CODE DECOMPOSITION

E.Fornasini[†], R.Pinto[§]

March 5, 2004

keywords: 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, 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, $\hat{\mathbf{w}}(d) := \sum_t \mathbf{w}_t d^t$. We will use these two representations of a trajectory, 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 notions of (external) controllability and observability, borrowed from the behavioral approach to systems theory. These notions provide conceptual descriptions of very natural operations we like to perform on the *codewords* (i.e., on the encoded sequences), and are somehow connected with the "memory" of the system.

Definition 2.1 [10] *Let $\mathcal{B}$ be a subset of $(\mathbb{F}^p)^{\mathbb{Z}}$.*

1. *$\mathcal{B}$ is N-controllable (for some $N \in \mathbb{N}$) 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 $\mathbf{r} \in \mathcal{B}$ such that $\mathbf{w}^{(1)} \underset{\theta}{\circ} \mathbf{r} \underset{\theta+N}{\circ} \mathbf{w}^{(2)} \in \mathcal{B}$.*

2. *$\mathcal{B}$ is L-observable (for some $L \in \mathbb{N}$) if, given any two trajectories $\mathbf{w}^{(1)}$ and $\mathbf{w}^{(2)}$ in $\mathcal{B}$ such that $\mathbf{w}^{(1)}|_{[j,j+L)} = \mathbf{w}^{(2)}|_{[j,j+L)}$ for some $j \in \mathbb{Z}$, the concatenation $\mathbf{w}^{(1)} \underset{j}{\circ} \mathbf{w}^{(2)}$ is in $\mathcal{B}$.*

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 $\mathbb{F}((d))$.
When dealing with a family of left compact trajectories which corresponds to an $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$, controllability and observability are equivalent properties. Furthermore they are also equivalent to the existence of a polynomial or rational basis, as stated in the following Proposition.

Proposition 2.2 [2] *Let $\mathcal{B}$ be an m-dimensional $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$, $m < p$. The following are equivalent:*

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

This Proposition leads to our definition of convolutional code.

Definition 2.3 [2] *Let $p > m > 0$, $p, m \in \mathbb{N}$. A $[p,m]$-convolutional code is an m-dimensional $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$, N-controllable for some $N \in \mathbb{N}$ (or, equivalently, L-observable for some $L \in \mathbb{N}$).*

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; two codewords that coincide in a certain time interval can be "glued" in any time instant of this interval. Furthermore, $[p,m]$-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 $\mathbb{F}(d)$. 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. 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

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

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 and column reduced [1] encoders. These encoders are called *canonical*. The column degrees ϕ_i, $i = 1, 2, \dots, m$ 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

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

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 .

In the class of causal encoders of a $[p, m]$-convolutional code $\mathcal{C}$, the encoders that have realizations of minimal dimension (and, therefore, can be realized by linear sequential circuits with minimum number of delay elements) are called minimal. All minimal encoders of $\mathcal{C}$ can be represented as MFD's whose numerator matrix is a *fixed* canonical encoder, as stated in the next Proposition.

Proposition 2.4 [2] *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 $G_c(d)$. ■

3 Decoupled encoders and code decomposition

Let $G(d)$ be an encoder of a $[p, m]$-convolutional code $\mathcal{C}$ and $p_1, \dots, p_k$ be nonzero integers such that $\sum_{i=1}^k p_i = p$. $G(d)$ is $(p_1, \dots, p_k)$-decoupled if there exist positive integers $m_1, \dots, m_k$ with $\sum_{i=1}^k m_i = m$ such that, possibly up to a column permutation,

$$G(d) = \mathrm{diag}\{G_1(d), \dots, G_k(d)\},$$

with $G_i(d) \in \mathbb{F}(d)^{m_i\times p_i}$, $i = 1, \dots, k$.

Upon partitioning $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$ into $[\hat{\mathbf{u}}_1(d) \dots \hat{\mathbf{u}}_k(d)]$, $\hat{\mathbf{u}}_i(d) \in \mathbb{F}((d))^{m_i}$, we have

$$\hat{\mathbf{u}}(d)G(d) = [\hat{\mathbf{w}}_1(d) \dots \hat{\mathbf{w}}_k(d)],$$

with $\hat{\mathbf{w}}_i(d) = \hat{\mathbf{u}}_i(d)G_i(d)$, $i = 1, \dots, k$, and therefore

$$\mathcal{C} = \mathcal{C}_1 \times \dots \times \mathcal{C}_k \qquad (3)$$

where $\mathcal{C}_i$ is the $[p_i, m_i]$-convolutional code generated by $G_i(d)$. As consequence, the existence of a decoupled encoder of $\mathcal{C}$ is equivalent to the possibility of representing $\mathcal{C}$ as a direct sum of smaller convolutional codes $\mathcal{C}_i$.

