STATE SPACE AND POLYNOMIAL MATRIX PARAMETRIZATION OF MINIMAL CONVOLUTIONAL ENCODERS

E.Fornasini[*], R.Pinto[†]

Algebraic system theory, sampled data systems, multivariable control, convolutional codes, signal processing.

Abstract

The paper discusses the possibility of characterizing some important properties of convolutional codes and its encoders and syndrome formers by means of matrix fraction descriptions and state space models. A complete parametrization is then provided for all minimal encoders and minimal syndrome formers of a given code. Finally state feedback and static precompensation (resp.output injection and postcompensation) allow to synthesize all minimal encoders (resp. minimal syndrome formers), when a minimal one is available.

1 Introduction

Since the early seventies, the pioneering work of Forney [3,4,5] made it clear that system theory provides a convenient setting for the analysis of convolutional codes. In fact, a convolutional code can be viewed as the set of output sequences generated by a linear discrete-time multivariable system over a finite field, an encoder is nothing else than an injective linear input-output map, associating codewords to information sequences, and a syndrome generator corresponds to a residual generator in a failure detection device.

Typically control theory and convolutional coding theory concentrate on different aspects of linear systems. Control interest centers around input-output relations, and the possibility of modifying their structure by resorting to various compensation strategies; in coding theory, instead, mostly important is the structure of the output sequence set that constitutes the code. There are however several tools, connected with matrix fraction descriptions (MFD's) and state space realizations of encoders, decoders and syndrome formers, that exhibit large relevance in both fields. Nowadays their impact in coding analysis is at least as impressive as in system theory: since the early work of Massey,

[*] Dipartimento di Elettronica e Informatica dell'Università di Padova, Via Gradenigo 6/a, 35131 Padova, ITALY, fax: +39-049-827-7699, e-mail: ettore.fornasini@unipd.it

[†] Departamento de Matemática, Universidade de Aveiro, Aveiro, PORTUGAL, e-mail: raquel@mat.ua.pt

Sain, Costello [7,8] and Forney, state space representations and polynomial matrices techniques provide the basis for the most relevant convolutional coding literature (see, for instance, [1,9]). Moreover, from a conceptual point of view, the behavioral approach recently provided a common methodological framework for dynamical systems and convolutional codes, treated as families of trajectories subject to suitable constraints.

In this communication we give an account of some topics of common interest in both areas, and show how classical ideas and tools of system theory can provide very neat solutions. The paper is organized as follows. In the first part we introduce convolutional codes and encoders, and discuss to what extent MFD's allow to characterize some properties of the encoders and the structure of the code. Subsequently, the problem of describing the set of all minimal encoders of a given code is considered, and a bijective parametrization of its elements is presented. Moreover, a concrete realization of all minimal encoders is obtained, based on state feedback and static precompensation. Finally, duality methods allow a parametrization of all minimal syndrome formers and their realization by application of output injection and postcompensation.

2 Convolutional codes and their encoders

Let $\mathbb{F}$ be a finite field, and denote by

$$\mathbf{w} : \mathbb{Z} \to \mathbb{F}^p : t \mapsto \mathbf{w}_t$$

any *discrete time signal ("trajectory")* with values in $\mathbb{F}^p$. Clearly, $\mathbf{w}$ can be represented either as a bilateral sequence indexed in $\mathbb{Z}$ or as a bilateral formal power series with vector coefficients, $\hat{\mathbf{w}}(d) := \sum_t \mathbf{w}_t d^t$. In the sequel we shall use the sequence and the corresponding series interchangeably, depending on the problem we are dealing with.
The *concatenation* $\mathbf{w}^{(1)} \underset{\theta}{\circ} \mathbf{w}^{(2)}$ of two signals $\mathbf{w}^{(1)}$ and $\mathbf{w}^{(2)}$ at time θ is defined as follows

$$(\mathbf{w}^{(1)} \underset{\theta}{\circ} \mathbf{w}^{(2)})_t := \begin{cases} \mathbf{w}_t^{(1)} & \text{if } \ t < \theta; \\ \mathbf{w}_t^{(2)} & \text{if } \ t \geq \theta. \end{cases}$$

The definition of convolutional codes we refer to is based on the notion of (external) controllability, borrowed from behavior theory. N-controllability provides the conceptual description of very natural operations we like to perform on the codewords, and allows for synthesizing encoders and decoders via finite dimensional devices.

Definition 2.1 [10] *A set $\mathcal{B} \subseteq (\mathbb{F}^p)^{\mathbb{Z}}$ of trajectories is controllable if, given any two trajectories $\mathbf{w}^{(1)}$ and $\mathbf{w}^{(2)}$ in $\mathcal{B}$ and an arbitrary time instant θ, there exists a suitable $\mathbf{r} \in \mathcal{B}$ and $N \in \mathbb{N}$ such that $\mathbf{w}^{(1)} \underset{\theta}{\circ} \mathbf{r} \underset{\theta+N}{\circ} \mathbf{w}^{(2)} \in \mathcal{B}$. If N does not depend on $\mathbf{w}^{(1)}$, $\mathbf{w}^{(2)}$ and θ, $\mathcal{B}$ is N-controllable.*

