Syndrome decoding of binary rate-k/n convolutional codes

th e

SYNDROME DECODING OF BINARY
RATE-k/n CONVOLUTIONAL CODES

by

J.P.M. Schalkwijk
A.J. Vinck
K.A. Post

TECHNISCHE HOGESCHOOL EINDHOVEN

NEDERLAND

AFDELING DER ELEKTROTECHNIEK

VAKGROEP TELECOMMUNICATIE

EINDHOVEN UNIVERSITY OF TECHNOLOGY

THE NETHERLANDS

DEPARTMENT OF ELECTRICAL ENGINEERING

GROUP TELECOMMUNICATIONS

SYNDROME DECODING OF BINARY RATE-k/n CONVOLUTIONAL CODES

by

J.P.M. Schalkwijk,

A.J. Vinck,

K.A. Post

TH-report 77-E-73

March 1, 1977

ISBN 90 6144 073 4

A B S T R A C T

This paper concerns a state space approach to syndrome decoding of binary rate-k/n convolutional codes. State space symmetries of a certain class of codes can be exploited to obtain an exponential reduction of decoder hardware. Aside from these hardware savings it is felt that the state space formalism developed in this paper has some intrinsic value of its own.

I. INTRODUCTION

This paper concerns a state space approach to syndrome decoding of binary rate-k/n convolutional codes. It extends and generalizes earlier work [1, 2, 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 for an exponential reduction of decoder hardware. Section V extends the results of the previous section to rate-k/n codes. Table I 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 2 memory elements. The input to this encoder are

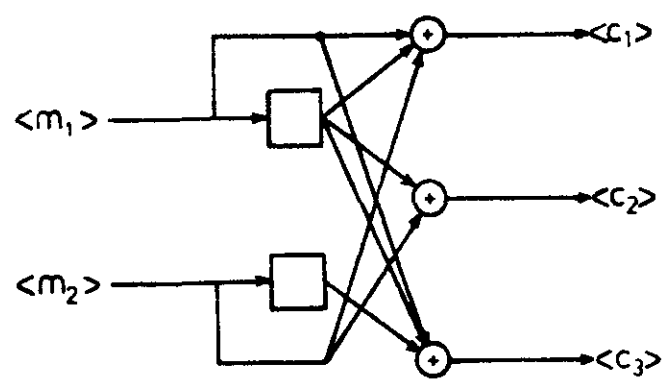

Fig. 1. A rate-2/3 convolutional encoder.

two binary message sequences

$$\langle m_i \rangle = \ldots, m_{i,-1}, m_{i0}, m_{i1}, \ldots \quad ; \; i = 1,2 \; .$$

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,

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

where $\oplus$ denotes modulo 2 addition.

With the input and output sequences, we associate sequences in the delay operator X:

$$m_i(X) = \ldots + m_{i,-1}X^{-1} + m_{i,0} + m_{i1}X + m_{i2}X^2 + \ldots \quad ; \; i = 1,2$$

$$c_j(X) = \ldots + c_{j,-1}X^{-1} + c_{j0} + c_{j1}X + c_{j2}X^2 + \ldots \quad ; \; j = 1,2,3,.$$

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

$$\underline{c} = \underline{m}G \quad , \qquad (1)$$

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

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

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

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

then the overall constraint length

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

(ν=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, $C^{\perp}$, code [5] to a convolutional code C is the linear space generated by the set of all n-tuples of finite (for infinite sequences the inner product may not be defined) sequences $\underline{d}(X)$ such that the inner product $(\underline{c},\underline{d}) \triangleq \underline{c}.\underline{d}^T$ (where T means transpose) is zero for all $\underline{c}$ 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 a syndrome former, and has the property that $\underline{c}H^T = 0$ if and only if $\underline{c} \in C$.

For the encoder, G, of Fig. 1 we have an invariant factor decomposition

$$\begin{bmatrix} 1+X & X & 1+X \\ 1 & 1 & X \end{bmatrix} = \begin{bmatrix} X & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & X \\ 1 & 0 & 1+X+X^2 \\ 0 & 0 & 1 \end{bmatrix}$$

Hence,

$$B = \begin{bmatrix} 1 & 1 & X \\ 1 & 0 & 1+X+X^2 \\ 0 & 0 & 1 \end{bmatrix}, \text{ so } B^{-1} = \begin{bmatrix} 0 & 1 & 1+X+X^2 \\ 1 & 1 & 1+X^2 \\ 0 & 0 & 1 \end{bmatrix} .$$

The H^T matrix is now given by the last column of the B^{-1} matrix, i.e.

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

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, compare Fig. 2.

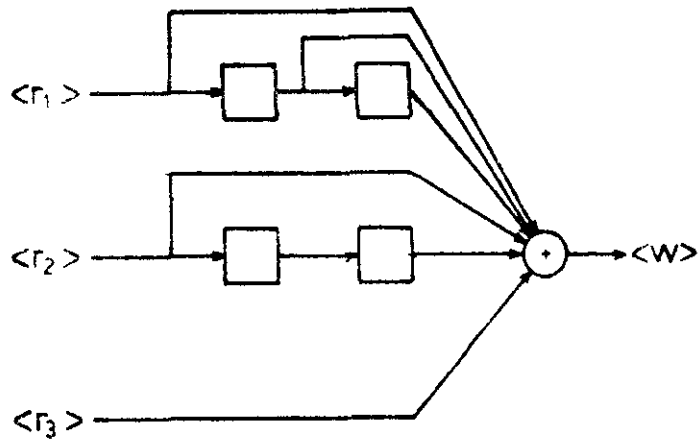

Fig. 2. A syndrome former for a rate-2/3 convolutional code.

This single output is the reason that in Sections II, III, and IV we first concentrate on rate-(n-1)/n codes. Second, in Table II 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 from the D^{-1} matrix a suitable encoder G. 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 $\underline{e}(X)$ be the error vector sequence, and let $\underline{r} = \underline{c} + \underline{e}$ be the received data vector sequence. We then define the syndrome vector sequence $\underline{\omega}(X)$ as

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

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

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

Using the codeword vector sequence estimate $\underline{\hat{c}}(X)$, the inverse encoder G^{-1} now forms an estimate $\hat{\underline{m}}(X)$ of the message vector sequence $\underline{m}(X)$, i.e.

$$\hat{\underline{m}} = \underline{\hat{c}}G^{-1} \ ,$$

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

$$G^{-1} = B^{-1}\Gamma^{-1}A^{-1} = \begin{bmatrix} 0 & 1 & 1+X+X^2 \\ 1 & 1 & 1+X^2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & X \end{bmatrix} = \begin{bmatrix} 1 & X \\ 1 & 1+X \\ 0 & 0 \end{bmatrix}$$

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

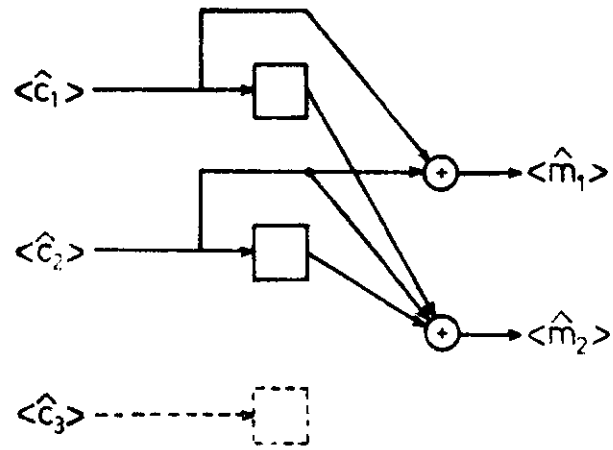

Fig. 3. An inverse encoder for the rate-2/3 convolutional code of Fig. 1.

