dim L[\alpha_1,\beta_1,\gamma_1,\cdots,\delta_1]$$
$$=\dim L[\epsilon_1,(\beta+b_h\alpha)_0,(\gamma+c_h\alpha)_0,\cdots,(\delta+d_h\alpha)_0].$$

Each state has at least one preimage. If $\tau_1=[s_1,s_2,\cdots,s_{h-1},0]$, then its right shift $\tau_0=[0,s_1,\cdots,s_{h-2},s_{h-1}]$ is a preimage under $[x,y,z,\cdots,t]=[0,0,0,\cdots,0]$. If $\tau_1=[s_1,s_2,\cdots,s_{h-1},1]$ then $(\tau+\alpha)_0$ is a preimage under $[x,y,z,\cdots,t]=[1,0,0,\cdots,0]$. But if a state τ_1 has a preimage, then it has at least 2^q preimages, i.e., all the states in the coset of $L[\epsilon_1,(\beta+b_h\alpha)_0,(\gamma+c_h\alpha)_0,\cdots,(\delta+d_h\alpha)_0]$ that contains the above preimage. We now have the following results. Each state σ_1 has exactly 2^q images, i.e., the sink-tuple of σ_1. On the other hand, each state τ_1 has at least 2^q preimages, i.e., the above mentioned coset of $L[\epsilon_1,(\beta+b_h\alpha)_0,(\gamma+c_h\alpha)_0,\cdots,(\delta+d_h\alpha)_0]$. We conclude that τ_1 has exactly 2^q preimages that constitute the "source-tuple" of τ_1. It is easily verified that each

source-tuples

		I	II	IV	III
sink-tuples	I	0	9	13	4
	II	2	11	15	6
	IV	10	3	7	14
	III	8	1	5	12

Fig. 7. State space partition in source/sink-tuples.

It is this source/sink-tuple description of the state space that will play an important role in the remainder of the paper. To make things more concrete we give a specific example for the syndrome former of Fig. 6. We have

$$\alpha_1=[\,1\quad 1\quad 0\quad 1\,]_2=13\qquad \epsilon_1=[\,1\quad 0\quad 0\quad 0\,]_2=8$$
$$\beta_1=[\,1\quad 0\quad 0\quad 1\,]_2=9$$
$$(\alpha+\beta)_0=[\,0\quad 0\quad 1\quad 0\,]_2=2.$$

Also,

Partition	Source-tuples		Sink-tuples
I	{0, 2, 8, 10}	→	{0, 4, 9, 13}
II	{1, 3, 9, 11}	→	{2, 6, 11, 15}
III	{4, 6, 12, 14}	→	{1, 5, 8, 12}
IV	{5, 7, 13, 15}	→	{3, 7, 10, 14}

Fig. 7 shows a partition of the state space in source/sink-tuples. Anticipating the results of Section IV, the states in Fig. 7 have been geometrically arranged in such a way that the metric equivalence classes {0}, {4}, {8}, {12}, {9, 13}, {6, 14}, {1, 5}, {2, 10}, and {3, 7, 11, 15} are easily distinguishable. Two states that are in the same metric equivalence class have the same metric value [7], irrespective of the noise vector sequence.

III. Algorithm

Given the syndrome sequence of a rate $(n-1)/n$ code (Fig. 4) the estimator must determine the state sequence that corresponds to a noise vector sequence estimate of minimum Hamming weight that may be a possible cause of the syndrome sequence. As the estimation algorithm to be described in this section is similar to Viterbi's [7], we can be very brief. To find the required state sequence we introduce the concept of a "metric function." A metric function is defined as a nonnegative integer-valued function on the states. With every state transition we now associate the Hamming weight W_H of its noise vector $[x,y,z,\cdots,t]$.

Problem: Given a metric function f and a syndrome digit w, find a metric function g that is state-wise minimal, and for every state is consistent with at least one of the values of f on its preimages under syndrome digit w, increased by the weight of its corresponding state transition. The solution to this problem expresses g in terms of f

source/sink-tuples of Section II. In fact, the values of g on a sink-tuple T_i are completely determined by the values of f on the corresponding source-tuple S_i and by the syndrome digit w. The equations that express g in terms of f and w are called "metric equations." They have the form

$$g(\tau_1)=\min\ \{f(\sigma_1)+W_H([x,y,z,\cdots,t])|\sigma_1 \underset{\searrow w}{\overset{\overset{[x,y,z,\cdots,t]}{\downarrow}}{\longmapsto}} \tau_1\ \}. \tag{4}$$

The particular preimage σ_1 in (4) that realizes the minimum is called the "survivor." When there are more preimages for which the minimum is achieved, one could flip a multi-coin to determine the survivor. However, we will shortly discover that a judicious choice of the survivor among the candidate preimages offers the possibility of significant savings in decoder hardware. The construction of (4) can be repeated, i.e., starting with a metric function f_0, given a syndrome sequence $w_1,w_2,w_3,\cdots$, one can form a sequence of metric functions $f_1,f_2,f_3,\cdots$, iteratively by means of the metric equations. The metric function f_s, whose value $f_s(\sigma_1)$ at an arbitrary state σ_1 equals the Hamming weight of the lightest path from the zero-state to σ_1 under an all-zero syndrome sequence $w_1,w_2,w_3,\cdots,=0,0,0,\cdots$, is called the "stable metric function." It has the property

$$f_s \overset{w=0}{\longmapsto} f_s.$$

Note that

$$d_{\text{free}}=\min\ \{f_s(\sigma_1)+W_H([x,y,z,\cdots,t])|\sigma_1 \underset{\searrow w=0}{\overset{\overset{[x,y,z,\cdots,t]}{\downarrow}}{\longmapsto}} 0,\ \sigma_1\neq 0\}.$$