The "universe" of all trajectories $(\mathbb{F}^p)^{\mathbb{Z}}$ is endowed with an $\mathbb{F}$-linear structure. Moreover the multiplication of a series $\hat{\mathbf{w}}(d) = \sum \mathbf{w}_t d^t$ by d (resp d^{-1}) induces the *one-step forward* (resp *backward*) *shift*,

$$\begin{aligned} \hat{\mathbf{w}}(d) &= \sum \mathbf{w}_t\, d^t \mapsto d\, \hat{\mathbf{w}}(d) = \sum \mathbf{w}_{t-1}\, d^t \\ \hat{\mathbf{w}}(d) &= \sum \mathbf{w}_t\, d^t \mapsto d^{-1}\, \hat{\mathbf{w}}(d) = \sum \mathbf{w}_{t+1}\, d^t \end{aligned}$$

A trajectory $\mathbf{w}$ is *left compact* if there exists $T \in \mathbb{Z}$ such that $\mathbf{w}_t = 0, \ \forall t < T$. Left compact trajectories are naturally represented by means of Laurent power series $\hat{\mathbf{w}}(d) = \sum \mathbf{w}_t d^t \in \mathbb{F}^p((d))$, and we are allowed to multiply a left compact support trajectory by an arbitrary scalar Laurent power series $s(d) = \sum_\tau s_\tau d^\tau$. Hence the set of left compact trajectories $\mathbb{F}^p((d))$ is isomorphic to the p-dimensional vector space $\mathbb{F}((d))^p$ over the field $\mathbb{F}((d))$.

Definition 2.2 *Let $p > m > 0, \quad p, m \in \mathbb{N}$. A $[p, m]$-convolutional code is an m-dimensional $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$, N-controllable for some $N \in \mathbb{N}$.*

The above definition highlights some “internal” properties of convolutional codes: the superposition of two codewords is again a codeword, backward and forward shift operators transform codewords into codewords, the “past” and the “future” of different codewords can be pasted into a new codeword, upon inserting a suitable block, whose length does not exceed a fixed value.

Interestingly enough, convolutional codes admit an equivalent characterization, based on the existence of polynomial or rational bases. For sake of brevity, we cannot present here a proof of this result, and refer the interested reader to [2]. We emphasize, however, the importance of its consequences, as $[p, m]$-convolutional codes exactly correspond to the output spaces of p-inputs, m-outputs linear sequential circuits (linear finite dimensional systems over a finite field), and their input-output maps are represented by rational (in particular, polynomial) transfer matrices with entries in $\mathbb{F}(d)$.

Proposition 2.3 *Let $\mathcal{C}$ be an m-dimensional $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$, $m < p$. The following are equivalent:*

(i) $\mathcal{C}$ is $[p, m]$ convolutional code, i.e. is N-controllable for some $N \in \mathbb{N}$;
(ii) $\mathcal{C}$ admits a polynomial basis $\hat{\mathbf{p}}_1(d), \dots, \hat{\mathbf{p}}_m(d) \in \mathbb{F}[d]^p$;
(iii) $\mathcal{C}$ admits a rational basis $\hat{\mathbf{g}}_1(d), \dots, \hat{\mathbf{g}}_m(d) \in \mathbb{F}(d)^p$. ■

Any $p \times m$ rational (in particular, polynomial) matrix $G(d) = [\,\hat{\mathbf{g}}_1(d) \quad \dots \quad \hat{\mathbf{g}}_m(d)\,]$ whose columns provide an $\mathbb{F}((d))$-basis for a $[p, m]$-convolutional code $\mathcal{C}$ is called an *encoder* of $\mathcal{C}$, and $\mathcal{C}$ is the *image of* $G(d)$, in the sense that

$$\mathcal{C} = \{\hat{\mathbf{w}}(d) : \hat{\mathbf{w}}(d) = G(d)\hat{\mathbf{u}}(d), \ \hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m\}.$$

Consequently, the encoders of $\mathcal{C}$ are injective rational transfer matrices, that associate to an arbitrary *information sequence* in $\mathbb{F}((d))^m$ a codeword in $\mathcal{C}$.

It is clear that a convolutional code admits infinitely many encoders, which amounts to say that infinitely many different rational input-output maps induce a bijection between the set of information sequences and the code. By definition, two full column rank rational matrices are *equivalent encoders* if the codes they generate are the same. If $G(d) \in \mathbb{F}(d)^{p \times m}$ is any encoder of a $[p, m]$ convolutional code $\mathcal{C}$, then

$$\hat{G}(d) = G(d)T(d) \tag{1}$$

parametrizes all the (rational) encoders of $\mathcal{C}$, as $T(d)$ ranges over the linear group $GL(m, \mathbb{F}(d))$ of nonsingular rational $m \times m$ matrices. Therefore two encoders are equivalent if and only if they differ each other by a rational nonsingular right factor.