The purpose of this section is to investigate the structure of the decoupled encoders of $\mathcal{C}$ and, in particular, of the minimal ones and to develop appropriate algorithms to compute direct summands

[1] Recall that a full column rank $p \times m$ polynomial matrix $P(d)$ with column degrees $k_1, k_2, \dots, k_m$ 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.

appearing in (3), starting from a set of generators of $\mathcal{C}$.

If $S_1, \ldots, S_k$ are $\mathbb{F}((d))-$subspaces of $\mathbb{F}((d))^m$, they are called independent if for every k-tuple

$$(\hat{\mathbf{w}}^{(1)}(d), \ldots, \hat{\mathbf{w}}^{(k)}(d)) \in S_1 \times \ldots \times S_k,$$

with $\hat{\mathbf{w}}^{(i)}(d) \neq 0$, $i = 1, \ldots, k,$, the series $\hat{\mathbf{w}}^{(1)}(d), \ldots, \hat{\mathbf{w}}^{(k)}(d)$ are linearly independent over $\mathbb{F}((d))$.

Definition 3.1 *A set of nonzero generators of $\mathbb{F}((d))^m$, $\mathcal{G} = \{\hat{\mathbf{v}}_1(d), \hat{\mathbf{v}}_2(d), \ldots, \hat{\mathbf{v}}_p(d)\}$ and a decomposition of $\mathbb{F}((d))^m$ in direct sum*

$$\mathbb{F}((d))^m = V_1 \oplus V_2 \oplus \ldots \oplus V_k, \tag{4}$$

are compatible if every vector of $\mathcal{G}$ belongs to a summand of (4) (and, obviously, to only one).

If a generator set $\mathcal{G}$ is compatible with (4), it is easy to check that

(i) $\mathcal{G}_i := V_i \cap \mathcal{G}$, *$i = 1, \ldots, k$, provide a partition of $\mathcal{G}$*

$$\mathcal{G} = \mathcal{G}_1 \,\dot{\cup}\, \mathcal{G}_2 \,\dot{\cup} \ldots \dot{\cup}\, \mathcal{G}_k$$

and $V_i = \operatorname{span}(\mathcal{G}_i)$, $i = 1, \ldots, k$.

(ii) if $\mathrm{B} := \{\hat{\mathbf{v}}_{i_1}(d), \ldots, \hat{\mathbf{v}}_{i_m}(d)\} \subset \mathcal{G}$ is a basis of $\mathbb{F}((d))^m$, the vectors of $\mathcal{G}_i$ are spanned by $\mathrm{B}_i := \mathcal{G}_i \cap \mathrm{B}$.

(iii) there exists a unique finest direct sum decomposition

$$\mathbb{F}((d))^m = \bar{V}_1 \oplus \bar{V}_2 \oplus \ldots \oplus \bar{V}_h \tag{5}$$

compatible with $\mathcal{G}$. Each summand of any other compatible decomposition of $\mathbb{F}((d))^m$ can be expressed as a suitable sum of some $\bar{V}_i$s in (5).

