Controlo 2014
Lecture Notes in Electrical Engineering p. 13-22
DOI: 10.1007/978-3-319-10380-8_2

Minimal State-Space Realizations of Convolutional Codes*

Telma Pinho[1], Raquel Pinto[1] and Paula Rocha[2]

[1] CIDMA, Department of Mathematics, University of Aveiro, Portugal
[2] CIDMA and Faculty of Engineering, University of Porto, Portugal

Abstract. In this work the minimality of state-space realizations of an input/output operator (encoder) and of the corresponding output behavior (code) are analyzed. Moreover, a procedure to obtain a minimal realization of a convolutional code starting from a minimal realization of an encoder of the code is provided.

1 Introduction

The problem of obtaining minimal state-space realizations for convolutional codes is a question of crucial importance not only due to implementation issues, but also because such realizations allow to construct codes with suitable properties, like, for instance, good error correcting capacity, [3].

State-space realizations for a convolutional code can be obtained via the realization of a corresponding encoder. However, since the same code admits encoders with different McMillan degrees (i.e., with different minimal state-space realization dimensions), an arbitrary choice of the encoder to be realized may lead to a non-minimal code realization.

This issue has been solved in [2, 5, 6], where a procedure to obtain all the minimal (McMillan degree) encoders of a code starting from an arbitrary encoder has been proposed. Such procedure allows obtaining a minimal state-space realization of a code starting from an arbitrary encoder $G(d)$ by first performing suitable transformations on $G(d)$ so as to obtain a minimal encoder $G^*(d)$, and then realizing $G^*(d)$ by a minimal state-space model. Although conceptually very elegant, this method implies dealing with polynomial matrices, which may constitute a drawback from the computational point of view.

Here we propose an alternative approach and provide a method to obtain a minimal realization of a convolutional code starting from a minimal realization of an arbitrary encoder of the code, and then, if necessary, reducing the dimension of this realization so as to obtain a minimal realization of the code. This only implies dealing with constant matrices.

* This work was supported by Portuguese funds through the CIDMA - Center for Research and Development in Mathematics and Applications, and the Portuguese Foundation for Science and Technology ("FCT – Fundação para a Ciência e a Tecnologia"), within project PEst-OE/MAT/UI4106/2014.

This paper is organized as follows: in the next section we present some preliminary results on convolutional codes and their encoders. In section 3, the realization problem is presented. Concretely, realizations of encoders and of codes are introduced and the minimality of such realizations is investigated. Our method is presented in section 4. Section 5 contains the concluding remarks.

2 Convolutional Codes and their Encoders

We consider convolutional codes constituted by sequences indexed by $\mathbb{Z}$ and taking values in $\mathbb{F}^n$, where $\mathbb{F}$ is a field. Such sequences $\{\mathbf{w}(i)\}_{i\in\mathbb{Z}}$ can be represented as elements of the set of bilateral formal power series over $\mathbb{F}^n$, denoted by $\mathcal{F}^n$, i.e.

$$\hat{\mathbf{w}}(d) = \sum_{i\in\mathbb{Z}} \mathbf{w}(i)d^i.$$

Note that $\mathcal{F}^n$ constitutes a module over the ring $\mathbb{F}[d]$ of polynomials in d over $\mathbb{F}$.

Given a subset $\mathcal{C}$ of the sequences indexed by $\mathbb{Z}$, taking values on $\mathbb{F}^n$, we denote by $\hat{\mathcal{C}}$ the subset of $\mathcal{F}^n$ defined by $\hat{\mathcal{C}} = \{\hat{w} : w \in \mathcal{C}\}$.

Definition 1. *A convolutional code $\mathcal{C}$ is a subset of sequences indexed by $\mathbb{Z}$ such that $\hat{\mathcal{C}}$ is a submodule of $\mathcal{F}^n$ which coincides with the image of $\mathcal{F}^k$ (for some $k \in \mathbb{N}$) by a polynomial matrix $G(d)$, i.e.,*

$$\hat{\mathcal{C}} = \text{Im } G(d) = \{\hat{\mathbf{w}}(d) = G(d)\hat{\mathbf{u}}(d),\ \hat{\mathbf{u}}(d) \in \mathcal{F}^k\};$$

with some abuse of language we also write $\mathcal{C} = \text{Im } G(d)$.