If we restrict our attention to polynomial encoders, it is easy to prove that a code $\mathcal{C}$ admits

- right prime encoders (*basic encoders*). They are related each other via (1), where $T(d)$ describes the group of $m \times m$ polynomial unimodular matrices;

- right prime and column reduced [1] encoders (*canonical encoders*). The column degrees $\phi_i,\ i = 1, 2, \ldots, m$ of a canonical encoder coincide, up to a permutation, with those of any other encoder of the same kind. They are called *Forney indices of* $\mathcal{C}$, and $\deg\, \mathcal{C} := \sum_i \phi_i$ is, by definition, the *degree of the code.*

In the analysis of rational encoders, it is quite useful to consider their (right) matrix fraction descriptions

$$G(d) = N(d)D(d)^{-1}, \tag{2}$$

where $N(d) \in \mathbb{F}[d]^{p\times m}$ and $D(d) \in \mathbb{F}[d]^{m\times m}$. The numerator matrix $N(d)$ is again an encoder of $\mathcal{C}$ (just put $T(d) = D(d)$ in (1)). Moreover, if $N(d)D(d)^{-1}$ is an irreducible rMFD, $G(d)$ is a *causal encoder* if and only if $D(0)$ is nonsingular. A causal encoder induces a "nonanticipatory" input-output map, so that the samples of the information sequence that occur after time t do not affect the sample at t of the corresponding codeword .

Given a basic encoder $G_b(d) \in \mathbb{F}[d]^{p\times m}$ of $\mathcal{C}$, all equivalent encoders of $\mathcal{C}$ can be parametrized just by noticing that their MFD's are

$$\bar{G}(d) = [G_b(d)\Delta(d)][\bar{D}(d)]^{-1}, \tag{3}$$

where $\Delta(d)$ and $\bar{D}(d)$ are nonsingular $m \times m$ polynomial matrices.
In particular, since (3) is irreducible if and only if $\Delta(d)\bar{D}(d)^{-1}$ is irreducible too, all causal encoders of $\mathcal{C}$ are represented by (3), when $\Delta(d)\bar{D}(d)^{-1}$ is irreducible and $\bar{D}(0)$ is invertible.

3 Minimal encoders

A linear n-dimensional state space model $\Sigma = (A, B, C, J)$, with m inputs and p outputs

$$\begin{aligned}\mathbf{x}_{t+1} &= A\,\mathbf{x}_t + B\,\mathbf{u}_t \\ \mathbf{w}_t &= C\,\mathbf{x}_t + J\,\mathbf{u}_t\end{aligned}$$

realizes a causal encoder $G(d)$ of a $[p, m]$-convolutional code $\mathcal{C}$ if, starting from zero initial conditions, Σ encodes every information series $\hat{\mathbf{u}}(d)$ into the corresponding codeword $\hat{\mathbf{w}}(d) = G(d)\hat{\mathbf{u}}(d)$. This happens if and only if

$$G(d) = J + C(I - dA)^{-1}Bd.$$

q Given an irreducible right MFD $\tilde{N}(z)\tilde{D}(z)^{-1}$ of a causal transfer matrix $W(z)$ in the indeterminate $z = d^{-1}$, well established procedures exist [6] for obtaining minimal state space realizations. Moreover, if $\tilde{D}(z)$ is column reduced, with column degrees $k_1, k_2, \ldots, k_m$, the

[1] Recall that a full column rank $p \times m$ polynomial matrix $P(d)$ with column degrees $k_1, k_2, \ldots, k_m$ is column reduced if the *external degree* extdeg $(P) := \sum_{i=1}^m k_i$ coincides with the *internal degree* intdeg (P), i.e. with the maximum degree of its m-th order minors.

McMillan degree $\mu(W)$ of $W(z)$, i.e. the dimension of its minimal realizations, is given by

$$\mu(W) = k_1 + k_2 + \ldots + k_m \tag{4}$$

It wouldn't be very difficult to obtain a minimal realization algorithm working in the $\mathbb{F}[d]$ domain [2]. We prefer however to connect some results in the $\mathbb{F}[d]$ and $\mathbb{F}[z]$ domains by the following easy Lemma:

Lemma 3.1 *Suppose that $N(d)D(d)^{-1}$ is an irreducible MFD of $G(d)$, with $D(0)$ invertible and $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$ column reduced, having column degrees $k_1, k_2, \ldots k_m$.*
If we define

$$\begin{bmatrix} \tilde{N}(z) \\ \tilde{D}(z) \end{bmatrix} := \begin{bmatrix} N(d) \\ D(d) \end{bmatrix} \begin{bmatrix} d^{-k_1} & & & \\ & d^{-k_2} & & \\ & & \ddots & \\ & & & d^{-k_m} \end{bmatrix} \Big|_{z=d^{-1}}$$

then $\tilde{N}(z)\tilde{D}(z)^{-1}$ is an irreducible MFD of $W(z) := G(z^{-1})$, with $\deg \operatorname{col}_i \tilde{N} \leq \deg \operatorname{col}_i \tilde{D}$ *and $\tilde{D}(z)$ column reduced, having column degrees $k_1, k_2, \ldots, k_m$.*
Vice-versa, if $\tilde{N}(z)\tilde{D}(z)^{-1}$ is an irreducible MFD of $W(z)$ satisfying the above conditions and

$$\begin{bmatrix} N(d) \\ D(d) \end{bmatrix} := \begin{bmatrix} \tilde{N}(z) \\ \tilde{D}(z) \end{bmatrix} \begin{bmatrix} z^{-k_1} & & & \\ & z^{-k_2} & & \\ & & \ddots & \\ & & & z^{-k_m} \end{bmatrix} \Big|_{d=z^{-1}}$$

then $N(d)D(d)^{-1}$ is an irreducible MFD of $G(d) := W(d^{-1})$ with $D(0)$ invertible and $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$ column reduced, having column degrees $k_1, k_2, \ldots k_m$. ■