In order to obtain a partition of $\mathcal{G} = \{\hat{\mathbf{v}}_1(d), \ldots, \hat{\mathbf{v}}_p(d)\}$ associated with the finest decomposition (5), we introduce on $\mathcal{G}$ an equivalence relation as follows.
Let $\mathrm{B} \in \mathcal{G}$ be a basis of $\mathbb{F}((d))^m$, and denote by $\mathcal{M}_\nu$ the smallest subset of $\mathcal{B}$ such that $\hat{\mathbf{v}}_\nu(d) \in \operatorname{span}(\mathcal{M}_\nu)$. For any $\hat{\mathbf{v}}_i(d), \hat{\mathbf{v}}_j(d) \in \mathcal{G}$, $\hat{\mathbf{v}}_i(d) \sim \hat{\mathbf{v}}_j(d)$ if there exists a chain $\mathcal{M}_i = \mathcal{M}_{\nu_1}, \mathcal{M}_{\nu_2}, \ldots, \mathcal{M}_{\nu_h} = \mathcal{M}_j$ such that $\mathcal{M}_{\nu_l} \cap \mathcal{M}_{\nu_{l+1}} \neq \emptyset$, $l = 1, \ldots, h-1$. As a consequence, $\hat{\mathbf{v}}_i(d) \sim \hat{\mathbf{v}}_j(d)$ if and only if $\hat{\mathbf{v}}_i(d)$ and $\hat{\mathbf{v}}_j(d)$ belong to the same subspace in the finest compatible direct sum decomposition (5). It is easy to see that this equivalence relation is independent of the chosen basis. Therefore, to find the partition of $\mathcal{G}$ associated with (5) it is sufficient to determine the equivalence classes of $\sim$, which is done by the following algorithm.

Step 1: Select an $m \times m$ nonsingular submatrix $B(d)$ of $[\hat{\mathbf{v}}_1(d) \ldots \hat{\mathbf{v}}_p(d)]$ and put

$$V(d) = B(d)^{-1}[\hat{\mathbf{v}}_1(d) \ldots \hat{\mathbf{v}}_p(d)].$$

Step 2: Construct the $m \times p$ boolean matrix A defined by

$$A_{ij} = \begin{cases} 1 & \text{if } V_{ij} \neq 0 \\ 0 & \text{if } V_{ij} = 0 \end{cases}.$$

Step 3: Compute $(A^T A)^{p-1}$ and determine a permutation matrix $P \in \mathbb{F}^{p \times p}$ such that

$$P^T (A^T A)^{p-1} P = \operatorname{diag}\{N_1, \ldots, N_k\},$$

where $N_i = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} [1 \ \ \ldots \ \ 1] \in \mathbb{F}^{p_i \times p_i}$, $i = 1, \ldots, k$.

Step 4: Partitionate $[\hat{\mathbf{v}}_1(d) \ldots \hat{\mathbf{v}}_p(d)]P$ into

$$[L_1(d)| \ldots |L_h(d)],\ L_i(d) \in \mathbb{F}((d))^{m \times p_i},\ i = 1, \ldots, h.$$

Then $\mathcal{G}_i$, $i = 1, \ldots, h$, is the subset of $\mathcal{G}$ whose vectors are the columns of $L_i(d)$.

Proposition 3.2 *Let $\mathcal{G} = \{\hat{\mathbf{v}}_1(d), \ldots, \hat{\mathbf{v}}_p(d)\}$ be a set of nonzero generators of $\mathbb{F}((d))^m$. The above algorithm provides the partition of $\mathcal{G}$ associated with the finest compatible decomposition of $\mathbb{F}((d))^m$.*

Proof *We prove first that*

$$\hat{\mathbf{v}}_i(d) \sim \hat{\mathbf{v}}_j(d) \Longleftrightarrow (A^T A)^{p-1}_{ij} = 1. \tag{6}$$

Observe that

$$A_{ij} = 1 \Longleftrightarrow \hat{\mathbf{v}}_i(d) \in \mathcal{M}_j.$$

On the other hand, as $(A^T A)_{ij} = 1$ if and only if there exists $s \in \{1, \ldots, p\}$ such that $A_{si} = A_{sj} = 1$, we have

$$\begin{aligned}(A^T A)_{ij} = 1 \quad &\Longleftrightarrow \quad \exists\, \hat{\mathbf{v}}_s(d) \in \mathcal{G} : \ \hat{\mathbf{v}}_s(d) \in \mathcal{M}_i \cap \mathcal{M}_j \\ &\Longleftrightarrow \quad \mathcal{M}_i \cap \mathcal{M}_j \neq \emptyset,\end{aligned}$$

and, more generally, for all $n \in \mathbb{N}$, $(A^TA)^n_{ij} = 1$ if and only if there exist $\nu_2,\dots,\nu_n$ such that

$$(A^TA)_{i\nu_2} = (A^TA)_{\nu_2\nu_3} = \dots = (A^TA)_{\nu_n j} = 1$$

which is equivalent to the existence of $\nu_1 = i, \nu_2, \dots, \nu_n, \nu_{n+1} = j$ such that

$$\mathcal{M}_{\nu_l} \cap \mathcal{M}_{\nu_{l+1}} \neq \emptyset,\ \ l=1,\dots,n.$$

