MTNS 2004
ISBN 90-5682-517-8

Bilateral Convolutional Codes Over a Finite Field

Ettore Fornasini
Department of Information Engineering
University of Padua, 35131 Padova, ITALY
E-mail: fornasini@dei.unipd.it

Raquel Pinto
Department of Mathematics
University of Aveiro, 3810-193 Aveiro, PORTUGAL
E-mail: raquel@mat.ua.pt

1 Introduction

Convolutional coding has been a common research area for coding and system theorists. This connection was first established by Massey and Sain, in the late 60's, when they described a convolutional encoder as a transfer function of a linear, time-invariant system, over a finite field [7]. In the early 70's, Forney reinforced this relation [4, 5] establishing the basis of a general algebraic theory of convolutional codes, which was strongly influenced by the algebraic theory of multivariable systems.
While systems theory studies the input/output relations of linear systems, coding theory concentrates on the set of output sequences, i.e., the code. The behavioral approach to systems theory, introduced by Willems [10], provided a common methodology framework for dynamical systems and convolutional codes, since a convolutional code is a linear, time-invariant behavior.
Convolutional codes over a finite field constituted by left compact sequences have been studied since many years [4, 5, 3, 6, 8]. In our previous work, we have also studied these codes. We have considered the behavioral approach to systems theory to present a new definition of a convolutional code over a finite field constituted by left compact sequences. In the analysis of the encoders of such codes, which are rational matrices, we used Matrix Fraction Descriptions (MFD's) and have characterized some properties of the encoders and the structure of the code. In the study of the minimal encoders of a convolutional code, we have constructed a simple parametrization of their MFD's and have obtained all minimal encoders of the code by application of static feedback and precompensation to a realization of a canonical one. These results are collected in [9].
In this communication, we extend these analysis to convolutional codes over a finite field constituted by bilateral sequences (bilateral convolutional codes). We give a definition of a bilateral convolutional code using the behavioral approach to systems theory and, next, we analyze the encoders of the code.

2 Bilateral convolutional codes

A dynamical system,

$$\Sigma = (\mathcal{T}, \mathcal{W}, \mathcal{B}),$$

models a phenomenon that evolves over the time set $\mathcal{T}$ and is described by *trajectories* that take values on $\mathcal{W}$. The set of all trajectories $\mathbf{w} \in \mathcal{W}^{\mathcal{T}}$ compatible with the laws of the system is called the *behavior* $\mathcal{B}$ [10].
Let us restrict to discrete-time systems, i.e., $\mathcal{T} = \mathbb{Z}$, over $\mathcal{W} = \mathbb{F}^p$, where $\mathbb{F}$ is a finite field and $p \in \mathbb{N}$. Any trajectory $\mathbf{w} : \mathbb{Z} \to \mathbb{F}^p : t \mapsto \mathbf{w}_t$ can also be represented as a *bilateral formal power series* with vector coefficients, $\hat{\mathbf{w}}(d) := \sum_{t\in\mathbb{Z}} \mathbf{w}_t d^t \in \mathcal{F}_\infty^p$. We will use these two representations of a trajectory, interchangeably, depending on the problem we are dealing with.

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

$$\hat{\mathbf{w}}(d) \mapsto d\,\hat{\mathbf{w}}(d) = \sum \mathbf{w}_{t-1}\, d^t \quad (\hat{\mathbf{w}}(d) \mapsto d^{-1}\,\hat{\mathbf{w}}(d) = \sum \mathbf{w}_{t+1}\, d^t).$$

A behavior $\mathcal{B} \in \mathcal{F}_\infty^p$ is *time-invariant* if it is closed under forward and backward shift. The time-invariant $\mathbb{F}$-subspaces of $\mathcal{F}_\infty^p$ are the $\mathbb{F}[d, d^{-1}]$-submodules of $\mathcal{F}_\infty^p$.
An important property of a behavior $\mathcal{B}$ is *completeness*, since it implies the existence of a mathematical representation of $\mathcal{B}$.

Definition 2.1 [10]: *A behavior $\mathcal{B}$ is said to be complete if when $\mathbf{w}|_I \in \mathcal{B}|_I$ for all $I \subset \mathbb{Z}$ then $\mathbf{w} \in \mathcal{B}$.*

The family of the complete, time-invariant $\mathbb{F}$-subspaces of $\mathcal{F}_\infty^p$ will be represented by $\mathbb{B}(\mathcal{F}_\infty^p)$.