As an immediate consequence, if $N(d)D(d)^{-1}$ and $\tilde{N}(z)\tilde{D}(z)^{-1}$ are irreducible MFD's, in the indeterminates d and $z = d^{-1}$ respectively, of a causal encoder $G(d)$ and the matrices $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$ and $\tilde{D}(z)$ are column reduced, their column degrees $k_1, \ldots, k_m$ are the same, up to a permutation. Taking into account (4), we have proved the following Proposition:

Proposition 3.2 *Suppose that $N(d)D(d)^{-1}$ is an irreducible MFD of a causal encoder $G(d)$ and*

$$\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$$

is column reduced, with column degrees $k_1, k_2, \ldots, k_m$. Then the McMillan degree of $G(d)$ is given by $\mu(G) = \sum_{i=1}^{m} k_i$.

If $G_c(d)$ is a canonical encoder of $\mathcal{C}$, $G_c(d)(I_m)^{-1}$ is an irreducible MFD and $\begin{bmatrix} G_c(d) \\ I_m \end{bmatrix}$ is column reduced. Therefore the McMillan degree of a canonical encoder of $\mathcal{C}$ coincides with the degree of the code $\mathcal{C}$. Basing on this remark, we can show that the McMillan degree of the canonical encoders is minimum among the degrees of all causal encoders of $\mathcal{C}$.

Proposition 3.3 *The McMillan degree of a causal encoder of $\mathcal{C}$ is greater than or equal to* $\deg \mathcal{C}$*, and in case of canonical encoders coincides with* $\deg \mathcal{C}$*.*

Proof Any causal encoder $G(d)$ admits an irreducible right MFD

$$G(d) = [G_c(d)\Delta(d)]D(d)^{-1}$$

with $D(0)$ invertible. In case $\begin{bmatrix} D(d) \\ G_c(d)\Delta(d) \end{bmatrix}$ is not column reduced, we multiply it on the right by a suitable unimodular $V(d)$, so that

$$\begin{bmatrix} D(d)V(d) \\ G_c(d)\Delta(d)V(d) \end{bmatrix}$$

is column reduced, with column degrees $k_1, k_2, \dots, k_m$.
$[G_c(d)\Delta(d)V(d)](D(d)V(d))^{-1}$ is still an irreducible MFD of $G(d)$, and consequently

$$\begin{aligned} \sum_i k_i &= \text{extdeg}\begin{bmatrix} DV \\ G_c\Delta V \end{bmatrix} \\ &\geq \text{extdeg}(G_c\Delta V) \geq \text{intdeg}(G_c\Delta V) \\ &\geq \text{intdeg}(G_c) = \text{extdeg}(G_c) = \sum_i \phi_i \qquad \blacksquare \end{aligned}$$

The encoders of $\mathcal{C}$ having minimal McMillan degree are called *minimal encoders (of $\mathcal{C}$)*, and their set does not include only of canonical encoders. A characterization of all minimal encoders can be given in terms of their MFD's structure.

Proposition 3.4 *Let $G(d) \in \mathbb{F}(d)^{p\times m}$ be a causal encoder of $\mathcal{C}$. Then $G(d)$ is minimal if and only if it admits a right MFD of the form $G_c(d)D(d)^{-1}$, where $G_c(d)$ is a canonical encoder and the degree of each column of $D(d)$ does not exceed that of the corresponding column in $G_c(d)$.*

Proof Consider an irreducible right MFD $N(d)D(d)^{-1}$ of $G(d)$, with $\begin{bmatrix} D(d) \\ N(d) \end{bmatrix}$ column reduced. Then, by Proposition 3.2,

$$\mu(G) = \text{extdeg}\begin{bmatrix} D \\ N \end{bmatrix}.$$

On the other hand, $N(d)$ is also an encoder of $\mathcal{C}$, and hence $\mu(N) \geq \deg \mathcal{C}$.
By Proposition 3.3, $G(d)$ is minimal if and only if $\deg \mathcal{C} = \mu(G)$. If this equality holds, we have

$$\deg\ \mathcal{C} = \mu(G) = \text{extdeg}\begin{bmatrix} D \\ N \end{bmatrix} \geq \text{extdeg}(N) \geq \deg\ \mathcal{C},$$

which amounts to say that $N(d)$ is canonical and $D(d)$ has column degrees that do not exceed the corresponding ones in $N(d)$. $\blacksquare$

Proposition 3.4 shows that any minimal encoder of $\mathcal{C}$ can be represented by a right MFD whose numerator matrix is a canonical encoder. Next proposition presents a stronger result, namely that all minimal encoders of $\mathcal{C}$ can be represented as MFD's whose numerator is a *fixed* canonical encoder $G_c(d)$. The proof can be found in [2].