In order to make things more concrete we now give a specific example. Fig. 8 represents one section of the trellis diagram [7] corresponding to the state diagram of Fig. 5. From Fig. 8 we find for the metric equations:

$$g(0)=\bar{w}\min\ [f(0),f(1)+2,f(2)+1,f(3)+3] + w\min\ [f(0)+1,f(1)+3,f(2),f(3)+2] \tag{5a}$$

$$g(1)=\bar{w}\min\ [f(0)+2,f(1)+2,f(2)+1,f(3)+1] + w\min\ [f(0)+1,f(1)+1,f(2)+2,f(3)+2] \tag{5b}$$

$$g(2)=\bar{w}\min\ [f(0)+2,f(1),f(2)+3,f(3)+1] + w\min\ [f(0)+3,f(1)+1,f(2)+2,f(3)] \tag{5c}$$

$$g(3)=\bar{w}\min\ [f(0)+2,f(1)+2,f(2)+1,f(3)+1] + w\min\ [f(0)+1,f(1)+1,f(2)+2,f(3)+2] \tag{5d}$$

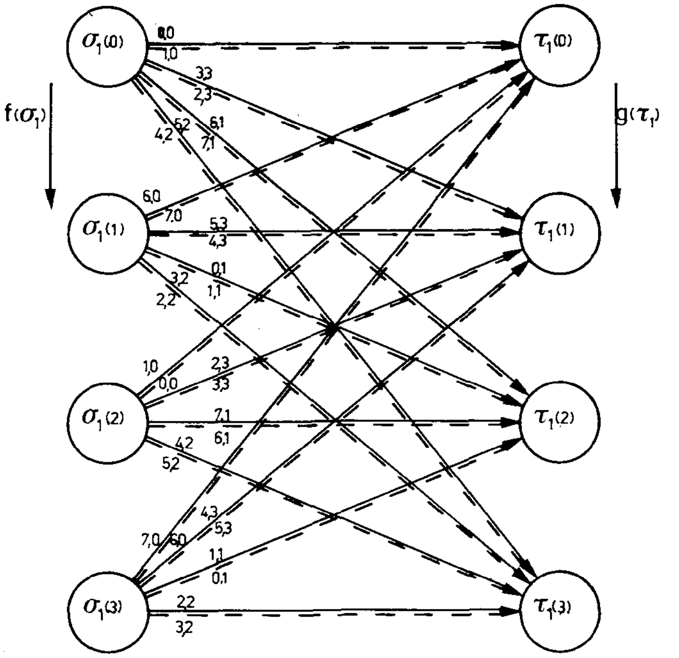

Fig. 8. One section of the trellis diagram.

where $\bar{w}=1-w$. Note that for each value $w=0$ or $w=1$ four arrows impinge on each image τ_1. The preimage σ_1 associated with the minimum within the relevant pair of brackets in (5) is the survivor. The case where we have more candidates for a survivor among the preimages will be considered shortly.

In the classical implementation of the Viterbi algorithm [7], each state $\tau_1(j), j=0,1,2,3$ has a metric register MR_j and a path register PR_j associated with it. The metric register is used to store the current value of the metric function f. As only the differences between the values of the metric function matter in the decoding algorithm,

$$\min_{0\leqslant j\leqslant 3}\ \{f[\tau_1(j)]\}$$

is subtracted from the contents of all metric registers, thus bounding the value of the contents of the metric registers. The path register PR_j stores the sequence of survivors leading up to state $\tau_1(j)$.

Observe that the right side of (5b) and (5d) are identical. Hence the states $\tau_1(1)$ and $\tau_1(3)$ have identical metric register contents. Moreover, selecting the identical survivor σ_1 in case of a tie, $\tau_1(1)$ and $\tau_1(3)$ also have the same path register contents. The metric register and the path register of either state $\tau_1(1)$ or state $\tau_1(3)$ can be eliminated. Apparently certain symmetries in the state space of the syndrome former can be exploited to reduce the amount of decoder hardware. In the next two sections, we further explore this possibility of reducing decoder hardware by introducing certain symmetries in the state space.

For further details of the implementation of the syndrome decoder the reader is referred to [3]. In the same paper Schalkwijk and Vinck also suggest a slightly modified decoder implementation that uses a read-only memory (ROM), thus eliminating the need for metric registers altogether.

IV. Special $R=(n-1)/n$ Codes—Metric/Path Register Savings

Without further ado we introduce the class $\Gamma_{n,h,l}$ of rate $(n-1)/n$ binary convolutional codes $(A,B,C,\cdots,D)$ that exhibits the state-space symmetries that will allow for an exponential reduction of decoder hardware. The definiton is that $(A,B,C,\cdots,D)\in\Gamma_{n,h,l}$ if and only if $A\neq B$, and

$$a_h=1 \tag{6a}$$

$$a_j=b_j, \qquad 0\leqslant j\leqslant l-1 \tag{6b}$$

$$a_j=b_j, \qquad h-l+1\leqslant j\leqslant h \tag{6c}$$

$$C,\cdots,D \text{ all have degree } \leqslant h-l \tag{6d}$$

$$\gcd(A,B,C,\cdots,D)=1 \tag{6e}$$

$$L[\epsilon_1,(\alpha+\beta)_0,\gamma_0,\cdots,\delta_0]\cap L[(\alpha+\beta)_1,\cdots,(\alpha+\beta)_{l-1}] = \{\mathbf{0}\}. \tag{6f}$$

Conditions (6a)–(6c) and (6e) reduce to known sufficient conditions for the rate $\frac{1}{2}$ case [1]–[3]. Conditions (6d) and (6f) will be discussed in Theorem 4 and Lemma 5, respectively. The code of Fig. 2 is an element of $\Gamma_{3,2,1}$, and the code of Fig. 6 is an element of $\Gamma_{2,4,2}$. As a consequence of (6) we have

$$\Gamma_{n,h,1}\supset\Gamma_{n,h,2}\supset\Gamma_{n,h,3}\supset\cdots. \tag{7}$$

If condition (6e) is satisfied, then it follows from the invariant factor theorem [4] that the n-tuple $(A,B,C,\cdots,D)$ is a set of syndrome polynomials for some noncatastrophic rate $(n-1)/n$ convolutional code (in fact, for a class of such codes).

