CONNECTIONS BETWEEN LINEAR SYSTEMS AND CONVOLUTIONAL CODES*

JOACHIM ROSENTHAL†

Abstract. The article reviews different definitions for a convolutional code which can be found in the literature. The algebraic differences between the definitions are worked out in detail. It is shown that bi-infinite support systems are dual to finite-support systems under Pontryagin duality. In this duality the dual of a controllable system is observable and vice versa. Uncontrollability can occur only if there are bi-infinite support trajectories in the behavior, so finite and half-infinite-support systems must be controllable. Unobservability can occur only if there are finite support trajectories in the behavior, so bi-infinite and half-infinite-support systems must be observable. It is shown that the different definitions for convolutional codes are equivalent if one restricts attention to controllable and observable codes.

Key words. Convolutional codes, linear time-invariant systems, behavioral system theory.

AMS(MOS) subject classifications. Primary 37B10, 93B25, 94B10.

1. Introduction. It is common knowledge that there is a close connection between linear systems over finite fields and convolutional codes. In the literature one finds however a multitude of definitions for convolutional codes, which can make it confusing for somebody who wants to enter this research field with a background in systems theory or symbolic dynamics. It is the purpose of this article to provide a survey of the different points of view about convolutional codes.

The article is structured as follow: In Section 2 we will review the way convolutional codes have often been defined in the coding literature [20, 21, 28, 35, 38].

Section 3 reviews a definition for convolutional codes that can be found in the literature on symbolic dynamics. From the symbolic dynamics point of view [24, 29, 32], a convolutional code is a linear irreducible shift space.

In Section 4 we will review the class of time-invariant, complete linear behaviors in the sense of Willems [50, 51, 52]. We will show how these behaviors relate to the definitions given in Section 2 and 3.

In Section 5 we will give a definition for convolutional codes in which it is required that the code words have finite support. Such a definition was considered by Fornasini and Valcher [48, 5] and by the author in collaboration with Schumacher, Weiner and York [42, 44, 49]. The study of behaviors with finite support has been done earlier in the context of automata the-

*The work was supported in part by NSF grant DMS-96-10389. This research has been carried out while the author was a guest professor at EPFL in Switzerland. The author would like to thank EPFL for its support and hospitality.

†Department of Mathematics, University of Notre Dame, Notre Dame, Indiana 46556-5683. *E-mail:* Rosenthal.1@nd.edu.

ory and we refer to Eilenberg's book [1]. We show in Section 5 how this module-theoretic definition relates to complete, linear and time-invariant behaviors by Pontryagin duality.

In Section 6 we will study different first-order representations connected with the different viewpoints. Finally, in Section 7 we compare the different definitions. We also show how cyclic redundancy check codes can naturally be viewed in the context of finite-support convolutional codes.

Throughout the paper we will emphasize the algebraic properties of the different definitions. We will also restrict ourselves to the concrete setting of convolutional codes defined over finite fields. It is however known that many of the concepts in this paper generalize to group codes [3, 12, 9] and multidimensional convolutional codes [4, 5, 16, 48, 49]. All of the definitions which we are going to give are quite similar, but there are some notable differences.

Since the paper draws from results from quite different research areas, one is faced with the problem that there is no uniform notation. In this paper we will adopt the convention used in systems theory in which vectors are regarded as column vectors. For the convenience of the reader, we conclude this section with a summary of some of the notation used in this paper:

$\mathbb{F}$	A fixed finite field;
$\mathbb{F}[z]$	The polynomial ring over $\mathbb{F}$;
$\mathbb{F}[z,z^{-1}]$	The Laurent polynomial ring over $\mathbb{F}$;
$\mathbb{F}(z)$	The field of rationals;
$\mathbb{F}[[z]]$	The ring of formal power series of the form $\sum_{i=0}^{\infty} a_i z^i$;
$\mathbb{F}((z))$	Field of formal Laurent series having the form $\sum_{i=d}^{\infty} a_i z^i$;
$\mathbb{F}[[z,z^{-1}]]$	The ring of formal power series of the form $\sum_{i=-\infty}^{\infty} a_i z^i$;
$\mathbb{Z}$	The integers;
$\mathbb{Z}_+$	The nonnegative integers;
$\mathbb{Z}_-$	The nonpositive integers.

Consider the ring of formal power series $\mathbb{F}[[z,z^{-1}]]$. We will identify the set $\mathbb{F}[[z,z^{-1}]]$ with the (two-sided) sequence space $\mathbb{F}^{\mathbb{Z}}$. We have natural embeddings:

$$\mathbb{F} \longrightarrow \mathbb{F}[z] \longrightarrow \mathbb{F}[z,z^{-1}] \longrightarrow \mathbb{F}(z) \longrightarrow \mathbb{F}((z)) \longrightarrow \mathbb{F}[[z,z^{-1}]].$$

With these embeddings we can view e.g. the set of rationals $\mathbb{F}(z)$ as a subset of the sequence space $\mathbb{F}^{\mathbb{Z}}$, and we will make use of such identifications throughout the paper.

The set of n-vectors with polynomial entries will be denoted by $\mathbb{F}^n[z]$. Similarly we define the sets $\mathbb{F}^n(z), \mathbb{F}^n((z))$ etc. All these sets are subsets of the two sided sequence space $(\mathbb{F}^n)^{\mathbb{Z}} = \mathbb{F}^n[[z,z^{-1}]]$. The definitions of convolutional codes which we will provide in the next sections will all be $\mathbb{F}$-linear subspaces of $(\mathbb{F}^n)^{\mathbb{Z}}$.

The idea of writing a survey on the different points of view about convolutional codes was suggested to the author by Paul Fuhrmann during a stimulating workshop on "Codes, Systems and Graphical Models" at the Institute for Mathematics and its Applications (IMA) in August 1999. A first draft of this paper was circulated in October 1999 to about a dozen people interested in these research issues. This generated an interesting 'Internet discussion' on these issues, in which the different opinions were exchanged by e-mail. Some of these ideas have been incorporated into the final version of the paper and the author would like to thank Dave Forney, Paul Fuhrmann, Heide Gluesing-Luerssen, Jan Willems and Sandro Zampieri for having provided valuable thoughts. The author wishes also to thank the IMA and its superb staff, who made the above mentioned workshop possible.

2. The linear algebra point of view. The theory of convolutional codes grew out and extended the theory of linear block codes into a new direction. Because of this reason we start the section with linear block codes and we introduce convolutional codes in a quite intuitive way.

An $[n, k]$ linear block code is by definition a linear subspace $\mathcal{C} \subset \mathbb{F}^n$ having dimension $\dim \mathcal{C} = k$. Let G be a $n \times k$ matrix with entries in $\mathbb{F}$. The linear map

$$\varphi : \mathbb{F}^k \longrightarrow \mathbb{F}^n, \ m \longmapsto c = Gm$$

is called an *encoding map* for the code $\mathcal{C}$ if $\mathrm{im}\,(\varphi) = \mathcal{C}$. If this is the case then we say G is a *generator matrix* or an *encoder* for the block code $\mathcal{C}$.

Assume that a sequence of message blocks $m_0, \ldots, m_t \subset \mathbb{F}^k$ should be encoded into a corresponding sequence of code words $c_i = Gm_i \in \mathbb{F}^n$, $i = 0, \ldots, t$. By introducing the polynomial vectors $m(z) = \sum_{i=0}^{t} m_i z^i \in \mathbb{F}^k[z]$ and $c(z) = \sum_{i=0}^{t} c_i z^i \in \mathbb{F}^n[z]$ it is possible to describe the encoding procedure through the module homomorphism:[1]

$$\varphi : \mathbb{F}^k[z] \longrightarrow \mathbb{F}^n[z], \ m(z) \longmapsto c(z) = Gm(z). \tag{2.1}$$

The original idea of a convolutional code goes back to the paper of Elias [2], where it was suggested to use a polynomial matrix $G(z)$ in the encoding procedure (2.1).

Polynomial encoders $G(z)$ are physically easily implemented through a feedforward linear sequential circuit. Massey and Sain [34, 45] showed that there is a close connection between linear systems and convolutional codes. Massey and Sain viewed the polynomial encoder $G(z)$ as a transfer function. More generally it is possible to realize a transfer function $G(z)$ with rational entries by (see e.g. [20, 21]) a linear sequential circuit whose elements include feedback components. If one allows rational entries in

[1] Throughout the paper we use the symbol φ to denote an encoding map. The context will make it clear what the domain and the range of this map is in each situation.

the encoding matrix then it seems natural to extend the possible message sequences to the set of rational vectors $m(z) \in \mathbb{F}^k(z)$ and to process this sequence by a 'rational encoder' resulting again in a rational code vector $c(z) \in \mathbb{F}^n(z)$. With this we have a first definition of a convolutional code as it can be found e.g. in the Handbook of Coding Theory [35, Definition 2.4]:

DEFINITION A. A $\mathbb{F}(z)$-linear subspace $\mathcal{C}$ of $\mathbb{F}^n(z)$ is called a convolutional code.

If $G(z)$ is a $n \times k$ matrix with entries in $\mathbb{F}(z)$ whose columns form a basis for $\mathcal{C}$, then we call $G(z)$ a generator matrix or an encoder for the convolutional code $\mathcal{C}$. $G(z)$ describes the encoding map:

$$\varphi : \ \mathbb{F}^k(z) \longrightarrow \mathbb{F}^n(z), \ m(z) \longmapsto c(z) = G(z)m(z).$$

The field of rationals $\mathbb{F}(z)$ viewed as a subset of the sequence space $\mathbb{F}^{\mathbb{Z}} = \mathbb{F}[[z, z^{-1}]]$ consists precisely of those sequences whose support is finite on the negative sequence space $\mathbb{F}^{\mathbb{Z}-}$ and whose elements form an ultimately periodic sequence on the positive sequence space $\mathbb{F}^{\mathbb{Z}+}$. It therefore seems that one equally well could restrict the possible message words $m(z) \in \mathbb{F}^k(z)$ to sequences whose coordinates consists of Laurent polynomials only, in other words to sequences of the form $m(z) \in \mathbb{F}^k[z, z^{-1}]$.

Alternatively one could allow message words $m(z)$ whose coordinates are not ultimately periodic and possibly not of finite support on the negative sequence space $\mathbb{F}^{\mathbb{Z}-}$. This would suggest that one should take as possible message words the whole sequence space $\left(\mathbb{F}^k\right)^{\mathbb{Z}} = \mathbb{F}^k[[z, z^{-1}]]$. The problem with this approach is that the multiplication of an element in $\mathbb{F}[[z, z^{-1}]]$ with an element in $\mathbb{F}(z)$ is in general not well defined. If one restricts however the message sequences to the field of formal Laurent series then the multiplication is well defined. This leads to the following definition which goes back to the work of Forney [7]. The definition has been adopted in the book by Piret [38] and the book by Johannesson and Zigangirov [21], and it appears as Definition 2.3 in the Handbook of Coding Theory [35]:

DEFINITION A'. A $\mathbb{F}((z))$-linear subspace $\mathcal{C}$ of $\mathbb{F}^n((z))$ which has a basis of rational vectors in $\mathbb{F}^n(z)$ is called a convolutional code.