It can be shown that given a convolutional code $\mathcal{C}$ there always exist full column rank matrices $G(d) \in \mathbb{F}[d]^{n\times k}$ such that $\mathcal{C} = \text{Im } G(d)$. The *encoders* of $\mathcal{C}$ are here defined to be such matrices. This definition of encoder is slightly different from the one in [2] where non full column rank polynomial matrices are allowed as encoders. However, our definition is motivated by the fact that only full column rank encoders are relevant for the purpose of obtaining minimal realizations of a code.

3 Realization Problem

In this section we consider discrete time state-space models. A discrete-time state-space model is a description of a linear, discrete and time-invariant system through equations of the form

$$\begin{cases} \sigma x(t) = Ax(t) + Bu(t) \\ w(t) = Cx(t) + Du(t) \end{cases}, \tag{1}$$

where A, B, C and D are matrices over $\mathbb{F}$ of size $m \times m$, $m \times k$, $n \times m$ and $n \times k$, respectively; $\sigma x(t) = x(t+1)$, for all $t \in \mathbb{Z}$, u is the input-variable, w is

the output-variable and x is the state-variable. The system described by (1) will be denoted by $\Sigma(A, B, C, D)$, and its dimension is defined to be the dimension of the state space, i.e., m.

Depending on what type of situation we are interested in, these models can be viewed from different perspectives, namely as realizations of input/output relations (corresponding to encoders) or as realizations of output behaviors (corresponding to codes).

3.1 Realizations of Encoders

Definition 2. *$\Sigma(A, B, C, D)$ is said to be a realization of the encoder $G(d) \in \mathbb{F}[d]^{n\times k}$ if*

$$\begin{aligned}\mathcal{B}_{(u,w)} &:= \{(u, w) :\ \hat{w}(d) = G(d)\hat{u}(d)\} \\ &= \{(u, w) :\ \exists\, x \text{ s.t. } (u, x, w) \text{ satisfies } (1)\}.\end{aligned}$$

In this case we write $\Sigma(A, B, C, D) = \Sigma(G)$.

Note that the set $\mathcal{B}_{(u,w)}$ is what is known in the behavioral approach to systems and control [1] as the (external) input/output behavior associated with (1).

Note further that, since for bilateral sequences, $\widehat{\sigma x} = d^{-1}\hat{x}$, equations (1) are equivalent to

$$\begin{cases}\hat{x}(d) = Ad\hat{x}(d) + Bd\hat{u}(d) \\ \hat{w}(d) = C\hat{x}(d) + D\hat{u}(d)\end{cases}, \tag{2}$$

which, by eliminating the variable $\hat{x}$, yields:

$$\hat{w}(d) = \left(C(I_m - Ad)^{-1}Bd + D\right)\hat{u}(d).$$

Therefore $\Sigma(A, B, C, D)$ is a realization of the encoder $G(d)$ if and only if

$$G(d) = C(I_m - Ad)^{-1}Bd + D.$$

A polynomial encoder $G(d) \in \mathbb{F}[d]^{n\times k}$ admits many realizations with possibly different dimensions. Efficiency leads to focusing on obtaining realizations of minimal dimension.

Definition 3. *Let $G(d) \in \mathbb{F}[d]^{n\times k}$ be a polynomial encoder. $\Sigma(A, B, C, D)$ is said to be a minimal realization of $G(d)$ if no other realization of $G(d)$ has smaller dimension, i.e., if the size of the state x is minimal among all the realizations of $G(d)$. The minimal dimension of a realization of $G(d)$ is called the McMillan degree of $G(d)$ and is represented by $\mu(G)$.*

It is well known that the minimal realizations of an encoder $G(d) \in \mathbb{F}[d]^{n\times k}$ are characterized by being simultaneously observable and controllable[1] [4].

[1] Recall that $\Sigma(A, B, C, D)$ of dimension m is controllable if and only if $\operatorname{rank}\left[B \mid AB \mid \cdots \mid A^{m-1}B\right] = m$, or, equivalently, if and only if

3.2 Realizations of Convolutional Codes

Definition 4. *$\Sigma(A,B,C,D)$ is said to be a realization of the convolutional code $\mathcal{C}$ if*

$$\mathcal{B}_w := \{w : \mathbb{Z} \to \mathbb{F}^n | \exists\, x, u \text{ s. t. } (u,x,w) \text{ satisfies } (1)\} = \mathcal{C}.$$

This is denoted by $\Sigma(A,B,C,D) = \Sigma(\mathcal{C})$.