Consequently,

$$\hat{\mathbf{v}}_i(d) \sim \hat{\mathbf{v}}_j(d) \iff (A^TA)^k_{ij}=1,\quad \exists k. \tag{7}$$

Since $(A^TA)_{ii}=1,\ i=1,\dots,p$, we have also

$$(A^TA)^n_{ij}=1 \Longrightarrow (A^TA)^{n+1}_{ij}=1,\ \ \forall n\in\mathbb{N},\ \ \forall i,j. \tag{8}$$

On the other hand, $(A^TA)^n_{ij}=1$ implies that

$$(A^TA)^{n-1}_{ij}=1,\ \forall\, i,j\in\{1,\dots,p\},\ \forall n\ge p. \tag{9}$$

In fact, if $(A^TA)^n_{ij}=1$, there exist $\mathcal{M}_i = \mathcal{M}_{\nu_1}, \mathcal{M}_{\nu_2},\dots,\mathcal{M}_{\nu_{n+1}} = \mathcal{M}_j$ with $\mathcal{M}_{\nu_l}\cap\mathcal{M}_{\nu_{l+1}}\neq\emptyset$, $l=1,\dots,n$. As $|\mathcal{G}|=p$, there exist $k_1<k_2$ such that $\nu_{k_1}=\nu_{k_2}$, and $\mathcal{M}_i = \mathcal{M}_{\nu_1},\mathcal{M}_{\nu_2},\dots,\mathcal{M}_{\nu_{k_1}} = \mathcal{M}_{\nu_{k_2}},\dots,\mathcal{M}_{\nu_{n+1}}=\mathcal{M}_j$ satisfies $\mathcal{M}_{\nu_l}\cap\mathcal{M}_{\nu_{l+1}}\neq\emptyset$, $l=1,\dots,k_1-1$, $l=k_2,\dots,n$. This, together with (8) imply $(A^TA)^{n-1}_{ij}=1$.
(6) follows immediately from (7) and (9).
It is clear now that a permutation matrix $P\in\mathbb{F}^{p\times p}$ sorts the columns of $[\hat{\mathbf{v}}_1(d)\dots\hat{\mathbf{v}}_p(d)]$ according to the equivalence classes of $\sim$ if and only if

$$P^T(A^TA)^{p-1}P = \mathrm{diag}\{N_1,\dots,N_h\},$$

where $N_i = \begin{bmatrix}1\\ \vdots\\ 1\end{bmatrix}[1\dots1] \in \mathbb{F}^{p_i\times p_i},\ i=1,\dots,h$, and the equivalence classes of $\sim$ are constituted by the columns of $L_i(d)\in\mathbb{F}(d)^{m\times p_i}$, $i=1,\dots,h$, in

$$[L_1(d)\mid\dots\mid L_h(d)] = [\hat{\mathbf{v}}_1(d)\dots\hat{\mathbf{v}}_p(d)]P.$$

■

The partition of the columns of an encoder of $\mathcal{C}$, associated with the finest decomposition (5) of $\mathbb{F}((d))^m$, is a code property, in the sense that is the same for every encoder of $\mathcal{C}$. In fact, let $G(d)$ and $\tilde G(d)$ be two encoders of $\mathcal{C}$, $P\in\mathbb{F}^{p\times p}$ a permutation matrix, $p_1,\dots,p_k$ positive integers such that $\sum_{i=1}^k p_i = p$, and consider the column partitions

$$G(d)P = [G_1(d)|\dots|G_k(d)],$$

with $G_i(d)\in\mathbb{F}(d)^{m\times p_i}$, $i=1,\dots,k$,

$$\tilde G(d)P = [\tilde G_1(d)|\dots|\tilde G_k(d)],$$

with $\tilde G_i(d)\in\mathbb{F}(d)^{m\times p_i}$, $i=1,\dots,k$.
Since

$$\tilde G(d) = T(d)G(d)$$

for some nonsingular matrix $T(d)\in\mathbb{F}(d)^{m\times m}$, it follows that $\mathrm{rank}\ G_i(d) = \mathrm{rank}\ \tilde G_i(d)$, $i=1,\dots,k$, and

$$\mathbb{F}((d))^m = \mathrm{span}\ G_1(d)\oplus\dots\oplus\mathrm{span}\ G_k(d)$$

if and only if

$$\mathbb{F}((d))^m = \mathrm{span}\ \tilde G_1(d)\oplus\dots\oplus\mathrm{span}\ \tilde G_k(d).$$

Therefore, two equivalent encoders of $\mathcal{C}$ exhibit the same column partitions, compatible with the finest sum decomposition of $\mathbb{F}((d))^m$.

