Some properties of linear recurrent error-control codes: A module-theoretic approach

Michel Fliess[‡,†]

[‡] **Centre de Mathématiques et Leurs Applications,**
École Normale Supérieure de Cachan
61 avenue du Président Wilson, 94235 Cachan, France
fliess@cmla.ens-cachan.fr

[†] **Laboratoire GAGE, École Polytechnique**
91128 Palaiseau, France

Abstract

We are extending to linear recurrent codes, *i.e.*, to time-varying convolutional codes, most of the classic structural properties of fixed convolutional codes. Those results are obtained thanks to a module-theoretic framework which has been developed in linear control.

Keywords: Linear recurrent codes, convolutional codes, linear systems, modules.

1 Introduction

This paper is devoted to various aspects of convolutional codes which are with linear block codes the most popular class of error-control codes. We are extending to linear recurrent codes, *i.e.*, to time-varying convolutional codes, most of the classic structural properties of fixed, *i.e.*, time-invariant, convolutional codes (see, *e.g.*, [3, 20, 25, 27]). Although Shannon's channel coding theorem has been extended to time-varying convolutional codes (see, *e.g.*, [32]) and not to fixed ones, those time-varying codes were much less utilised in practice than the time-invariant counterparts (see, nevertheless, [20]).

Our approach is another instance of the well known ties between convolutional codes and linear systems (see, *e.g.*, [4, 15, 16, 17, 18, 19, 20, 21, 25, 24, 28, 29, 30]). Our main mathematical tool is a particular module-theoretic setting for linear control [5, 7, 8, 11, 14], which has been quite useful in practice (see, *e.g.*, [12, 13]). We are utilising some elementary notions of difference algebra [2], homological algebra [31], and non-commutative algebra [23, 26], which is most natural in the time-varying case.

In the first part we define, following [20], *transducers*, *i.e.*, input-output systems, and study their main properties: state-variable representation, controllability, observability, transfer matrices, input-output inversion. In particular, an *encoder* is a right invertible transducer. The second part is devoted to codes. A code, here, is an equivalence class between encoders having the same output. We derive syndrome formers, dual codes, parity check matrices, polynomial and basic encoders, and Forney's theory in a manner which is often very short thanks to our algebraic framework.

2 Linear recurrent transducers

2.1 Algebraic preliminaries

2.1.1 Difference fields

A *difference field* [2] is a commutative field F, equipped with a *transformation* $\delta : F \to F$, *i.e.*, a monomorphism. Here δ should be understood as the *delay operator* of one unit of time. A *constant* is an element $c \in F$, such that $c\delta = c$ (mappings are written on the right). The *subfield of constants* of F is the subfield of all constant elements of F. A *field of constants* is a difference field which coincide with its subfield of constants. The *inversive closure* $F^{\maltese}$ [2] of F, which is unique up to isomorphism, is the smallest difference overfield of F such that δ is an isomorphism. The difference field F is said to be *inversive* if, and only if, $F = F^{\maltese}$.

Example 2.1 *Let $\mathbb{F}(t)$ be the field of rational functions in the indeterminate t over the field $\mathbb{F}$, a finite field for instance. With the $\mathbb{F}$-automorphism $\delta : \mathbb{F}(t) \to \mathbb{F}(t)$, $t \mapsto t - 1$, $\mathbb{F}(t)$ becomes an inversive difference field, where the subfield of constants is $\mathbb{F}$.*

2.1.2 A principal right ideal ring

The set of polynomials of the form

$$\sum_{\text{finie}} \delta^s a_s \tag{2.1}$$

$a_s \in F$, is a *principal right ideal ring* $F[\delta]$. It is commutative if, and only if, F is a field of constants.

2.2 Input-output system

A *system* is a finitely generated right $F[\delta]$-module, where F is an inversive difference field[1]. A *linear recurrent transducer*, or a *time-varying convolutional transducer*, or a *linear input-output system*, $\mathcal{T}$ is a system with the following properties:

- There is an *input*, *i.e.*, a finite subset $\boldsymbol{u} = (u_1, \ldots, u_k)$ of $\mathcal{T}$, such that the quotient module $\mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{u})$ is torsion. The input will be assumed to be *independent*, *i.e.*, the module $\mathrm{span}_{F[\delta]}(\boldsymbol{u})$ is free, of rank k.
- There is an *output*, *i.e.*, a finite subset $\boldsymbol{y} = (y_1, \ldots, y_n)$ of $\mathcal{T}$.
- The system $\mathcal{T}$ is *causal* (cf. [7]), or *nonanticipative*, *i.e.*, the semi-linear mapping[2] $\delta : \mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{u}) \to \mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{u})$ is injective.

[1] This assumption on F being inversive will simplify several further developments. It does not seem to bring any limitation from a practical viewpoint (see, *e.g.*,[20]).