The requirement that $\mathcal{C}$ has a basis with rational entries guarantees that $\mathcal{C}$ has also a basis with only polynomial entries. $\mathcal{C}$ can therefore be represented by a $n \times k$ generator matrix $G(z)$ whose entries consist only of rationals or even polynomials. The encoding map with respect to $G(z)$ is given through:

$$\varphi : \ \mathbb{F}^k((z)) \longrightarrow \mathbb{F}^n((z)), \ m(z) \longmapsto c(z) = G(z)m(z). \tag{2.2}$$

If $G(z)$ is a polynomial matrix, then finitely many components of $m(z)$ influence only finitely many components of $c(z)$, and the encoding procedure may be physically implemented by a simple feedforward linear shift register.

If $G(z)$ contains rational entries, then it is in general the case that a finite (polynomial) message vector is encoded into an infinite (rational) code vector of the form $c(z) = \sum_{i=s}^{\infty} c_i z^i$. This might cause some difficulties in the decoder. For the encoding process, $G(z)$ can be physically realized by linear shift registers, in general with feedback (see e.g. [20, 21]).

From a systems theory point of view, it is classical [23] to view the encoding map (2.2) as an input-output linear system. This was the point of view taken by Massey and Sain [34, 45] and thereafter in most of the coding literature. However unlike in systems theory, the important object in coding theory is the code $\mathcal{C} = \mathrm{im}\,(\varphi)$. As a result one calls encoders φ which generate the same image $\mathrm{im}\,(\varphi)$ equivalent; we will say more about this in a moment. In Sections 3 and 4 we will view (2.2) as an image representation of a time-invariant behavior in the sense of Willems [50, 51], which we believe captures the coding situation in a more natural way.

Assume that $G(z)$ and $\tilde{G}(z)$ are two $n \times k$ rational encoding matrices defining the same code $\mathcal{C}$ with respect to either Definition A or A$'$. In this case we say that $G(z)$ and $\tilde{G}(z)$ are equivalent encoders. The following lemma is a simple result of linear algebra:

LEMMA 2.1. *Two $n \times k$ rational encoders $G(z)$ and $\tilde{G}(z)$ are equivalent with respect to either Definition A or A$'$ if and only if there is a $k \times k$ invertible rational matrix $R(z)$ such that $\tilde{G}(z) = G(z)R(z)$.*

It follows from this lemma that Definition A and Definition A$'$ are completely equivalent with respect to equivalence of encoders.

From an algebraic point of view we can identify a convolutional code in the sense of Definition A or Definition A$'$ through an equivalence class of rational matrices. The following theorem singles out a set of very desirable encoders inside each equivalence class.

THEOREM 2.2. *Let $G(z)$ be a $n \times k$ rational encoding matrix of rank k defining a code $\mathcal{C}$. Then there is a $k \times k$ invertible rational matrix $R(z)$ such that $\tilde{G}(z) = G(z)R(z)$ has the properties:*
(i) *$\tilde{G}(z)$ is a polynomial matrix.*
(ii) *$\tilde{G}(z)$ is right prime.*
(iii) *$\tilde{G}(z)$ is column reduced with column degrees $\{e_1, \ldots, e_k\}$.*
Furthermore, every polynomial encoding matrix of $\mathcal{C}$ which is right prime and column-reduced has (unordered) column degrees $\{e_1, \ldots, e_k\}$. Thus these indices are invariants of the convolutional code.

The essence of Theorem 2.2 was proved by Forney [6, Theorem 3]. In [8] Forney related the indices appearing in (iii) to the controllability and observability indices of a controllable and observable system. Paper [8] had an immense impact in the linear systems theory literature. We will follow here the suggestion of McEliece [35] and call these indices the *Forney indices* of the convolutional code, despite the fact that Theorem 2.2 can be traced back to the last century, when Kronecker, Hermite and in particular Dedekind and Weber studied matrices over the rationals and more general

function fields. In Sections 4 and 5 we will make a distinction between the Forney indices as defined above and the Kronecker indices of a submodule of $\mathbb{F}^n[z]$.

In the coding literature [21, 38], an encoder satisfying conditions (i), (ii) and (iii) of Theorem 2.2 is called a *minimal basic encoder*.

So far we have used encoding matrices to describe a convolutional code. As is customary in linear algebra, one often describes a linear subspace as the kernel of a matrix. This leads to the notion of a *parity-check matrix*. The following theorem is well known (see e.g. [38]).

THEOREM 2.3. *Let $\mathcal{C} \subset \mathbb{F}^n((z))$ be a rank-k convolutional code in the sense of Definition A'. Then there exists an $r \times n$ matrix $H(z)$ such that the code is equivalently described as the kernel of $H(z)$:*

$$\mathcal{C} = \{\ c(z) \in \mathbb{F}^n((z)) \ \mid \ H(z)c(z) = 0\ \}.$$

Moreover, it is possible to choose $H(z)$ in such a way that:
(i) *$H(z)$ is a polynomial matrix.*
(ii) *$H(z)$ is left prime.*
(iii) *$H(z)$ is row-reduced having row degrees $\{f_1, \ldots, f_r\}$.*
Furthermore, every polynomial parity check matrix of $\mathcal{C}$ which is left prime and row reduced will have (unordered) row degrees $\{f_1, \ldots, f_r\}$. Thus these indices are invariants of the convolutional code.

Properties (i)–(iii) essentially follow from the fact that the transpose $H^t(z)$ is a generator matrix for the dual (orthogonal) code $\mathcal{C}^\perp$.

The set of indices $\{e_1, \ldots, e_k\}$ and $\{f_1, \ldots, f_r\}$ differ in general, their sum is however always the same, and is called the *degree* of the convolutional code. One says that a rank-k code $\mathcal{C} \subset \mathbb{F}^n((z))$ has *transmission rate* k/n, *controller memory* $m := \max\{e_1, \ldots, e_k\}$ and *observer memory* $n := \max\{f_1, \ldots, f_r\}$.

Another important code parameter is the *free distance*. The free distance of a code measures the smallest distance between any two different code words, and is formally defined as:

$$d_{\text{free}}(\mathcal{C}) := \min_{\substack{u,v \in \mathcal{C} \\ u \neq v}} \sum_{t \in \mathbb{Z}} d_H(u_t, v_t), \tag{2.3}$$

where $d_H(\ ,\ )$ denotes the usual Hamming distance on $\mathbb{F}^n$.

3. The symbolic dynamics point of view. In this section we present a definition of convolutional codes as it can be found in the symbolic dynamics literature [24, 29, 32]. Convolutional codes in this framework are exactly the linear, compact, irreducible and shift-invariant subsets of $\mathbb{F}^n[[z, z^{-1}]]$. In order to make this precise, we will have to develop some basic notions from symbolic dynamics.

In the sequel we will work with the finite alphabet $\mathcal{A} := \mathbb{F}^n$. A *block* over the alphabet $\mathcal{A}$ is a finite sequence $\beta = x_1 x_2 \ldots x_k$ consisting of k

elements $x_i \in \mathcal{A}$. If $w = w(z) = \sum_i w_i z^i \in \mathbb{F}^n[[z, z^{-1}]]$ is a sequence, one says that the block β occurs in w if there is some integer j such that $\beta = w_j w_{j+1} \dots w_{k+j-1}$. If $X \subset \mathbb{F}^n[[z, z^{-1}]]$ is any subset, we denote by $\mathcal{B}(X)$ the set of blocks which occur in some element of X.

The fundamental objects in symbolic dynamics are the *shift spaces*. For this let $\mathcal{F}$ be a set of blocks, possibly infinite.

DEFINITION 3.1. The subset $X \subset \mathbb{F}^n[[z, z^{-1}]]$ consisting of all sequences $w(z)$ which do not contain any of the (forbidden) blocks of $\mathcal{F}$ is called a *shift space*.

The left-shift operator is the $\mathbb{F}$-linear map

$$\sigma : \mathbb{F}[[z, z^{-1}]] \longrightarrow \mathbb{F}[[z, z^{-1}]], \quad w(z) \longmapsto z^{-1} w(z). \tag{3.1}$$

Let I_n be the $n \times n$ identity matrix. The shift map σ extends to the shift map

$$\sigma I_n : \mathbb{F}^n[[z, z^{-1}]] \longrightarrow \mathbb{F}^n[[z, z^{-1}]].$$

One says that $X \subset \mathbb{F}^n[[z, z^{-1}]]$ is a *shift-invariant set* if $(\sigma I_n)(X) \subset X$. Clearly shift spaces are shift-invariant subsets of $\mathbb{F}^n[[z, z^{-1}]]$.

It is possible to characterize shift spaces in a topological manner. For this we will introduce a metric on $\mathbb{F}^n[[z, z^{-1}]]$:

DEFINITION 3.2. If $v(z) = \sum_i v_i z^i$ and $w(z) = \sum_i w_i z^i$ are both elements of $\mathbb{F}^n[[z, z^{-1}]]$ we define their distance through:

$$d(v(z), w(z)) := \sum_{i \in \mathbb{Z}} 2^{-|i|} d_H(v_i, w_i). \tag{3.2}$$

In this metric two elements $v(z), w(z)$ are 'close' if they coincide over a 'large block around zero'. One readily verifies that $d(\ ,\ )$ indeed satisfies all the properties of a metric and therefore induces a topology on $\mathbb{F}^n[[z, z^{-1}]]$. Using this topology we can characterize shift spaces:

THEOREM 3.3. *A subset of* $\mathbb{F}^n[[z, z^{-1}]]$ *is a shift space if and only if it is shift-invariant and compact.*

Proof. The metric introduced in Definition 3.2 is equivalent to the metric described in [29, Example 6.1.10]. The induced topologies are therefore the same. The result follows therefore from [29, Theorem 6.1.21]. □

The topological space $\mathbb{F}^n[[z, z^{-1}]]$ is a typical example of a linearly compact vector space, a notion introduced by S. Lefschetz. There is a large theory on linearly compact vector spaces, and several of the results which we are going to derive are valid in this broader context. We refer the interested reader to [25, §10] for more details.

A further important concept is irreducibility which will turn out to be equivalent to the concept of controllability in our concrete setting.

DEFINITION 3.4. A shift space $X \subset \mathbb{F}^n[[z,z^{-1}]]$ is called *irreducible* if for every ordered pair of blocks β, γ of $\mathcal{B}(X)$ there is a block μ such that the concatenated block $\beta\mu\gamma$ is in $\mathcal{B}(X)$.

We are now prepared to give the symbolic dynamics definition for a convolutional code and to work out the basic properties for these codes.

DEFINITION B. A linear, compact, irreducible and shift-invariant subset of $\mathbb{F}^n[[z,z^{-1}]]$ is called a convolutional code.

This is an abstract definition and it is not immediately clear how one should encode messages with such convolutional codes. The following will make this clear.

Let $G(z)$ be a $n \times k$ matrix with entries in the ring of Laurent polynomials $\mathbb{F}[z,z^{-1}]$. Consider the encoding map:

$$\varphi : \mathbb{F}^k[[z,z^{-1}]] \longrightarrow \mathbb{F}^n[[z,z^{-1}]],\ m(z) \longmapsto c(z) = G(\sigma)m(z). \tag{3.3}$$

In terms of polynomials the map φ is simply described through $m(z) \longmapsto c(z) = G(z^{-1})m(z)$.