Assume $\Gamma_{n,h,l}\neq\varnothing$. For $(A,B,C,\cdots,D)\in\Gamma_{n,h,l}$ an "l-singleton state" is defined to be a state the last l components of which vanish. Linear combinations and left shifts of l-singleton states are also l-singleton states. For every state ϕ_1, the left shifts $\phi_i (i\geqslant l+1)$ are l-singleton states. We state the following lemma and theorems without proof.

Lemma 1: For every state σ_1, there exists a unique l-singleton state ϕ_{l+1} and a unique index set $I\subset\{1,2,\cdots,l\}$ such that

$$\sigma_1=\phi_{l+1}+\sum_{i\in I}\alpha_i. \tag{8}$$

Using this lemma, we now associate with the state σ_1 the set $[\sigma_1]^{(l)}$ defined by

$$[\sigma_1]^{(l)}=\left\{\phi_{l+1}+\sum_{i\in I}[\alpha_i+r_i(\alpha+\beta)_i]\,|\,r_i\in\{0,1\}, \text{ for all } i\right\}.$$

Then we have the following.

Theorem 2: The collection of all sets $[\sigma_1]^{(l)}$ forms a partition of the state space.

Corollary: Based on the partition of the state space according to Theorem 2, an equivalence relation $R_{n,h,l}$ can be defined where two states σ_1 and σ_1' are called $R_{n,h,l}$-equivalent iff $[\sigma_1]^{(l)}=[\sigma_1']^{(l)}$.

The one-element equivalence classes of $R_{n,h,l}$ consist of exactly one l-singleton state. Examples are the states 0, 4, 8, and 12 in Fig. 7. The number $N_{n,h,l}$ of $R_{n,h,l}$-equivalence classes can be found as follows. First, take $I\subset\{1,2,\cdots,l]$ in (8) fixed, and let j denote the cardinality of I. The last l components of an l-singleton state are zero. Hence there are 2^{h-l} l-singleton states. Now 2^j of these 2^{h-l} l-singleton states correspond to the same $R_{n,h,l}$-equivalence class, i.e., all l-singleton states differing by a linear combination of $\{(\alpha+\beta)_i|i\in I\}$. Hence there are 2^{h-l-j} $R_{n,h,l}$-equivalence classes for each I of cardinality j. Thus

$$N_{n,h,l}=\sum_{j=0}^{l}\binom{l}{j}2^{h-l-j}=2^{h-2l}3^l. \tag{9}$$

Theorem 3: Let $(A,B,C,\cdots,D)\in\Gamma_{n,h,l}$, and assume that $1\leqslant l'\leqslant l$. Then every $R_{n,h,l}$-equivalence class of $(A,B,C,\cdots,D)$ is a union of $R_{n,h,l'}$-equivalence classes of $(A,B,C,\cdots,D)$ (see (7)).

In Fig. 7, we exhibit the $R_{2,4,2}$-equivalence classes for the syndrome former of Fig. 6. We claimed that any two states within the same equivalence class have the same metric value irrespective of the noise vector sequence. We are now ready to prove this result.

Theorem 4: Assume that $(A,B,C,\cdots,D)\in\Gamma_{n,h,l}$. Let f_0 be any starting metric function, and let $w_1,w_2,w_3,\cdots$ be any syndrome sequence. Then every iterate f_u is constant on the $R_{n,h,u}$-equivalence classes of $(A,B,C,\cdots,D)$, $1\leqslant u\leqslant l$.

Proof: The proof is by induction on u. Consider the two $R_{n,h,1}$-equivalent states $\phi_2+\alpha_{1'}$ and $\phi_2+\beta_1$. Obviously they belong to the same sink-tuple. We list their preimages, corresponding noise vectors, and syndrome digits according to (3) in Table I. We see that on every line, i.e.,

TABLE I

	$\phi_2+\alpha_1$	$\phi_2+\beta_1$
Preimage	Noise; Syndrome	Noise; Syndrome
$\phi_1\qquad +z\gamma_0+\cdots+t\delta_0$	$[1,0,z,\cdots,t]^T;w_1$	$[0,1,z,\cdots,t]^T;w_1$
$\phi_1\quad +(\alpha+\beta)_0+z\gamma_0+\cdots+t\delta_0$	$[0,1,z,\cdots,t]^T;w_1$	$[1,0,z,\cdots,t]^T;w_1$
$\phi_1+\epsilon_1\qquad +z\gamma_0+\cdots+t\delta_0$	$[1,0,z,\cdots,t]^T;\bar{w}_1$	$[0,1,z,\cdots,t]^T;\bar{w}_1$
$\phi_1+\epsilon_1+(\alpha+\beta)_0+z\gamma_0+\cdots+t\delta_0$	$[0,1,z,\cdots,t]^T;\bar{w}_1$	$[1,0,z,\cdots,t]^T;\bar{w}_1$

for every preimage, the syndrome bits and the Hamming weights of the state transitions to $\phi_2+\alpha_1$, and $\phi_2+\beta_1$ are identical. Hence $f_1(\phi_2+\alpha_1)=f_1(\phi_2+\beta_1)$ for every f_0 and every w_1. This proves the assertion for $u=1$. Now let us assume that the statement is true for a fixed u, $1\leqslant u\leqslant l-1$. Let f_0 be any starting metric function, and let $w_1,w_2,w_3,\cdots$ be any syndrome sequence. Then by our induction hypothesis f_u is constant on the $R_{n,h,u}$-equivalence classes. Let χ_1 and χ_1' be any pair of $R_{n,h,u}$-equivalent states. Then there is a state ψ_{u+1} and an index set $I\subset\{1,2,\cdots,u\}$ such that for some $r_i\in\{0,1\}$

$$\chi_1=\psi_{u+1}+\sum_{i\in I}\alpha_i \qquad \chi_1'=\psi_{u+1}+\sum_{i\in I}\left[\alpha_i+r_i(\alpha+\beta)_i\right].$$

