Universidade de Aveiro Departamento de Matemática
2003

Maria Raquel Rocha Pinto

Representações Matriciais Fraccionárias em Codificação Convolucional

Matrix Fraction Descriptions in Convolutional Coding

Universidade de Aveiro Departamento de Matemática
2003

Maria Raquel Rocha Pinto

Representações Matriciais Fraccionárias em Codificação Convolucional

Matrix Fraction Descriptions in Convolutional Coding

tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Matemática, realizada sob a orientação científica dos Professores Doutores Ettore Fornasini, Professore Ordinario do Dipartimento di Ingegneria dell'Informazione da Università di Padova e Maria Paula Macedo Rocha Malonek, Professora Catedrática do Departamento de Matemática da Universidade de Aveiro.

o júri

presidente

Reitora da Universidade de Aveiro

vogais

Ettore Fornasini
Professore Ordinario do Dipartimento di Ingegneria dell'Informazione
da Università di Padova, Itália (Orientador)

Fernando Abel da Conceição Silva
Professor Catedrático da Faculdade de Ciências da
Universidade de Lisboa

Maria Paula Macedo Rocha Malonek
Professora Catedrática do Departamento de Matemática da
Universidade de Aveiro (Co-orientadora)

Sandro Zampieri
Professore Straordinario do Dipartimento di Ingegneria dell'Informazione
da Università di Padova, Itália

Isabel Alexandra Vieira Brás
Professora Auxiliar do Departamento de Matemática da
Universidade de Aveiro

agradecimentos

Al Professore Ettore Fornasini, con il quale è stato un piacere lavorare, per i suoi insegnamenti, per l'amicizia e per la pazienza.

À Professora Paula Rocha por me ter feito descobrir a Teoria dos Sistemas e me ter ajudado a dar os primeiros passos nesta área. Agradeço ainda todo o apoio humano e científico que me deu ao longo destes anos, em especial na fase final.

Ao Departamento de Matemática da Universidade de Aveiro, por todo o apoio e facilidades concedidas para a realização deste trabalho. E a todos os meus colegas e amigos pelo ambiente de trabalho proporcionado. Não posso deixar de agradecer à Virgínia e à Rita pela ajuda que me deram neste último ano de escrita da tese.

Al Dipartimento di Ingengeria dell'Informazione della Università di Padova per aver reso possibile questo lavoro. E a tutti i colleghi per il piacevole ambiente di lavoro e per l'aiuto che molto spesso mi hanno offerto.

A tutti gli amici di Padova, Tanja, William, Giovanna, Roberto, Paola, Nic, Lucio, Massimo, che mi hanno fatto sentire a casa.

Aos meus Amigos, Paula, Carla, Isabel, Batel e Neves, que estiveram sempre presentes e que me guiaram até ao fim desta caminhada.

Ao Amaral, Paolo e Ricardo pela preciosa ajuda que me deram nos últimos pormenores de escrita da tese e na preparação da apresentação.

Aos meus pais, à Belinha e ao Samuel, por tudo, adoro-vos.

À Fundação para a Ciência e Tecnologia pelo apoio financeiro, sem o qual não teria efectuado a minha estadia na Universidade de Pádua. Estadia essa que me permitiu a realização deste trabalho.

resumo

Os objectos de estudo desta tese são os códigos convolucionais sobre um corpo, constituídos por sequências com suporte compacto à esquerda.

Aplicando a abordagem comportamental à teoria dos sistemas, é obtida uma nova definição de código convolucional baseada em propriedades estruturais do próprio código.

Os codificadores e os formadores de síndrome de um código convolucional são, respectivamente, as representações de imagem e as representações de núcleo do código. As suas estruturas e propriedades são estudadas, utilizando representações matriciais fraccionárias (RMF's). Seguidamente, são analisados os codificadores e formadores de síndrome minimais de um código convolucional, sendo apresentada uma parametrização simples das suas RMF's. Mostra-se também como obter todos os codificadores minimais de um código convolucional por aplicação de realimentação estática do estado e pré-compensação. De modo análogo, obtêm-se todos os formadores de síndrome minimais utilizando injecção da saída e pós-compensação.