Recall that a continuous map is called closed if the image of a closed set is closed. Using the fact that $\mathbb{F}^n[[z,z^{-1}]]$ is compact, one (easily) proves the following result:

LEMMA 3.5. *The encoding map* (3.3) *is* $\mathbb{F}$*-linear, continuous and closed.*

Clearly $\mathrm{im}\,(\varphi)$ is also shift-invariant, and one shows [29] that the image of an irreducible set under φ is irreducible again.

In summary we have shown that $\mathrm{im}\,(\varphi)$ describes a convolutional code in the sense of Definition B. Actually the converse is true as well:

THEOREM 3.6. $\mathcal{C} \subset \mathbb{F}^n[[z,z^{-1}]]$ *is a convolutional code in the sense of Definition B if and only if there exists a Laurent polynomial matrix* $G(z)$ *such that* $\mathcal{C} = \mathrm{im}\,(\varphi)$*, where* φ *is the map in* (3.3).

A proof of this theorem will be given in the next section after Theorem 4.8.

The question now arises how Definition B relates to Definition A and Definition A′. The following theorem will provide a partial answer to this question.

THEOREM 3.7. *Assume that* $\mathcal{C} \subset \mathbb{F}^n[[z,z^{-1}]]$ *is a nonzero convolutional code in the sense of Definition A or Definition A′. Then* $\mathcal{C}$ *is not closed, but the closure of* $\bar{\mathcal{C}}$ *of* $\mathcal{C}$ *is a convolutional code in the sense of Definition B.*

Proof. Let $G(z)$ be a minimal basic encoder of $\mathcal{C}$ and let $w(z) \in \mathbb{F}^n[z]$ be the first column of $G(z)$. Note that $w(z) \in \mathcal{C}$ and that there is at least one entry of $w(z)$ which does not contain the factor $(z-1)$. Let $\phi_N(z) := \sum_{i=-N}^{N} z^i \in \mathbb{F}[z,z^{-1}]$ and consider the sequence of code words $w^N(z) := \phi_N(z)w(z)$. For each $N > 0$ one has that $w^N(z) \in \mathcal{C}$. However

$\lim_{N\mapsto\infty} w^N(z)$ is in $\mathbb{F}^n[[z,z^{-1}]] \setminus \mathbb{F}^n((z)) \subset \mathbb{F}^n[[z,z^{-1}]] \setminus \mathcal{C}$. This shows that $\mathcal{C}$ is not a closed set inside $\mathbb{F}^n[[z,z^{-1}]]$. The closure $\bar{\mathcal{C}}$ is obtained by extending the input space $F^k((z))$ to all of $F^k[[z,z^{-1}]]$. The image of $F^k[[z,z^{-1}]]$ under the encoding map (3.3) is closed by Lemma 3.5, hence the closure is a code in the sense of Definition B. □

Actually one can show that there is a bijective correspondence between the convolutional codes in the sense of Definition A (respectively Definition A′) and the convolutional codes in the sense of Definition B, as we will show in Theorem 7.1 and Theorem 7.2. It is also worthwhile to remark that already in 1983 Staiger published a paper [47] where he studied the closure of convolutional codes generated by a polynomial generator matrix.

In analogy to Lemma 2.1, one has:

LEMMA 3.8. *Two $n \times k$ encoding matrices $G(z)$ and $\tilde{G}(z)$ defined over the Laurent polynomial ring $\mathbb{F}[z,z^{-1}]$ are equivalent with respect to Definition B if and only if there is a $k \times k$ invertible rational matrix $R(z)$ such that $\tilde{G}(z) = G(z)R(z)$.*

We leave the proof again as an exercise for the reader. We remark that rational transformations of the form $R(z)$ are needed to describe the equivalence, even though it is in general not possible to use a rational encoder $G(z)$ in the encoding procedure (3.3). This is simply due to the fact that in general the multiplication of an element of $\mathbb{F}(z)$ with an element of $\mathbb{F}[[z,z^{-1}]]$ is not defined. The following example should make this clear. (Compare also with Remark 4.4.)

EXAMPLE 3.9. Consider $f(z) = \frac{1}{1-z} = \sum_{i=0}^{\infty} z^i \in \mathbb{F}(z)$ and $g(z) = \sum_{i=-\infty}^{\infty} z^i \in \mathbb{F}[[z,z^{-1}]]$. Trying to multiply the two power series $f(z), g(z)$ would result in a power series in which each coefficient would be infinite.

In the same way as at the end of Section 2 we define the transmission rate, the degree, the memory and the free distance of a convolutional code $\mathcal{C}$ in the sense of Definition B.

4. Linear time-invariant behaviors. In this section we will take the point of view that a convolutional code is a linear time-invariant behavior in the sense of Willems [50, 51, 52]. Of course behavioral system theory is quite general, allowing all kinds of time axes and signal spaces. In order to relate the behavioral concepts to the previous points of view, we will restrict our study to linear behaviors in $(\mathbb{F}^n)^{\mathbb{Z}} = \mathbb{F}^n[[z,z^{-1}]]$ and $(\mathbb{F}^n)^{\mathbb{Z}_+} = \mathbb{F}^n[[z]]$.

Let σ be the shift operator defined in (3.1). One says that a subset $\mathcal{B} \subset \mathbb{F}^n[[z,z^{-1}]]$ is *time-invariant* if $(\sigma I_n)(\mathcal{B}) \subset \mathcal{B}$. The concept therefore coincides with the symbolic dynamics concept of shift-invariance.

In addition to linearity and time-invariance, there is a third important concept usually required of a time-invariant behavior:

DEFINITION 4.1. A behavior $\mathcal{B} \subset \mathbb{F}^n[[z,z^{-1}]]$ is said to be *complete* if $w \in \mathbb{F}^n[[z,z^{-1}]]$ belongs to $\mathcal{B}$ whenever $w|_J$ belongs to $\mathcal{B}|_J$ for every finite subinterval $J \subset \mathbb{Z}$.

The definition simply says that $\mathcal{B}$ is complete if membership can be decided on the basis of finite windows. Completeness is an important well behavedness property for linear time-invariant behaviors, as Willems [50, p. 567] emphasized with the remark:

> As such, it can be said that the study of non-complete systems does not fall within the competence of system theorists and could be left to cosmologists or theologians.

In Definition 3.2 we introduced a metric on the vector space $\mathbb{F}^n[[z, z^{-1}]]$. We remark that with respect to this metric a subset $\mathcal{B} \subset \mathbb{F}^n[[z, z^{-1}]]$ is complete if and only if every Cauchy sequence converges inside $\mathcal{B}$. In other words, the completeness notion of Definition 4.1 coincides with the usual topological notion of completeness.

The following result is known for linearly compact vector spaces, a proof can be found in [50]:

LEMMA 4.2. *A linear subset $\mathcal{B} \subset \mathbb{F}^n[[z, z^{-1}]]$ is complete if and only if it is closed and hence compact.*

With these preliminaries we can define a convolutional code as follows:

DEFINITION C. A linear, time-invariant and complete subset $\mathcal{B} \subset \mathbb{F}^n[[z, z^{-1}]]$ is called a convolutional code.

It is immediate from Lemma 4.2 that the convolutional codes defined in Definition B are complete and that Definition C is more general than Definition B, since no irreducibility is required. It also follows from Theorem 3.7 and Lemma 4.2 that the convolutional codes defined in Definition A and Definition A$'$ are in general not complete.

Before we elaborate on these differences we would like also to treat the situation when the time axis is $\mathbb{Z}_+$ since traditionally a large part of linear systems theory has been concerned with systems defined on the positive time axis. We first define the left-shift operator acting on $(\mathbb{F}^n)^{\mathbb{Z}_+} = \mathbb{F}^n[[z]]$ through:

$$\sigma : \mathbb{F}[[z]] \longrightarrow \mathbb{F}[[z]], \quad w(z) \longmapsto z^{-1}(w(z) - w(0)). \tag{4.1}$$

We have used the same symbol as in (3.1) since the context will always make it clear if we work over $\mathbb{Z}$ or $\mathbb{Z}_+$. In analogy to (3.1) σ extends to the shift map $\sigma I_n : \mathbb{F}^n[[z]] \longrightarrow \mathbb{F}^n[[z]]$, and one says a subset $X \subset \mathbb{F}^n[[z]]$ is time-invariant if $(\sigma I_n)(X) \subset X$. Notice however that the map of (4.1), unlike that of (3.1), is not invertible.

With this we have:

DEFINITION C$'$. A linear, time-invariant and complete subset $\mathcal{B} \subset \mathbb{F}^n[[z]]$ is called a convolutional code.

The following fundamental theorem was proved by Willems [50, Theorem 5].

THEOREM 4.3. *A subset $\mathcal{B} \subset \mathbb{F}^n[[z,z^{-1}]]$ (respectively a subset $\mathcal{B} \subset \mathbb{F}^n[[z]]$) is linear, time-invariant and complete if and only if there is a $r \times n$ matrix $P(z)$ having entries in $\mathbb{F}[z]$ such that*

$$\mathcal{B} = \{\ w(z)\ \mid\ P(\sigma)w(z) = 0\ \}. \tag{4.2}$$

By Lemma 3.5 the linear map $\psi :\ \mathbb{F}^n[[z,z^{-1}]] \longrightarrow \mathbb{F}^n[[z,z^{-1}]],\ w(z) \longmapsto P(\sigma)w(z)$ is continuous and its kernel is therefore a complete set. It is therefore immediate that the behavior defined in (4.2) is linear, time-invariant and complete. The harder part of Theorem 4.3 is the converse statement.

Equation (4.2) is often referred to as a kernel (or AR) representation of a behavioral system. We will denote a behavior having the form (4.2) by $\ker P(\sigma)$. By contrast, the encoding map φ defined in (3.3) describes an image (or MA) representation of the behavior $\mathrm{im}\,(\varphi) = \mathrm{im}\,G(\sigma)$.

The most general representation is an ARMA representation. For this let $P(z)$ and $G(z)$ be matrices of size $r \times n$ and $r \times k$ respectively, having entries in the Laurent polynomial ring $\mathbb{F}[z,z^{-1}]$. Then

$$\mathcal{B} = \Big\{ w(z) \in \mathbb{F}^n[[z,z^{-1}]]\ \mid\ \exists m(z) \in \mathbb{F}^k[[z,z^{-1}]] : P(\sigma)w(z) = G(\sigma)m(z) \Big\} \tag{4.3}$$

is called an ARMA model. One immediately verifies that the set $\mathcal{B}$ is linear and time-invariant. It is a direct consequence of Lemma 3.5 that $\mathcal{B}$ is also closed and hence complete. Theorem 4.3 therefore states that it is possible to eliminate the so called 'latent variable' $m(z)$ and describe the behavior $\mathcal{B}$ by a simpler kernel representation of the form (4.2). It follows in particular that the code $\mathrm{im}\,(\varphi) = \mathrm{im}\,G(\sigma)$ defined in (3.3) has an equivalent kernel representation of the form (4.2) but that in general the converse is not true.