[2] Consider a right $F[\delta]$-module M as a F-vector space. A mapping $\sigma : M \to M$ is said to be *semi-linear* if, and only if, the following to properties are satisfied:

1. $\forall m_1, m_2 \in M$, $(m_1 + m_2)\sigma = m_1\sigma + m_2\sigma$,

Example 2.2 *The transducer $y\delta = u$, i.e., $y(t-1) = u(t)$, where $k = n = 1$, should obviously be viewed as noncausal. It is also noncausal in our abstract setting. As a matter of fact the quotient module $\mathcal{T}/\mathrm{span}_{F[\delta]}(u)$ is a 1-dimensional F-vector space spanned by an element corresponding to $u(t+1)$, which is mapped to 0 by δ.*

When F is a field of constants, a linear recurrent transducer is called a *(fixed) convolutional transducer.*

2.3 State-variable representation

When viewed as a F-vector space, the finitely generated torsion module $\mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{u})$ is of finite dimension, m. Take a basis $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$. The next lemma is clear.

Lemma 2.1 *$\boldsymbol{\xi}\delta$ is also a basis.*

Corollary 2.1 *$\boldsymbol{\xi} = \boldsymbol{\xi}\delta\ A$, $A \in F^{m\times m}$, $\det(A) \neq 0$.*

Take in $\mathcal{T}$ a m-tuple $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_m)$ the image of which in $\mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{u})$ is $\boldsymbol{\xi}$. Then Corollary 2.1 yields a *generalized state-variable representation* of the transducer $\mathcal{T}$

$$\boldsymbol{\eta} = \boldsymbol{\eta}\delta\ A + \sum_{\mu=0}^{\nu} \boldsymbol{u}\delta^{\mu}\ \bar{B}_{\mu} \tag{2.2}$$

$$\boldsymbol{y} = \boldsymbol{\xi}\ \bar{C} + \sum_{\text{finite}} \boldsymbol{u}\delta^{\iota}\ \bar{D}_{\iota} \tag{2.3}$$

$\bar{B}_{\mu} \in F^{k\times m}$, $\bar{C} \in F^{m\times n}$, $\bar{D}_{\iota} \in F^{k\times n}$. Let $\boldsymbol{\xi}'$ be another basis of $\mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{u})$. Thus $\boldsymbol{\xi}' = \boldsymbol{\xi}P$, $P \in F^{m\times m}$, $\det(P) \neq 0$. Take a m-tuple $\boldsymbol{\eta}' = (\eta'_1, \ldots, \eta'_m)$ in $\mathcal{T}$ the image of which in $\mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{u})$ is $\boldsymbol{\xi}'$. Then

$$\boldsymbol{\eta}' = \boldsymbol{\eta} + \sum_{\text{finite}} \boldsymbol{u}\delta^{\iota}\ Q_{\iota} \tag{2.4}$$

$Q \in F^{k\times m}$. Note that (2.4) is input-dependent. If in (2.2) $\nu \geq 2$ and $\bar{B}_{\nu} \neq 0$, set

$$\boldsymbol{\eta} = \tilde{\boldsymbol{\eta}} - \boldsymbol{u}\delta^{\nu-1}\ (\bar{B}_{\nu}A^{-1}\delta^{-1})$$

It yields

$$\tilde{\boldsymbol{\eta}} = \tilde{\boldsymbol{\eta}}\delta\ A + \sum_{\mu=0}^{\nu-1} \boldsymbol{u}\delta^{\mu}\ \tilde{B}_{\mu}$$

If $\bar{B}_0 \neq 0$, setting

$$\tilde{\boldsymbol{\eta}} = \overline{\boldsymbol{\eta}} + \boldsymbol{u}\ \bar{B}_0$$

2. $\forall a \in F$, $\forall m \in M$, $(ma)\sigma = (m\sigma)(a\sigma)$.

If F is a field of constants, σ is a F-linear mapping.

yields

$$\overline{\boldsymbol{\eta}} = \overline{\boldsymbol{\eta}}\delta + \sum_{\mu=1}^{\nu-1} \boldsymbol{u}\delta^{\mu} \ \overline{B}_{\mu}$$

We have proved the following time-varying generalisation of [7]:

Theorem 2.1 *A causal linear recurrent transducer may be given the* Kalman state-variable representation

$$\begin{aligned} \boldsymbol{x} &= \boldsymbol{x}\delta \ A + \boldsymbol{u}\delta \ B \qquad (2.5) \\ \boldsymbol{y} &= \boldsymbol{x} \ C + \sum_{\text{finie}} \boldsymbol{u}\delta^{\iota} \ D_{\iota} \qquad (2.6) \end{aligned}$$

where $\boldsymbol{x} = (x_1, \ldots, x_m)$*,* $m = \dim_F(\mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{u}))$*,* $A \in F^{m\times m}$*,* $\det A \neq 0$*,* $B \in F^{k\times m}$*,* $C \in F^{m\times n}$*,* $D_{\iota} \in F^{k\times m}$*.*