Proposition 3.5 *Let $G_c(d)$ be a canonical encoder of $\mathcal{C}$. All minimal encoders of $\mathcal{C}$ can be represented as*

$$G(d) = G_c(d)D(d)^{-1},$$

upon varying the denominator $D(d)$ in the set of all $m \times m$ polynomial invertible matrices such that $D(0)$ is nonsingular and the column degrees of $D(d)$ are not greater than the corresponding ones of $G_c(d)$. In particular, all polynomial minimal encoders of $\mathcal{C}$ are obtained by restricting $D(d)$ to unimodular matrices. ■

4 State feedback and minimal encoders

The purpose of this section is to show that all minimal encoders of $\mathcal{C}$ can be obtained from a minimal one, by applying static feedback and static precompensation to a minimal state realization of a canonical encoder $G_c(d)$.

Consider the minimal realization of $G_c(d)$ obtained via the procedure given below. For simplicity, we assume that all Forney indices ϕ_i are strictly positive; if not, minor adjustments are needed [2].

1. Define $J := G_c(0)$, $\bar{G}_c(d) := G_c(d) - J$, $n := \sum_i \phi_i$

2. Denote by M_i the $i \times i$ nilpotent Jordan block

$$M_i = \begin{bmatrix} 0 & & & \\ 1 & \ddots & & \\ & \ddots & 0 & \\ & & 1 & 0 \end{bmatrix},$$

   and introduce the following matrices

$$\begin{aligned} A &:= M_{\phi_1} \oplus M_{\phi_2} \oplus \ldots \oplus M_{\phi_m}, \\ B &:= [\, \mathbf{e}_1 \quad \mathbf{e}_{1+\phi_1} \quad \ldots \quad \mathbf{e}_{1+\phi_1+\ldots+\phi_{m-1}} \,], \end{aligned}$$

   of dimension $n \times n$ and $n \times m$, respectively.

3. Since

$$S(d) := (I_n - Ad)^{-1}dB = \begin{bmatrix} d & & & \\ \vdots & & & \\ d^{\phi_1} & & & \\ & d & & \\ & \vdots & & \\ & d^{\phi_2} & & \\ & & \ddots & \\ & & & d \\ & & & \vdots \\ & & & d^{\phi_m} \end{bmatrix},$$

there exists $C \in \mathbb{F}^{p \times n}$ such that

$$\bar{G}_c(d) = CS(d) = C(I_n - Ad)^{-1}dB.$$

Consequently $G_c(d) = J + C(I_n - Ad)^{-1}dB$, and (A, B, C, J) is a minimal realization of $G_c(d)$.

If a state feedback $K \in \mathbb{F}^{m \times n}$ is applied to Σ, the input sequence becomes the sum of an information sequence $\{\mathbf{u}_t\}$ and a feedback sequence $\{K\mathbf{x}_t\}$, and the equations of the state model modify into

$$\begin{aligned} \mathbf{x}_{t+1} &= A\mathbf{x}_t + B[\mathbf{u}_t + K\mathbf{x}_t] = [A + BK]\mathbf{x}_t + B\mathbf{u}_t \\ \mathbf{w}_t &= C\mathbf{x}_t + J[\mathbf{u}_t + K\mathbf{x}_t] = [C + JK]\mathbf{x}_t + J\mathbf{u}_t \end{aligned}$$

The series $\hat{\mathbf{x}}(d) := \sum_t \mathbf{x}_t d^t$, corresponding to the forced state evolution of $\Sigma^{(K)}$, and the information series $\hat{\mathbf{u}}(d) := \sum_t \mathbf{u}_t d^t$ are connected by $\hat{\mathbf{x}}(d) = (I_n - Ad)^{-1}dB(\hat{\mathbf{u}}(d) + K\hat{\mathbf{x}}(d))$, which implies

$$\hat{\mathbf{x}}(d) = (I_n - dA)^{-1}dB[I_m - K(I_n - dA)^{-1}dB]^{-1}\hat{\mathbf{u}}(d).$$

As the output $\hat{\mathbf{w}}(d) := \sum_t \mathbf{w}_t d^t$ is given by

$$(C + JK)\hat{\mathbf{x}}(d) + J\hat{\mathbf{u}}(d),$$

the transfer matrix of the feedback system $\Sigma^{(K)} = (A + BK, B, C + JK, J)$ is represented by the right MFD

$$\begin{aligned} G^{(K)}(d) &= [J + C(I_n - dA)^{-1}dB][I_m - K(I_n - dA)^{-1}dB]^{-1} \\ &= G_c(d)[I_m - KS(d)]^{-1}. \end{aligned}$$

As K varies in $\mathbb{F}^{m \times n}$, the matrix $(I_m - KS(d))$ describes all polynomial matrices in $\mathbb{F}^{m \times m}$ having I_m as constant term and the i-th column degree not greater than ϕ_i, $i = 1, 2, \ldots, m$.