We now consider the cosets S and S' of $L[\epsilon_1,(\alpha+\beta)_0,\gamma_0,\cdots,\delta_0]$ to which χ_1 and χ_1' belong, respectively, and compare them element-wise. The states

$$\chi_1+p\epsilon_1+q(\alpha+\beta)_0+r\gamma_0+\cdots+s\delta_0$$
$$\chi_1'+p\epsilon_1+q(\alpha+\beta)_0+r\gamma_0+\cdots+s\delta_0$$

are obviously $R_{n,h,u}$-equivalent for all $p,q,r,\cdots,s\in\{0,1\}$, since by the definition of ϵ_1 and by (6c), (6d) the last u components of $p\epsilon_1+q(\alpha+\beta)_0+r\gamma_0+\cdots+s\delta_0$ vanish. Furthermore, by (6b) we have

$$\sum_{i\in I}a_i=\sum_{i\in I}\left[a_i+r_i(a_i+b_i)\right].$$

Hence by (3) the preimages

$$\chi_1+p\epsilon_1+q(\alpha+\beta)_0+r\gamma_0+\cdots+s\delta_0$$
$$\chi_1'+p\epsilon_1+q(\alpha+\beta)_0+r\gamma_0+\cdots+s\delta_0$$

give rise to identical syndrome digits in response to an input vector $[x,y,z,\cdots,t]$. These arguments together, however, imply that the values of f_{u+1} on the corresponding state transition images are equal, and hence f_{u+1} is constant on the $R_{n,h,u+1}$-equivalence classes of $(A,B,C,\cdots,D)$. Q.E.D.

Theorem 4 proves that only one metric register is needed for each $R_{n,h,l}$-equivalence class. We will now show that, except for the last $l-1$ stages, the same is true for the path registers. Let $(A,B,C,\cdots,D)\in\Gamma_{n,h,l}$. Condition (6f), where $\{(\alpha+\beta)_1,(\alpha+\beta)_2,\cdots,(\alpha+\beta)_{l-1}\}=\{\mathbf{0}\}$, for $l=1$, implies that a coset of $L[\epsilon_1,(\alpha+\beta)_0,\gamma_0,\cdots,\delta_0]$ and a coset of $L[(\alpha+\beta)_1,(\alpha+\beta)_2,\cdots,(\alpha+\beta)_{l-1}]$ can have at most one element in common. Hence we have the following.

Lemma 5: No two distinct $R_{n,h,l-1}$-equivalent states can belong to the same source-tuple.

On the other hand from the proof of Theorem 4, it follows that whenever χ_1 and χ_1' are $R_{n,h,l-1}$-equivalent, then the same holds for the states

$$\chi_1+p\epsilon_1+q(\alpha+\beta)_0+r\gamma_0+\cdots+s\delta_0$$
$$\chi_1'+p\epsilon_1+q(\alpha+\beta)_0+r\gamma_0+\cdots+s\delta_0,$$
$$\text{if } p,q,r,\cdots,s\in\{0,1\},$$

which form the source-tuples containing χ_1 and χ_1'. These results lead to a natural equivalence between source-tuples. Two source-tuples are said to be equivalent if they contain a pair of $R_{n,h,l-1}$-equivalent states. This relation is an equivalence relation. The unique and natural one-to-one correspondence between the states of two equivalent source-tuples, which is induced by the intersection with $R_{n,h,l-1}$-equivalence classes, is consistent with the algebraic difference structure of the source-tuples (see the proof of Theorem 4). Hence in view of Theorem 4, we see that for the mth iterate f_m, $m\geqslant l-1$, of any metric function f_0 under any syndrome sequence $w_1,w_2,w_3,\cdots$, the values of f_m on the corresponding states of two equivalent source-tuples are identical.

Given two successive iterates f_{j-1} and f_j, $j\geqslant l$, of a metric function f_0 linked by the syndrome digit w_j,

$$f_{j-1}\overset{w_j}{\longmapsto}f_j,$$

in Viterbi decoding [6] one determines for each state τ_1 a survivor σ_1 such that

$$f_j(\tau_1)=f_{j-1}(\sigma_1)+W_H([x,y,z,\cdots,t]),$$

subject to (4). Survivors of a state τ_1 in the sink-tuple T_i always belong to the corresponding source-tuple S_i, (see Section II). However, as discussed in Section III, there are situations in which more than one survivor may be chosen, i.e., when two or more σ_1 in (4) achieve the minimum. In this case, one has a choice of two possible strategies that result in the same decoded error rate by transmission over a binary symmetric channel (BSC), i.e., i) flip a (multi) coin or ii) decide for every tie-pattern once and for ever which survivor shall be taken. We shall use the second strategy. Using the properties of equivalent source-tuples, this can be realized in the following way. Whenever two source-tuples S_i and S_i' are equivalent (and hence have identical f_{j-1}-values), then corresponding survivors be chosen for the respective sink-tuples T_i and T_i' in such a way that $R_{n,h,1}$-equivalent states get the same survivor. Given a sequence of metric function iterates

$$f_0\overset{w_1}{\longmapsto}f_1\overset{w_2}{\longmapsto}\cdots\overset{w_{j-1}}{\longmapsto}f_{j-1}\overset{w_j}{\longmapsto}f_j,$$

then a sequence of successive survivors can be constructed for every state σ_1

$$\sigma_1^{(-j)}\longleftarrow\!\!\dashv\sigma_1^{(-j+1)}\longleftarrow\!\!\dashv\cdots\longleftarrow\!\!\dashv\sigma_1^{(-1)}\longleftarrow\!\!\dashv\sigma_1, \qquad j\geqslant l,$$

and the following theorem holds.