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. This line is persued in the remainder of the paper.

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 $\underline{\hat{m}}(x)$ of the message vector sequence $\underline{m}(X)$ can also be written as

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

The first term $\underline{r}G^{-1}$ on the RHS of above eqn. can be easily obtained from the received data vector sequence $\underline{r}(X)$ using the simple circuitry of Fig. 3. As in refs. [1, 2, 3], it turns out that the overall decoder requires less hardware if we let the estimator determine the second term, $\underline{\hat{e}}G^{-1}$, directly. Hence, we define the message (as opposed to the codeword) vector sequence correction, $\underline{\hat{e}}_m(X)$, as

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

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,...,D) of binary polynomials, see Fig. 4. The n-tuple (A,B,C,...,D) is obtained from the

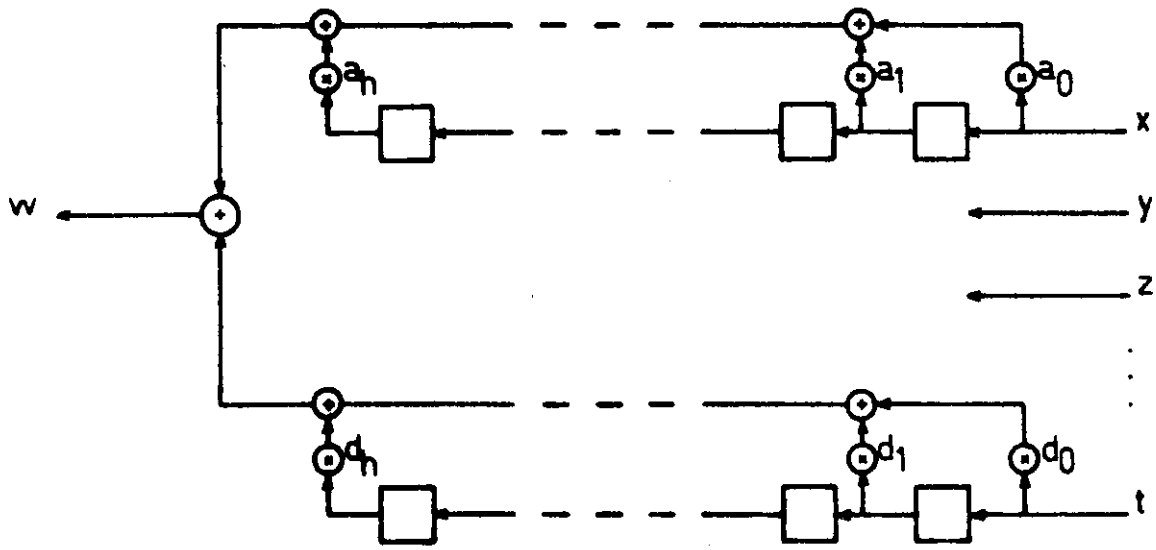

Fig. 4. The syndrome former for a rate-(n-1)/n convolutional code.

matrix $H = [h_1(X), h_2(X), \ldots, h_n(X)]$ of Section I by putting $a_i = h_{1i}$, $b_i = h_{2i}$, $c_i = h_{3i}, \ldots, d_i = h_{ni}$, $i=0,1,2,\ldots,h$, where

$$h = \max_{1 \le j \le n} \deg h_j(X) .$$

Obviously, one single noise vector in the sequence $\ldots,[e_{1,-1}, e_{2,-1},\ldots,e_{n,-1}]^T$, $[e_{10},e_{20},\ldots,e_{n0}]^T$, $[e_{11},e_{21},\ldots,e_{n1}]^T,\ldots$ can at most influence h+1 successive syndrome digits. 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 phenomenom occurs that two different initial physical states are syndrome-indistinguishable, i.e. that under every noise vector sequence $[e_{10},e_{20},\ldots,e_{n0}]^T,[e_{11},e_{21},\ldots,e_{n1}]^T,\ldots$ their syndrome sequences are identical. It is left to the reader [3,4] to prove that this natural concept of syndrome-indistinguishability is exactly the same as the following equivalence relation: Two physical states are called equivalent if their difference has a sequence of syndrome digits identically zero under a sequence of noise vectors identically zero. In fact, we may restrict ourselves in this definition to sequences of zero-noise vectors of length h, since all following zero-noise vectors simply must yield zero-syndrome digits.

The equivalence classes of the above equivalence relation will be called "abstract states", of briefly "states" of the system. There are several equivalent state descriptions. In ref. [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 represent the state. In the present paper we opt for this latter description.

We are now ready to introduce some convenient notation: States (given by their zero-noise syndrome sequence) are denoted by lower case greek letters with a subscript, e.g.

$\sigma_1 \triangleq [s_1,s_2,s_3,\ldots,s_{h-2},s_{h-1},s_h]$, and its left shifts

$\sigma_2 \triangleq [s_2,s_3,s_4,\ldots,s_{h-1},s_h,0]$,

$\sigma_3 \triangleq [s_3,s_4,s_5,\ldots,s_h,0,0]$, and so on.

Occasionally, i.e. if sufficiently many terminating components $s_h, s_{h-1}, \ldots$ vanish, we also write the right shifts, e.g.

$$\sigma_0 \triangleq [0, s_1, s_2, \ldots, s_{h-3}, s_{h-2}, s_{h-1}] \text{ if } s_h = 0,$$
$$\sigma_{-1} \triangleq [0, 0, s_1, \ldots, s_{h-4}, s_{h-3}, s_{h-2}] \text{ if } s_h = s_{h-1} = 0.$$

Finally, we introduce the symbols α_1, β_1, $\gamma_1, \ldots$, δ_1 to denote the generator states of the system, i.e.