It is not difficult to see that a realization of an encoder of a convolutional code is also a realization of the corresponding code, however the converse is not true.

It turns out that a code $\mathcal{C}$ can be regarded as a behavior, the main object of study of the already mentioned behavioral approach developed by J.C. Willems [1]. The behaviors corresponding to codes constitute a particular class of behaviors, known as controllable behaviors, that are precisely sets of sequences that constitute the image of a polynomial shift-operator (in coding language, the encoder). Within the behavioral approach, a particular type of state-space representations for a behavior $\mathcal{B}$ have been introduced, called state/driving-variable (s/dv) representations, whose input is an auxiliary variable (the driving-variable); the behavior $\mathcal{B}$ corresponds to the output behavior of the s/dv model. Thus, the realizations of a code $\mathcal{C}$ are nothing else than s/dv realizations of the controllable behavior $\mathcal{B} = \mathcal{C}$.

Definition 5. *$\Sigma(\mathcal{C})$ is said to be a minimal realization of the code $\mathcal{C}$ if the size of (x,u) is minimal among all the realizations of $\mathcal{C}$. The minimal size of (x,u) is denoted by $\eta(\mathcal{C})$.*

A complete characterization for the minimality of code realizations is given by the conditions for the of minimality of s/dv realizations for controllable behaviors that can be derived from [Theorem 4.2, [1]], and are stated as follows using the terminology of codes.

Theorem 1. *[Theorem 4.2, [1]] A realization $\Sigma(A,B,C,D)$ of a convolutional code $\mathcal{C}$ is minimal if and only if the following conditions are satisfied.*

(i) $\begin{bmatrix} B \\ D \end{bmatrix}$ *has full column rank;*
(ii) (A,B) *is a controllable pair;*
(iii) $\ker D \subseteq \ker B$*, i.e., there exists a matrix L such that $B = LD$;*
(iv) Let L be as in (iii), and let Λ be a minimal left-annihilator (mla)[2] *of D. Then the pair $(A - LC, \Lambda C)$ is observable.*

---

rank $\begin{bmatrix} \lambda I_m - A \mid B \end{bmatrix} = m, \quad \forall \lambda \in \bar{\mathbb{F}}$. $\Sigma(A,B,C,D)$ is observable if and only if rank $\begin{bmatrix} C \\ CA \\ \vdots \\ CA^{m-1} \end{bmatrix} = m$, or, equivalently, if and only if rank $\begin{bmatrix} \lambda I_m - A \\ C \end{bmatrix} = m, \quad \forall \lambda \in$ $\bar{\mathbb{F}}$. Here $\bar{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$.

[2] Λ is a mla of D if $\Lambda D = 0$ and for all Λ^* such that $\Lambda^* D = 0$ there exists $\tilde{\Lambda}$ satisfying $\Lambda^* = \tilde{\Lambda}\Lambda$.

Remark 1. Note that (i) and (iii) are equivalent to (i') - D has full column rank - and (iii).

The next example shows that a minimal realization of an encoder $G(d)$ of a code $\mathcal{C}$ is not necessarily a minimal realization of the code $\mathcal{C}$.

Example 1. Consider the following polynomial encoder of a code $\mathcal{C}$

$$G(d) = \begin{bmatrix} 1+d-d^3 & -1+d^3 \\ d+d^2-d^3 & -1-d^2+d^3 \\ d+d^2 & -1-d-d^2 \end{bmatrix}.$$