Theorem 6: If σ_1 and η_1 are distinct $R_{n,h,m}$-equivalent states, then $\sigma_1^{(-m)}=\eta_1^{(-m)}$, $m=1,2,\cdots,l$.

Proof: The proof is by induction on m. For $m=1$ the assertion is part of our assumption. Now assume that the statement is true for $m=u$, u fixed, $1\leqslant u\leqslant l-1$. Let σ_1 and η_1 be two $R_{n,h,u+1}$-equivalent states that are not $R_{n,h,u}$-equivalent (otherwise $\sigma_1^{(-u)}=\eta_1^{(-u)}$, and hence immediately $\sigma_1^{(-u-1)}=\eta_1^{(-u-1)}$). Then

$$\sigma_1=\phi_{u+2}+\alpha_{u+1}+\sum_{i\in I}\alpha_i$$

$$\eta_1=\sigma_{u+2}+\beta_{u+1}+\sum_{i\in I}\left[\alpha_i+r_i(\alpha+\beta)_i\right],$$

where $I \subset \{1,2,\cdots,u\}$. It is easy to find preimages $\tilde{\sigma}_1$ and $\tilde{\eta}_1$ of σ_1 and η_1 respectively, viz:

$$\tilde{\sigma}_1 = \phi_{u+1} + \alpha_u + \sum_{i \in I \setminus \{1\}} \alpha_{i-1}$$

$$\tilde{\eta}_1 = \phi_{u+1} + \beta_u + \sum_{i \in I \setminus \{1\}} \left[\alpha_{i-1} + r_i(\alpha+\beta)_{i-1} \right].$$

Obviously $\tilde{\sigma}_1$ and $\tilde{\eta}_1$ are $R_{n,h,u}$-equivalent and by Theorem 3 also $R_{n,h,l-1}$-equivalent. Therefore, the source-tuples containing $\tilde{\sigma}_1$ and $\tilde{\eta}_1$ are equivalent. Furthermore, we observe that

$$\sigma_1 = \tilde{\sigma}_2 + \begin{cases} 0, & \text{if } 1 \notin I \\ \alpha_1, & \text{if } 1 \in I \end{cases}$$

$$\eta_1 = \tilde{\eta}_2 + \begin{cases} 0, & \text{if } 1 \notin I \\ \alpha_1 + r_1(\alpha+\beta)_1, & \text{if } 1 \in I. \end{cases}$$

Because of the assumption made above, the survivors $\sigma_1^{(-1)}$ and $\eta_1^{(-1)}$ are corresponding states, i.e., $R_{n,h,l-1}$-equivalent states. The algebraic difference structure of equivalent source-tuples is identical, and hence

$$\tilde{\sigma}_1 - \sigma_1^{(-1)} = \tilde{\eta}_1 - \eta_1^{(-1)} \in L[\epsilon_1, (\alpha+\beta)_0, \gamma_0, \cdots, \delta_0].$$

Therefore $\tilde{\sigma}_1 - \sigma_1^{(-1)} = \tilde{\eta}_1 - \eta_1^{(-1)}$ is a u-singleton state. Hence $\sigma_1^{(-1)}$ and $\eta_1^{(-1)}$ are $R_{n,h,u}$-equivalent, and therefore by the induction hypothesis $\sigma_1^{(-u-1)} = \eta_1^{(-u-1)}$. Q.E.D.

Theorem 6 shows that, except perhaps for the last $l-1$ stages, $R_{n,h,l}$-equivalent states have the same path register contents irrespective of the noise vector sequence. Thus roughly speaking, only one path register is needed for each $R_{n,h,l}$-equivalence class of states. By Theorem 4, only one metric register is needed for each $R_{n,h,l}$-equivalence class. Hence the complexity [3] of a syndrome decoder for a code $(A,B,C,\cdots,D) \in \Gamma_{n,h,l}$ is proportional to the number $N_{n,h,l}$ of $R_{n,h,l}$-equivalence classes, i.e., by (9) the complexity is proportional to $2^{h-2l}3^l$. As an example, take a code in $\Gamma_{2,2l,l}$, i.e., a rate $\frac{1}{2}$ code with a complementary middle connection only. The syndrome decoder for such a code has a complexity proportional to $3^l = (\sqrt{3})^h$. The classical Viterbi decoder [7] for the same code has complexity 2^h. Hence by exploiting the state-space symmetry, we achieve an exponential saving in hardware.

Before extending our present results to rate k/n codes, one comment concerning the free distance of codes $(A,B,C,\cdots,D) \in \Gamma_{n,h,l}$ is in order. It is obvious that constraints like (6) can reduce the maximum obtainable free distance for a given n and h. We are not yet able to derive a lower bound on the free distance of codes $(A,B,C,\cdots,D) \in \Gamma_{n,h,l}$. However, Table II of the next section lists the free distance of some short constraint length codes in $\Gamma_{n,h,l}$. It turns out that at least for these constraint lengths, the free distance for the codes satisfying the constraints (6) is very close to the maximum achievable free distance for the given values of n and h.