Finalmente, estudam-se os codificadores desacoplados de um código convolucional, que estão directamente ligados à sua decomposição. Apresenta-se um algoritmo para determinação de um codificador desacoplado maximal, que permitirá obter a decomposição máxima do código. Quando se restringe a análise dos codificadores desacoplados aos minimais, obtém-se um codificador canónico desacoplado e parametriza-se, utilizando RMF's, todos os codificadores minimais que apresentam grau máximo de desacoplamento.

abstract

The objects of study of this thesis are the convolutional codes over a field, constituted by left compact sequences.

To define a convolutional code we consider the behavioral approach to systems theory, and present a new definition of convolutional code, taking into account its structural properties.

Matrix Fractions Descriptions (MFD's) are used as a tool for investigating the structure of the encoders and the syndrome formers of a convolutional code, which are, respectively, the image and the kernel representations of the code. Next, we concentrate on the study of the minimal encoders and syndrome formers, and obtain a simple parametrization of their MFD's. We also show that static feedback and precompensation allow to obtain all minimal encoders of the code. The same is done for the minimal syndrome formers, using output injection and postcompensation.

Finally, we analyse the decoupled encoders of a convolutional code, which are associated with code decomposition. We provide an algorithm to determine a maximally decoupled encoder, and, consequently, the finest decomposition of the code. Restricting to minimal decoupled encoders, we first obtain a canonical decoupled one, and parametrize, via MFD's, all minimal decoupled encoders realizing the finest decomposition of the code.

Contents

1 Introduction **iii**

2 Matrix Fraction Descriptions **1**

2.1 Polynomial matrices 2

2.2 Matrix fraction descriptions of rational matrices 18

3 Convolutional codes **25**

3.1 Behavioral approach 27

3.2 Convolutional codes and their encoders 39

3.3 Code decomposition 50

3.4 Conclusion 57

4 Minimal encoders **59**

4.1 State space realization and minimal encoders 59

4.2 Structure of minimal encoders 67

4.3 Abstract states 83

4.4 State feedback and parametrization of minimal encoders 90

4.5 Conclusion 94

5 Syndrome formers **97**

5.1 Dual code 98
5.2 Syndrome formers 99
5.3 Minimal syndrome formers 104
5.4 Decoupled syndrome formers 108
5.5 Conclusion 111

6 Conclusions **113**

References **117**

Chapter 1

Introduction

"*The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.*"

in "A Mathematical Theory of Communication"; Claude E. Shannon, 1948

Efficient and reliable digital information transmission and data storage have been a major concern in the last decades. Transmission and storage of digital data have as a common feature that both transfer data from an *information source* to a *destination*. A schematic representation of a communication (or storage) system is given in Figure 1.1.

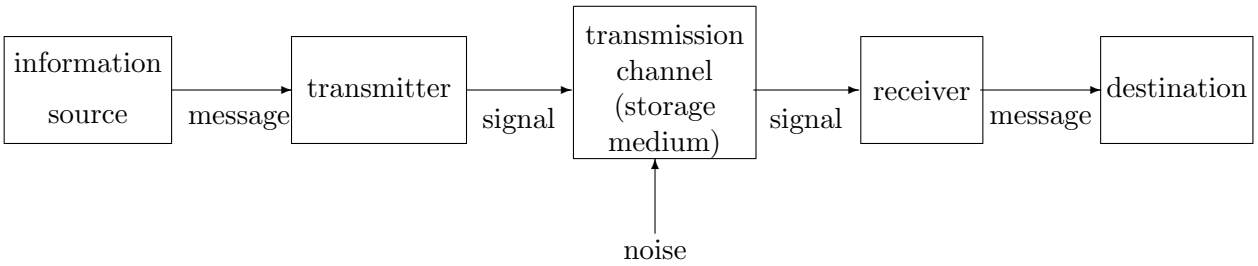

Figure 1.1 - Communication (storage) system

The scope of such system is to communicate a *message* from an information source to a destination, over a specific *transmission channel* or *storage medium*. The message is transformed into a suitable signal to be transmitted over the channel, by the *transmitter*.

To recover the original message, the *receiver* performs the inverse operation to the signal transmitted by the channel (storage medium), and delivers the reconstructed message to the destination.