REMARK 4.4. As we explained in Section 2 it is quite common to use rational encoders for convolutional codes. In the ARMA model (4.3) we required that the entries of $P(z)$ and $G(z)$ be from the Laurent polynomial ring. If $P(z)$ and $G(z)$ were rational matrices, then the behavior $\mathcal{B} \subset \mathbb{F}^n[[z,z^{-1}]]$ appearing in (4.3) might not be well defined, as we showed in Example 3.9. On the other hand if one restricts the behavior to the positive time axis $\mathbb{Z}_+$, i.e. if one assumes that $\mathcal{B} \subset \mathbb{F}^n[[z]]$, then the set (4.3) is defined even if $P(z)$ and $G(z)$ are rational encoders. This is certainly one reason why much classical system theory focused on shift spaces $\mathcal{B} \subset \mathbb{F}^n[[z]]$ or $\mathcal{B} \subset \mathbb{F}^n((z))$.

In the sequel we will concentrate on representations of the form (4.2). Again the question arises, when are two kernel representations equivalent?

LEMMA 4.5. *Two $r \times n$ matrices $P(z)$ and $\tilde{P}(z)$ defined over the Laurent polynomial ring $\mathbb{F}[z,z^{-1}]$ describe the same behavior $\ker P(\sigma) = \ker \tilde{P}(\sigma) \subset \mathbb{F}^n[[z,z^{-1}]]$ if and only if there is a $r \times r$ matrix $U(z)$, unimodular over $\mathbb{F}[z,z^{-1}]$, such that $\tilde{P}(z) = U(z)P(z)$.*

Proof. [52, Proposition III.3]. □

Similarly, if $P(z)$ and $\tilde{P}(z)$ are defined over $\mathbb{F}[z]$, then these matrices define the same behavior $\ker P(\sigma) = \ker P(\sigma) \subset \mathbb{F}^n[[z]]$ if and only if there is a matrix $U(z)$, unimodular over $\mathbb{F}[z]$, such that $\tilde{P}(z) = U(z)P(z)$.

The major difference between Definition B and Definition C seems to be that Definition C does not require irreducibility. This last concept corresponds to the term controllability (see [10]) in systems theory. We first start with some notation taken from [42]:

For a sequence $w = \sum_{-\infty}^{\infty} w_i z^i \in \mathbb{F}^n[[z, z^{-1}]]$, we use the symbol w^+ to denote the 'right half' $\sum_0^{\infty} w_i z^i$ and the symbol w^- to denote the 'left half' $\sum_{-\infty}^{0} w_i z^i$.

DEFINITION 4.6. A behavior $\mathcal{B}$ defined on $\mathbb{Z}$ is said to be *controllable* if there is some integer ℓ such that for every w and w' in $\mathcal{B}$ and every integer j there exists a $w'' \in \mathcal{B}$ such that $(z^j w'')^- = (z^j w)^-$ and $(z^{j+\ell} w'')^+ = (z^{j+\ell} w')^+$.

REMARK 4.7. Loeliger and Mittelholzer [30] speak of *strongly controllable* if a behavior satisfies the conditions of Definition 4.6. 'Weakly controllable' in contrast requires an integer ℓ which may depend on the trajectories w and w'. The notions are equivalent in our concrete setting.

We leave it as an exercise for the reader to show that irreducibility as introduced in Definition 3.4 is equivalent to controllability for linear, time-invariant and complete behaviors $\mathcal{B} \subset \mathbb{F}^n[[z, z^{-1}]]$. The next theorem gives equivalent conditions for a behavior to be controllable.

THEOREM 4.8. *(cf. [51, Prop. 4.3]) Let $P(z)$ be a $r \times n$ matrix of rank r defined over $\mathbb{F}[z, z^{-1}]$. The following conditions are equivalent:*

(i) *The behavior $\mathcal{B} = \ker P(\sigma) = \{w(z) \in \mathbb{F}^n[[z, z^{-1}]] \mid P(\sigma)w(z) = 0\}$ is controllable.*

(ii) *$P(z)$ is left prime over $\mathbb{F}[z, z^{-1}]$.*

(iii) *The behavior $\mathcal{B}$ has an image representation. This means there exists an $n \times k$ matrix $G(z)$ defined over $\mathbb{F}[z, z^{-1}]$ such that*

$$\mathcal{B} = \{w(z) \in \mathbb{F}^n[[z, z^{-1}]] \mid \exists m(z) \in \mathbb{F}^k[[z, z^{-1}]] : w(z) = G(\sigma)m(z)\}.$$

Combining the theorem with the facts that completeness corresponds to compactness and irreducibility corresponds to controllability gives a proof of Theorem 3.6.

We conclude the section by defining some parameters of a linear, time-invariant and complete behavior. For simplicity we will do this in an algebraic manner. We will first treat behaviors $\mathcal{B} \subset \mathbb{F}^n[[z]]$, i.e. behaviors in the sense of Definition C′. In Remark 4.10 we will explain how the definitions have to be adjusted for behaviors defined on the time axis $\mathbb{Z}$.

Assume that $P(z)$ is a $r \times n$ polynomial matrix of rank r defining the behavior $\mathcal{B} = \ker P(\sigma)$. There exists a matrix $U(z)$, unimodular over

$\mathbb{F}[z]$, such that $\tilde{P}(z) = U(z)P(z)$ is row-reduced with ordered row degrees $\nu_1 \geq \ldots \geq \nu_r$. The indices $\nu = (\nu_1, \ldots, \nu_r)$ are invariants of the row module of $P(z)$ (and hence also invariants of the behavior $\mathcal{B}$), and are sometimes referred to as the *Kronecker indices* or *observability indices* of $\mathcal{B}$. The invariant $\delta := \sum_{i=1}^{r} \nu_i$ is called the *McMillan degree* of the behavior $\mathcal{B}$. If we think of $\mathcal{B}$ as a convolutional code in the sense of Definition C′ then we say that $\mathcal{B}$ has transmission rate $\frac{n-r}{n}$. Finally, the free distance of the code is defined as in (2.3).

REMARK 4.9. The Kronecker indices ν are in general different from the minimal row indices (in the sense of Forney [8]) of the $\mathbb{F}(z)$-vector space generated by the rows of $P(z)$. They coincide with the minimal row indices if and only if $P(z)$ is left prime.

REMARK 4.10. If $\mathcal{B} \subset \mathbb{F}^n[[z, z^{-1}]]$ is a linear, time-invariant and complete behavior, then we can define parameters like the Kronecker indices and the McMillan degree in the following way: Assume $P(z)$ has the property that $\mathcal{B} = \ker P(\sigma)$. There exists a matrix $U(z)$, unimodular over $\mathbb{F}[z, z^{-1}]$, such that $\tilde{P}(z) = U(z)P(z)$ is row-reduced and $P(0)$ has full row rank r. One shows again that the row degrees of $\tilde{P}(z)$ are invariants of the behavior. The McMillan degree, the transmission rate and the free distance are then defined in the same way as for behaviors $\mathcal{B} \subset \mathbb{F}^n[[z]]$.

5. The module point of view. Fornasini and Valcher [5, 48] and the present author in joint work with Schumacher, Weiner and York [42, 44, 49] proposed a module-theoretic approach to convolutional codes. The module point of view simplifies the algebraic treatment of convolutional codes to a large degree, and this simplification is probably almost necessary if one wants to study convolutional codes in a multidimensional setting [5, 48, 49].

From a systems theoretic point of view, the module-theoretic approach studies linear time-invariant systems whose states start at zero and return to zero in finite time. Such dynamical systems have been studied by Hinrichsen and Prätzel-Wolters [18, 19], who recognized these systems as convenient objects for the study of systems equivalence.

In our development we will again deal with the time axes $\mathbb{Z}$ and $\mathbb{Z}_+$ in a parallel manner.

DEFINITION D. A submodule $\mathcal{C}$ of $\mathbb{F}^n[z, z^{-1}]$ is called a convolutional code.

We like the module-theoretic language. If one prefers to define everything in terms of trajectories then one could equivalently define $\mathcal{C}$ as $\mathbb{F}$-linear, time-invariant subset of $\mathbb{F}^n[[z, z^{-1}]]$ whose elements have finite support.

The analogous definition for codes supported on the positive time axis $\mathbb{Z}_+$ is:

DEFINITION D′. A submodule $\mathcal{C}$ of $\mathbb{F}^n[z]$ is called a convolutional code.

Since both the rings $\mathbb{F}[z,z^{-1}]$ and $\mathbb{F}[z]$ are principal ideal domains (PID), a convolutional code $\mathcal{C}$ has always a well-defined rank k, and there is a full-rank matrix $G(z)$ of rank k such that $\mathcal{C} = \mathrm{colsp}_{\mathbb{F}[z,z^{-1}]}G(z)$ (respectively $\mathcal{C} = \mathrm{colsp}_{\mathbb{F}[z]}G(z)$ if $\mathcal{C}$ is defined as in Definition D$'$). We will call $G(z)$ an encoder of $\mathcal{C}$, and the map

$$\varphi : \ \mathbb{F}^k[z,z^{-1}] \longrightarrow \mathbb{F}^n[z,z^{-1}], \ m(z) \longmapsto c(z) = G(z)m(z) \tag{5.1}$$

an encoding map.

REMARK 5.1. In contrast to the situation of Section 3, it is possible to define a convolutional code in the sense of Definition D (respectively Definition D$'$) using a rational encoder. For this, assume that $G(z)$ is an $n \times k$ matrix with entries in $\mathbb{F}(z)$. Then

$$\mathcal{C} = \left\{ \ c(z) \in \mathbb{F}^n[z,z^{-1}] \ \mid \ \exists m(z) \in \mathbb{F}^k[z,z^{-1}] : \ c(z) = G(z)m(z) \ \right\}$$

defines a submodule of $\mathbb{F}^n[z,z^{-1}]$. Note that the map (5.1) involving a rational encoding matrix $G(z)$ has to be 'input-restricted' in this case.

In analogy to Lemma 3.8 we have:

LEMMA 5.2. *Two $n \times k$ matrices $G(z)$ and $\tilde{G}(z)$ defined over the Laurent polynomial ring $\mathbb{F}[z,z^{-1}]$ (respectively over the polynomial ring $\mathbb{F}[z]$) generate the same code $\mathcal{C} \subset \mathbb{F}^n[z,z^{-1}]$ (respectively $\mathcal{C} \subset \mathbb{F}^n[z]$) if and only if there is a $k \times k$ matrix $U(z)$, unimodular over $\mathbb{F}[z,z^{-1}]$ (respectively over $\mathbb{F}[z]$), such that $\tilde{G}(z) = G(z)U(z)$.*

As we already mentioned earlier convolutional codes in the sense of Definitions D and D$'$ are linear and time-invariant. The following theorem answers any question about controllability (i.e. irreducibility) and completeness.

THEOREM 5.3. *A nonzero convolutional code with either Definition D or D$'$ is controllable and incomplete.*

Sketch of Proof. The proof of the completeness part of the Theorem is analogous to the proof of Theorem 3.7. In order to show controllability, let $G(z)$ be an encoding matrix for a code $\mathcal{C} \subset \mathbb{F}^n[z]$ and consider two code words $w(z) = G(z)(a_0+a_1+\cdots+a_sz^s)$ and $w'(z) = G(z)(b_0+b_1+\cdots+b_sz^s)$. The codeword $w''(z)$ required by Definition 4.6 can be constructed in the form

$$G(z)(a_0 + a_1 + \cdots + a_jz^j + b_{j+\ell}z^{j+\ell} + \cdots + \cdots + b_sz^s).$$

□

Submodules of $\mathbb{F}^n[z,z^{-1}]$ (respectively of $\mathbb{F}^n[z]$) form the Pontryagin dual of linear, time-invariant and complete behaviors in $\mathbb{F}^n[[z,z^{-1}]]$ (respectively $\mathbb{F}^n[[z]]$). In the following we follow [42] and explain this in a very explicit way when the time axis is $\mathbb{Z}$. Of course everything can be done *mutatis mutandis* when the time axis is $\mathbb{Z}_+$.