It can be easily checked that

$$\Sigma\left(\begin{bmatrix} 0&0&0\\1&0&0\\0&1&0 \end{bmatrix}, \begin{bmatrix} 1&-1\\0&0\\0&-1 \end{bmatrix}, \begin{bmatrix} 1&0&-1\\1&1&-1 \end{bmatrix}, \begin{bmatrix} 1&-1\\0&-1\\0&-1 \end{bmatrix}\right)$$

is a realization of $G(d)$ which is controllable and observable and therefore is minimal. However $\Sigma(A,B,C,D)$ is not a minimal realization of $\mathcal{C}$, as not all the conditions of Theorem 1 are satisfied. Indeed, condition (iii) is fulfilled for

$$L = \begin{bmatrix} 1&0&0\\0&0&0\\0&0&1 \end{bmatrix};$$

however, considering the minimal left annihilator $\Lambda = \begin{bmatrix} 0 & 1 & -1 \end{bmatrix}$ of D, we have that

$$A - LC = \begin{bmatrix} -1&0&1\\1&0&0\\-1&0&0 \end{bmatrix} \quad \text{and} \quad \Lambda C = \begin{bmatrix} 0 & 0 & -1 \end{bmatrix},$$

are such that the pair $(A-LC, \Lambda C)$ is not observable.

$\Diamond$

Minimal encoders are defined as the ones for which a minimal realization is also minimal as a code realization; this is formalized in the following definition.

Definition 6. *Let $\mathcal{C} \subset \mathcal{F}^n$ be a convolutional code and $G(d) \in \mathbb{F}[d]^{n\times k}$ and encoder of $\mathcal{C}$. $G(d)$ is said to be a minimal encoder of $\mathcal{C}$ if*

$$\mu(G) + k = \eta(\mathcal{C}).$$

The situation illustrated in the previous example is due to the fact that when realizing an input/output operator (encoder) $G(d)$ one has no freedom in performing transformations in the input. This restriction is not present in the realization of the corresponding output behavior (code), where the input-variables may be transformed. Therefore, given a minimal realization of a non-minimal encoder $G(d)$, it is still possible to reduce its dimension in order to obtain a minimal realization of the corresponding code. This reduction procedure is carried out in the next section.

4 Minimal Code Realization Procedure

The following procedure shows precisely how to obtain a minimal realization $\tilde{\Sigma}(\mathcal{C}) = \tilde{\Sigma}(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})$ of a code $\mathcal{C}$ by performing operations and reducing the number of variables in a minimal realization $\Sigma(G) = \Sigma(A, B, C, D)$ of a corresponding encoder $G(d)$.

Let us consider a minimal realization $\Sigma(A, B, C, D)$ of $G(d)$. Then

$$\begin{aligned} G(d) &= C(I_m - Ad)^{-1}Bd + D \\ &= \left[C(I_m - Ad)^{-1}d \mid I_k\right] \begin{bmatrix} B \\ D \end{bmatrix}. \end{aligned}$$

Since encoders have full column rank, clearly $\begin{bmatrix} B \\ D \end{bmatrix}$ must have full column rank and hence condition (i) of Theorem 1 is satisfied. Moreover, the minimality of $\Sigma(A, B, C, D)$ as realization of the encoder $G(d)$ implies the controllability of the pair (A, B). Thus, a minimal realization of the encoder $G(d)$ satisfies condition (ii) of Theorem 1.

Suppose now that condition (iii) of the Theorem 1 is not satisfied i.e., $Ker\ D \not\subseteq KerB$. Then we can suppose, without loss of generality, that

$$D = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} B_1 & B_2 \end{bmatrix}, \tag{3}$$

with $B_2 = \begin{bmatrix} 0 \\ S \end{bmatrix}$ full column rank of size $m \times (k-r)$, where S is a square invertible matrix of size $k - r$, and $B_1 = \begin{bmatrix} B_{11} \\ B_{21} \end{bmatrix}$ of size $m \times r$ [3].
Therefore, (1) is of the form

$$\begin{cases} \sigma x_1 = A_{11}x_1 + A_{12}x_2 + B_{11}u_1 & \text{(4a)} \\ \sigma x_2 = A_{21}x_1 + A_{22}x_2 + B_{21}u_1 + Su_2 & \text{(4b)} \\ w_1 = C_{11}x_1 + C_{12}x_2 + Iu_1 & \text{(4c)} \\ w_2 = C_{21}x_1 + C_{22}x_2 & \text{(4d)} \end{cases}$$

where the variables x, u and w have been partitioned according to the given matrix partitions. Equations (4a-4d) show that x_2 is a free variable. Indeed, given x_2 and u_1, it is possible to find x_1, w_1 and w_2 such that equations (4a), (4c) and (4d) are satisfied. Moreover, since S is invertible, there exists u_2 such that (4b) holds. Therefore, this latter equation can be eliminated from the description of the code $\mathcal{C}$, and x_2 can assume the role of a driving variable. This means that