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

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 output of the syndrome former, see Fig. 4, at time t and the state at time t+1 are completely determined by the state σ_1 and the input $[e_{1t}, e_{2t}, e_{3t}, \ldots, e_{nt}]^T$ at time t, $t = \ldots, -1, 0, +1, \ldots$.
As the syndrome former is supposed to be time invariant there is no purpose in retaining the subscript t in the state space analysis. Thus, we denote the syndrome former input by $[x, y, z, \ldots, t]^T$. The corresponding state transition and the output ω are given by

$$[x,y,z,\ldots,t]^T$$

$$\sigma_1 \longmapsto \sigma_2 + x\alpha_1 + y\beta_1 + z\gamma_1 + \ldots + t\delta_1 \qquad (3)$$

$$\omega = s_1 + xa_0 + yb_0 + zc_0 + \ldots td_0 \ .$$

Fig. 5 gives the state diagram of the syndrome former of Fig. 2. Solid lines correspond to a syndrome digit ω=0 and dashed lines to a

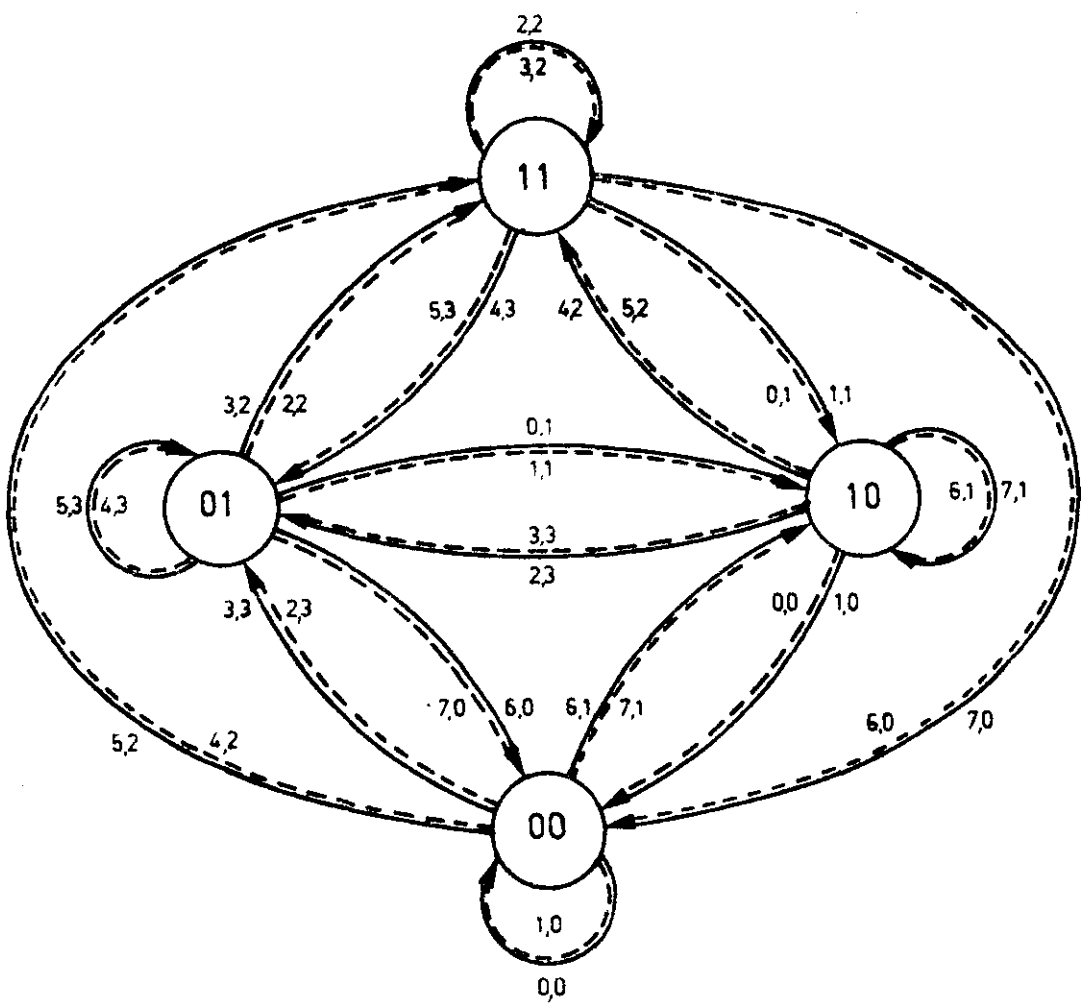

Fig. 5. State diagram of syndrome former.

syndrome digit ω=1. Indicated along the edges are the numerical values of $[\hat{e}_1,\hat{e}_2,\ldots,\hat{e}_n]_2$, $[\hat{e}_{m1},\hat{e}_{m2},\ldots,\hat{e}_{mk}]_2$ intepreted as binary numbers, where the latter vector represents the generic term $[\hat{e}_{m1t},\hat{e}_{m2t},\ldots,\hat{e}_{mkt}]$, t=...,-1,0,+1,... , of the message vector sequence correction $\underline{\hat{e}}_m(X)$ of (2), with the redundant subscript t removed.

The fact that the message vector correction is solely determined by the next state [3], see Fig. 5, follows from Forney [5]. According to Forney the syndrome former state uniquely determines the encoder state and vise versa if G and H^T are connected by a noiseless (dashed in Fig. 6) channel. The vector sequence $\underline{\hat{e}}^t{}_m(X)$ in Fig. 6 is such that

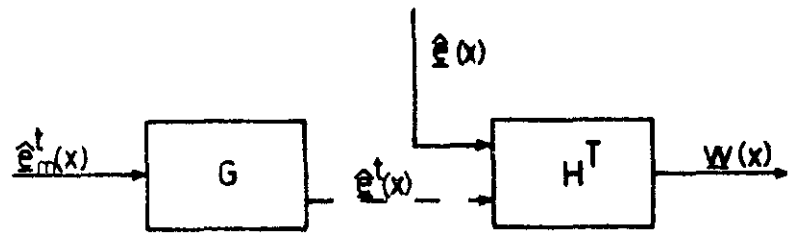

Fig. 6. Encoder and syndrome former connected back to back.

$\underline{\hat{e}}^t = \underline{\hat{e}}^t{}_m G$ stears the syndrome former H^T to the same state at time t, t=...,-1,0,+1,... , as does $\underline{\hat{e}}(X)$. As we can equate the encoder state to its recent inputs, $[\hat{e}^t{}_{m1t},\hat{e}^t{}_{m2t},\ldots,\hat{e}^t{}_{mkt}]$ is uniquely determined by the state of the syndrome former at time t+1, t=...,-1,0,+1,... . But, as G^{-1} is an instantaneous right inverse of G we have $[\hat{e}_{m1t},\ldots,\hat{e}_{mkt}] = [\hat{e}^t{}_{m1t},\ldots,\hat{e}^t{}_{mkt}]$, t=...,-1,0,+1,... .

Now consider the linear subspace spanned by the generators α_1, β_1, $\gamma_1,\ldots,$ δ_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 from a coset of the linear subspace $L[\alpha_1,\beta_1,\gamma_1,\ldots,\delta_1]$. This coset will be called the "sink-tuple" of σ_1.