In his papers [47], Shannon showed that a large class of problems related to information transmission can be approached in a systematic and disciplined way, and founded a new chapter of Mathematics: *Information Theory*.

He considered two major issues in communication, *data representation* and *message transmission over a noisy channel*.

Data representation is concerned with efficient representation of the message generated by the information source, by removing redundancy and thus compacting information. The objective is to reduce the number of "bits" that have to be sent to the receiver.

Considering the second issue, Shannon showed that with sufficient but finite redundancy, properly introduced in the message, it is possible to reconstruct the message, after channel transmission, to any desired degree of accuracy. This was stated on the Fundamental Theorem for a Discrete Channel With Noise, which, in imprecise terms, says that if the channel has capacity C (i.e., can transmit C bits per second) and rate of transmission $R < C$ bits per second, there exist encoding and decoding operations which permit to reproduce the transmitted message with a probability of error as small as desired. Note that Shannon only showed the existence of these encoding and decoding operations, he did not construct any procedure with these properties.

So, before being received by the transmitter (see Figure 1.1) the message is submitted to two operations. The first one to produce a compact data representation, and, afterwards, a second operation to introduce redundancy in an appropriate way, to allow error detection and correction, after channel transmission. The first operation is performed by the *source encoder*, while the second one is executed by the *channel encoder*. In this thesis we will only deal with channel encoders, and from now on, they will be simply called *encoders*. The *code* is the set of possible codewords produced by the encoder. Obviously, the inverse operations must be performed on the data produced by the receiver, to reconstruct the message to deliver to destination.

In 1950, Richard Hamming, motivated by the task of protecting from corruption a small

number of bits on magnetic storage media, wrote a paper [21] introducing error-correcting codes, where he described a class of single-error correcting codes, i.e., codes that can detect and correct one error in a codeword.

Although Shannon's paper [47] was published earlier than Hamming's article [21], he uses one code from Hamming's construction as an example, and cites Hamming for this code. On the other hand, Hamming does not cite Shannon's paper, but cites a short article by Golay [20], who in turn cites Shannon's paper, which shows that also Hamming was aware of Shannon's work. So, Shannon's and Hamming's works were chronologically and technically intertwined and complement each other. Hamming focusses on combinatorial aspects, and his results were constructive, while Shannon's work is based on probabilistic models and obtained existence results [49]. These works mark the beginning of a new subject of Information Theory, called *Coding Theory* [49]. Although, initially both works were cited equally often, today, many authors ascribe the origin of the entire theory to Shannon [52, 23, 1, 10, 25].

Hamming's codes were disappointingly weak compared with the stronger codes promised by the Fundamental Theorem for a Discrete Channel With Noise, stated by Shannon, and from that time, much research has been made to find better codes.

In order to more easily find good codes which are reasonably simple to implement, the class of *linear codes* has been introduced. Such codes are obtained as follows. The information sequence is divided into blocks of m information bits each. At time i, the encoder shifts an m-block of the information sequence and generates a block of p encoded bits. If $\mathbb{F}$ is a finite field, a $[p, m]$-linear code over $\mathbb{F}$ is an m-dimensional subspace of the vector space $\mathbb{F}^p$. Linear codes are the most common and seem to be as strong as general ones [50]. Most of the strongest theoretical properties are useful only for such codes, and therefore, the research for new linear codes is much more well developed compared to nonlinear ones. When dealing with sequences of discrete symbols, as considered above, which is the common representation of information, there are two basic types of linear codes: *linear block codes* and *convolutional codes*.

The basic difference between linear block codes and convolutional codes is the following. Linear block codes encode the data into independent blocks of length p, i.e., the encoded block at time i depends only on the information block at time i. In convolutional coding,

adjacent blocks of size p are interdependent, i.e., more precisely, the encoded block at time i depends not only on the information block at time i, but also on a fixed number of previous information blocks. Thus, a convolutional encoder requires memory.

Hamming's codes [21] were the first linear block codes, and no better class of codes was found until the end of the decade. These codes and their variations have been widely used for error control in digital communication and data storage [29].