[3] If this is not the case, changes of coordinates in the u, x, w spaces allow bringing D and B to the desired form. The coordinate change in the w space modifies the code under consideration, but can be reversed at the end of the reasoning that will be presented.

$$\begin{cases} \sigma x_1 = A_{11}x_1 + \bar{B}\bar{u} \\ w = C_{11}x_1 + \bar{D}\bar{u} \end{cases}, \tag{5}$$

with $\bar{B} = \begin{bmatrix} A_{12} \; B_{11} \end{bmatrix}$, $\bar{u} = \begin{bmatrix} x_2 \\ u_1 \end{bmatrix}$ and $\bar{D} = \begin{bmatrix} C_{12} \; I \\ C_{22} \; 0 \end{bmatrix}$ is still a realization of the code with smaller dimension than the initial one (recall that the dimension of a code realization is defined as the size of the joint state and driving-variable vector).

Note that the new system obtained in (5) still satisfies the condition (ii) of Theorem 1 since if the pair

$$(A, B) = \left(\begin{bmatrix} A_{11} \; A_{12} \\ A_{21} \; A_{22} \end{bmatrix}, \begin{bmatrix} B_{11} \; 0 \\ B_{21} \; S \end{bmatrix} \right)$$

is controllable, then the pair

$$(A_{11}, \bar{B}) = \left(A_{11}, \begin{bmatrix} A_{12} \; B_{11} \end{bmatrix} \right)$$

is also controllable. Indeed the controllability condition

$$\text{rank} \; \begin{bmatrix} \lambda I_m - A \mid B \end{bmatrix} = m, \quad \forall \, \lambda \in \bar{\mathbb{F}},$$

becomes

$$\text{rank} \; \begin{bmatrix} \lambda I_{m_1} - A_{11} & -A_{12} & B_{11} \; 0 \\ -A_{21} & \lambda I_{m_2} - A_{22} & B_{21} \; S \end{bmatrix} = m_1 + m_2 = m, \quad \forall \lambda \in \bar{\mathbb{F}},$$

which implies that

$$\begin{aligned} \text{rank} \; \begin{bmatrix} \lambda I_{m_1} - A_{11} \mid A_{12} \mid B_{11} \end{bmatrix} &= \text{rank} \; \begin{bmatrix} \lambda I_{m_1} - A_{11} \mid -A_{12} \mid B_{11} \end{bmatrix} \\ &= m_1, \end{aligned}$$

meaning that $(A_{11}, \bar{B})$ is a controllable pair.

Moreover, in case $\begin{bmatrix} \bar{B} \\ \bar{D} \end{bmatrix}$ is not full column rank, there exists an invertible matrix T such that

$$\begin{bmatrix} \bar{B} \\ \bar{D} \end{bmatrix} T = \begin{bmatrix} \bar{\bar{B}} \; 0 \\ \bar{\bar{D}} \; 0 \end{bmatrix},$$

with $\begin{bmatrix} \bar{\bar{B}} \\ \bar{\bar{D}} \end{bmatrix}$ full column rank. Partitioning $T^{-1}\bar{u}$ accordingly as $T^{-1}\bar{u} = \begin{bmatrix} \bar{\bar{u}} \\ \tilde{u} \end{bmatrix}$, equations (5) become

$$\begin{cases} \sigma x_1 = A_{11}x_1 + \bar{\bar{B}}\bar{\bar{u}} \\ w = C_{11}x_1 + \bar{\bar{D}}\bar{\bar{u}}, \end{cases}, \tag{6}$$

which again yields a realization of the code $\mathcal{C}$ with smaller dimension as the previous one, that now satisfies condition (i) of Theorem 1.