Remark 2.1 *Setting* $\boldsymbol{x} = \bar{\boldsymbol{x}} - \boldsymbol{u} \ (BA^{-1}\delta^{-1})$ *yields* $\bar{\boldsymbol{x}} = \bar{\boldsymbol{x}}\delta \ A + \boldsymbol{u} \ (BA^{-1}\delta^{-1})$ *which might also be interesting in some applications.*

2.4 Controllability and observability

2.4.1 Controllability

The transducer $\mathcal{T}$ is called *controllable* if, and only if, the module $\mathcal{T}$ is free. The next result, which is a discrete-time version of [5], is an extension to (2.5) of the classic Kalman controllability criterion (compare with [33]):

Proposition 2.1 *The transducer* $\mathcal{T}$ *is controllable if, and only if, the matrix*

$$\left(B, B\delta A, \ldots, B(\delta A)^{m-1}\right)$$

is of rank m*.*

Proof It is easy to check that $\mathrm{rk}(B, B\delta A, \ldots, B(\delta A)^{m-1}) < m$ is equivalent to the existence of a nontrivial torsion submodule of $\mathcal{T}$.

2.4.2 Observability

The transducer $\mathcal{T}$ is called *observable* if, and only if, the modules $\mathcal{T}$ and $\mathrm{span}_{F[\delta]}(\boldsymbol{u}, \boldsymbol{y})$ coincide. The next result, which is a discrete-time version of [5], is an extension to (2.5-2.6) of the classic Kalman observability criterion (compare with [33]):

Proposition 2.2 *The transducer* $\mathcal{T}$ *is observable if, and only if, the matrix*

$$\begin{pmatrix} C \\ C\delta A^{-1} \\ \vdots \\ C(\delta A^{-1})^{m-1} \end{pmatrix}$$

is of rank m*.*

Proof Utilize $\boldsymbol{x}\delta = \boldsymbol{x}\ A^{-1} - \boldsymbol{u}\delta\ BA^{-1}$ for expressing $\boldsymbol{y}\delta^{\iota}$, $\iota = 1, \ldots, m-1$, as F-linear combinations of the components of $\boldsymbol{x}$ and $\boldsymbol{u}\delta^{\kappa}$, $\kappa \geq 0$.

Remark 2.2 *By utilizing the inverse $A\delta^{-1}$ of δA^{-1}, the Kalman observability criterion becomes*

$$\mathrm{rk} \begin{pmatrix} C \\ C\delta^{-1}A\delta^{-1} \\ \vdots \\ C(A\delta^{-1})^{m-1} \end{pmatrix} = m$$

2.5 Transfer matrices

2.5.1 Definition

Let $F(\delta)$ be the quotient field of $F[\delta]$ which is a right Ore ring. The $F(\delta)$-vector space $\hat{\mathcal{T}} = \mathcal{T} \otimes_{F[\delta]} F(\delta)$ is called the *transfer vector space* of $\mathcal{T}$ [8]. The $F[\delta]$-linear mapping $\mathcal{T} \rightarrow \hat{\mathcal{T}}$, $\tau \mapsto \hat{\tau} = \tau \otimes 1$, is the *(formal) Laplace transform* [8]. Its kernel is the torsion submodule of T. It is thus injective if, and only if, the module F is free. As $\boldsymbol{u}$ is independent, $\hat{\boldsymbol{u}} = (\hat{u}_1, \ldots, \hat{u}_k)$ is a basis of $\hat{\mathcal{T}}$. It yields

$$\hat{\boldsymbol{y}} = (\hat{y}_1, \ldots, \hat{y}_n) = \hat{\boldsymbol{u}}\ G \tag{2.7}$$

where $G \in F(\delta)^{m \times n}$ is the *rational transfer matrix*, or the *rational generating matrix*, of the transducer (compare with [22]). When $k = n = 1$, G is called a *rational transfer*, or *generating*, *function*.

Any element of $F(\delta)$ may be written as a Laurent series $\sum_{\nu \geq \nu_0} \delta^{\nu} a_{\nu}$, $a_{\nu} \in F$, $\nu_0 \in \mathbb{Z}$. It is said to be *causal* if, and only if, $\nu_0 \geq 0$. The matrix G is said to be *causal* if, and only if, all its entries are causal.

Theorem 2.2 *Any causal linear recurrent transducer possesses a rational causal transfer matrix. Conversely, any rational causal matrix is the transfer matrix of a causal linear recurrent transducer, which is controllable and observable.*

Proof The first part is an immediate consequence of the definition of causality in subsection 2.2 and of the input-output relation (2.7). For the second part, utilize the right coprime factorization $G = ND^{-1}$, $N \in F[\delta]^{k \times n}$, $D \in F[\delta]^{n \times n}$, where D is invertible (see [8]). The transfer matrix of the transducer $\boldsymbol{y}D = \boldsymbol{u}N$, which is both controllable and observable (see [8]), is G.