If an invertible static precompensator $M \in \mathbb{F}^{m \times m}$ is applied to the input of $\Sigma^{(K)}$, the equations of the resulting state model become

$$\begin{aligned} \mathbf{x}_{t+1} &= [A + BK]\mathbf{x}_t + BM\mathbf{u}_t \\ \mathbf{w}_t &= [C + JK]\mathbf{x}_t + JM\mathbf{u}_t \end{aligned}$$

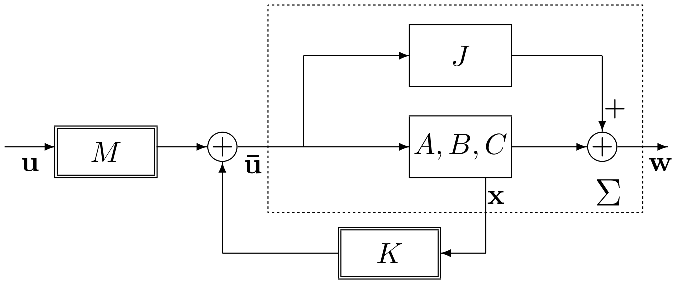

Fig. 1 – *Minimal encoders parametrization*

and the transfer matrix of the resulting system

$$\Sigma^{(K,M)} = (A + BK, BM, C + JK, JM)$$

is represented by the following right MFD

$$\begin{aligned} G^{(K,M)}(d) &= [J + C(I_n - dA)^{-1}dB] \\ &\quad \times [M^{-1} - M^{-1}K(I_n - dA)^{-1}dB]^{-1} \\ &= G_c(d)[M^{-1} - M^{-1}KS(d)]^{-1}. \end{aligned}$$

By Proposition 3.5, each minimal encoder of $\mathcal{C}$ is represented by $G(d) = G_c(d)D(d)^{-1}$, where $D(d) \in \mathbb{F}[d]^{m\times m}$ is an invertible matrix with column degrees not greater than the corresponding ones in $G_c(d)$ and $D(0)$ invertible. Hence it is possible to determine a unique precompensator $M = D(0)^{-1}$ and a unique state feedback matrix K such that

$$D(d) = M^{-1} - M^{-1}KS(d).$$

We summarize the above discussion in the following Proposition,

Proposition 4.1 *Let $G_c(d)$ be a canonical encoder of a $[p, m]$ convolutional code $\mathcal{C}$ of degree n. The set $\mathcal{M}$ of all minimal encoders of $\mathcal{C}$ is constituted by the transfer matrices of all systems*

$$\Sigma^{(K,M)} = (A + BK, BM, C + JK, JM),$$

obtained by application of static feedback and (nonsingular) precompensation to a minimal realization $\Sigma = (A, B, C, J)$ of $G_c(d)$. Therefore, the set of the pairs $(K, M) \in \mathbb{F}^{m\times n} \times$ $\mathrm{Gl}(m, \mathbb{F})$ biuniquely parametrizes $\mathcal{M}$. ■

5 Syndrome formers

To every m-dimensional $\mathbb{F}((d))$-subspace $\mathcal{C}$ of $\mathbb{F}((d))^p$ we associate the orthogonal subspace of $\mathbb{F}((d))^p$, of dimension $p - m$,

$$\mathcal{C}_\perp := \{\hat{\mathbf{v}}_\perp(d) \in \mathbb{F}((d))^p : \hat{\mathbf{v}}_\perp(d)^T\hat{\mathbf{w}}(d) = 0,\ \forall \hat{\mathbf{w}}(d) \in \mathcal{C}\}$$

If $\mathcal{C}$ is a convolutional code, it admits a polynomial basis $\hat{\mathbf{g}}_1(d), \dots, \hat{\mathbf{g}}_m(d) \in \mathbb{F}[d]^p$. Consequently, we can determine a polynomial basis $\hat{\mathbf{g}}_{1_\perp}(d), \dots, \hat{\mathbf{g}}_{(p-m)_\perp}(d) \in \mathbb{F}[d]^p$ of $\mathcal{C}_\perp$ and, by proposition 2.3, $\mathcal{C}_\perp$ is $\bar{N}$-controllable for some $\bar{N} \in \mathbb{N}$.
It is easy to see that $\mathcal{C}_\perp$ uniquely determines $\mathcal{C}$. Actually, if $G_\perp(d) \in \mathbb{F}(d)^{p\times(p-m)}$ is any encoder of $\mathcal{C}_\perp$, then

$$G_\perp(d)^T\hat{\mathbf{w}}(d) = 0 \Leftrightarrow \hat{\mathbf{w}}(d) \in \mathcal{C}$$

The rational matrix $S(d) := G_\perp(d)^T \in \mathbb{F}(d)^{(p-m)\times p}$ is called a syndrome former of $\mathcal{C}$, and $T(d)S(d)$ provides all syndrome formers of $\mathcal{C}$ as $T(d)$ varies on the group of nonsingular $(p - m) \times (p - m)$ rational matrices. Once a syndrome former $S(d)$ has been selected, for every $\hat{\mathbf{w}}(d) \in \mathbb{F}((d))^p$ the syndrome of $\hat{\mathbf{w}}(d)$ is given by $\hat{\mathbf{s}}(d) := S(d)\hat{\mathbf{w}}(d)$ and $\hat{\mathbf{w}}(d)$ is in $\mathcal{C}$ if and only if its syndrome is zero.