The *concatenation* $\mathbf{w}^{(1)} \underset{\theta}{\circ} \mathbf{w}^{(2)}$ of two trajectories $\mathbf{w}^{(1)}$ and $\mathbf{w}^{(2)}$ at time θ is defined as follows

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

A fundamental notion for the definition of bilateral convolutional codes that we refer is *controllability*. Controllability of a behavior $\mathcal{B}$ is related with the "independence" of restrictions of $\mathcal{B}$ to time intervals that are sufficiently "separated".

Definition 2.2 [10]: *A behavior $\mathcal{B}$ 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*

$$\mathbf{w}^{(1)} \underset{\theta}{\circ} \mathbf{r} \underset{\theta+N}{\circ} \mathbf{w}^{(2)} \in \mathcal{B}.$$

As it is well known, controllable behaviors in $\mathbb{B}(\mathcal{F}_\infty^p)$ are the ones that admit an image representation, as stated on the following Proposition.

Proposition 2.1 [10]: *Let $\mathcal{B} \in \mathbb{B}(\mathcal{F}_\infty^p)$. The following are equivalent:*

i) $\mathcal{B}$ *is* N*-controllable, for some* $N \in \mathbb{N}$;

ii) there exists an integer $m \in \mathbb{N}$ *and a left prime matrix* $G(d, d^{-1}) \in \mathbb{F}[d, d^{-1}]^{m \times p}$ *such that*

$$\begin{aligned} \mathcal{B} &= \mathrm{Im}_\infty\, G(d, d^{-1}) \\ &= \{\hat{\mathbf{w}}(d) \in \mathcal{F}_\infty^p : \hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)\, G(d, d^{-1}),\ \hat{\mathbf{u}}(d) \in \mathcal{F}_\infty^m\}, \end{aligned}$$

where $\mathbb{F}[d, d^{-1}]$ *represents the ring of Laurent polynomials.*

Let $\mathcal{B} \in \mathbb{B}(\mathcal{F}_\infty^p)$ be N-controllable, for some $N \in \mathbb{N}$, and $\mathcal{B}^{\mathrm{fin}} := \mathcal{B} \cap \mathbb{F}[d, d^{-1}]^p$, i.e., $\mathcal{B}^{\mathrm{fin}}$ is constituted by the finite support sequences of $\mathcal{B}$. $\mathcal{B}^{\mathrm{fin}}$ is an $\mathbb{F}[d, d^{-1}]$-submodule of $\mathbb{F}[d, d^{-1}]^p$, and if $G(d, d^{-1}) \in \mathbb{F}[d, d^{-1}]^{m \times p}$ is a left prime matrix such that $\mathcal{B} = \mathrm{Im}_\infty\, G(d, d^{-1})$, then the rows of $G(d, d^{-1})$ constitute a basis of $\mathcal{B}^{\mathrm{fin}}$. Therefore, $\mathcal{B}^{\mathrm{fin}}$ is a free module, and therefore all basis of $\mathcal{B}^{\mathrm{fin}}$ have the same cardinality [1]. Moreover, all basis of $\mathcal{B}^{\mathrm{fin}}$ also generate $\mathcal{B}$, as stated in the following Proposition.

Proposition 2.2 [10, 2]: *Let* $\mathcal{B} \in \mathbb{B}(\mathcal{F}_\infty^p)$ *be* N*-controllable, for some* $N \in \mathbb{N}$*, such that* $\mathcal{B}^{\mathrm{fin}}$ *is an* $\mathbb{F}[d, d^{-1}]$*-submodule of* $\mathbb{F}[d, d^{-1}]^p$ *of dimension* m*. Then if* $G(d, d^{-1}) \in \mathbb{F}[d, d^{-1}]^{m \times p}$ *is a matrix whose rows constitute a basis of* $\mathcal{B}^{\mathrm{fin}}$*, then* $\mathcal{B} = \mathrm{Im}_\infty\, G(d, d^{-1})$.

Definition 2.3 *Let* $p > m > 0$, $p, m \in \mathbb{N}$. *A* $[p, m]$*-convolutional code* $\mathcal{C}$ *is an* N*-controllable element of* $\mathbb{B}(\mathcal{F}_\infty^p)$*, for some* $N \in \mathbb{N}$*, such that* $\mathcal{B}^{\mathrm{fin}}$ *is an* m*-dimensional* $\mathbb{F}[d, d^{-1}]$*-submodule of* $\mathbb{F}[d, d^{-1}]^p$.