Consider the bilinear form:

$$(5.2)\qquad \begin{aligned} (\,,\,): \quad \mathbb{F}^n[[z,z^{-1}]] \times \mathbb{F}^n[z,z^{-1}] &\longrightarrow \mathbb{F} \\ (w,v) &\mapsto \sum_{i=-\infty}^{\infty} \langle w_i, v_i \rangle, \end{aligned}$$

where $\langle\,,\,\rangle$ represents the standard dot product on $\mathbb{F}^n$. One shows that $(\,,\,)$ is well defined and nondegenerate, in particular because there are only finitely many nonzero terms in the sum. For any subset $\mathcal{C}$ of $\mathbb{F}^n[z,z^{-1}]$ one defines the annihilator

$$(5.3)\qquad \mathcal{C}^\perp = \{w \in \mathbb{F}^n[[z,z^{-1}]] \mid (w,v) = 0, \forall v \in \mathcal{C}\}$$

and the annihilator of a subset $\mathcal{B}$ of $\mathbb{F}^n[[z,z^{-1}]]$ is

$$(5.4)\qquad \mathcal{B}^\perp = \{v \in \mathbb{F}^n[z,z^{-1}] \mid (w,v) = 0, \forall w \in \mathcal{B}\}.$$

The relation between these two annihilator operations is given by:

THEOREM 5.4. *If $\mathcal{C} \subseteq \mathbb{F}^n[z,z^{-1}]$ is a convolutional code with generator matrix $G(z)$, then $\mathcal{C}^\perp$ is a linear, left-shift-invariant and complete behavior with kernel representation $P(z) = G^t(z)$. Conversely, if $\mathcal{B} \subseteq \mathbb{F}^n[[z,z^{-1}]]$ is a linear, left-shift-invariant and complete behavior with kernel representation $P(z)$, then $\mathcal{B}^\perp$ is a convolutional code with generator matrix $G(z) = P^t(z)$.*

REMARK 5.5. An elementary proof of Theorem 5.4 in the case of the positive time axis $\mathbb{Z}_+$ is given in [42].

REMARK 5.6. Theorem 5.4 is a special instance of a broad duality theory between solution spaces of difference equations on the one hand and modules on the other, for which probably the most comprehensive reference is Oberst [37]. In this article Oberst [37, p. 22] works with a bilinear form which is different from (5.2). This bilinear form induces however the same duality as shown in [16]. Extensions of duality results to group codes were derived by Forney and Trott in [12].

For finite support convolutional codes in the sense of Definition D or Definition D′ the crucial issue is *observability*. In the literature there have been several definitions of observability [4, 11, 5, 9, 30, 42] and it is not entirely clear how these definitions relate to each other.

In the sequel we will follow [4, 42].

DEFINITION 5.7. (cf. [4, Prop. 2.1]) A code $\mathcal{C}$ is *observable* if there exists an integer N such that, whenever the supports of v and v' are separated by a distance of at least N and $v + v' \in \mathcal{C}$, then also $v \in \mathcal{C}$ and $v' \in \mathcal{C}$.

With this we have the 'Pontryagin dual statement' of Theorem 4.8:

THEOREM 5.8. *(cf. [42, Prop. 2.10]) Let $G(z)$ be a $n \times k$ matrix of rank k defined over $\mathbb{F}[z,z^{-1}]$. The following conditions are equivalent:*

(i) *The convolutional code* $\mathcal{C} = \text{colsp}_{\mathbb{F}[z,z^{-1}]}G(z)$ *is observable.*
(ii) $G(z)$ *is right prime over* $\mathbb{F}[z,z^{-1}]$.
(iii) *The code* $\mathcal{C}$ *has a kernel representation. This means there exists an* $r \times n$ *'parity-check matrix'* $H(z)$ *defined over* $\mathbb{F}[z,z^{-1}]$ *such that*

$$\mathcal{C} = \{\ v(z) \in \mathbb{F}^n[z,z^{-1}] \ \mid \ H(z)v(z) = 0\ \}.$$

REMARK 5.9. The concept of observability is clearly connected to the coding concept of non-catastrophicity. Indeed an encoder is non-catastrophic if and only if the code generated by this encoder is observable. In the context of Definition A (respectively Definition A′) every code has a catastrophic as well as a non-catastrophic encoder. In the module setting of Definition D every encoder of an observable code is non-catastrophic and every encoder of an non-observable code is catastrophic. If one defines a convolutional code by Definition D then one could talk of a 'non-catastrophic convolutional code'. The term observable seems however much more appropriate.

As at the end of Section 4, we now define the code parameters. We do it only for codes given by Definition D′ and leave it to the reader to adapt the definitions to codes given by Definition D.

Assume that $G(z)$ is an $n \times k$ polynomial matrix of rank k defining the code $\mathcal{C} = \text{colsp}_{\mathbb{F}[z]}G(z)$. There exists a unimodular matrix $U(z)$ such that $\tilde{G}(z) = G(z)U(z)$ is column-reduced with ordered column degrees $\kappa_1 \geq \ldots \geq \kappa_k$. The indices $\kappa = (\kappa_1, \ldots, \kappa_k)$ are invariants of the code $\mathcal{C}$, which we call the *Kronecker indices* or *controllability indices* of $\mathcal{C}$. The invariant $\delta := \sum_{i=1}^{r} \kappa_i$ is called the *degree* of the code $\mathcal{C}$. The free distance of the code is defined as in (2.3). Finally we say that $\mathcal{C}$ has transmission rate $\frac{k}{n}$.

6. First-order representations. In this section we provide an overview of the different first-order representations (realizations) associated with the convolutional codes and encoding maps which we have defined.

We start with the encoding map (2.2). As is customary in most of the coding literature, we view the map (2.2) as an input-output operator from the message space to the code space. The existence of associated state spaces and realizations can be shown on an abstract level. Kalman [22, 23] first showed how the encoding map (2.2) can be 'factored' resulting in a realization of the encoding matrix φ. Fuhrmamnn [13] refined the realization procedure in an elegant way. (Compare also [15, 17].)

In the sequel we will simply assume that a realization algorithm exists. We summarize the main results in the following two theorems:

THEOREM 6.1. *Let* $T(z)$ *be a* $p \times m$ *proper transfer function of McMillan degree* δ. *Then there exist matrices* (A, B, C, D) *of size* $\delta \times \delta$, $\delta \times m$, $p \times \delta$ *and* $p \times m$ *respectively such that*

$$T(z) = C(zI - A)^{-1}B + D. \tag{6.1}$$

The minimality conditions are that (A, B) *forms a controllable pair and* (A, C) *forms an observable pair. Finally* (6.1) *is unique in the sense that if* $T(z) = \tilde{C}(zI - \tilde{A})^{-1}\tilde{B} + \tilde{D}$ *with* $(\tilde{A}, \tilde{B})$ *controllable and* $(\tilde{A}, \tilde{C})$ *observable, then there is a unique invertible matrix* S *such that*

$$(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D}) = (SAS^{-1}, SB, CS^{-1}, D). \tag{6.2}$$

Consider the encoding map (2.2) with generator matrix $G(z)$. Let $m(z) = \sum_{i=s}^{t} m_i z^i \in \mathbb{F}^k((z))$ and $c(z) = \sum_{i=s}^{t} c_i z^i \in \mathbb{F}^n((z))$ be the sequence of message and code symbols respectively. Then one has:

THEOREM 6.2. *Assume that* $G(z)$ *has the property that* $\operatorname{rank} G(0) = k$. *Then* $G(z^{-1})$ *is a proper transfer function, and by Theorem 6.1 there exist matrices* (A, B, C, D) *of appropriate sizes such that* $G(z^{-1}) = C(zI - A)^{-1}B + D$. *The dynamics of* (2.2) *are then equivalently described by:*

$$\begin{aligned} x_{t+1} &= Ax_t + Bm_t, \\ c_t &= Cx_t + Dm_t. \end{aligned} \tag{6.3}$$

The realization (6.3) is useful if one wants to describe the dynamics of the encoder $G(z)$. It is however less useful if one is interested in the construction of codes having certain properties. The problem is that every code $\mathcal{C}$ has many equivalent encoders whose realizations appear to be completely different.

EXAMPLE 6.3. The encoders

$$G(z) = \begin{pmatrix} \dfrac{1-z}{z-4} \\ \dfrac{1+z}{z-4} \end{pmatrix} \qquad \text{and} \qquad \tilde{G}(z) = \begin{pmatrix} \dfrac{1-z}{(z-2)(z+3)} \\ \dfrac{1+z}{(z-2)(z+3)} \end{pmatrix}$$

are equivalent since they define the same code in the sense of Definition A. The transfer functions $G(z^{-1})$ and $\tilde{G}(z^{-1})$ are however very different from a systems theory point of view. Indeed, they have different McMillan degrees, and over the reals the first is stable whereas the second is not. The state space descriptions are therefor very different for these encoders.

This example should make it clear that for the purpose of constructing good convolutional codes, representation (6.3) is not very useful.

We are now coming to the realization theory of the behaviors and codes of Section 4 and 5. We will continue with our algebraic approach. The results are stated for the positive time axis $\mathbb{Z}_+$, but they hold mutatis mutandis for the time axis $\mathbb{Z}$.

THEOREM 6.4 (Existence). *Let* $P(z)$ *be an* $r \times n$ *matrix of rank* r *describing a behavior* $\mathcal{B}$ *of the form* (4.2) *with McMillan degree* δ. *Let*

$k = n - r$. Then there exist (constant) matrices G, F of size $\delta \times (\delta + k)$ and a matrix H of size $n \times (\delta + k)$ such that $\mathcal{B}$ is equivalently described by:

$$\mathcal{B} = \Big\{ w(z) \in \mathbb{F}^n[[z]] \mid \exists \zeta(z) \in \mathbb{F}^{\delta+k}[[z]] : (\sigma G - F)\zeta(z) = 0, w(z) = H\zeta(z) \Big\}. \tag{6.4}$$

Moreover the following minimality conditions will be satisfied:

(i) *G has full row rank;*

(ii) $\begin{bmatrix} G \\ H \end{bmatrix}$ *has full column rank;*

(iii) $\begin{bmatrix} zG - F \\ H \end{bmatrix}$ *is right prime.*

For a proof, see [26, Thm. 4.3] or [27, 41]. Equation (6.4) describes the behavior locally in terms of a time window of length 1. The computation of the matrices G, F, H from a kernel description is not difficult. It can even be done 'by inspection', i.e., just by rearranging the data [41]. The next result describes the extent to which minimal first-order realizations are unique. A proof is given in [26, Thm. 4.34].