Since

$$\left[\lambda I_{m_1} - A_{11} \mid \bar{\bar{B}} \mid 0\right] = \left[\lambda I_{m_1} - A_{11} \mid \bar{B}T\right] = \left[\lambda I_{m_1} - A_{11} \mid \bar{B}\right] \begin{bmatrix} I & 0 \\ 0 & T \end{bmatrix},$$

where I denotes the identity matrix of suitable size, and

$$\begin{aligned} \text{rank } \left[\lambda I_{m_1} - A_{11} \mid \bar{\bar{B}}\right] &= \text{rank } \left[\lambda I_{m_1} - A_{11} \mid \bar{\bar{B}} \mid 0\right] \\ &= \text{rank } \left[\lambda I_{m_1} - A_{11} \mid \bar{B}\right], \end{aligned}$$

the controllability of the pair $(A_{11}, \bar{B})$ implies that the pair $(A_{11}, \bar{\bar{B}})$ is controllable, and the realization (6) also satisfies condition (ii) of Theorem 1.

In case this realization does not satisfy condition (iii) of Theorem 1, the procedure can be restarted and repeated, yielding successive realizations of the code with smaller dimension, till a realization of the code is obtained that simultaneously satisfies conditions (i), (ii) and (iii). To avoid introducing too much notation, this realization will be again denoted by $\Sigma(A, B, C, D)$ (as the original one).

Suppose now that $\Sigma(A, B, C, D)$ does not satisfy condition (iv) of Theorem 1. From (1), and because condition (iii) is satisfied, we have that

$$\begin{cases} \sigma x = Ax + LDu \\ w = Cx + Du \end{cases}. \tag{7}$$

Since $Du = w - Cx$ implies $LDu = Lw - LCx$, (7) is equivalent to

$$\begin{cases} \sigma x = (A - LC)x + Lw \\ w = Cx + Du \end{cases}. \tag{8}$$

Let Λ be a *mla* of D with full row rank. Then, there exists a matrix X such that $V = \begin{bmatrix} X \\ \Lambda \end{bmatrix}$ is invertible and $VD = \begin{bmatrix} X \\ \Lambda \end{bmatrix} D = \begin{bmatrix} I_k \\ 0 \end{bmatrix}$. Let $\bar{w} := Vw = \begin{bmatrix} X \\ \Lambda \end{bmatrix} w$ be partitioned in the obvious way as $\bar{w} = \begin{bmatrix} \bar{w}_1 \\ \bar{w}_2 \end{bmatrix} = \begin{bmatrix} Xw \\ \Lambda w \end{bmatrix}$. It follows from (8) that

$$\begin{cases} \sigma x = (A - LC)x + LV^{-1}\bar{w} \\ \bar{w}_1 = XCx + u \\ \bar{w}_2 = \Lambda Cx \end{cases}. \tag{9}$$

The second equation of (9) shows that $\bar{w}_1$ is a free variable, which may be taken as a new driving-variable, replacing u. Letting V^{-1} be suitably partitioned as $\left[R\ Q\right]$, this yields

$$\begin{cases} \sigma x = (A - LC)x + LR\bar{w}_1 + LQ\bar{w}_2 \\ \bar{w}_2 = \Lambda Cx \end{cases}. \tag{10}$$

Since $\Sigma(A,B,C,D)$ does not satisfy condition (iv) of Theorem 1, the pair $(A-LC, \Lambda C)$ is not observable; thus by reducing equations (10) to the Kalman observability decomposition form through a coordinate change in the state-space, and eliminating the nonobservable states we obtain a description

$$\begin{cases} \sigma\bar{x} = \bar{A}\bar{x} + \bar{B}_1\bar{w}_1 + \bar{B}_2\bar{w}_2 \\ \bar{w}_2 = \bar{C}\bar{x} \end{cases}, \tag{11}$$

for the same set of $(\bar{w}_1, \bar{w}_2)$ trajectories as (10), where the size of the state $\bar{x}$ is smaller than the one of x.
Equations (11) can still be written as

$$\begin{cases} \sigma\bar{x} = (\bar{A} + \bar{B}_2\bar{C})\bar{x} + \bar{B}_1\bar{u}_1 \\ \bar{w}_1 = \bar{u}_1 \\ \bar{w}_2 = \bar{C}\bar{x} \end{cases}, \tag{12}$$