To find a parametrization of all minimal decoupled encoders of $\mathcal{C}$, we start by constructing a canonical decoupled one. Let $G_c(d)$ be a canonical encoder of $\mathcal{C}$, and consider the partition $G_c(d)P = [G_1(d)|\dots|G_k(d)]$, $G_i(d)\in\mathbb{F}[d]^{m\times p_i}$, with $\mathrm{rank}\ G_i(d) = m_i$, $i=1,\dots,k$, compatible with the finest sum decomposition of $\mathbb{F}((d))^m$. Select an $m_i\times p_i$ full rank submatrix of $G_i(d)$, $\tilde G_i(d)$, $i=1,\dots,k$ and factorize it into

$$\tilde G_i(d) = M_i(d)\bar G_i(d)$$

where $\bar G_i(d)\in\mathbb{F}[d]^{m_i\times p_i}$ is left prime, and $M_i(d)\in\mathbb{F}[d]^{m_i\times m_i}$ is a left maximal divisor of $\tilde G_i(d)$.
If $\hat{\mathbf{r}}(d)\in\mathbb{F}[d]^{1\times p_i}$ is any row of $G_i(d)$, there exists a rational row vector $\hat{\mathbf{x}}(d)$ such that

$$\hat{\mathbf{r}}(d) = \hat{\mathbf{x}}(d)\bar G_i(d)$$

and therefore $\hat{\mathbf{r}}(d)\bar G_i(d)^{-1} = \hat{\mathbf{x}}(d)$. As $\bar G_i(d)^{-1}$ is polynomial and right prime, $\hat{\mathbf{x}}(d)$ is polynomial too. Consequently,

$$G_i(d) = X_i(d)\bar G_i(d),\ X_i(d)\in\mathbb{F}[d]^{m\times m_i}.$$

and we have

$$G_c(d)P = [X_1(d)|\dots|X_k(d)]\mathrm{diag}\{\bar G_1(d),\dots,\bar G_k(d)\}.$$

As $\bar G_i(d)$, $i=1,\dots,k$, are left prime, so is $\mathrm{diag}\{\bar G_1(d),\dots,\bar G_k(d)\}$, which implies, in particular, that $[X_1(d)|\dots|X_k(d)]$ is unimodular.

For a suitable choice of $X_i(d)$, the submatrices $\bar{G}_i(d)$, $i = 1, \dots, k$, and therefore also $\operatorname{diag}\{\bar{G}_1(d), \dots, \bar{G}_k(d)\}$, are row reduced. Thus, $\operatorname{diag}\{\bar{G}_1(d), \dots, \bar{G}_k(d)\} = [X_1(d)| \dots |X_k(d)]^{-1} G_c(d) P$ is a canonical decoupled encoder of $\mathcal{C}$, and any other minimal decoupled encoder realizing the finest decomposition of $\mathcal{C}$ is given by

$$\begin{bmatrix} D_1(d) & & \\ & \ddots & \\ & & D_k(d) \end{bmatrix}^{-1} [X_1(d)| \dots |X_k(d)]^{-1} G_c(d) P =$$

$$= [X_1(d)D_1(d)| \dots |X_k(d)D_k(d)]^{-1} G_c(d) P,$$

where $D_i(d) \in \mathbb{F}[d]^{m_i \times m_i}$ is an invertible polynomial matrix, whose row degrees do not exceed the corresponding row degrees in $\bar{G}_i(d)$ and $D_i(0)$ is nonsingular.

4 Decoupled 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 $p - m$, $\mathcal{C}_\perp$.

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 2.2, $\mathcal{C}_\perp$ is a convolutional code.

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 with encoders, there can be considered decoupled syndrome formers.