THEOREM 6.5 (Uniqueness). *The matrices (G, F, H) are unique in the following way: If $(\tilde{G}, \tilde{F}, \tilde{H})$ is a second triple of matrices describing the behavior $\mathcal{B}$ through* (6.4) *and if the minimality conditions (i), (ii) and (iii) are satisfied, then there exist unique invertible matrices S and T such that*

$$(\tilde{G}, \tilde{F}, \tilde{G}) \;=\; (SGT^{-1}, SFT^{-1}, HT^{-1}). \tag{6.5}$$

The relation to the traditional state-space theory is as follows: Assume that $P(z)$ can be partitioned into $P(z) = (Y(z)\, U(z))$ with $U(z)$ a square $r \times r$ matrix and $\deg \det U(z) = \delta$, the McMillan degree of the behavior $\mathcal{B}$. Assume that (G, F, H) provides a realization for $\mathcal{B}$ through (6.4). Then one shows that the pencil $\begin{bmatrix} zG - F \\ H \end{bmatrix}$ is equivalent to the pencil:

$$\begin{bmatrix} zI_\delta - A & B \\ 0 & I_k \\ C & D \end{bmatrix}. \tag{6.6}$$

The minimality condition (iii) simply translates into the condition that (A, C) forms an observable pair, showing that the behavior $\mathcal{B}$ is observable. One also verifies that the matrices (A, B, C, D) form a realization of the proper transfer function $U(z)^{-1}Y(z)$ and that this is a minimal realization if and only if (A, B) forms a controllable pair. Finally (A, B) is controllable if and only if the behavior $\mathcal{B}$ is controllable.

The Pontryagin dual statements of Theorem 6.4 and 6.5 are (see [42]):

THEOREM 6.6 (Existence). *Let $G(z)$ be an $n \times k$ polynomial matrix generating a rate $\frac{k}{n}$ convolutional code $\mathcal{C} \subseteq \mathbb{F}^n[z]$ of degree δ. Then there*

exist $(\delta + n - k) \times \delta$ *matrices* K, L *and a* $(\delta + n - k) \times n$ *matrix* M *(all defined over* $\mathbb{F}$*) such that the code* $\mathcal{C}$ *is described by*

$$\mathcal{C} = \left\{ v(z) \in \mathbb{F}^n[z] \mid \exists x(z) \in \mathbb{F}^\delta[z] : \; zKx(z) + Lx(z) + Mv(z) = 0 \right\}. \tag{6.7}$$

Moreover the following minimality conditions will be satisfied:
(i) *K has full column rank;*
(ii) *$[K \;\; M]$ has full row rank;*
(iii) *$[zK + L \;\; | \;\; M]$ is left prime.*

Equation (6.7) describes the behavior again locally in terms of a time window of length 1.

THEOREM 6.7 (Uniqueness). *The matrices* (K, L, M) *are unique in the following way: If* $(\tilde{K}, \tilde{L}, \tilde{M})$ *is a second triple of matrices describing the code* $\mathcal{C}$ *through* (6.7) *and if the minimality conditions (i), (ii) and (iii) are satisfied, then there exist unique invertible matrices* T *and* S *such that*

$$(\tilde{K}, \tilde{L}, \tilde{M}) \;=\; (TKS^{-1}, TLS^{-1}, TM). \tag{6.8}$$

If $G(z)$ can be partitioned into $G(z) = \begin{bmatrix} Y(z) \\ U(z) \end{bmatrix}$ with $U(z)$ a square $k \times k$ matrix and $\deg \det U(z) = \delta$, the degree of the code $\mathcal{C}$, then the pencil $[zK + L \;\; | \;\; M]$ is equivalent to the pencil:

$$\begin{bmatrix} zI_\delta - A & 0_{\delta \times (n-k)} & -B \\ -C & I_{n-k} & -D \end{bmatrix}. \tag{6.9}$$

The minimality condition (iii) then translates into the condition that (A, B) forms a controllable pair, showing that the code $\mathcal{C}$ is controllable. One also verifies that the matrices (A, B, C, D) form a realization of the proper transfer function $Y(z)U(z)^{-1}$, that this is a minimal realization if and only if (A, C) forms an observable pair, and that this is the case if and only if the code $\mathcal{C}$ is observable. Finally, the Kronecker indices of $\mathcal{C}$ coincide with the controllability indices of the pair (A, B) [44].

The systems-theoretic meaning of the representation (6.9) is as follows (see [44]). Partition the code vector $v(z)$ into:

$$v(z) = \begin{bmatrix} y(z) \\ u(z) \end{bmatrix} \in \mathbb{F}^n[z]$$

and consider the equation:

$$\begin{bmatrix} zI_\delta - A & 0_{\delta \times (n-k)} & -B \\ -C & I_{n-k} & -D \end{bmatrix} \begin{bmatrix} x(z) \\ y(z) \\ u(z) \end{bmatrix} = 0. \tag{6.10}$$

Let

$$\begin{aligned} x(z) &= x_0 z^\gamma + x_1 z^{\gamma-1} + \ldots + x_\gamma; \quad x_t \in \mathbb{F}^\delta, t = 0, \ldots, \gamma, \\ u(z) &= u_0 z^\gamma + u_1 z^{\gamma-1} + \ldots + u_\gamma; \quad u_t \in \mathbb{F}^k, t = 0, \ldots, \gamma, \\ y(z) &= y_0 z^\gamma + y_1 z^{\gamma-1} + \ldots + y_\gamma; \quad y_t \in \mathbb{F}^{n-k}, t = 0, \ldots, \gamma. \end{aligned}$$

Then (6.10) is satisfied if and only if

$$\begin{aligned} x_{t+1} &= Ax_t + Bu_t, \\ y_t &= Cx_t + Du_t, \\ v_t &= \begin{pmatrix} y_t \\ u_t \end{pmatrix}, \ x_0 = 0, \ x_{\gamma+1} = 0, \end{aligned} \tag{6.11}$$

is satisfied. Note that the state-space representation (6.11) is different from the representation (6.3). Equation (6.11) describes the dynamics of the *systematic* and *rational* encoder

$$G(z)U^{-1}(z) = \begin{bmatrix} Y(z)U(z)^{-1} \\ I_k \end{bmatrix}.$$

The encoding map $u(z) \mapsto y(z) = G(z)U^{-1}(z)u(z)$ is input-restricted, i.e. $u(z)$ must be in the column module of $U(z)$ in order to make sure that $y(z)$ and $x(z)$ have finite support. In terms of systems theory, this simply means that the state should start at zero and return to zero in finite time. Linear systems satisfying these requirements have been studied by Hinrichsen and Prätzel-Wolters [18, 19].

7. Differences and similarities among the definitions. After having reviewed these different definitions for convolutional codes, we would like to make some comparison.

The definitions of Section 2 and Section 3 viewed convolutional codes as linear, time-invariant, controllable and observable behaviors, not necessarily complete. Definition C and Definition C$'$ were more general in the sense that non-controllable behaviors were accepted as codes. Definition D and Definition D$'$ were more general in the sense that non-observable codes were allowed.

In the following subsection we show that all definitions are equivalent for all practical purposes if one restricts oneself to controllable and observable codes.

7.1. Controllable and observable codes. Consider a linear, time-invariant, complete behavior $\mathcal{B} \subset \mathbb{F}^n[[z, z^{-1}]]$, i.e. a convolutional code in the sense of Definition C. Let

$$\mathcal{C} := \mathcal{B} \cap \mathbb{F}^n((z)).$$

Then one has

THEOREM 7.1. *$\mathcal{C}$ is a convolutional code in the sense of Definition A′, and its completion $\bar{\mathcal{C}}$ is the largest controllable sub-behavior of $\mathcal{B}$. Moreover, one has a bijective correspondence between controllable behaviors $\mathcal{B} \subset \mathbb{F}^n[[z, z^{-1}]]$ and convolutional codes $\mathcal{C} \subset \mathbb{F}^n((z))$ in the sense of Definition A′.*

Sketch of Proof. Let $\mathcal{B} = \ker P(\sigma) = \{w(z) \in \mathbb{F}^n[[z, z^{-1}]] \mid P(\sigma)w(z) = 0\}$. If $\mathcal{B}$ is not controllable, then $P(z)$ is not left prime and one has a factorization $P(z) = V(z)\tilde{P}(z)$, where $\tilde{P}(z)$ is left prime and describes the controllable sub-behavior $\ker \tilde{P}(\sigma) \subset \mathcal{B}$. Since $\ker V(\sigma)$ is an autonomous behavior it follows that

$$\mathcal{C} = \mathcal{B} \cap \mathbb{F}^n((z)) = \ker P(\sigma) \cap \mathbb{F}^n((z)) = \ker \tilde{P}(\sigma) \cap \mathbb{F}^n((z)).$$

It follows (compare with Theorem 3.7) that the completion $\bar{\mathcal{C}} = \ker \tilde{P}(\sigma)$. □

Consider now a convolutional code $\mathcal{C} \subset \mathbb{F}^n((z))$ in the sense of Definition A′. Define:

$$\check{\mathcal{C}} := \mathcal{C} \cap \mathbb{F}^n[z, z^{-1}]$$
$$\check{\check{\mathcal{C}}} := \mathcal{C} \cap \mathbb{F}^n[z].$$

Conversely if $\mathcal{C} \subset \mathbb{F}^n[z]$ is a convolutional code in the sense of Definition D′, then define:

$$\hat{\mathcal{C}} := \mathrm{span}_{\mathbb{F}[z,z^{-1}]}\{v(z) \mid v(z) \in \mathcal{C}\}.$$
$$\hat{\hat{\mathcal{C}}} := \mathrm{span}_{\mathbb{F}((z))}\{v(z) \mid v(z) \in \mathcal{C}\}.$$

By definition it is clear that $\hat{\mathcal{C}} \subset \hat{\hat{\mathcal{C}}}$ are convolutional codes in the sense of Definition D and Definition A′ respectively.

THEOREM 7.2. *Assume that $\mathcal{C} \subset \mathbb{F}^n((z))$ is a convolutional code in the sense of Definition A′. Then $\check{\check{\mathcal{C}}} \subset \mathbb{F}^n[z]$ is an observable code in the sense of Definition A′. Moreover the operations $\hat{}$ and $\check{}$ induce a bijective correspondence between the observable codes $\mathcal{C} \subset \mathbb{F}^n[z]$ and convolutional codes $\mathcal{C} \subset \mathbb{F}^n((z))$ in the sense of Definition A′.*

Theorem 7.2 is essentially the Pontryagin dual statement of Theorem 7.1; we leave it to the reader to work out the details. Theorem 7.1 and 7.2 together show that there is a bijection between controllable and observable codes in the sense of one definition and another definition. For controllable and observable codes the code parameters like the rate k/n, the degree δ and the Forney (Kronecker) indices are all the same. Moreover the free distance is in every case the same as well. For all practical purposes one can therefore say that the frameworks are completely equivalent, if one is only interested in controllable and observable codes.

The advantage of Definition D (respectively Definition D′) over the other definitions lies in the fact that non-observable codes become naturally part of the theory. It also seems that for construction purposes the relation between quasi-cyclic codes and convolutional codes [33, 46] is best described in a module-theoretic framework.

Definition C (respectively Definition C′) allows one to introduce non-controllable codes in a natural way.

A Laurent series setting as in Definition A′ seems to be most natural if one is interested in the description of the encoder and/or syndrome former. Extensions of the Laurent series framework to multidimensional convolutional codes is however much less natural than the polynomial framework, which is why the theory of multidimensional convolutional codes has mainly been developed in a module-theoretic framework [5, 48, 49].