TABLE II
MAXIMUM FREE DISTANCE OF VARIOUS $\Gamma_{n,h,l}^{(n-k)}$ CLASSES

	(k,n) = (1,2)				(k,n) = (2,3)				(k,n) = (1,3)				
ℓ	1	2	3	4	1	2	3	4	N	1	2	3	4
h													
2	5				3				8	7			
3	6				4				10	9			
4	7	7			5	5			12	11	10		
5	8	8			6	6			13	12	12		
6	10	9	8		6	6	6		15	14	14	13	
7	10	10	10		8	7	6		16	16	16	15	
8	12	11	10	10	8	8	8	6	18	18	17	16	16
9	12	12	12	11	8	8	8	8	20	20	19	18	18

TABLE III
OPTIMAL $\Gamma_{n,2l,l}^{(n,k)}$ CODES

	(k,n) = (1,2)	(k,n) = (2,3)	(k,n) = (1,3)	
ℓ	S	S	S^1	S^2
1	5,7	5,7,1	5,7,0	6,4,1
2	23,27	23,27,5	37,33,0	32,36,1
3	107,117	103,113,7	133,123,0	124,134,1
4	453,473	403,423,7	453,473,0	464,444,1

V. SPECIAL $R = k/n$ CODES—COHERENCE—METRIC/PATH REGISTER SAVINGS

The syndrome former of a rate k/n convolutional code consists of $n-k$ syndrome formers of the type considered in Section II, all sharing the same set of nh memory cells (Fig. 4). Hence the $n-k$ syndrome formers in the set $\{\mathbb{S}^1, \mathbb{S}^2, \cdots, \mathbb{S}^{n-k}\}$, where $\mathbb{S}^i \triangleq (A_i, B_i, C_i, \cdots, D_i)$, all have the same physical state, i.e., the contents of the nh memory cells they have in common. To obtain the metric/path register savings that were realized in Section IV, each of the syndrome formers $\mathbb{S}^i$, $i = 1,2,\cdots,n-k$, should be in $\Gamma_{n,h,l}$, and the common physical states should have the same equivalence classes with respect to the equivalence relation of syndrome-indistinguishability in each of the $n-k$ individual syndrome formers.

Definition: A set of rate $(n-1)/n$ syndrome formers that share common physical states is called "coherent" if the individual syndrome formers have the same abstract states.

Let $\Gamma_{n,h,l}^{(n-k)}$ be the class of codes that are defined by $n-k$ coherent syndrome formers each of which is in $\Gamma_{n,h,l}$. Table II lists the maximum free distance for various values of the parameters k, n, h, and l. The $\Gamma_{n,h,l}^{(n-k)}$ classes with $(k,n) = (1,3)$ are defined by two coherent syndrome formers. The column with "N" at the top gives the maximum free distance for the relevant values of k, n, and h, dropping the coherence requirement. Comparing the N-column with the $l = 1$-column for $(k,n) = (1,3)$ gives some idea of the effect of the coherence requirement on the free distance. Table III lists several optimal $\Gamma_{n,2l,l}^{(n-k)}$ codes in terms of their syndrome former connections, in octal notation.

The remainder of this section will be devoted to a study of the newly defined concept of coherence of syndrome formers. Consider two syndrome formers

$$\mathbb{S} \triangleq (A,B,C,\cdots,D) \qquad \mathbb{S}' \triangleq (A',B',C',\cdots,D')$$

sharing the same set of nh memory cells (Fig. 4). From a mathematical point of view, the syndrome-indistinguishability classes of a syndrome former $\mathbb{S}$ can be considered as cosets of the set of those physical states that have an all-zero syndrome sequence in response to a sequence of all-zero noise vectors. Hence we may state that $\mathbb{S}$ and $\mathbb{S}'$ are coherent if and only if for all nh-tuples

$$(x_1,\cdots,x_h;y_1,\cdots,y_h;z_1,\cdots,z_h;\cdots;t_1,\cdots,t_h)$$

we have

$$\sum_{i=1}^{h} (x_i\alpha_{h+1-i}+y_i\beta_{h+1-i}+\cdots+t_i\delta_{h+1-i})=\mathbf{0}$$
$$\Leftrightarrow \sum_{i=1}^{h} (x_i\alpha'_{h+1-i}+y_i\beta'_{h+1-i}+\cdots+t_i\delta'_{h+1-i})=\mathbf{0}.$$

We shall now discuss some consequences of this definition.

Property 1: Let $\mathbb{S}$ and $\mathbb{S}'$ be coherent syndrome formers, and assume as before that $a_h = 1$. Then $\{\alpha_1,\alpha_2,\cdots,\alpha_h\}$ is a basis for the abstract state space of $\mathbb{S}$. In other words

$$\sum_{i=1}^{h} x_i\alpha_{h+1-i}=\mathbf{0}\Leftrightarrow x_1=x_2=\cdots=x_h=0$$

so that by coherence

$$\sum_{i=1}^{h} x_i\alpha'_{h+1-i}=\mathbf{0}\Leftrightarrow x_1=x_2=\cdots=x_h=0.$$

Hence $\{\alpha'_1,\alpha'_2,\cdots,\alpha'_h\}$ is a basis for the abstract state space of $\mathbb{S}'$ and $a'_h=1$.

Property 2: Let $\mathbb{S}$ and $\mathbb{S}'$ be coherent syndrome formers, $a_h=a'_h=1$. Then the correspondence

$$\sum_{i=1}^{h} (x_i\alpha_{h+1-i}+\cdots+t_i\delta_{h+1-i})$$
$$\Leftrightarrow \sum_{i=1}^{h} (x_i\alpha'_{h+1-i}+\cdots+t_i\delta'_{h+1-i})$$

is an isomorphism between the abstract state spaces of $\mathbb{S}$ and $\mathbb{S}'$.