2.5.2 Interconnection

Let $h_{\upsilon} : \Sigma \rightarrow \mathcal{S}_{\upsilon}$, $\upsilon \in \Upsilon$, be a morphism of systems, *i.e.*, of finitely generated right $F[\delta]$-modules. The corresponding fibered sum is a *system interconnection* (cf. [10]). Parallel and series interconnections are particular instances of system interconnections. The proof of the following result is straightforward.

Proposition 2.3 *The transfer matrix of the parallel (resp. series) interconnection of linear recurrent transducers is the sum (resp. product) of the transfer matrices.*

Remark 2.3 *Interconnections as simple as those in Proposition 2.3 may lead to a lost of controllability or observability*[3] *which is not readable via transfer matrices [10].*

2.6 Input-output inversion

2.6.1 General results

The *output rank* of the transducer $\mathcal{T}$ is $\varrho = \mathrm{rk}(\mathrm{span}_{F[\delta]}(\boldsymbol{y}))$. Obviously, $0 \leq \varrho \leq \min(k, n)$. The transducer $\mathcal{T}$ is said to be *right invertible* (resp. *left invertible*) if, and only if, $\varrho = k$ (resp. $\varrho = n$).

Proposition 2.4 *$\mathcal{T}$ is right invertible, if and only if, the quotient module $\mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{y})$ is torsion.*

Proof We have $\mathrm{rk}(\mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{y})) = \mathrm{rk}(\mathcal{T}) - \varrho$. Since $\mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{u})$ is torsion, $\mathrm{rk}(\mathcal{T}) = \mathrm{rk}(\mathrm{span}_{F[\delta]}(\boldsymbol{u})) = k$. Thus $\mathrm{rk}(\mathcal{T}/\mathrm{span}_{F[\delta]}(\boldsymbol{y})) = 0$ if, and only if, $\varrho = k$.

In a more down to earth language, Lemma 2.4 means that $\boldsymbol{u}$ may be obtained from $\boldsymbol{y}$ thanks to difference equations. The example $y = u\delta$, where $k = n = 1$, shows that the right inverse transducer is not generally causal. Left invertibility means that the components of $\boldsymbol{y}$ are $F[\delta]$-linearly independent.

The next results are clear.

Proposition 2.5 *The linear recurrent transducer $\mathcal{T}$ is right (resp. left) invertible if, and only if, its transfer matrix is right (resp. left) invertible.*

Corollary 2.2 *If the linear recurrent transducer $\mathcal{T}$ is right (resp. left) invertible, then $n \geq k$ (resp. $n \leq k$).*

If $k = n$, the transducer is said to be *square*. Then right and left invertibilities coincide. An *invertible* square transducer is right and left invertible.

2.6.2 Encoders

A linear recurrent transducer, which is right invertible, is called a *linear recurrent encoder*, or a *(time-varying) convolutional encoder*. If F is a field of constants, it is called a *(fixed) convolutional encoder*[4]. A square encoder is called a *linear recurrent encrypter*.

[3] The continuous-time examples in [10] (see also the references therein) may trivially be adapted to our discrete-time context.

[4] Even if F is a finite field, the existing literature does not seem to propose a unique definition of convolutional encoders.

2.7 Some useful constructions

2.7.1 Blocking

For any integer $\Omega > 1$, $F[\delta^\Omega] \subset F[\delta]$. Thus any right $F[\delta]$-module $\boldsymbol{M}$ may also be viewed as a right $F[\delta^\Omega]$-module $\boldsymbol{M}_\Omega$ called the Ω^{th}*-blocking*, or Ω^{th}*-interleaving*, module.

Lemma 2.2 $\mathrm{rk}(\boldsymbol{M}_\Omega) = \Omega\ \mathrm{rk}(\boldsymbol{M})$.

Proof If $\xi_1, \ldots, \xi_\ell$ are $F[\delta]$-linearly independent elements in $\boldsymbol{M}$, then the elements

$$\xi_1, \xi_1\delta, \ldots, \xi_1\delta^{\Omega-1}, \ldots, \xi_\ell, \xi_\ell\delta, \ldots, \xi_\ell\delta^{\Omega-1}$$

are $F[\delta^\Omega]$-linearly independent.

The Ω^{th}-blocking transducer, or Ω^{th}-interleaving transducer, $\mathcal{T}_\Omega$ of $\mathcal{T}$ is the linear recurrent transducer defined by (compare with [25]):

- its module is the Ω^{th}-blocking module $\mathcal{T}_\Omega$,
- its input and output are respectively $(\boldsymbol{u}, \boldsymbol{u}\delta, \ldots, \boldsymbol{u}\delta^{\Omega-1})$ and $(\boldsymbol{y}, \boldsymbol{y}\delta, \ldots, \boldsymbol{y}\delta^{\Omega-1})$.