Bose and Ray-Chaudhari, in 1960, [2], and Hocquenghem, in 1959, [22], independently found a remarkable generalization of the Hamming codes for multiple-error correction, over the binary field, called the BCH codes. In 1960, Reed and Solomon, [42], built a related class of codes for nonbinary channels, the Reed-Solomon codes. These codes remain among the most important class of codes. Thereafter, new codes have been discovered. There exists a well-developed algebraic theory of linear block codes, which permitted the great development of such codes. More details about linear block codes can be found in the following classical books [52, 23, 32, 29].

Convolutional codes were introduced in 1955 by Elias [7] and became popular after the invention of attractive decoding algorithms such as sequential decoding, threshold decoding and the Viterbi algorithm.

Sequential decoding was suggested first by Wozencraft in 1957 [57], as the first practical decoding method for convolutional codes, and it was further developed by Fano, in 1963, [9], who presented a most ingenious decoding algorithm, subsequently referred to as the Fano algorithm. A few years later, Zigangirov [59], in 1966, and Jelinek [24], in 1969, introduced, independently, the conceptually simplest algorithm for sequential decoding, called the stack or ZJ algorithm.

In 1963, Massey [34] showed that threshold decoding, first introduced for block codes, was also applicable to convolutional codes. It is a decoding method which is simpler to implement than sequential decoding, although less efficient.

In his famous paper [53], Viterbi presented the Viterbi algorithm as a "new probabilistic nonsequential decoding algorithm". It is an optimum decoding method for convolutional codes [29], although its performance depends on the quality of the channel and the decoding

effort grows exponentially with memory orders. In case of codes with long memory orders, sequential decoding is preferable as its decoding effort is independent of memory orders.

These decoding methods have allowed the application of convolutional codes in many diverse systems. Practical applications of convolutional codes, and also linear block codes, can be found in [29].

In the late 1960's, Massey and Sain [35, 36] established the basic connections between systems theory and convolutional coding, describing a convolutional encoder as a transfer function of a linear, time-invariant system, over a finite field. This was the point of view used thereafter in most of the coding literature [44]. In the early 1970's, Forney, in his famous paper [14], reinforced this relation. He was strongly influenced by the state-space approach to systems theory that had been introduced by Kalman [27]. In this work he layed the basis for a general algebraic theory of convolutional codes. The monograph of Piret [40] is probably the most substantial descendant of this work. It summarizes the work developed by this author on the classes of convolutional codes whose properties could be effectively analyzed by algebraic methods. In a second paper [15], Forney studied certain questions concerning convolutional codes considering dual codes. These papers provided a linear-system-theoretic structure theory for convolutional codes, and showed that the natural setting for an algebraic theory of convolutional codes is the algebraic theory of multivariable systems. Thereafter, a great number of systems theorists have worked on convolutional coding [13, 46, 48, 8].

In his paper [16], Forney decided to present the results obtained in [14] for a systems theorists audience. These two papers became an important reference (see [26],section 6.3) in this field, and are now a basic tool for algebraic theory of multivariable systems.

However, while systems theory concentrates on the input/output relation, in coding theory the important object is the set of output sequences produced by the encoder, i.e. the code.

In the 80's, Willems [55] introduced the behavioral approach to systems theory. In this approach a dynamical system is viewed as an entity which interacts with its environment. This interaction obeys to some system laws, and is expressed in terms of certain attributes and their evolution in time. If $\mathcal{W}$ is the set of values that attributes can take, and $\mathcal{T}$ the

time set, an admissible trajectory is an element of $\mathcal{W}^{\mathcal{T}}$ which satisfies the system laws, and the set of admissible trajectories is called the *behavior* of the system. A mathematical description of the system is provided by a set of equations that represent the system laws, and is called a representation of the system. Observe that although it can be specified by different (equivalent) sets of equations, the behavior of a system is unique and constitutes therefore its most intrinsic feature. For this reason, a system is identified with its behavior instead of with a set of equations that represent its laws, as happens in the classical approach.

This approach is closer to the coding situation, since a code is exactly a linear, time-invariant behavior, and an encoder is a representation of this behavior (code). Loeliger and Mittelholzer were the first ones introducing this approach in convolutional coding [31] and many other authors have used it ever since, [18, 51, 30, 58]. We will also use this approach in our definition of a convolutional code.