As syndrome formers of $\mathcal{C}$ are exactly the transpose of the encoders of $\mathcal{C}_{\perp}$, we may expect that a discussion on the syndrome formers structure could mirror that on the encoders of $\mathcal{C}$ in secs. 2-4. A preliminary, fundamental connection between syndrome formers and basic encoders of $\mathcal{C}$ is provided by the following lemma.

Lemma 5.1 [2] *Suppose that $G_b(d) \in \mathbb{F}[d]^{p\times m}$ is a basic encoder of $\mathcal{C}$. Select $C(d)$ in $\mathbb{F}^{p\times(p-m)}[d]$ so that $[\,G_b(d) \mid C(d)\,]$ is unimodular, and $D(d) \in \mathbb{F}[d]^{m\times p}$ and $S(d) \in \mathbb{F}[d]^{(p-m)\times p}$ so that*

$$\begin{bmatrix} D(d) \\ S(d) \end{bmatrix} [\,G_b(d) \mid C(d)\,] = I_p.$$

Then $S(d)$ is a basic *(i.e. left prime) syndrome former of $\mathcal{C}$, and its maximal order minors are equal, up to units, to the complementary maximal order minors of $G_b(d)$* ■

The above lemma has several interesting consequences. First of all, the degree of $\mathcal{C}_{\perp}$ is equal to the degree of $\mathcal{C}$, and column degrees $\psi_1, \dots, \psi_{p-m}$ of any canonical encoder of $\mathcal{C}_{\perp}$ satisfy

$$\sum_{i=1}^{p-m} \psi_i = \sum_{i=1}^{m} \phi_i = \deg\mathcal{C}.$$

Given any canonical encoder $G_{c_\perp}(d)$ of $\mathcal{C}_{\perp}$, its transpose $S_c(d) := G_{c_\perp}(d)^T$ is a polynomial syndrome former of $\mathcal{C}$, left prime and row reduced (with row degrees $\psi_1, \dots, \psi_{p-m}$), that will be called *canonical.* Consequently, all *minimal syndrome formers* of $\mathcal{C}$ have McMillan degree $\sum_{i=1}^{p-m} \psi_i$, and are biuniquely parametrized by the MFD's $Q(d)^{-1}S_c(d)$, as $Q(d)$ sweeps all $(p-m)\times(p-m)$ polynomial matrices with $\deg \mathrm{row}_i(Q) \leq \deg \mathrm{row}_i(S_c), i = 1, \dots, p-m$ and $Q(0)$ invertible.

Upon applying arbitrary output injection and static output compensation to a minimal state space realization of a canonical syndrome former $S_c(d)$ of $\mathcal{C}$, we obtain all minimal syndrome former of $\mathcal{C}$.

Actually, suppose that $\Sigma_{\perp} = (A_{\perp}, B_{\perp}, C_{\perp}, J_{\perp})$ is a minimal realization of the canonical encoder $S_c(d)^T$ of $\mathcal{C}_{\perp}$. Then the dual system $\Sigma = (A_{\perp}^T, C_{\perp}^T, B_{\perp}^T, J_{\perp}^T)$

$$\begin{aligned} \bar{\mathbf{x}}_{t+1} &= A_{\perp}^T \bar{\mathbf{x}}_t + C_{\perp}^T \mathbf{w}_t \\ \mathbf{s}_t &= B_{\perp}^T \bar{\mathbf{x}}_t + J_{\perp}^T \mathbf{w}_t \end{aligned}$$

provides a minimal realization of $S_c(d)$. An output injection $L\mathbf{s}_t$, $L \in \mathbb{F}^{n\times(p-m)}$, modifies the above equations as follows

$$\begin{aligned} \bar{\mathbf{x}}_{t+1} &= A_{\perp}^T\, \bar{\mathbf{x}}_t + C_{\perp}^T\, \mathbf{w}_t + L\mathbf{s}_t \\ &= (A_{\perp}^T + LB_{\perp}^T)\, \bar{\mathbf{x}}_t + (C_{\perp}^T + LJ_{\perp}^T)\, \mathbf{w}_t \\ \mathbf{s}_t &= B_{\perp}^T\, \bar{\mathbf{x}}_t + J_{\perp}^T\, \mathbf{w}_t \end{aligned}$$

and the transfer matrix of the resulting system $\Sigma^{(L)} = (A_{\perp}^T + LB_{\perp}^T,\ C_{\perp}^T + LJ_{\perp}^T,\ B_{\perp}^T, J_{\perp}^T)$ is given by

$$\begin{aligned} S^{(L)}(d) &= [I_{p-m} - B_{\perp}^T d(I_n - dA_{\perp}^T)^{-1}L]^{-1} \\ &\quad \times [B_{\perp}^T d(I_n - dA_{\perp}^T)^{-1}C_{\perp}^T + J_{\perp}^T] \\ &= [I_{p-m} - X(d)L]^{-1} S_c(d), \end{aligned}$$

where $X(d) := B_\perp^T d(I_n - dA_\perp^T)^{-1}$. If the minimal realization of $G_{c_\perp}(d)$ is obtained via the procedure of sec. 4, we have that $X(d) \in \mathbb{F}^{n\times(p-m)}$ has the following structure

$$\begin{bmatrix} d & \dots & d^{\psi_1} & & & & & & \\ & & & d & \dots & d^{\psi_2} & & & \\ & & & & & & \ddots & & \\ & & & & & & d & \dots & d^{\psi_{p-m}} \end{bmatrix}$$

and, consequently, the matrix $I_{p-m} - X(d)L$ describes all $(p-m)\times(p-m)$ polynomial matrices with constant term I_{p-m} and ith -row degree not greater than $\psi_i,\ i = 1,\dots,p{-}m$, as L varies in $\mathbb{F}^{n\times(p-m)}$.