The next result is clear:

Proposition 2.6 *If $\mathcal{T}$ is controllable (resp. observable, right invertible, left invertible), then $\mathcal{T}_\Omega$ is also controllable (resp. observable, right invertible, left invertible).*

2.7.2 Puncturing

Puncturing a linear recurrent transducer $\mathcal{T}$ means taking a linear recurrent transducer $\mathcal{T}_P$ defined by the same module, the same input and by an output which is a subset of $\boldsymbol{y}$. The next result is clear:

Proposition 2.7 *If $\mathcal{T}$ is controllable (resp. left invertible), then $\mathcal{T}_P$ is also controllable (resp. left invertible). If $\mathcal{T}$ is observable (resp. right invertible), then $\mathcal{T}_P$ is not necessarily observable (resp. right invertible).*

3 Some properties of linear recurrent codes

3.1 Equivalence of encoders and codes

3.1.1 Equivalence

Two linear recurrent encoders with inputs $\boldsymbol{u} = (u_1, \ldots, u_k)$, $\boldsymbol{u}' = (u_1, \ldots, u'_{k'})$ and outputs $\boldsymbol{y} = (y_1, \ldots, y_n)$, $\boldsymbol{y}' = (y_1, \ldots, y'_{n'})$ are said to be *equivalent* if, and only if, the following conditions are satisfied:

1. $n = n'$.

2. There exists $\sigma \in \mathrm{S}_n$, where S_n is the symmetric group over $\{1, \ldots, n\}$, such that the mapping $y_\iota \mapsto y'_{\sigma\iota}$, $\iota = 1, \ldots, n$, defines an isomorphism between the modules $\mathrm{span}_{F[\delta]}(\boldsymbol{y})$ and $\mathrm{span}_{F[\delta]}(\boldsymbol{y}')$.

Proposition 3.1 *The inputs of two equivalent linear recurrent encoders possess the same number of components.*

Proof Let ϱ and ϱ' be the output ranks of the encoders $\mathcal{T}$ and $\mathcal{T}'$. The right invertibility of $\mathcal{T}$ and $\mathcal{T}'$ implies $\varrho = k$ and $\varrho' = k'$. The equivalence of $\mathcal{T}$ and $\mathcal{T}'$ implies $\varrho = \varrho'$.

3.1.2 Codes

A *linear recurrent code*, or a *(time-varying) convolutional code* is an equivalence between linear recurrent encoders. From Proposition 3.1, we know already two integers k, n, $0 < k \leq n$ which are attached to the code, which is therefore called a (n, k) linear recurrent code. Its *rate* is $\frac{k}{n}$. By a slight abuse of language, $\mathrm{span}_{F[\delta]}(\boldsymbol{y})$ is sometimes called a linear recurrent code, or a (time-varying) convolutional code. When F is a finite field of constants, a linear recurrent code is called a *(fixed) convolutional code.* A code is said to be *free*, or *controllable* if, and only if, the module $\mathrm{span}_{F[\delta]}(\boldsymbol{y})$ is free.

3.2 Syndrome formers

Let $\mathcal{F}_n$ be the free right $F[\delta]$-module, with basis $\bar{y}_1, \ldots, \bar{y}_n$. The mapping $\bar{y}_\iota \mapsto y_\iota$, $\iota = 1, \ldots, n$, defines an epimorphism $\mathcal{F}_n \to \mathrm{span}_{F[\delta]}(\boldsymbol{y})$ and the short exact sequence

$$0 \to \mathcal{F}_{n-k} \to \mathcal{F}_n \to \mathrm{span}_{F[\delta]}(\boldsymbol{y}) \to 0 \tag{3.8}$$

where $\mathcal{F}_{n-k}$ a free right $F[\delta]$-module of rank $n - k$. A *syndrome former* of the code is a presentation matrix of $\mathrm{span}_{F[\delta]}(\boldsymbol{y})$, which corresponds here to the monomorphism $\mathcal{F}_{n-k} \to \mathcal{F}_n$.

The sequence (3.8) splits, *i.e.*, $\mathcal{F}_n \simeq \mathcal{F}_{n-k} \oplus \mathrm{span}_{F[\delta]}(\boldsymbol{y})$, if, and only if, the code is free.

3.3 Some properties of free codes

¿From now on and until the end of the paper codes are assumed to be free[5]. When F is a finite field of constants, a (fixed) convolutional code may be defined as a certain $F[\delta]$-submodule of the $F[\delta]$-module $\mathcal{L} = \{\sum_{\upsilon \geq 0} \delta^\upsilon a_{1\upsilon}, \ldots, \sum_{\upsilon \geq 0} \delta^\upsilon a_{n\upsilon}\}$ of n-tuple of formal power series. The relationship with our approach[6] is given by $\mathrm{Hom}\left(\mathrm{span}_{F[\delta]}(\boldsymbol{y}), \mathcal{L}\right)$, *i.e.*, by $F[\delta]$-module morphisms $\Phi = (\phi_1, \ldots, \phi_n) : \mathrm{span}_{F[\delta]}(\boldsymbol{y}) \to \mathcal{L}$, $(y_1, \ldots, y_n) \mapsto (y_1\phi, \ldots, y_n\phi)$ (compare with [28]).