The encoders of a convolutional code are image representations of the code, i.e., are polynomial or rational matrices, whose rows constitute a basis of the code. In analyzing the rational encoders of a code, a very powerful tool are the Matrix Fraction Descriptions (MFD's). An MFD is a representation of a rational matrix as the "ratio" of two polynomial matrices, i.e., as the product of a polynomial matrix by the inverse of another polynomial matrix, which are called numerator and denominator, respectively. There exist many MFD's of a rational matrix, and irreducible ones can also be considered, which are MFD's with numerator and denominator having only "trivial" common factors, i.e., unimodular matrices. The set of unimodular matrices is rather large, which allows to consider irreducible MFD's of a rational matrix with different structural properties. In particular, multiplying by a unimodular matrix we can operate modifications on the degrees of the entries of a polynomial matrix, which allows to obtain a polynomial matrix with reduced (row or column) degrees. So, by eliminating a common unimodular factor we can obtain MFD's whose numerator and/or denominator satisfy some degree properties. This feature does not take place in the scalar case, obviously, and is very useful in the analysis of multi-input/multi-output transformations, and therefore, also in the analysis of the encoders of a code.

In this thesis we will investigate the structure of a convolutional code and of the family of its encoders and syndrome formers (which are the kernel representations of the code), using MFD's. A special class of encoders, and syndrome formers, are the minimal ones. We will

analyze these encoders, and syndrome formers, in detail, providing a parametrization and a realization procedure for them.

This monograph has been divided into 6 chapters. A brief outline of the content of each chapter is given as follows.

Chapter 2 - Matrix Fraction Descriptions

This chapter contains some definitions and results about polynomial and rational matrices. We begin by presenting some notions concerning polynomial matrices, which will be useful in the analysis of polynomial encoders and in the study of MFD's of rational matrices. In the second part of the chapter, MFD's of rational matrices are going to be analyzed with some detail.

Although we present well known results and we could have given them in appendix, we opted to collect them in a chapter, since Matrix Fraction Descriptions constitute the main tool used in this thesis.

Chapter 3 - Convolutional codes

According to Willems's approach, we define a dynamical system as a behavior constituted by bilateral discrete time trajectories over $\mathcal{W} = \mathbb{F}^p$, where $\mathbb{F}$ is a field, i.e., by trajectories with values on $\mathbb{F}^p$ and time set $\mathbb{Z}$. Next, we consider several structural properties of such systems, like strong controllability and strong observability. Restricting to left compact trajectories, i.e., to trajectories that start at some time $k \in \mathbb{Z}$, we will prove that strong controllability, strong observability and the existence of a polynomial basis are equivalent conditions, when we consider a behavior which is a subspace of the vector space of all left compact trajectories over $\mathbb{F}^p$. This equivalence is stated on Proposition 3.1.1, and constitutes a fundamental result of this thesis as it is the basis for our definition of convolutional code.

In a second stage, polynomial and rational encoders are analyzed, by considering MFD's for the study of the latter. Some of the results on encoders that will be considered are well known, and will be presented without proof, together with the reference of the respective author(s) or to standard textbooks where a proof is provided. We opted to present them here

for completeness. Other results have also been discovered by other author(s) but we have proved them differently, mostly, using MFD's. In these cases, we present a proof, together with the reference to the work where they have been introduced.

Finally, we concentrate on the problem of obtaining decoupled encoders of a code, which permits a decomposition of the code into smaller codes. We provide an algorithm to determine a maximally decoupled encoder, i.e., an encoder associated with the finest decomposition of the code.

Chapter 4 - Minimal encoders

In this chapter we concentrate on the study of minimal encoders, i.e., encoders that can be physically implemented with a minimal number of memory elements when considering all encoders of the code.

We start by giving a parametrization of all minimal encoders of a code in terms of their MFD's, with numerator matrix being a fixed canonical encoder. Restricting to decoupled encoders, we obtain a canonical decoupled encoder, and parametrize, via MFD's, all minimal decoupled encoders of the code.

Abstract states provide another characterization of minimal encoders, in the sense that an encoder is minimal if it has minimal number of abstract states among all encoders of the code. We will investigate how some properties of irreducible MFD's of an encoder influence the structure of its abstract state space, and obtain a classical characterization of minimal encoders, due to Forney.

We end this chapter with the presentation of a feedback realization procedure to obtain all minimal encoders of the code.