Definition 4.1 *Let $p_1, \dots, p_k$ be positive integers such that $\sum_{i=1}^k p_i = p$. $S(d) \in \mathbb{F}(d)^{p \times (p-m)}$ is a $(p_1, \dots, p_k)$-decoupled syndrome former of $\mathcal{C}$ if there exist positive integers $m_1, \dots, m_k$ satisfying $\sum_{i=1}^k m_i = m$, such that, up to a row permutation*

$$S(d) = \begin{bmatrix} S_1(d) & & \\ & \ddots & \\ & & S_k(d) \end{bmatrix}, \quad S_i(d) \in \mathbb{F}(d)^{p_i \times (p_i - m_i)}.$$

Decoupled syndrome formers permit to more efficiently verify if a series $\hat{\mathbf{r}}(d) \in \mathbb{F}((d))^p$ belongs to $\mathcal{C}$. In fact, if $S(d)$ is a $(p_1, \dots, p_k)$-decoupled syndrome former as defined above, then $\hat{\mathbf{r}}(d) = [\hat{\mathbf{r}}_1(d) \cdots \hat{\mathbf{r}}_k(d)]$, $\hat{\mathbf{r}}_i(d) \in \mathbb{F}((d))^{p_i}$, $i = 1, \dots, k$, is in $\mathcal{C}$ if and only if $\hat{\mathbf{r}}_i(d) S_i(d) = 0$, $i = 1, \dots, k$.

The existence of $(p_1, \dots, p_k)$-decoupled syndrome formers of $\mathcal{C}$ is connected with the existence of $(p_1, \dots, p_k)$-decoupled encoders of $\mathcal{C}$, as shown in the next proposition.

Proposition 4.2 *A $[p, m]$-convolutional code $\mathcal{C}$ admits a $(p_1, \dots, p_k)$-decoupled encoder if and only if admits a $(p_1, \dots, p_k)$-decoupled syndrome former.*

Proof *Assume that $\mathcal{C}$ admits a $(p_1, \dots, p_k)$-decoupled encoder and let*

$$G(d) = \operatorname{diag}\{G_1(d), \dots, G_k(d)\} P^{-1}, \quad G_i(d) \in \mathbb{F}(d)^{m \times p_i},$$

with P a permutation matrix, be a canonical $(p_1, \dots, p_k)$-decoupled encoder of $\mathcal{C}$ (see Proposition ...).

Consider a syndrome former $S_i(d) \in \mathbb{F}(d)^{p_i \times (p_i - m_i)}$ of the $[p_i, m_i]$-convolutional code $\mathcal{C}_i$ generated by $G_i(d)$, $i = 1, \dots, k$. [2] *Then*

$$S(d) = P \operatorname{diag}\{S_1(d), \dots, S_k(d)\}$$

is a $(p_1, \dots, p_k)$-decoupled syndrome former of $\mathcal{C}$, as

$$G(d)S(d) = \operatorname{diag}\{G_1(d), \dots, G_k(d)\} \operatorname{diag}\{S_1(d), \dots, S_k(d)\} = 0.$$

Conversely, suppose that

$$S(d) = P \begin{bmatrix} S_1(d) & & \\ & \ddots & \\ & & S_k(d) \end{bmatrix}, \; S_i(d) \in \mathbb{F}(d)^{p_i \times (p_i - m_i)}, \; i = 1, \dots$$

[2] Observe that if $p_i = m_i$, i.e., if $G_i(d)$ is a full rank $m_i \times m_i$ matrix, its orthogonal subspace is the zero space, and therefore $\mathcal{C}_i$ does not admit syndrome formers. So, the decoupled syndrome former of $\mathcal{C}$, will not have the block matrix $S_i(d)$, but will have p_i zero rows between the blocks $S_{i-1}(d)$ and $S_{i+1}(d)$.

is a syndrome former of $\mathcal{C}$ and $G(d)$ is an encoder of $\mathcal{C}$. To see that $\mathcal{C}$ admits a $(p_1, \ldots, p_k)$-decoupled encoder it is enough to prove (see the algorithm on section 3) that if we consider the partition