The linear subspace $L[\alpha_1,\beta_1,\gamma_1,\ldots,\delta_1]$ is identical to the linear subspace $L[\alpha_1,\beta_1 + b_h\alpha_1, \gamma_1 + c_h\alpha_1,\ldots, \delta_1 + d_h\alpha_1]$. However, as $a_h=1$, the vectors $\beta_1 + b_h\alpha_1, \gamma_1 + c_h\alpha_1,\ldots, \delta_1 + d_h\alpha_1$ have a rightmost coordinate equal to 0. Thus, these vectors have a right shift. Furthermore,

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

Define,

$$\varepsilon_1 \triangleq [1,0,0,\ldots,0],$$

a row vector of length h. Then

$$\dim L[\alpha_1,\beta_1,\gamma_1,\ldots,\delta_1] = \dim L[\varepsilon_1,(\beta+b_h\alpha)_0,(\gamma+c_h\alpha)_0,\ldots,(\delta+d_h\alpha)_0].$$

Each state has at least one primage. If $\tau_1 = [s_1,s_2,\ldots,s_{h-1},0]$, then

$\tau_0 = [0,s_1,\ldots,s_{h-2},s_{h-1}]$ is a preimage under $[x,y,z,\ldots,t] = [0,0,0,\ldots,0]$. If $\tau_1 = [s_1,s_2,\ldots,s_{h-1},1]$, then $(\tau+\alpha)_0$ is a preimage under $[x,y,z,\ldots,t] = [1,0,0,\ldots,0]$. 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 $L[\varepsilon_1,(\beta+b_h\alpha)_0, (\gamma+c_h\alpha)_0,\ldots,(\delta+d_h\alpha)_0]$ that contains the particular 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 $L[\varepsilon_1,(\beta+b_h\alpha)_0,(\gamma+c_h\alpha)_0,\ldots,(\delta+d_h\alpha)_0]$. Hence, we conclude that τ_1 has exactly 2^q preimages that constitute the "source-tuple" of τ_1. It is easily verified that each element σ_1 of a source tuple has the same sink-tuple.

It is this source/sink-tuple description of the state space that will play an important role in the remainder of the paper. Hence, to make things more concrete, we give a specific example for the syndrome former of Fig. 7.

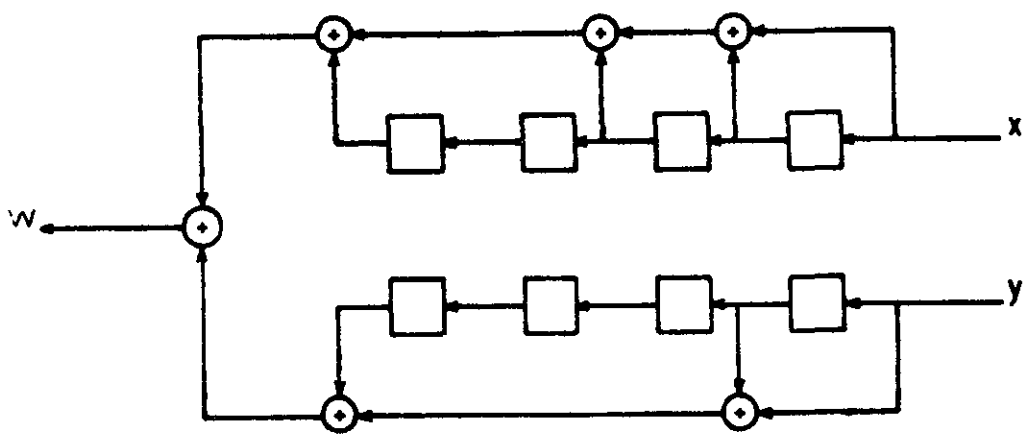

Fig. 7. The syndrome former for a rate-$\frac{1}{2}$ convolutional code.

We have

$$\alpha_1 = [1\ 1\ 0\ 1]_2 = 13 \qquad \varepsilon_1 = [1\ 0\ 0\ 0]_2 = 8$$

$$\beta_1 = [1\ 0\ 0\ 1]_2 = 9 \qquad (\alpha+\beta)_0 = [0\ 0\ 1\ 0]_2 = 2$$

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

Fig. 8 shows a partition of the state space in source/sink-tuples.

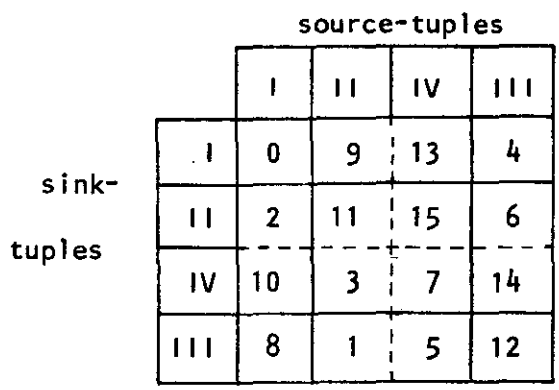

Fig. 8. State space partition in source/sink-tuples.

Anticipating on Section IV the states in Fig. 8 have been geometrically arranged in such a way that also 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 [6], irrespective of the received data vector sequence $\underline{r}(X)$.

III. ALGORITHM

Given the syndrome sequence $\omega(X)$ of a rate-$(n-1)/n$ code, compare Fig. 4, the estimator is to determine the state sequence that corresponds to a noise vector sequence estimate $\underline{\hat{e}}(X)$ of minimum Hamming weight that can be a possible cause of $\omega(X)$. According to Section II this state sequence can be stored in terms of an equivalent message vector sequence correction $\hat{e}_m(X)$. As the estimation algorithm to be described in this section is similar to Viterbi's [6], we can be very brief. To find the required state sequence Viterbi introduces 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 $[x,y,z,\ldots,t]^T$.

PROBLEM: Given a metric function f and a syndrome digit ω, find a metric function g which is statewise minimal, and for every state is consistent with at least one of the values of f on its preimages under syndrome digit ω, increased by the weight of its corresponding state transition.

The solution to this problem expresses g in terms of f and ω, and can be formulated in terms of the 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 ω. The equations that express g in terms of f and ω are called "metric equations". They have the form

$$g(\tau_1) = \min \{ f(\sigma_1) + W_H([x,y,z,\ldots,t]^T) \mid \sigma_1 \xrightarrow{[x,y,z,\ldots,t]^T} \tau_1, \omega \} \qquad (4)$$

The particular preimage σ_1 in (4) that realizes the minimum is called the "survivor". When there are more preimages for which the minimum in (4) 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 $\omega_1,\omega_2,\omega_3,\ldots$ one can form a sequence of metric functions $f_1,f_2,f_3,\ldots$ iteratively by means of the metric equations:

$$f_0 \overset{\omega_1}{\longmapsto} f_1 \overset{\omega_2}{\longmapsto} f_2 \overset{\omega_3}{\longmapsto} f_3 \longmapsto \ldots \quad .$$

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, $\omega_1,\omega_2,\omega_3,\ldots=0,0,0,\ldots$, is called the "stable metric function". It has the property

$$f_s \overset{\omega=0}{\longmapsto} f_s \quad .$$

In order to make things more concrete we now give a specific example. Fig. 9 represents the t-th section, $t=\ldots,-1,0,+1,\ldots$, of the trellis diagram [6] corresponding to the state diagram of Fig. 5. From Fig. 9 we find for the metric equations:

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

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

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

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

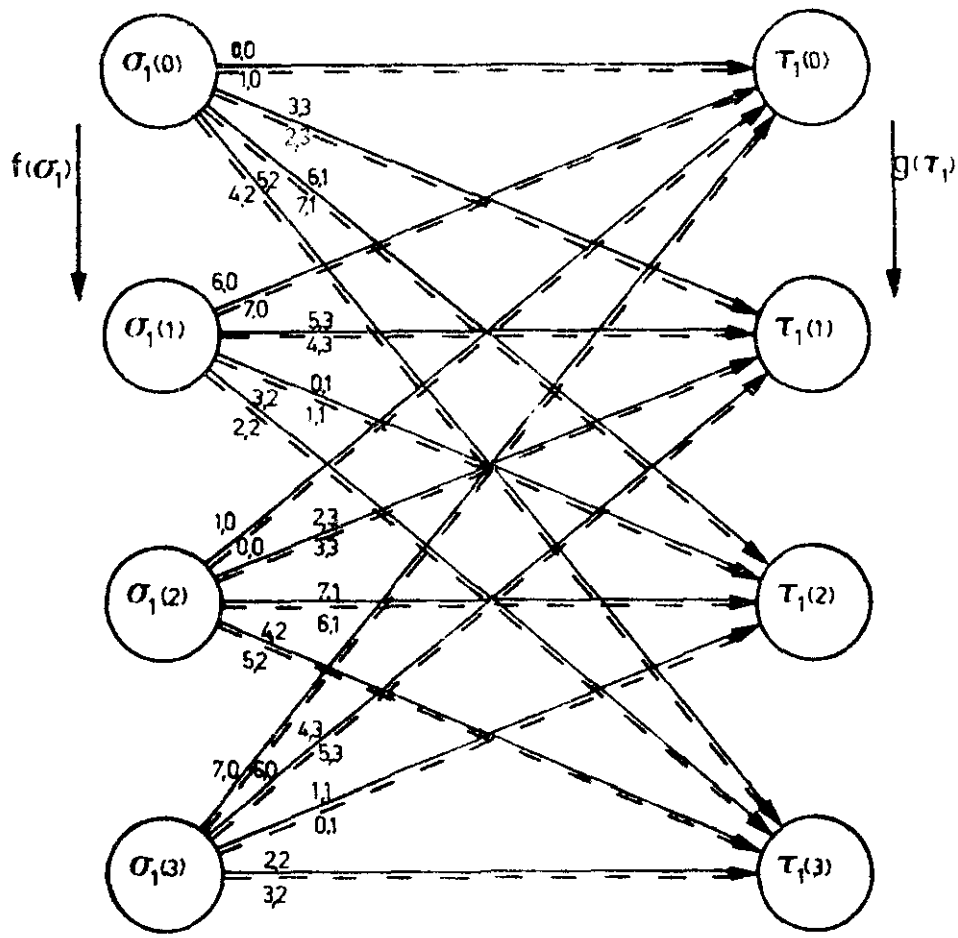

Fig. 9. The t-th section of the trellis diagram, t=...,-1,0,+1,... .

where $\bar{\omega}$ is the modulo 2 complement of ω. Note that for each value ω=0 or ω=1 four arrows impinge on each image τ_1. The preimage σ_1 associated with the minimum within the relevant pair of square brackets in (5) is the survivor. The case where we have more candidates for survivor among the preimages will be considered shortly.

In the classical implementation of the Viterbi algorithm [6] 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 $f_t[\tau_1(j)]$, $t=\ldots,-1,0,+1,\ldots$, of the metric function. As only the differences between the values of the metric function matter in the decoding algorithm

$$\min_{0\leq j\leq 3} \{f_t[\tau_1(j)]\}$$

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 $\tau_1(j)$ at time t. The survivor sequence is stored in terms of the associated message vector corrections $\ldots,[\hat{e}_{m1,t-1},\ldots,\hat{e}_{mk,t-1}]$, $[\hat{e}_{m1,t},\ldots,\hat{e}_{mk,t}]$; $t=\ldots,-1,0,+1,\ldots$. Observe that all quantities that are crucial to the estimation algorithm that determines $\underline{\hat{e}}_m(X)$ given $\omega(X)$ are contained in the trellis section of Fig. 9.

Now observe that (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. As far as metric register and path register contents are concerned, the states $\tau_1(1)$ and $\tau_1(3)$ are not distinct. 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 on the implementation of the syndrome decoder one is referred to [3]. In this 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 now introduce the class $\Gamma_{n,h,\ell}$ of rate-(n-1)/n binary convolutional codes (A,B,C,...,D), i.e. in terms of their syndrome formers, that exhibits state space symmetries that allow for an exponential reduction of decoder hardware. To wit (A,B,C,...,D) $\in \Gamma_{n,h,\ell}$ if and only if

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

$$a_j = b_j \; ; \; 0 \leq j \leq \ell-1 \tag{6b}$$

$$a_j = b_j \; ; \; h-\ell+1 \leq j \leq h \tag{6c}$$

$$C,\ldots,D \text{ all have degree } \leq h-\ell \tag{6d}$$

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

$$L[\varepsilon_1,(\alpha+\beta)_0,\gamma_0,\ldots,\delta_0] \cap L[(\alpha+\beta)_1,\ldots,(\alpha+\beta)_{\ell-1}] = \{\underline{0}\} \tag{6f}$$

Note that the code $A(X) = 1+X+X^2$, $B(X) = 1+X^2$, $C(X) = 1$ of Fig. 2 is an element of $\Gamma_{3,2,1}$. The code $A(X) = 1+X+X^2+X^4$, $B(X) = 1+X+X^4$ of Fig. 7 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,...,D) is a set of syndrome polynomials for some non-catastrophic rate-(n-1)/n convolutional code (in fact, for a class of such codes).

Assume $\Gamma_{n,h,\ell} \neq \phi$. For (A,B,C,...,D) $\in \Gamma_{n,h,\ell}$ 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 ℓ-singleton

states, too. For every state ϕ_1 the states $\phi_i (i \geq \ell+1)$ are ℓ-singleton states. We have the following lemma, the proof of which is left to the reader.

LEMMA 1: For every state σ_1 there exists a unique ℓ-singleton state $\phi_{\ell+1}$ and a unique index set $I \subset \{1,2,\ldots,\ell\}$ such that

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

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

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

We shall prove the following theorem:

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

PROOF: Obviously the union of all $[\sigma_1]^{(\ell)}$ is equal to the state space. So, we only have to prove that $[\sigma_1]^{(\ell)} = [\sigma_1']^{(\ell)}$ whenever $[\sigma_1]^{(\ell)} \cap [\sigma_1']^{(\ell)} \neq \phi$. Let us assume that $[\sigma_1]^{(\ell)} \cap [\sigma_1']^{(\ell)} \neq \phi$. Then there exist r_i and s_i such that

$$\phi_{\ell+1} + \sum_{i \in I} [\alpha_i + r_i(\alpha+\beta)_i] = \phi'_{\ell+1} + \sum_{i \in I'} [\alpha_i + s_i(\alpha+\beta)_i] \ ,$$

or

$$\phi_{\ell+1} - \phi'_{\ell+1} + \sum_{i \in I} r_i(\alpha+\beta)_i - \sum_{i \in I'} s_i(\alpha+\beta)_i = \sum_{i \in I \Delta I'} \alpha_i \ .$$

Now the LSH of above equation is an ℓ-singleton state by (6c) so that the symmetric difference $I \Delta I'$ must be empty, in other words $I=I'$. Therefore we get

$$\phi'_{\ell+1} - \phi_{\ell+1} = \sum_{i \in I} (r_i - s_i)(\alpha+\beta)_i \ ,$$

i.e. $\phi'_{\ell+1}$ and $\phi_{\ell+1}$ differ by some linear combination of $\{(\alpha+\beta)_i \mid i \in I\}$. But then we must have $[\sigma_1]^{(\ell)} = [\sigma_1']^{(\ell)}$, since in the construction of these classes all linear combinations of $\{(\alpha+\beta)_i \mid i \in I\}$ are involved.