Finally, if the output of $\Sigma^{(L)}$ is filtered through an invertible nondynamical system $N \in \mathbb{F}^{(p-m)\times(p-m)}$, we end up with a state space model $\Sigma^{(L,N)} = (A_\perp^T + LB_\perp^T,\ C_\perp^T + LJ_\perp^T,\ NB_\perp^T, NJ_\perp^T)$ of a new syndrome former, with equations

$$\begin{aligned} \bar{\mathbf{x}}_{t+1} &= (A_\perp^T + LB_\perp^T)\bar{\mathbf{x}}_t + (C_\perp^T + LJ_\perp^T)\mathbf{w}_t \\ \mathbf{s}_t &= NB_\perp^T\bar{\mathbf{x}}_t + NJ_\perp^T\mathbf{w}_t. \end{aligned}$$

and transfer matrix

$$\begin{aligned} S^{(L,N)}(d) &= [N^{-1} - B_\perp^T d(I_n - dA_\perp^T)^{-1}LN^{-1}]^{-1} \qquad (5) \\ &\quad \times [B_\perp^T d(I_n - dA_\perp^T)^{-1}C_\perp^T + J_\perp^T] \\ &= [N^{-1} - X(d)LN^{-1}]^{-1}S_c(d). \qquad (6) \end{aligned}$$

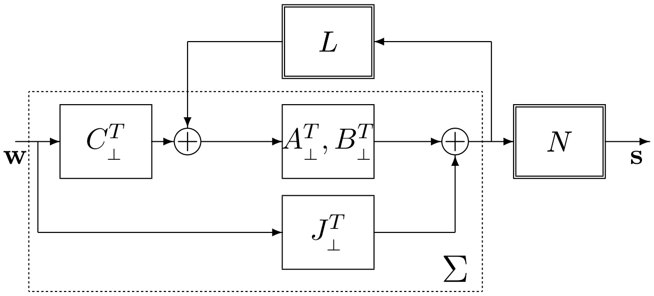

Fig. 2 – *Minimal syndrome formers parametrization*

Varying N in $Gl(p-m,\mathbb{F})$ and L in $\mathbb{F}^{n\times(p-m)}$, the denominator matrix $N^{-1} - X(d)LN^{-1}$ in (6) represents biuniquely a $(p-m)\times(p-m)$ invertible matrix $Q(d)$ with invertible constant term $Q(0)$ and column degrees not greater than the corresponding ones in $S_c(d)$. Hence (6) provides all minimal syndrome formers of $\mathcal{C}$.

6 Acknowledgements

R.Pinto has been supported by Fundacão para a Ciência e a Tecnologia, Portugal.

7 References

1. J.Feigenbaum, G.D.Forney, B.H.Marcus, R.J.McEliece (eds) *Codes and Complexity* Special Issue of IEEE Trans on Information Theory, vol 42, n.6, 1996
2. E.Fornasini, R.Pinto *Matrix Fraction Descriptions in Convolutional Coding*, submitted for publication, 2000
3. G.D.Forney *Convolutional Codes I: Algebraic Structure*, IEEE Trans On Inf.Theory, vol IT-16, pp. 720-38, 1970
4. G.D.Forney *Minimal Bases of Rational Vector Spaces, with Applications to Multivariable Systems*, SIAM J.Control, vol.13, pp. 493-520, 1975
5. G.D.Forney *Algebraic Structure of Convolutional Codes, and Algebraic System Theory*, in A.Antoulas "Mathematical System Theory", pp. 527-557, Springer-Verlag, Berlin-Heidelberg, 1991
6. T.Kailath *Linear Systems*, Englewood Cliffs, N.J.:Prentice Hall, 1980
7. J.L.Massey, M.K.Sain *Inverses of linear sequential circuits* IEEE Trans. Comput., vol C-17, pp.330-37, 1968
8. J.L.Massey, D.J.Costello *Nonsystematic convolutional codes for sequential decoding in space applications* IEEE Trans. Comm. Tecnol. vol COM-19, pp.806-13, 1971
9. R.J.McEliece *The Algebraic Theory of Convolutional Codes*, in Handbook of Coding Theory, vol. 1, V.S.Pless, W.C.Huffman, R.A.Brualdi eds., North Holland, Amsterdam,1998
10. J.Rosenthal, J.M.Schumacher, E.V.York *On behaviors and convolutional codes*, IEEE Trans On Inf.Theory, vol IT-42, pp. 1881-91, 1996