Sketch of Proof: By Property 1, $\{\alpha_1,\alpha_2,\cdots,\alpha_h\}$ and $\{\alpha'_1,\alpha'_2,\cdots,\alpha'_h\}$ are bases of the state spaces above. Hence for example

$$\beta_1+u_1\alpha_1+u_2\alpha_2+\cdots+u_h\alpha_h=\mathbf{0},$$

so that by coherence

$$\beta'_1+u_1\alpha'_1+u_2\alpha'_2+\cdots+u_h\alpha'_h=\mathbf{0},$$

and so forth.

Property 3: Let $\mathbb{S}$ and $\mathbb{S}'$ be coherent syndrome formers, $a_h=a'_h=1$. Then $\mathbb{S}$ and $\mathbb{S}'$ have isomorphic source/sink-tuple structures.

Proof: Sink-tuples in the state space of $\mathbb{S}$ are cosets of $L[\alpha_1,\beta_1,\gamma_1,\cdots,\delta_1]$, and this subspace corresponds by Property 2, in the obvious way by coherence, to $L[\alpha'_1,\beta'_1,\gamma'_1,\cdots,\delta'_1]$. Source-tuples in the state space of $\mathbb{S}$ are cosets of the set S_0 of those abstract states that have image $\mathbf{0}$ under state transition. Let $\sigma_1 \triangleq \sum_{i=1}^{h}u_i\alpha_i$ such that $\sigma_1\mapsto\mathbf{0}$ under state transition with the noise vector $[x,y,z,\cdots,t]$. Then we have

$$\sum_{i=1}^{h-1} u_i\alpha_{i+1}+x\alpha_1+y\beta_1+z\gamma_1+\cdots+t\delta_1=\mathbf{0},$$

so that by coherence

$$\sum_{i=1}^{h-1} u_i\alpha'_{i+1}+x\alpha'_1+y\beta'_1+z\gamma'_1+\cdots+t\delta'_1=\mathbf{0},$$

which means that in the state space of $\mathbb{S}'$, when we define $\sigma'_1 \triangleq \sum_{i=1}^{h}u_i\alpha'_i$, also $\sigma'_1\mapsto\mathbf{0}$ under state transition with noise vector $[x,y,z,\cdots,t]$ and vice versa. Hence coherence implies that both

$$L[\alpha_1,\beta_1,\gamma_1,\cdots,\delta_1]\longleftrightarrow L[\alpha'_1,\beta'_1,\gamma'_1,\cdots,\delta'_1] \qquad S_0\longleftrightarrow S'_0,$$

by the isomorphism defined in Property 2. This implies that the cosets of $L[\alpha_1,\beta_1,\gamma_1,\cdots,\delta_1]$ and S_0, and the cosets of $L[\alpha'_1,\beta'_1,\gamma'_1,\cdots,\delta'_1]$ and S'_0 have isomorphic intersections. Q.E.D.

Property 4: Finally we can restate the coherence of $\mathbb{S}$ and $\mathbb{S}'$ in terms of a condition on their polynomials $A,B,C,\cdots,D$ and $A',B',C',\cdots,D'$ as follows. Let $\mathbb{S}$ and $\mathbb{S}'$ be coherent syndrome formers, $a_h=a'_h=1$. Let the isomorphism between their state spaces, which is generated by the mapping $\alpha_j\mapsto\alpha'_j$, $j=h,h-1,\cdots,1$, with respect to the natural basis of unit vectors be given by the (invertible) matrix Q, i.e.,

$$Q\begin{bmatrix} 1 & 0 & 0 & \cdot & 0 \\ a_{h-1} & 1 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1 & a_2 & a_3 & \cdot & 1 \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 & \cdot & 0 \\ a'_{h-1} & 1 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a'_1 & a'_2 & a'_3 & \cdot & 1 \end{bmatrix}. \tag{10}$$

It is immediate that Q itself has the form

$$Q=\begin{bmatrix} 1 & 0 & 0 & \cdot & 0 \\ q_{h-1} & 1 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ q_1 & q_2 & q_3 & \cdot & 1 \end{bmatrix}.$$

The matrix identity (10) can be reformulated as a polynomial congruence, i.e.,

$$\left(\sum_{i=0}^{h-1} q_{h-i}X^i\right)\left(\sum_{i=0}^{h-1} a_{h-i}X^i\right)\equiv \sum_{i=0}^{h-1} a'_{h-i}X^i(\bmod X^h), \qquad q_h \triangleq 1.$$

The isomorphism also implies that

$$\left(\sum_{i=0}^{h-1} q_{h-i}X^i\right)\left(\sum_{i=0}^{h-1} b_{h-i}X^i\right)\equiv \sum_{i=0}^{h-1} b'_{h-i}X^i(\bmod X^h),$$

and etc. Elimination of $\sum_{i=0}^{h-1}q_{h-i}X^i$ yields

$$\left(\sum_{i=0}^{h-1} a'_{h-i}X^i\right)\left(\sum_{i=0}^{h-1} b_{h-i}X^i\right)-\left(\sum_{i=0}^{h-1} a_{h-i}X^i\right)\left(\sum_{i=0}^{h-1} b'_{h-i}X^i\right)\equiv 0 \;(\bmod X^h).$$

Reversing the order of the coefficients in the polynomials of this congruence, we find

$$\deg\left[\sum_{i=0}^{h-1} a'_{i+1}X^i \sum_{i=0}^{h-1} b_{i+1}X^i - \sum_{i=0}^{h-1} a_{i+1}X^i \sum_{i=0}^{h-1} b'_{i+1}X^i\right] \leqslant h-2,$$

or

$$\deg\left[A'(X)B(X)-B'(X)A(X)\right] \leqslant h.$$

This reasoning can also be given in the opposite direction, where we construct for a given $a_h = a'_h = 1$ the polynomial $\tilde{Q}(X)$ and hence the transformation Q as

$$\tilde{Q}(X) \triangleq \sum_{i=0}^{h-i} q_{h-i}X^i = \left(\sum_{i=0}^{h-i} a'_{h-i}X^i\right) \cdot \left(\sum_{i=0}^{h-i} a_{h-i}X^i\right)^{-1} \bmod X^h.$$

Note that $a_h = 1$, and so the polynomial $\Sigma_{i=0}^{h-1} a_{h-i}X^i$ is invertible mod X^h. Therefore we have the following theorem.