[5] When F is a finite field of constants, a (fixed) convolutional code is often defined as a vector subspace of $F(\delta)^{1\times n}$ (see, e.g., [25] and the references therein.). With respect to this transfer matrix setting the freeness may always be assumed.

[6] This is more generally the relationship (see [6]) between our module-theoretic setting and Willems' *behavioral approach* [34].

3.3.1 Dual codes and parity check matrices

The image of $\mathcal{F}_{n-k}$ in $\mathcal{F}_n$ is called the *dual code*. A syndrome former of the dual code is called a *parity check matrix* of the code.

Remark 3.1 *When F is a finite field of constants, the dual code of a convolutional code is usually defined as for block codes via an orthogonality relation. The explicit relationship with our definition will be given elsewhere [9].*

3.3.2 Polynomial and basic encoders

A controllable and observable encoder $\mathcal{E}$ is said to be *polynomial* if, and only if, $\boldsymbol{u}$ is a basis of the free module $\mathcal{E}$. The next property is an immediate consequence of Theorem 2.2:

Proposition 3.2 *A controllable and observable encoder is polynomial if, and only if, the entries of its transfer matrix are polynomial, i.e., belong to $F[\delta]$.*

The polynomial encoder $\mathcal{E}$ is said to be *basic* if, and only if, $\mathcal{E} = \mathrm{span}_{F[\delta]}(\boldsymbol{y})$. By taking for $\boldsymbol{u}$ any basis of the free module $\mathrm{span}_{F[\delta]}(\boldsymbol{y})$ we obtain the

Proposition 3.3 *Any free code admits a basic encoder.*

3.3.3 Systematic encoders

Proposition 3.4 *Any free code admits a* systematic *encoder, i.e., an encoder where k components of the output are identical to the k components of the input.*

Proof The result is clear if $k = n$: $\boldsymbol{y}$ is a basis of $\mathrm{span}_{F[\delta]}(\boldsymbol{y})$ and can be taken as an input. Assume that the result holds for $n = n_0 \geq k$. Take $n = n_0 + 1$. Since the components of $\boldsymbol{y}$ are $F[\delta]$-linearly dependent we may write

$$y_1\gamma_1 + \cdots + y_{n_0+1}\gamma_{n_0+1} = 0 \tag{3.9}$$

where $\gamma_1, \ldots, \gamma_{n_0+1} \in F[\delta]$ are right coprime. At least one of the coefficients γ_ι, $\iota = 1, \ldots, n_0+1$, γ_{n_0+1} for instance, when expressed as a sum (2.1), is such that $a_0 \neq 0$. Apply the assumption to the code spanned by $y_1, \ldots, y_{n_0}$ and utilise the causal relation $y_{n_0+1} = -(y_1\gamma_1 + \cdots + y_{n_0}\gamma_{n_0})\gamma_{n_0+1}^{-1}$.

3.3.4 Non-catastrophic encoders

The ring of Laurent polynomials $F[\delta, \delta^{-1}]$ is the localized ring of $F[\delta]$ by the multiplicative monoid $\{\delta^s \mid s \geq 0\}$, which satisfies the right Ore condition. The corresponding localized right $F[\delta, \delta^{-1}]$-module $\mathcal{E} \otimes_{F[\delta]} F[\delta, \delta^{-1}]$ of $\mathrm{span}_{F[\delta]}(\boldsymbol{u})$ is free, if $\mathcal{E}$ is controllable. The canonical mapping $\mathcal{E} \to \mathcal{E} \otimes_{F[\delta]} F[\delta, \delta^{-1}]$, $\upsilon \mapsto \upsilon \otimes 1$, being injective, $\mathcal{E}$ may be considered as a subset of $\mathcal{E} \otimes_{F[\delta]} F[\delta, \delta^{-1}]$. A controllable encoder is said to be *non-catastrophic* if, and only if, $\boldsymbol{u}$ belongs to $\mathrm{span}_{F[\delta]}(\boldsymbol{y}) \otimes_{F[\delta]} F[\delta, \delta^{-1}]$. The next result is an immediate consequence of Proposition 3.3.

Proposition 3.5 *Any free code admits a non-catastrophic encoder.*

3.4 Forney's theorem

3.4.1 An important filtration

Define a *filtration* of $F[\delta]$ by setting $\mathbf{F}_\alpha = \{\delta^\alpha P\}$, $\alpha \geq 0$, $P \in F[\delta]$. Thus $F[\delta] = \mathbf{F}_0 \supset \mathbf{F}_1 \supset \dots$. The corresponding filtration for the free module $\mathrm{span}_{F[\delta]}(\boldsymbol{y})$ is obtained by setting $\mathbf{C}_\alpha = \mathrm{span}_{F[\delta]}(\boldsymbol{y})\mathbf{F}_\alpha$. Thus $\mathrm{span}_{F[\delta]}(\boldsymbol{y}) = \mathbf{C}_0 \supset \mathbf{C}_1 \supset \dots$. Any element $x \in \mathrm{span}_{F[\delta]}(\boldsymbol{y})$ may be written uniquely as a finite sum

$$x = \sum_{\alpha=\nu}^{\mu} \xi_\alpha \delta^\alpha \tag{3.10}$$

where $\xi_\alpha \delta^\alpha$ is *homogeneous*, of *weight* α (ξ_α is homogeneous of weight 0). The element x is said to be of *order* ν (resp. *degree* μ) if, and only if, $\xi_\nu \neq 0$ (resp. $\xi_\mu \neq 0$). It is homogeneous if, and only if, $\nu = \mu$. The next results are clear.