7.2. Duality. In (5.2) we introduced a bilinear form which induced a bijection between behaviors $\mathcal{B} \subset \mathbb{F}^n[[z,z^{-1}]]$ and modules $\mathcal{C} \subset \mathbb{F}^n[z,z^{-1}]$. This duality is a special instance of Pontryagin duality, and generalizes to group codes [12] and multidimensional systems [37].

In this subsection we show that the bilinear form (5.2) can also be used to obtain a duality between modules and modules (both in $\mathbb{F}^n[z,z^{-1}]$) or between behaviors and behaviors (both in $\mathbb{F}^n[[z,z^{-1}]]$).

For this let $\mathcal{C} \subset \mathbb{F}^n[z,z^{-1}]$ be a submodule. Define:

$$\mathcal{C}^{\vdash} := \mathcal{C}^{\perp} \cap \mathbb{F}^n[z,z^{-1}]. \tag{7.1}$$

One immediately verifies that $\mathcal{C}^{\vdash}$ is a submodule of $\mathbb{F}^n[z,z^{-1}]$, which necessarily is observable. One always has $\mathcal{C} \subset (\mathcal{C}^{\vdash})^{\vdash}$.

One can do something similar for behaviors. For this let $\mathcal{B} \subset \mathbb{F}^n[[z,z^{-1}]]$ be a behavior. Define:

$$\mathcal{B}^{\vdash} := \left(\mathcal{B} \cap \mathbb{F}^n[z,z^{-1}]\right)^{\perp} = \overline{\mathcal{B}^{\perp}}. \tag{7.2}$$

Then it is immediate that $\mathcal{B}^{\vdash}$ is a controllable behavior, $(\mathcal{B}^{\vdash})^{\vdash} \subset \mathcal{B}$ and $(\mathcal{B}^{\vdash})^{\vdash}$ describes the controllable sub-behavior of $\mathcal{B}$.

It is also possible to adapt (5.2) for a duality of subspaces $\mathcal{C} \subset \mathbb{F}^n((z))$. For such a subspace we define:

$$\mathcal{C}^{\vdash} := \left(\mathcal{C} \cap \mathbb{F}^n[z,z^{-1}]\right)^{\perp} \cap \mathbb{F}^n((z)). \tag{7.3}$$

The duality (7.1) does not in general correspond to the linear algebra dual of the $R = \mathbb{F}[z,z^{-1}]$ module $\mathcal{C} \subset R^n$ since there is some 'time reversal' involved. The same is true for the duality (7.3), which does not correspond to the linear algebra dual of the $\mathbb{F}((z))$ vector space $\mathcal{C}$ without time reversal.

If one works however with the 'time-reversed' bilinear form:

$$\begin{array}{rccc} [\,,\,]: & \mathbb{F}^n[[z,z^{-1}]] \times \mathbb{F}^n[z,z^{-1}] & \longrightarrow & \mathbb{F} \\ & (w(z),v(z)) & \mapsto & \displaystyle\sum_{i=-\infty}^{\infty} \langle w_i, v_{-i} \rangle \end{array} \tag{7.4}$$

then the definitions (7.1) and (7.3) do correspond to the module dual (and the linear algebra dual respectively), used widely in the coding literature [38]. In this case one has: If $G(z)$ is a generator matrix of $\mathcal{C}^{\vdash}$ then $H(z) := G^t(z)$ is a parity check matrix of $(\mathcal{C}^{\vdash})^{\vdash}$.

In the Laurent-series context it is also possible to induce the duality (7.3) directly through the time-reversed bilinear form defined on the set $\mathbb{F}^n((z)) \times \mathbb{F}^n((z))$:

$$
\begin{array}{rccc}
[\,,\,]: & \mathbb{F}^n((z)) \times \mathbb{F}^n((z)) & \longrightarrow & \mathbb{F} \\
 & (w(z), v(z)) & \mapsto & \displaystyle\sum_{i=-\infty}^{\infty} \langle w_i, v_{-i} \rangle .
\end{array}
\tag{7.5}
$$

Note that the sum appearing in (7.5) is always well defined. This bilinear form has been widely used in functional analysis and in systems theory [14].

7.3. Convolutional codes as subsets of $\mathbb{F}[[z, z^{-1}]]$, a case study. In this subsection we illustrate the differences of the definitions in the peculiar case $n = 1$.

If one works with Definition A or Definition B then there exist only the two trivial codes having the 1×1 generator matrix (1) and (0) as subsets of $\mathbb{F}[[z, z^{-1}]]$.

The situation of Definition C is already more interesting. For each polynomial $p(z)$ one has the associated 'autonomous behavior':

$$
\mathcal{B} = \{\ w(z) \ \mid \ p(\sigma)w(z) = 0 \ \}\,. \tag{7.6}
$$

Autonomous behaviors are the extreme case of uncontrollable behaviors. If $\deg p(z) = \delta$, then $\mathcal{B}$ is a finite-dimensional $\mathbb{F}$-vector space of dimension δ. For coding purposes $\mathcal{B}$ is not useful at all. Indeed, the code allows only δ symbols to be chosen freely, say the symbols $w_0, w_1, \ldots, w_{\delta-1}$. With this the codeword $w(z) = \sum_{i=-\infty}^{\infty} w_i z^i \in \mathcal{B}$ is determined, and the transmission of $w(z)$ requires infinite symbols in the past and infinite symbols in the future. In other words, the code has transmission rate 0. The distance of the code is however very good, namely $d_{\text{free}}(\mathcal{B}) = \infty$. If $\mathcal{B}$ is defined on the positive time axis, i.e. $\mathcal{B} \subset \mathbb{F}[[z]]$ then the situation is only slightly better. Indeed in this situation, one sends first δ message words and then an infinite set of 'check symbols'. As these remarks make clear, a code of the form (7.6) is not very useful.

The most interesting situation happens in the setup of Definition D and Definition D'. In this situation the codes are exactly the ideals $< g(z) > \subset \mathbb{F}[z, z^{-1}]$ (respectively $< g(z) > \subset \mathbb{F}[z]$). We now show that ideals of the form $< g(z) >$ are of interest in the coding context.

EXAMPLE 7.3. Let $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$. Consider the ideal generated by $g(z) = (z+1)$. $< g(z) > \subset \mathbb{F}[z, z^{-1}]$ consists in this case of the even-weight

sequences, namely the set of all sequences with a finite and even number of ones. This code is controllable but not observable.

Ideals of the form $< g(z) >$ are the extreme case of non-observable behaviors. In principle this makes it impossible for the receiver to decode a message. However with some additional 'side-information' decoding can still be performed, as we now explain.

One of the most often used codes in practice is probably the *cyclic redundancy check code* (CRC code). These codes are the main tool to ensure error-free transmissions over the Internet. They can be defined in the following way: Let $g(z) \in \mathbb{F}[z]$ be a polynomial. Then the encoding map is simply defined as:

$$\varphi : \mathbb{F}[z] \longrightarrow \mathbb{F}[z], \ m(z) \longmapsto c(z) = g(z)m(z). \tag{7.7}$$

The code is then the ideal $< g(z) > = \mathrm{im}\,(\varphi)$. The distance of this code is 2, since there exists an integer N such that $(z^N - 1) \in < g(z) >$. As we already mentioned the code is not observable. Assume now that the sender gives some additional side information indicating the start and the end of a message. This can be either done by saying: "I will send in a moment 1 Mb", or it can be done by adding some 'stop signal' at the end of the transmission. Once the receiver knows that the transmission is over, he applies long division to compute

$$c(z) = \tilde{m}(z)g(z) + r(z), \quad \deg r(z) < \delta.$$

If $r(z) = 0$ the receiver accepts the message $\tilde{m}(z)$ as the transmitted message $m(z)$. Otherwise he will ask for retransmission.

The code performs best over a channel (like the Internet) which has the property that the whole message is transmitted correctly with probability p and with probability $1-p$ whole blocks of the message are corrupted during transmission. One immediately sees that the probability that a corrupted message $\tilde{m}(z)$ is accepted is $q^{-\delta}$, where $q = |\mathbb{F}|$ is the field size.

One might argue that the code $< g(z) > = \mathrm{im}\,(\varphi)$ is simply a cyclic block code, but this is not quite the case. Note that the protocol does not specify any length of the code word and in each transmission a different message length can be chosen. In particular the code can be even used if the message length is longer than N, where N is the smallest integer such that $(z^N - 1) \in < g(z) >$.

EXAMPLE 7.4. Let $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$ and let $g(z) = z^{20} + 1$. Assume transmission is done on a channel with very low error probability where once in a while a burst error might happen destroying a whole sequence of bits. Assume that the sender uses a stop signal where he repeats the 4 bits 0011 for 100 times. Under these assumptions the receiver can be reasonably sure once a transmission has been complete. The probability of failure to detect a burst error is in this case 2^{-20} which is less than 10^{-6}. Note that $g(z)$ is a very poor generator for a cyclic code of any block length.

REMARK 7.5. CRC codes are in practice often implemented in a slightly different way than we described it above (see e.g. [36]). The sender typically performs long division on $z^\delta m(z)$ and computes

$$z^\delta m(z) = f(z)g(z) + r(z), \quad \deg r(z) < \delta.$$

He then transmits the code word $c(z) := z^\delta m(z) - r(z) \in < g(z) >$. Clearly the schemes are equivalent. The advantage of the latter is that the message sequence $m(z)$ is transmitted in 'plain text', allowing processing of the data immediately.

7.4. Some geometric remarks. One motivation for the author to take a module-theoretic approach to convolutional coding theory has come from algebraic-geometric considerations. As is explained in [31, 39, 40], a submodule of rank k and degree δ in $\mathbb{F}^n[z]$ describes a quotient sheaf of rank k and degree δ over the projective line $\mathbb{P}^1$. The set of all such quotient sheaves having rank k and degree at most δ has the structure of a smooth projective variety denoted by $X^\delta_{k,n}$. This variety has been of central interest in the recent algebraic geometry literature. In the context of coding theory, it has actually been used to predict the existence of maximum-distance-separable (MDS) convolutional codes [43].

The set of convolutional codes in the sense of Definition A or A′ or B having rate $\frac{k}{n}$ and degree at most δ form all proper Zariski open subsets of $X^\delta_{k,n}$. The points in the closure of these Zariski open sets are exactly the non-observable codes if the rate is $\frac{1}{n}$. These geometric considerations suggest that non-observable convolutional codes should be incorporated into a complete theory of convolutional codes. The following example will help to clarify these issues:

EXAMPLE 7.6. Let $\delta = 2$, $k = 1$ and $n = 2$, i.e., consider $X^2_{1,2}$. Any code of degree at most 2 then has an encoder of the form:

$$G(z) = \begin{pmatrix} g_1(z) \\ g_2(z) \end{pmatrix} = \begin{pmatrix} a_0 + a_1 z + a_2 z^2 \\ b_0 + b_1 z + b_2 z^2 \end{pmatrix}$$

We can identify the encoder through the point $(a_0, a_1, a_2, b_0, b_1, b_2) \in \mathbb{P}^5$. The variety $X^2_{1,2}$ is in this example exactly the projective space $\mathbb{P}^5$. For codes in the sense of Definition A or A′ or B, $G(z)$ must be taken as a basic minimal encoder in order to have a unique parameterization. This requires that $g_1(z)$ and $g_2(z)$ are coprime polynomials. The set of coprime polynomials $g_1(z), g_2(z)$ viewed as a subset of $\mathbb{P}^5$ forms a Zariski open subset $U \subset \mathbb{P}^5$ described by the resultant condition

$$\det \begin{pmatrix} a_0 & 0 & b_0 & 0 \\ a_1 & a_0 & b_1 & b_0 \\ a_2 & a_1 & b_2 & b_1 \\ 0 & a_2 & 0 & b_2 \end{pmatrix} \neq 0.$$

For codes in the sense of Definition D, we require that a_0 and b_0 are not simultaneously zero in order to have a unique parameterization. Definition D leads to a larger Zariski open set V, i.e. $U \subset V \subset \mathbb{P}^5$. Only with Definition D$'$ does one obtain the whole variety $X^2_{1,2} = \mathbb{P}^5$.