$$G(d)P = [G_1(d)| \ldots |G_k(d)]$$

with $G_i(d) \in \mathbb{F}(d)^{m \times p_i}$, $i = 1, \ldots, k$, then $\operatorname{span} G_1(d) \oplus \ldots \oplus \operatorname{span} G_k(d) = \mathbb{F}((d))^m$.
Observe that $0 = G(d)S(d) = [G_1(d)| \ldots |G_k(d)]\operatorname{diag}\{S_1(d), ..., S_k(d)\}$, which implies that $G_i(d)S_i(d) = 0$, $i = 1, \ldots, k$.
Let $0 \neq \hat{\mathbf{w}}_i(d) \in$ span $G_i(d)$, i.e, $\hat{\mathbf{w}}_i(d) = G_i(d)\hat{\mathbf{a}}_i(d)$ for some $\hat{\mathbf{a}}_i(d) \in \mathbb{F}((d))^{p_i} \backslash \{0\}$, and $\alpha_i(d) \in \mathbb{F}((d))$, $i = 1, \ldots, k$. Since

$$\begin{aligned} & \alpha_1(d)\hat{\mathbf{w}}_1(d) + \ldots + \alpha_k(d)\hat{\mathbf{w}}_k(d) \\ = \; & \alpha_1(d)G_1(d)\hat{\mathbf{a}}_1(d) + \ldots + \alpha_k(d)G_k(d)\hat{\mathbf{a}}_k(d) \\ = \; & [G_1(d)| \ldots |G_k(d)] \begin{bmatrix} \alpha_1(d)\hat{\mathbf{a}}_1(d) \\ \vdots \\ \alpha_k(d)\hat{\mathbf{a}}_k(d) \end{bmatrix} \end{aligned}$$

we have that

$$\begin{aligned} & \alpha_1(d)\hat{\mathbf{w}}_1(d) + \ldots + \alpha_k(d)\hat{\mathbf{w}}_k(d) = 0 \\ \iff \; & G(d)P \begin{bmatrix} \alpha_1(d)\hat{\mathbf{a}}_1(d) \\ \vdots \\ \alpha_k(d)\hat{\mathbf{a}}_k(d) \end{bmatrix} = 0, \end{aligned}$$

which happens if and only if the rows of $\left(P \begin{bmatrix} \alpha_1(d)\hat{\mathbf{a}}_1(d) \\ \vdots \\ \alpha_k(d)\hat{\mathbf{a}}_k(d) \end{bmatrix} \right)^T$ belong to $\mathcal{C}_\perp$, i.e., if and only
if there exists $\hat{\mathbf{b}}_i(d) \in \mathbb{F}((d))^{p_i - m_i}$, $i = 1, \ldots, k$, such that

$$\left(P \begin{bmatrix} \alpha_1(d)\hat{\mathbf{a}}_1(d) \\ \vdots \\ \alpha_k(d)\hat{\mathbf{a}}_k(d) \end{bmatrix} \right)^T = [\hat{\mathbf{b}}_1(d) \cdots \hat{\mathbf{b}}_k(d)]S(d)^T$$

$$\Leftrightarrow P \begin{bmatrix} \alpha_1(d)\hat{\mathbf{a}}_1(d) \\ \vdots \\ \alpha_k(d)\hat{\mathbf{a}}_k(d) \end{bmatrix} = S(d) \begin{bmatrix} \hat{\mathbf{b}}_1(d) \\ \vdots \\ \hat{\mathbf{b}}_k(d) \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} \alpha_1(d)\hat{\mathbf{a}}_1(d) \\ \vdots \\ \alpha_k(d)\hat{\mathbf{a}}_k(d) \end{bmatrix} = \begin{bmatrix} S_1(d) & & \\ & \ddots & \\ & & S_k(d) \end{bmatrix} \begin{bmatrix} \hat{\mathbf{b}}_1(d) \\ \vdots \\ \hat{\mathbf{b}}_k(d) \end{bmatrix},$$

which is equivalent to $\alpha_i(d)\hat{\mathbf{a}}_i(d) = S_i(d)\hat{\mathbf{b}}_i(d)$, $i = 1, \ldots k$.
Then $\alpha_i(d)\hat{\mathbf{w}}_i(d) = \alpha_i(d)G_i(d)\hat{\mathbf{a}}_i(d) = G_i(d)S_i(d)\hat{\mathbf{b}}_i(d) = 0$, $i = 1, \ldots, k$, which implies that $\alpha_i(d) = 0$, $i = 1, \ldots, k$, as $\hat{\mathbf{w}}_i(d) \neq 0$, $i = 1, \ldots, k$, and therefore $\operatorname{span} G_1(d), \ldots, \operatorname{span} G_k(d)$ are independent. ■

5 Acknowledgements

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

6 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, 2003*
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*