Lemma 3.1 *The semi-linear linear mapping $\delta^\ell : \boldsymbol{C}_\alpha \rightarrow \boldsymbol{C}_{\alpha+\ell}$, $\ell > 0$, is bijective.*

Corollary 3.1 *For any homogeneous element $x_{\alpha+\ell}$ of order $\alpha+\ell$ there exists a homogeneous element x_α of order α such that $x_\alpha \delta^\ell = x_{\nu+\ell}$.*

Lemma 3.2 *Homogeneous elements of order ν are $F[\delta]$-linearly independent if, and only if, they are F-linearly independent.*

Corollary 3.2 *The F-vector space $\boldsymbol{C}_\alpha / \boldsymbol{C}_{\alpha+1}$ is of dimension k.*

3.4.2 The result

Let ε_1 be the highest degree of the components of $\boldsymbol{y}$, when written as in (3.10). Let V_1 be the ϖ_1-dimensional F-vector space spanned by the corresponding homogeneous elements. Choose according to Corollary 3.1 homogeneous elements $u_1, \dots, u_{\varpi_1}$, of degree 0, such that $V_1 = \mathrm{span}(u_1\delta^{\varepsilon_1}, \dots, u_{\varpi_1}\delta^{\varepsilon_1})$. Let $\varepsilon_2 < \varepsilon_1$ be the first integer such that $u_1\delta^{\varepsilon_2}, \dots, u_{\varpi_1}\delta^{\varepsilon_2}$ does not span the F-vector space spanned by the homogeneous components of order ε_2 in $\boldsymbol{y}$. Complete then $u_1, \dots, u_{\varpi_1}$ as above. We obtain a basis $\boldsymbol{u} = (u_1, \dots, u_m)$ and a corresponding polynomial transfer matrix with lines of degrees[7] $e_1 \leq e_2 \leq \dots \leq e_k$.

We must show that the above basic encoder is *minimal*, *i.e.*, that the degrees $f_1 \leq f_2 \leq \dots \leq f_k$ of the lines of any polynomial generating matrix verify $e_\iota \leq f_\iota$, $\iota = 1, \dots, k$. The next lemma, which is obvious, demonstrates that this result holds true if $k = 1$.

Lemma 3.3 *Take a free $F[\delta]$-module M of rank 1. Two bases b and b' are related by $b = \gamma b'$, $\gamma \in F$, $\gamma \neq 0$. Let $N \supseteq M$ be another free $F[\delta]$-module of rank 1. Then, for any basis c of N, $b = \pi b$, $\pi \in F[\delta]$.*

[7] The degree of a line is the maximum degree of its entries.

By considering the quotient module $\mathrm{span}_{F[\delta]}(\boldsymbol{y})/\mathrm{span}_{F[\delta]}(u_1)$, which is free of rank $k-1$, we obtain the minimality for any $k \geq 2$, assuming that it holds true for $k-1$.

We have proved

Theorem 3.1 *For any free linear recurrent code, there exists a basic encoder, called* minimal*, such that est the degrees of the lines of its transfer matrix are $e_1 \leq e_2 \leq \cdots \leq e_k$. The degrees $f_1 \leq f_2 \leq \cdots \leq f_k$ of the lines of a transfer matrix of any equivalent polynomial encoder verify $e_\kappa \leq f_\kappa$, $\kappa = 1, \ldots, k$.*

A corresponding input is called a *Forney input*.

4 Conclusion

More details might be found in [9] as well as a new connection between convolutional and block codes. The following topics will be discussed in subsequent works:

- Turbo-codes [1]. They are often given by two convolutional encoders in parallel with an interleaver. They are known to be related to time-varying convolutional codes.
- Non-linear tree codes which correspond to non-linear encoders, *i.e.*, to right invertible non-linear input-output systems.
- Cryptography which will be associated to invertible square input-output systems.

References

[1] C. Berrou, A. Glavieux, Near-optimum error-correcting coding and decoding: Turbo-codes, *IEEE Trans. Communicat.* **44** (1996) 1261-1271.

[2] R.M. Cohn, *Difference Algebra*. Interscience (1965).

[3] A. Dholakia, *Introduction to Convolutional Codes with Applications*. Kluwer (1994).