Q.E.D.

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

The one-element equivalence classes of $R_{n,h,\ell}$ consists of exactly one ℓ-singleton state. An example are the states 0,4,8 and 12 in Fig. 8. The number $N_{n,h,\ell}$ of $R_{n,h,\ell}$-equivalence classes can be found as follows. First, take $I \subset \{1,2,\ldots,\ell\}$ 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 $2^{h-\ell}$ ℓ-singleton states. Now 2^j of these $2^{h-\ell}$ ℓ-singleton states correspond to the same $R_{n,h,\ell}$-equivalence class, i.e. all ℓ-singleton states differing by a linear combination of $\{(\alpha+\beta)_i \mid i \in I\}$. Hence there are $2^{h-\ell-j}$ $R_{n,h,\ell}$-equivalence classes for each I of cardinality j. Thus

$$N_{n,h,\ell} = \sum_{j=0}^{\ell} \binom{\ell}{j} 2^{h-\ell-j} = 2^{h-2\ell} 3^{\ell} \ . \qquad (9)$$

THEOREM 3: Let $(A,B,C,\ldots,D) \in \Gamma_{n,h,\ell}$, and assume that $1 \leq \ell' \leq \ell$. Then every $R_{n,h,\ell}$-equivalence class of $(A,B,C,\ldots,D)$ is a union of $R_{n,h,\ell'}$-equivalence classes of $(A,B,C,\ldots,D)$, cf (7).

PROOF: Let σ_1 and τ_1 be $R_{n,h,\ell'}$-equivalent states of $(A,B,C,\ldots,D)$. Then we may write for some $r_i \in \{0,1\}$, $i \in I' \subset \{1,2,\ldots,\ell'\}$:

$$\sigma_1 = \phi_{\ell'+1} + \sum_{i \in I'} \alpha_i ,$$

$$\tau_1 = \phi_{\ell'+1} + \sum_{i \in I'} [\alpha_i + r_i(\alpha+\beta)_i] .$$

On the other hand, for some $I'' \subset \{\ell'+1,\ldots,\ell\}$ and some $\Psi_{\ell+1}$ we have

$$\phi_{\ell'+1} = \Psi_{\ell+1} + \sum_{i \in I''} \alpha_i .$$

Letting $I = I' \cup I''$, $r_i=0$ for $i \in I''$ we now obtain

$$\sigma_1 = \Psi_{\ell+1} + \sum_{i \in I} \alpha_i$$

$$\tau_1 = \Psi_{\ell+1} + \sum_{i \in I} [\alpha_i + r_i(\alpha+\beta)_i] ,$$

i.e. σ_1 and τ_1 are $R_{n,h,\ell}$-equivalent Q.E.D.

In Fig. 8 we exhibit the $R_{2,4,2,}$-equivalence classes for the $A(X) = 1+X+X^2+X^4$, $B(X) = 1+X+X^4$ code. We claimed that any two states within the same equivalence class have the same metric value irrespective of the received data vector sequence $\underline{r}(X)$. We are now ready to prove this result.

THEOREM 4: Assume that $(A,B,C,\ldots,C) \in \Gamma_{n,h,\ell}$. Let f_0 be any starting metric function, and let $\omega_1, \omega_2, \omega_3, \ldots$ be any syndrome sequence. Then every iterate f_u is constant on the $R_{n,h,u}$-equivalence classes of $(A,B,C,\ldots,D)$, $1 \leq u \leq \ell$.

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).

Preimage	$\phi_2+\alpha_1$	$\phi_2+\beta_1$
	Noise;Syndrome	Noise;Syndrome
$\phi_1 \quad +z\gamma_0+\ldots+t\delta_0$	$[1,0,z,\ldots,t]^T;\omega_1$	$[0,1,z,\ldots,t]^T;\omega_1$
$\phi_1 \quad +(\alpha+\beta)_0+z\gamma_0+\ldots+t\delta_0$	$[0,1,z,\ldots,t]^T;\omega_1$	$[1,0,z,\ldots,t]^T;\omega_1$
$\phi_1+\epsilon_1 \quad +z\gamma_0+\ldots+t\delta_0$	$[1,0,z,\ldots,t]^T;\bar{\omega}_1$	$[0,1,z,\ldots,t]^T;\bar{\omega}_1$
$\phi_1+\epsilon_1+(\alpha+\beta)_0+z\gamma_0+\ldots+t\delta_0$	$[0,1,z,\ldots,t]^T;\bar{\omega}_1$	$[1,0,z,\ldots,t]^T;\bar{\omega}_1$

We see that on every line, i.e. 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 ω_1. This proves the assertion for u=1. Now let us assume that the statement is true for a fixed u, $1 \leq u \leq \ell-1$. Let f_0 be any starting metric function and let $\omega_1,\omega_2,\omega_3,\ldots$ 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 $I \subset \{1,2,\ldots,u\}$ such that for some $r_i \in \{0,1\}$

$$\chi_1 = \Psi_{u+1} + \sum_{i \in I} \alpha_i ,$$

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

We now consider the cosets S and S' of $L[\varepsilon_1,(\alpha+\beta)_0,\gamma_0,\ldots,\delta_0]$ to which χ_1 and χ_1' belong, respectively, and compare them element wise. The states

$$\chi_1 + p\varepsilon_1 + q(\alpha+\beta)_0 + r\gamma_0 + \ldots + s\delta_0,$$

and

$$\chi_1' + p\varepsilon_1 + q(\alpha+\beta)_0 + r\gamma_0 + \ldots + s\delta_0$$

are obviously $R_{n,h,u}$-equivalent for all $p,q,r,\ldots,s \in \{0,1\}$, since by the definition of ε_1 and by (6c,d) the last u components of $p\varepsilon_1 + q(\alpha+\beta)_0 + r\gamma_0 + \ldots + s\delta_0$ vanish. Furthermore, by (6b) we have

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

Hence, by (3) the preimages

$$\chi_1 + p\varepsilon_1 + q(\alpha+\beta)_0 + r\gamma_0 + \ldots + s\delta_0,$$

and

$$\chi_1' + p\varepsilon_1 + q(\alpha+\beta)_0 + r\gamma_0 + \ldots + s\delta_0$$

give rise to identical syndrome digits in response to an input vector $[x,y,z,\ldots,t]^T$. 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,...,D). Q.E.D.