Theorem 7: Two syndrome formers $\mathcal{S} \triangleq (A, B,$ C,$\cdots$,D) *and* $\mathcal{S}' \triangleq$ (A′,B′,C′,$\cdots$,D′), *where* $h = h'$, *are coherent if and only if all* 2×2 *subdeterminants of the polynomial matrix*

$$\begin{bmatrix} A,B,C,\cdots,D \\ A',B',C',\cdots,D' \end{bmatrix}$$

have deg $\leqslant h$.

We conclude this section with an example (using the delay operator notation of Section I). Consider the binary rate $1/3$ convolutional code generated by an encoder with connection polynomials $1+D^2+D^5+D^6$, $1+D^2+D^3+D^5+D^6$, and $D^3+D^4+D^5+D^6$. The inverse encoder of minimal degree is unique and is given by the polynomials $1+D+D^2$, D, and D^2. The free distance of the code is 13 (the maximum free distance for a rate $1/3$ code with polynomials of deg 6 is 15). A set of syndrome formers of minimal degree is given by $1+D+D^3$, $1+D$, $D+D^3$, and D^2, D^2+D^3, and $1+D+D^3$. The implementation of a decoder using this particular set of syndrome formers requires $2^6 = 64$ metric/path register combinations. The set of syndrome formers $1+D^3+D^6$, $1+D^3$, $1+D+D^4+D^6$, and $1+D+D^2+D^4+D^5+D^6$, $1+D+D^2+D^3$, $D^2+D^5+D^6$ is coherent, but a decoder using this particular set of syndrome formers also requires $2^6 = 64$ metric/path register combinations. The set of syndrome formers $1+D+D^6$, $1+D+D^4+D^6$, $1+D+D^3+D^4$, and $1+D^2+D^5+D^6$, $1+D^2+D^3+D^4+D^5+D^6$, $D+D^2+D^4$ is coherent and is a subset of $\Gamma_{3,6,2}$. Hence our code belongs to $\Gamma_{3,6,2}^{(3-1)}$ and by (9) the corresponding decoder can be implemented with $N_{3,6,2} = 36$ metric/path register combinations!

VI. Conclusions

This paper describes the operation of a syndrome decoder for binary rate k/n convolutional codes in terms of the state space of its syndrome former. A class $\Gamma_{n,h,l}^{(n-k)}$ of convolutional codes is defined that exhibits certain state-space symmetries that allow for an exponential reduction of decoder hardware. The maximum free distance of several short constraint length $\Gamma_{n,h,l}^{(n-k)}$ classes is listed in Table II. Codes achieving the maximum free distance of several $\Gamma_{n,2l,l}^{(n-k)}$ classes are given in Table III. These $\Gamma_{n,2l,l}^{(n-k)}$ classes offer the largest hardware savings.

The syndrome decoder can be adapted to perform soft decision decoding. However, as most of the hardware saving symmetries of $\Gamma_{n,h,l}^{(n-k)}$ are lost, no definite advantage over classical Viterbi decoding accrues.

Preliminary simulation results obtained by A. J. P. de Paepe, W. J. H. M. Lippmann, and A. J. Vinck indicate that the state-space formalism can also be used to advantage in sequential decoding. In Fano and stack decoding, one obtains major savings in number of computations and storage by exploiting the state-space symmetries of $\Gamma_{n,h,l}^{(n-k)}$. With sequential decoding it is interesting to find long constraint length codes with a large free distance. Computer search programs can again take advantage of the symmetries of $\Gamma_{n,h,l}^{(n-k)}$.

Acknowledgment

The authors wish to thank A. J. P. de Paepe, W. J. H. M. Lippmann, and A. P. C. van Schendel for several useful discussions and Mrs. G. H. Driever for accurate typing of the manuscript. We also wish to thank a referee for bringing to our attention another decoding method [8] that makes use of the dual code.

References

[1] J. P. M. Schalkwijk and A. J. Vinck, "Syndrome decoding of convolutional codes," *IEEE Trans. Commun.* (Corresp.), vol. COM-23, pp. 789–792, July 1975.

[2] J. P. M. Schalkwijk, "Symmetries of the state diagram of the syndrome former of a binary rate $\frac{1}{2}$ convolutional code," Lecture Notes, CISM Udine Summer School on Coding, Udine, Italy, Sept. 2–12, 1975.

[3] J. P. M. Schalkwijk and A. J. Vinck, "Syndrome decoding of binary rate $\frac{1}{2}$ convolutional codes," *IEEE Trans. Commun.*, vol. COM-24, pp. 977–985, Sept. 1976.

[4] G. D. Forney, Jr., "Convolutional codes I: Algebraic structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720–738, Nov. 1970; and vol. IT-17, p. 360, May 1971.

[5] G. D. Forney, Jr., "Structural analysis of convolutional codes via dual codes." *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 512–518, July 1973.

[6] R. V. Andree, "Modern Abstract Algebra." London: Constable, 1958.

[7] A. J. Viterbi, "Convolutional codes and their performance in communication systems," *IEEE Trans. Commun. Technol.* (Special Issue on Error Correcting Codes—Part II), vol. COM-19, pp. 751–772, Oct. 1971.

[8] C. R. P. Hartmann and L. D. Rudolph, "An optimum symbol-by-symbol decoding rule for linear codes," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 514–518, Sept. 1976.