In the general situation $X^\delta_{k,n}$ naturally contains the non-observable codes as well. If $k = 1$, then $X^\delta_{1,n} = \mathbb{P}^{n(\delta+1)-1}$, and the codes in the sense of Definition D$'$ having rate $\frac{1}{n}$ and degree at most δ are exactly parameterized by $X^\delta_{1,n}$.

8. Conclusion. The paper surveys a number of different definitions of convolutional codes. All definitions have in common that a convolutional code is a subset $\mathcal{C} \subset \mathbb{F}^n[[z, z^{-1}]]$ which is both linear and time-invariant. The definitions differ in requirements such as controllability, observability, completeness and restriction to finite support.

If one requires that a code be both controllable and observable, then the restriction to any finite time window will result in equivalent definitions. Actually Loeliger and Mittelholzer [30] define a convolutional code locally in terms of one trellis section and they require in their definition that a code is controllable and observable. Algebraically such a trellis section is simply described through the generalized first order description (6.4) or (6.7).

If one wants to have a theory which allows one to work with rational encoders, then it will be necessary that the code has finite support on the negative time axis $\mathbb{Z}_-$ (or alternatively on the positive time axis $\mathbb{Z}_+$). This is one reason why a large part of the coding literature works with the field of formal Laurent series.

If one wants in addition to have a theory which can accommodate non-observable codes (and such a theory seems to have some value) then it is best to work in a module-theoretic setting.

REFERENCES

[1] S. Eilenberg. *Automata, languages, and machines. Vol. A.* Academic Press, New York, 1974. Pure and Applied Mathematics, vol. **59**.

[2] P. Elias. Coding for noisy channels. *IRE Conv. Rec.*, **4**:37–46, 1955.

[3] F. Fagnani and S. Zampieri. Minimal syndrome formers for group codes. *IEEE Trans. Inform. Theory*, **45**(1):3–31, 1999.

[4] E. Fornasini and M.E. Valcher. Observability and extendability of finite support nD behaviors. In *Proc. of the 34th IEEE Conference on Decision and Control*, pp. 3277–3282, New Orleans, Louisiana, 1995.

[5] E. Fornasini and M.E. Valcher. Multidimensional systems with finite support behaviors: Signal structure, generation, and detection. *SIAM J. Control Optim.*, **36**(2):760–779, 1998.

[6] G.D. Forney. Convolutional codes I: Algebraic structure. *IEEE Trans. Inform. Theory*, IT-**16**(5):720–738, 1970.

[7] G.D. Forney. Structural analysis of convolutional codes via dual codes. *IEEE Trans. Inform. Theory*, IT-**19**(5):512–518, 1973.

[8] G.D. Forney. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. Control*, **13**(3):493–520, 1975.

[9] G.D. FORNEY. Group codes and behaviors. In G. Picci and D.S. Gilliam, editors, *Dynamical Systems, Control, Coding, Computer Vision: New Trends, Interfaces, and Interplay*, pp. 301–320. Birkäuser, Boston-Basel-Berlin, 1999.

[10] G.D. FORNEY, B. MARCUS, N.T. SINDHUSHAYANA, AND M. TROTT. A multilingual dictionary: System theory, coding theory, symbolic dynamics and automata theory. In *Different Aspects of Coding Theory*, Proceedings of Symposia in Applied Mathematics number **50**, pp. 109–138. American Mathematical Society, 1995.

[11] G.D. FORNEY AND M.D. TROTT. Controllability, observability, and duality in behavioral group systems. In *Proc. of the 34th IEEE Conference on Decision and Control*, pp. 3259–3264, New Orleans, Louisiana, 1995.

[12] G.D. FORNEY AND M.D. TROTT. The dynamics of group codes: Dual abelian group codes and systems. Preprint, August 1997; submitted to IEEE Trans. Inform. Theory, January 2000.

[13] P.A. FUHRMANN. Algebraic system theory: An analyst's point of view. *J. Franklin Inst.*, **301**:521–540, 1976.

[14] P.A. FUHRMANN. Duality in polynomial models with some applications to geometric control theory. *IEEE Trans. Automat. Control*, **26**(1):284–295, 1981.

[15] P.A. FUHRMANN. *A Polynomial Approach to Linear Algebra.* Universitext. Springer-Verlag, New York, 1996.

[16] H. GLUESING-LUERSSEN, J. ROSENTHAL, AND P.A. WEINER. Duality between multidimensional convolutional codes and systems. E-print math.OC/9905046, May 1999.

[17] M.L.J. HAUTUS AND M. HEYMANN. Linear feedback—an algebraic approach. *SIAM J. Control*, **16**:83–105, 1978.

[18] D. HINRICHSEN AND D. PRÄTZEL-WOLTERS. Solution modules and system equivalence. *Internat. J. Control*, **32**:777–802, 1980.

[19] D. HINRICHSEN AND D. PRÄTZEL-WOLTERS. Generalized Hermite matrices and complete invariants of strict system equivalence. *SIAM J. Control Optim.*, **21**:289–305, 1983.

[20] R. JOHANNESSON AND Z. WAN. A linear algebra approach to minimal convolutional encoders. *IEEE Trans. Inform. Theory*, IT-**39**(4):1219–1233, 1993.

[21] R. JOHANNESSON AND K. SH. ZIGANGIROV. *Fundamentals of Convolutional Coding.* IEEE Press, New York, 1999.

[22] R. E. KALMAN. Algebraic structure of linear dynamical systems. I. The module of $\sum$. *Proc. Nat. Acad. Sci. U.S.A.*, **54**:1503–1508, 1965.

[23] R.E. KALMAN, P.L. FALB, AND M.A. ARBIB. *Topics in Mathematical System Theory.* McGraw-Hill, New York, 1969.

[24] B. KITCHENS. Symbolic dynamics and convolutional codes. Preprint, February 2000.

[25] G. KÖTHE. *Topological Vector Spaces I.* Springer Verlag, 1969.

[26] M. KUIJPER. *First-Order Representations of Linear Systems.* Birkhäuser, Boston, 1994.

[27] M. KUIJPER AND J.M. SCHUMACHER. Realization of autoregressive equations in pencil and descriptor form. *SIAM J. Control Optim.*, **28**(5):1162–1189, 1990.

[28] S. LIN AND D.J. COSTELLO. *Error Control Coding: Fundamentals and Applications.* Prentice-Hall, Englewood Cliffs, NJ, 1983.

[29] D. LIND AND B. MARCUS. *An Introduction to Symbolic Dynamics and Coding.* Cambridge University Press, 1995.

[30] H.A. LOELIGER AND T. MITTELHOLZER. Convolutional codes over groups. *IEEE Trans. Inform. Theory*, **42**(6):1660–1686, 1996.

[31] V. LOMADZE. Finite-dimensional time-invariant linear dynamical systems: Algebraic theory. *Acta Appl. Math*, **19**:149–201, 1990.

[32] B. MARCUS. Symbolic dynamics and connections to coding theory, automata theory and system theory. In *Different aspects of coding theory (San Francisco, CA, 1995)*, vol. **50** of *Proc. Sympos. Appl. Math.*, pp. 95–108. Amer. Math. Soc., Providence, RI, 1995.

[33] J.L. Massey, D.J. Costello, and J. Justesen. Polynomial weights and code constructions. *IEEE Trans. Inform. Theory*, IT-**19**(1):101–110, 1973.

[34] J.L. Massey and M.K. Sain. Codes, automata, and continuous systems: Explicit interconnections. *IEEE Trans. Automat. Contr.*, AC-**12**(6):644–650, 1967.

[35] R.J. McEliece. The algebraic theory of convolutional codes. In V. Pless and W.C. Huffman, editors, *Handbook of Coding Theory*, volume **1**, pages 1065–1138. Elsevier Science Publishers, Amsterdam, The Netherlands, 1998.

[36] H. Nussbaumer. *Computer Communication Systems*, vol. **1**. John Wiley & Sons, Chichester, New York, 1990. Translated by John C.C. Nelson.

[37] U. Oberst. Multidimensional constant linear systems. *Acta Appl. Math*, **20**:1–175, 1990.

[38] Ph. Piret. *Convolutional Codes, an Algebraic Approach*. MIT Press, Cambridge, MA, 1988.

[39] M.S. Ravi and J. Rosenthal. A smooth compactification of the space of transfer functions with fixed McMillan degree. *Acta Appl. Math*, **34**:329–352, 1994.

[40] M.S. Ravi and J. Rosenthal. A general realization theory for higher order linear differential equations. *Systems & Control Letters*, **25**(5):351–360, 1995.

[41] J. Rosenthal and J.M. Schumacher. Realization by inspection. *IEEE Trans. Automat. Contr.*, AC-**42**(9):1257–1263, 1997.

[42] J. Rosenthal, J.M. Schumacher, and E.V. York. On behaviors and convolutional codes. *IEEE Trans. Inform. Theory*, **42**(6, Part I):1881–1891, 1996.

[43] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput.*, **10**(1):15–32, 1999.

[44] J. Rosenthal and E.V. York. BCH convolutional codes. *IEEE Trans. Inform. Theory*, **45**(6):1833–1844, 1999.

[45] M.K. Sain and J.L. Massey. Invertibility of linear time-invariant dynamical systems. *IEEE Trans. Automat. Contr.*, AC-**14**:141–149, 1969.

[46] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions of MDS-convolutional codes. Submitted to IEEE Trans. Inform. Theory, August 1999.

[47] L. Staiger. Subspaces of $GF(q)^\omega$ and convolutional codes. *Information and Control*, **59**:148–183, 1983.

[48] M.E. Valcher and E. Fornasini. On 2D finite support convolutional codes: An algebraic approach. *Multidim. Sys. and Sign. Proc.*, **5**:231–243, 1994.

[49] P. Weiner. *Multidimensional Convolutional Codes*. PhD thesis, University of Notre Dame, 1998. Available at http://www.nd.edu/~rosen/preprints.html.

[50] J.C. Willems. From time series to linear system. Part I: Finite dimensional linear time invariant systems. *Automatica*, **22**:561–580, 1986.

[51] J.C. Willems. Models for dynamics. In U. Kirchgraber and H.O. Walther, editors, *Dynamics Reported*, volume **2**, pp. 171–269. John Wiley & Sons Ltd, 1989.

[52] J.C. Willems. Paradigms and puzzles in the theory of dynamical systems. *IEEE Trans. Automat. Control*, AC-**36**(3):259–294, 1991.