Theorem 4 proves that one needs only one metric register for each $R_{n,h,\ell}$-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,...,D) $\in \Gamma_{n,h,\ell}$. Condition (6f), where $\{(\alpha+\beta)_1,(\alpha+\beta)_2,\ldots,(\alpha+\beta)_{\ell-1}\} = \{\underline{0}\}$ for ℓ=1, implies that a coset of $L[\varepsilon_1,(\alpha+\beta)_0,\gamma_0,\ldots,\delta_0]$ and a coset of $L[(\alpha+\beta)_1,(\alpha+\beta)_2,\ldots,(\alpha+\beta)_{\ell-1}]$ can have at most one element in common, i.e.

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

On the other hand, from the proof of Theorem 4 it follows that whenever X_1 and X_1' are $R_{n,h,\ell-1}$-equivalent, then the same holds for the states

$$X_1 + p\varepsilon_1 + q(\alpha+\beta)_0 + r\gamma_0 + \ldots + s\delta_0 \quad ,$$

and

$$X_1' + p\varepsilon_1 + q(\alpha+\beta)_0 + r\gamma_0 + \ldots + s\delta_0 \quad , \quad p,q,r,\ldots,s \in \{0,1\} \quad ,$$

that form the source-tuples containing X_1 and X_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 $R_{n,h,\ell-1}$-equivalent states. It is left to the reader to prove that this relation is an equivalence relation. The unique and natural one-to-one correspondence between the states of two equivalent source-tuples, that is induced by the intersection with $R_{n,h,\ell-1}$-equivalence classes is, by the proof

of Theorem 4, consistent with the algebraic difference structure of the source-tuples. Hence, in view of Theorem 4, we see that for the m-th iterate f_m, $m \geq \ell-1$, of any metric function f_0 under any syndrome sequence $\omega_1,\omega_2,\omega_3,\ldots$ 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, $j \geq \ell$, of a metric function f_0, linked by the syndrome digit ω_j,

$$f_{j-1} \xmapsto{\omega_j} f_j \ .$$

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

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

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's 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, that according to the properties of equivalent source-tuples can be realized in the following way: Whenever two source-tuples S_i and S_i' are equivalent (and, hence, have statewise identical f_{j-1}-values) then let for the

respective sink-tuples T_i and T_i' statewise corresponding survivors be chosen in such a way, that $R_{n,h,1}$-equivalent states get the same survivor. Given a sequence of metric function iterates

$$f_0 \xrightarrow{\omega_1} f_1 \xrightarrow{\omega_2} f_2 \longmapsto \ldots \longmapsto f_{j-2} \xrightarrow{\omega_{j-1}} f_{j-1} \xrightarrow{\omega_j} f_j \ , \ j \geq \ell \ ,$$

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

$$\sigma_1^{(-j)} \longleftarrow \sigma_1^{(-j+1)} \longleftarrow \sigma_1^{(-j+2)} \longleftarrow \ldots \longleftarrow \sigma_1^{(-2)} \longleftarrow \sigma_1^{(-1)} \longleftarrow \sigma_1 \ ,$$

and the following theorem holds.

THEOREM 5: If σ_1 and η_1 are distinct $R_{n,h,m}$-equivalent states then $\sigma_1^{(-m)} = \eta_1^{(-m)}$, $m=1,2,\ldots,\ell$.

PROOF: The proof is by induction on m. For m=1 the assertion is part of our assumption above. Now assume that the statement is true for m=u, u fixed, $1 \leq u \leq \ell-1$, and 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 we may write

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

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

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

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

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

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

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

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

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

$$\tilde{\sigma}_1 - \sigma_1^{(-1)} = \tilde{\eta}_1 - \eta_1^{(-1)} \in L[\varepsilon_1,(\alpha+\beta)_0,\gamma_0,\ldots,\delta_0] .$$

So, $\tilde{\sigma}_1 - \sigma_1^{(-1)} = \tilde{\eta}_1 - \eta_1^{(-1)}$ 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 5 shows that except perhaps for the last ℓ-1 stages, $R_{n,h,\ell}$-equivalent states have the same path register contents irrespective of the received data vector sequence $\underline{r}(X)$. Thus, roughly,

speaking, one needs only one path register for each $R_{n,h,\ell}$-equivalence class of states. By Theorem 4 one only needs one metric register per $R_{n,h,\ell}$-equivalence class. Hence, the complexity [3] of a syndrome decoder for a code $(A,B,C,\ldots,D) \in \Gamma_{n,h,\ell}$ is proportional to the number $N_{n,h,\ell}$ of $R_{n,h,\ell}$-equivalence classes, i.e. by (9) the complexity is proportional to $2^{h-2\ell}3^{\ell}$. As an example take a code in $\Gamma_{2,2\ell,\ell}$, i.e. a rate-$\frac{1}{2}$ code with

$$A(X) = X^{2\ell} + A_{2\ell-1}X^{2\ell-1} + \ldots + A_1X + 1 ,$$
$$B(X) = A(X) + X^{\ell} .$$

The syndrome decoder for such a code has complexity proportional to $3^{\ell} = (\sqrt{3})^{h}$. The classical Viterbi decoder [6] 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 $(A,B,C,\ldots,D) \in \Gamma_{n,h,\ell}$ is in order. It is quite obvious that constraints like (6) can reduce the maximum obtainable free distance for given n, and h. We are not yet able to derive a lower bound on the free distance of codes $(A,B,C,\ldots D) \in \Gamma_{n,h,\ell}$. However, Table I of the next section lists the free distance of some short constraint length codes in $\Gamma_{n,h,\ell}$. 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.

V. SPECIAL R=k/n CODES-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, compare Fig. 4. Hence, the n-k syndrome formers in the set $\{\Sigma^1,\Sigma^2,\ldots,\Sigma^{n-k}\}$, where $\Sigma^i \triangleq (A_i,B_i,C_i,\ldots,D_i)$, 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 Σ^i, i=1,2,...,n-k , should be in $\Gamma_{n,h,\ell}$, and the common physical states should have the same equivalence classes w.r.t. the equivalence relation of syndrome-indistinguishability in each of the n-k individual syndrome formers. We will call a set of rate-(n-1)/n syndrome formers that share a common physical state "coherent" if the individual syndrome formers have the same abstract states.

Let $\Gamma^{(n-k)}_{n,h,\ell}$ be the class of codes that are defined by n-k coherent syndrome formers each of which is in $\Gamma_{n,h,\ell}$. Table I lists the maximum free distance for various values of the parameters k,n,h, and ℓ. The $\Gamma^{(n-k)}_{n,h,\ell}$ classes with (k,n) = (1,3) are defined by two coherent syndrome formers. The column with "N" on 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 both for (k,n) = = (1,3) gives some idea of the effect of the coherence requirement on the free distance. Table II lists several optimal $\Gamma^{(n-k)}_{n,2\ell,\ell}$ codes in terms of their syndrome former connections, geometrically arranged as in Fig. 4.