[4] F. Fagnani, S. Zampieri, System-theoretic properties of convolutional codes over rings, *IEEE Trans. Information Theory* **47** (2001) 2256-2274.

[5] M. Fliess, Some basic structural properties of generalized linear systems, *Systems Control Lett.* **15** (1990) 391-396.

[6] M. Fliess, A remark on Willems' trajectory characterization of linear controllability. *Systems Control Lett.* **19** (1992) 43-45.

[7] M. Fliess, Reversible linear and nonlinear discrete-time dynamics, *IEEE Trans. Automat. Control* **37** (1992) 1144-1153.

[8] Fliess M., Une interprétation algébrique de la transformation de Laplace et des matrices de transfert, *Linear Algebra Appl.* **203-204** (1994) 429-442.

[9] M. Fliess, On the structure of linear recurrent error-control codes, to appear in *ESAIM: Control Optimisation Calculus Variations*.

[10] M. Fliess, H. Bourlès, Discussing some examples of linear system interconnections, *Systems Control Lett.* **27** (1996) 1-7.

[11] M. Fliess, J. Lévine, P. Martin, P. Rouchon, Flatness and defect of non-linear systems: introductory theory and applications, *Internat. J. Control* **61** (1995) 1327-1361.

[12] M. Fliess, R. Marquez, Continuous-time linear predictive control and flatness: a module-theoretic setting with examples, *Internat. J. Control* **73** (2000) 606-623.

[13] M. Fliess, R. Marquez, Une approche intrinsèque de la commande prédictive linéaire discrète, *APII J. europ. Syst. automat.* **35** (2001) 127-147.

[14] M. Fliess, H. Mounier, Controllability and observability of linear delay systems: an algebraic approach, *ESAIM: Control Optimisation Calculus Variations* **3** (1998) 301-314.

[15] G.D. Forney, Jr, Convolutional codes I: Algebraic structure, *IEEE Trans. Information Theory* **16** (1970) 720-738.

[16] G.D. Forney, Jr, Minimal bases of rational vector spaces, with applications to multivariable linear systems, *SIAM J. Control* **13** (1975) 493-520.

[17] G.D. Forney, Jr, Algebraic structure of convolutional codes and algebraic system theory, in *Mathematical System Theory - The Influence of R.E. Kalman*, A.C. Antoulas Ed., Springer (1991) 527-557.

[18] G.D. Forney, Jr, M.D. Trott, The dynamics of group codes: state-space, trellis diagrams and canonical encoders, *IEEE Trans. Information Theory* **39** (1993) 1491-1513.

[19] G.D. Forney, Jr, B. Marcus, N.T. Sindhushayana, M. Trott, A multilingual dictionary: System theory, coding theory, symbolic dynamics and automata theory, in *Different Aspects of Coding Theory*, Proc. Symp. Appl. Math. **50**, Amer. Math. Soc. (1995) 109-138.

[20] R. Johannesson, K. Sh. Zigangirov, *Fundamentals of Convolutional Coding*. IEEE Press (1999).

[21] T. Kailath, *Linear Systems*. Prentice-Hall (1979).

[22] E.W. Kamen, P.P. Khargonekar, K.R. Poola, A transfer-function approach to linear time-varying discrete-time systems, *SIAM J. Control Optimiz.* **23** (1985) 550-565.

[23] T.Y. Lam, *Lectures on Rings and Modules*. Springer (1999).

[24] J.L. Massey, M.K. Sain, Codes, automata and contnuous systems: explicit interconnections, *IEEE Trans. Automat. Control* **12** (1967) 644-650.

[25] R.J. McEliece, The algebraic theory of convolutional codes, in *Handbook of Coding Theory*, Pless V., Huffman W.C. (Eds), Elsevier, vol. 1 (1998) 1065-1138.

[26] J.C. McConnel, J.C. Robson, *Noncommutative Noetherian Rings*. Wiley (1987).

[27] P. Piret, *Convolutional Codes, an Algebraic Approach*. MIT Press (1988).

[28] J. Rosenthal, Connections between linear systems and convolutional codes, in *Codes, Systems and Graphical Models*, B. Marcus, J. Rosenthal (Eds), Springer (2000) 39-66.

[29] J. Rosenthal, J.M. Schumacher, E.V. York, On behaviors and convolutional codes, *IEEE Trans. Informat. Theory* **42** (1996) 1881-1891.

[30] J. Rosenthal, E.V. York, BCH convolutional codes, *IEEE Trans. Informat. Theory* **45** (1999) 1833-1844.

[31] J. Rotman, *An Introduction to Homological Algebra*. Academic Press (1979).

[32] A.J. Viterbi, J.K. Omura, *Principles of Digital Communication and Coding*. McGraw-Hill (1979).

[33] L. Weiss, Controllability, realization and stability of discrete-time systems, *SIAM J. Control* **10** (1972) 230-251.

[34] J.C. Willems, Paradigms and puzzles in the theory of dynamical systems, *IEEE Trans. Automat. Control* **36** (1991) 259-294.