which, by noting that

$$w = V^{-1}\bar{w} = \begin{bmatrix} R\ Q \end{bmatrix} \begin{bmatrix} \bar{w}_1 \\ \bar{w}_2 \end{bmatrix} = R\bar{w}_1 + Q\bar{w}_2 = R\bar{u}_1 + Q\bar{C}\bar{x}$$

finally yields:

$$\begin{cases} \sigma\bar{x} = \bar{\bar{A}}\bar{x} + \bar{B}_1\bar{u}_1 \\ w = \bar{\bar{C}}\bar{x} + \bar{D}\bar{u}_1 \end{cases}, \tag{13}$$

with $\bar{\bar{A}} = \bar{A} + \bar{B}_2\bar{C}$, $\bar{\bar{C}} = Q\bar{C}$ and $\bar{D} = R$.

This is a state-space realization for the same code as Σ(A,B,C,D), but with smaller dimension.

If one of the conditions of Theorem 1 is not satisfied by the realization $\Sigma(\bar{\bar{A}}, \bar{B}, \bar{\bar{C}}, \bar{D})$, then one can perform the relevant steps described above, reducing each time the dimension of the code realization. In this way a minimal state/driving-variable realization of the initial code is obtained in a finite number of steps.

It is however worth mentioning the following. As we have just seen, the state-space system that satisfies all conditions of Theorem 1 obtained by this procedure (and that we once more denote by $\Sigma(A,B,C,D)$, with dimension m, by resetting the notation) is a minimal realization of $\mathcal{C}$. Nevertheless it can happen that $C(I_m - Ad)^{-1}Bd + D$ is no longer polynomial and hence is not an encoder of $\mathcal{C}$. In that case, due to the controllability of the pair (A,B), there exists a matrix K of suitable size such that $A - BK$ has only zero eigenvalues, and is therefore nilpotent. This implies that the square $(m \times m)$ polynomial matrix $M(d) := I_m - Ad$ is such that

$$\text{rank } M(\lambda) = m \quad \forall \lambda \in \bar{\mathbb{F}},$$

meaning that $\det M(d)$ must be a nonzero constant, or equivalently, that $M(d)$ is unimodular. Therefore, applying the feedback $u = \bar{u} - Kx$ to the system

$$\begin{cases} \sigma x = Ax + Bu \\ w = Cx + Du \end{cases} \tag{14}$$

yields the system

$$\begin{cases} \sigma x = (A - BK)x + B\bar{u} \\ w = (C - DK)x + D\bar{u} \end{cases} . \tag{15}$$

It can be shown that $\Sigma(A-BK, B, C-DK, D)$ is still a minimal realization of the code. Moreover, the polynomial matrix $G(d) = (C - DK)(I - d(A - BK))^{-1}Bd + D$ is a minimal encoder of the code.

5 Conclusion

In this paper we have analyzed the minimality of realizations of convolutional codes. It turns out that, when realizing an encoder (input/output operator) $G(d)$, one has no freedom in performing transformations in the input; however, this restriction is not present in the realization of the corresponding code (output behavior) $\mathcal{C} = \text{Im } G(d)$, where the input variables may be transformed. This can be exploited in order to reduce the dimension of the obtained state-space realizations. In this way, code realizations can have lower dimension than encoder realizations. Here we proposed a procedure that overcomes this problem and allows obtaining a minimal realization of a convolutional code starting from a minimal realization of an arbitrary encoder of the code.

Acknowledgment

We would like to thank Professor Ettore Fornasini for helpful discussions about this topic.

References

1. Willems, J. C.: Models for Dynamics.Dynamics Reported. 2,171–269 (1989)
2. Fornasini, E., Pinto,R.: Matrix Fraction Descriptions in Convolutional Conding, Linear Algebra and its Applications. 392, 119-158 (2004)
3. Rosenthal, J. and Schumacher, J. M.: A state space approach for constructing MDS rate $\frac{1}{n}$ convolutional codes, In: 1998 Information Theory Workshop, 116–117 (1998)
4. Kailath, T.: Linear Systems, Prentice Hall, Englewood Cliffs (1980)
5. Forney, G.: Convolutional Codes I: Algebraic Structure, IEEE Trans. Inform. Theory, 16(6), 720–738(1970)
6. Forney, G.: Minimal Bases of Rational Vector Spaces, with Applications to Multivariable Systems, SIAM J. Control. 493–520 (1975)