TABLE I

MAXIMUM FREE DISTANCE OF VARIOUS $\Gamma^{(n-k)}_{n,h,\ell}$ - CLASSES

(k,n)	(k,n) = (1,2)				(k,n) = (2,3)				(k,n) = (1,3)				
l / h	1	2	3	4	1	2	3	4	N	1	2	3	4
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 II

OPTIMAL $\Gamma^{(n-k)}_{n,2\ell,\ell}$ - CODES

(k,n) / ν	(k,n) = (1,2)	(k,n) = (2,3)	(k,n) = (1,3)	
	Σ	Σ	Σ^1	Σ^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

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

$$\Sigma \triangleq (A,B,C,\ldots,D) ,$$

and

$$\Sigma' \triangleq (A',B',C',\ldots,D')$$

sharing the same set of nh memory cells, compare Fig. 4. From the mathematical point of view the syndrome-indistinguishability classes of a syndrome former Σ 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 Σ and Σ' are coherent if and only if for all nh-tuples

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

we have

$$\sum_{i=1}^{h} (x_i\alpha_{h+1-i} + y_i\beta_{h+1-i} + \ldots + t_i\delta_{h+1-i}) = \underline{0} \Leftrightarrow$$

$$\Leftrightarrow \sum_{i=1}^{h} (x_i\alpha'_{h+1-i} + y_i\beta'_{h+1-i} + \ldots + t_i\delta'_{h+1-i}) = \underline{0} .$$

We shall now discuss some consequences of this concept of coherence. 1/ Let Σ and Σ' be coherent syndrome formers, and assume as before that $a_h = 1$. Then $\{\alpha_1,\alpha_2,\ldots,\alpha_h\}$ is a basis for the abstract state space of Σ. In other words

$$\sum_{i=1}^{h} x_i \alpha_{h+1-i} = \underline{0} \iff x_1 = x_2 = \ldots = x_h = 0$$

so that by coherence

$$\sum_{i=1}^{h} x_i \alpha'_{h+1-i} = \underline{0} \iff x_1 = x_2 = \ldots = x_h = 0 \ .$$

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

2/ Let Σ and Σ' be coherent syndrome formers, $a_h = a'_h = 1$.

Then the correspondence

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

is an isomorphism between the abstract state spaces of Σ and Σ'.

SKETCH OF PROOF: By 1/, $\{\alpha_1, \alpha_2, \ldots, \alpha_h\}$ and $\{\alpha'_1, \alpha'_2, \ldots, \alpha'_h\}$ are bases of the state spaces above. Hence, for example

$$\beta_1 = u_1\alpha_1 + u_2\alpha_2 + \ldots + u_h\alpha_h \ ,$$

or

$$-\beta_1 + u_1\alpha_1 + u_2\alpha_2 + \ldots + u_h\alpha_h = \underline{0} \ ,$$

so that by coherence

$$-\beta'_1 + u_1\alpha'_1 + u_2\alpha'_2 + \ldots + u_h\alpha'_h = \underline{0},$$

i.e.

$$\beta'_1 = u_1\alpha'_1 + u_2\alpha'_2 + \ldots + u_h\alpha'_h \ , \qquad \text{etc.}$$

3/ Let Σ and Σ' be coherent syndrome formers, i.e. $a_h = a'_h = 1$. Then Σ and Σ' have isomorphic source/sink-tuple structures.

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

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

so that by coherence

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

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

$$L[\alpha_1,\beta_1,\gamma_1,\ldots,\delta_1] \leftrightarrow L[\alpha'_1,\beta'_1,\gamma'_1,\ldots,\delta'_1] ,$$

and

$$S \leftrightarrow S'$$

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

4/ Finally, we can restate the coherence of Σ and Σ' in terms of a condition of their polynomials A,B,C,...,D , and A',B',C',...,D' as follows. Let Σ and Σ' be coherent syndrome formers, $a_h = a'_h = 1$. Let the isomorphism between their state spaces, which is generated by the mapping $\alpha_j \mapsto \alpha'_j$, $j = h,h-1,\ldots,1$, w.r.t. the natural basis of unit vectors be given by the (invertible) matrix Q, i.e.

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

It is immediately verified that Q itself has the form

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

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

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

The isomorphism also entails that

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

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

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

$$\equiv 0 \pmod{X^h} .$$

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

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

or

$$\text{degree}\ [A'(X)B(X) - B'(X)A(X)] \leq h, \text{ etc.}$$

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

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

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

THEOREM 6: Two syndrome formers $\Sigma \triangleq (A,B,C,\ldots,D)$ and $\Sigma' \triangleq (A',B',C',\ldots,D')$, where $h = h'$, are coherent if and only if all 2x2 subdeterminants of the polynomial matrix

$$\begin{bmatrix} A(X) & B(X) & C(X) & \cdots & D(X) \\ A'(X) & B'(X) & C'(X) & \cdots & D'(X) \end{bmatrix}$$

have degree $\leq h$.

We conclude this section with an example. Consider the binary rate-1/3 convolutional code generated by an encoder with connection polynomials $1+X^2+X^5+X^6$, $1+X^2+X^3+X^5+X^6$, and $X^3+X^4+X^5+X^6$. The inverse encoder of minimal degree is unique, and is given by the polynomials $1+X+X^2$, X, and X^2. The free distance of the above code is 13 (the maximum free distance for a rate-1/3 code with polynomials of degree 6 is 15). A set of syndrome formers of minimal degree is given by $1+X+X^3$, $1+X$, $X+X^3$, and X^2 , X^2+X^3 , $1+X+X^3$. 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 $1+X^3+X^6$, $1+X^3$, $1+X+X^4+X^6$, and $1+X+X^2+X^4+X^5+X^6$, $1+X+X^2+X^3$, $X^2+X^5+X^6$ 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 $1+X+X^6$, $1+X+X^4+X^6$, $1+X+X^3+X^4$, and $1+X^2+X^5+X^6$, $1+X^2+X^3+X^4+X^5+X^6$, $X+X^2+X^4$ is coherent and is a subset of $\Gamma_{3,6,2}$ and, hence, our code belongs to $\Gamma_{3,6,2}^{(3-1)}$ and therefore, 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 $\Gamma^{(n-k)}_{n,h,\ell}$ 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 $\Gamma^{(n-k)}_{n,h,\ell}$ classes is listed in Table I. Codes achieving the maximum free distance of several $\Gamma^{(n-k)}_{n,2\ell,\ell}$ classes are given in Table II. These $\Gamma^{(n-k)}_{n,2\ell,\ell}$ classes offer the largest hardware savings!

Presently, we are investigating whether the state space formalism developed in this paper can also be used to advantage in sequential decoding. It will then become interesting to find the maximum free distance of classes of long constraint length codes that exhibit certain state space symmetries. This is one of our present topics of research.

ACKNOWLEDGEMENT

The authors want to thank A.J.P. de Paepe for several useful discussions and Miss G. van Hulsen for the accurate typing of the manuscript.

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-½ convolutional code",
Lecture Notes, CISM Udine Summer School on Coding, Udine,
Italy, September 2-12, 1975.

[3] J.P.M. Schalkwijk and A.J. Vinck,
"Syndrome decoding of binary rate-½ convolutional codes",
IEEE Trans. Commun., vol. COM-24, pp. 977-985, September 1976.

[4] G.D. Forney, Jr.,
"Convolutional codes I: Algebraic structure",
IEEE Trans. Inform. Theory, vol. IT-16, pp. 720-738,
November 1970;
also, correction appears in 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] 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, October 1971.