So, from Proposition 2.1, bilateral convolutional codes admit an equivalent characterization as the image of Laurent polynomial matrices. The time-invariance of such codes implies the existence of polynomial (causal) matrices that generate the code, and consequently, bilateral $[p, m]$-convolutional codes correspond to the output spaces of m-input p-output linear sequential circuits (linear finite dimensional systems over a finite field). Moreover, as stated in the next Proposition, the N-controllability of a bilateral convolutional code $\mathcal{C}$ is connected with the degree of a polynomial matrix that generates $\mathcal{C}$ (i.e., with the degree of a basis of $\mathcal{C}^{\mathrm{fin}}$).

Proposition 2.3: *Let* $\mathcal{B} \in \mathbb{B}(\mathcal{F}_\infty^p)$. *The following are equivalent:*

i) $\mathcal{B}$ *is* N*-controllable;*

ii) there exists a polynomial matrix $P(d) = P_0 + P_1 d + P_2 d^2 + \cdots + P_N d^N \in \mathbb{F}[d]^{m \times p}$*, with* $P_N \neq 0$*, such that* $\mathcal{B} = \mathrm{Im}_\infty\, P(d) = \{\hat{\mathbf{w}}(d) \in \mathcal{F}_\infty^p : \hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d) P(d),\ \hat{\mathbf{u}}(d) \in \mathcal{F}_\infty^m\}$.

3 Encoders of a bilateral convolutional code

A bilateral $[p, m]$-convolutional code is the image of a map

$$\begin{array}{rccc} \chi: & \mathcal{F}_\infty^m & \to & \mathcal{F}_\infty^p \\ & \hat{\mathbf{u}}(d) & \mapsto & \hat{\mathbf{u}}(d) G(d, d^{-1}) \end{array}$$

where $G(d, d^{-1})$ is an $m \times p$ full rank Laurent matrix.
To allow the inverse operation, in order to recover the sent information sequence, the map χ must be injective, and χ is injective if and only if $G(d, d^{-1})$ is left prime.

Definition 3.1 *An encoder of a $[p, m]$-convolutional code $\mathcal{C} \subseteq \mathcal{F}_\infty^p$ is a left prime $m \times p$ Laurent polynomial matrix $G(d, d^{-1})$ such that $\mathcal{C} = \mathrm{Im}_\infty\, G(d, d^{-1})$.*

Equivalent encoders (i.e., encoders that generate the same code) differ by a Laurent unimodular left factor.

Restricting to causal encoders, we obtain the encoders over $\mathbb{F}[d]$. Minimal encoders are causal encoders which have a physical realization with minimum number of delay elements. Here we will show that all minimal encoders of a convolutional code are obtained fixing a polynomial encoder which is left prime and row reduced. We will also derive a parametrization similar to the one obtained for the case of codes formed by left compact sequences.

References

[1] P. Cohn. *Algebra, vol I.* John Wiley and Sons, Chichester, 1982.

[2] E. Fornasini. *Dispensa di Sistemi Multivariabili.* University of Padua, 2002.

[3] G. Forney. Algebraic Structure of Convolutional Codes, and Algebraic System Theory. In *Mathematical System Theory.*

[4] G. Forney. Convolutional Codes I: Algebraic Structure. *IEEE Trans. Inform. Theory*, 16:720–738, 1970. Correction, Ibid., IT-17,pp. 360, 1971.

[5] G. Forney. Structural Analysis of Convolutional Codes via Dual Codes. *IEEE Trans. Inform. Theory*, 19:512–518, 1973.

[6] R. Johannesson and K. Zigangirov. *Fundamentals of Convolutional Coding.* IEEE Press Series in Digital and Mobile Comm., 1999.

[7] J. Massey and M. Sain. Codes, Automata, and Continuous Systems: Explicit Interconnections. *IEEE Trans. Autom. Control*, 12(6):644–650, 1967.

[8] R. 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.

[9] R. Pinto. *Representações Matriciais Fraccionárias em Codificação Convolucional - Matrix Fraction Descriptions in Convolutional Coding.* Ph.D. dissertation, University of Aveiro, 2003.

[10] J. Willems. Models for Dynamics. *Dynamics Reported*, 2:171–269, 1988.