Chapter 5 - Syndrome formers

A convolutional code $\mathcal{C}$ also admits kernel representations, called the syndrome formers of the code. Syndrome formers are the transposes of the encoders of the dual code of $\mathcal{C}$. In this chapter we will use duality methods to extended some results on encoders, studied in the previous chapters, to syndrome formers. In particular, considering minimal syndrome formers, we will provide an MFD parametrization, and a realization procedure, resorting

to output injection and postcompensation, of all minimal syndrome formers of a code. We will also prove the existence of decoupled syndrome formers of a code, related with its finest decomposition.

Chapter 6 - Conclusions

Finally, in the last chapter, we summarize the main results obtained, and discuss some future work to be made.

Chapter 2

Matrix Fraction Descriptions

In this chapter we are going to introduce matrix fraction descriptions of a rational matrix, which are the fundamental tool of this thesis. We will start by presenting some definitions and results of polynomial and rational matrices that will be needed. Most of the results are well known and are given in detail in the literature [19, 26, 14, 11], and therefore their proofs will not be given.

We consider that the reader is familiarized with the basic notions in the theory of rings and fields, in particular with the ring of polynomials and the field of rational functions with coefficients in a field [3, 28].

Given a field $\mathbb{F}$, let $\mathbb{F}[d]$ and $\mathbb{F}(d)$ denote, as usually, the ring of polynomials and the field of rational functions with coefficients in $\mathbb{F}$, respectively. $\mathbb{F}[d, d^{-1}]$ represents the set of polynomials in d and d^{-1}, called *Laurent polynomials*. If $p(d, d^{-1}) = \sum_{m \leq i \leq M} p_i d^i,\ p_m p_M \neq 0$ is a Laurent polynomial, m and M will be called the *order* and the *degree* of $p(d, d^{-1})$, respectively, and $\mathbb{F}[d, d^{-1}]$ is an euclidean domain with respect to the difference $M - m$. Obviously, $\mathbb{F}[d]$ is a subset of $\mathbb{F}[d, d^{-1}]$. The units of $\mathbb{F}[d, d^{-1}]$ are the monomials $\alpha d^n, \alpha \in \mathbb{F}\backslash\{0\}, n \in \mathbb{Z}$.

Denote by $\mathbb{F}(d)^{m \times p}$ the $\mathbb{F}(d)$-vector space of the $m \times p$ matrices with entries in $\mathbb{F}(d)$ - rational matrices - and by $\mathbb{F}[d]^{m \times p}$ ($\mathbb{F}[d, d^{-1}]^{m \times p}$) the restriction of $\mathbb{F}(d)^{m \times p}$ to the matrices with entries in $\mathbb{F}[d]$ ($\mathbb{F}[d, d^{-1}]$) - polynomial matrices. As subsequent developments do not require higher generality, the matrices we shall consider are full (row or column) rank, unless

otherwise specified.

2.1 Polynomial matrices

Polynomial vectors are linearly independent over $\mathbb{F}(d)$ if and only if are linearly independent using only polynomial coefficients. So, linear dependence properties of polynomial matrices will be considered over the field $\mathbb{F}(d)$.

With this fact in mind, we introduce the following *elementary row (column) operations* on a polynomial matrix $P(d) \in \mathbb{F}[d]^{m\times p}$:

(O1) Multiply the i-th row (column) by a nonzero $\alpha \in \mathbb{F}$.

(O2) Interchange rows (columns) i and j.

(O3) Add to the i-th row (column) the j-th row (column) multiplied by an arbitrary polynomial $q(d) \in \mathbb{F}[d]$.

These operations on the rows and columns of $P(d)$ can be achieved by pre- and post-multiplication, respectively, of $P(d)$ by appropriate elementary matrices, of suitable dimension, called *elementary matrices*:

(E1) $E_1(d) = \begin{array}{c} \\ \\ \\ \\ \\ \end{array}\!\!\begin{array}{c} \begin{matrix} & & & i & & & \end{matrix} \\ \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & & \alpha & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix} \end{array}, \alpha \in \mathbb{F}\backslash\{0\};$

(E2) $E_2(d) = \begin{array}{c} \\ \\ \\ \\ \\ \end{array}\!\!\begin{array}{c} \begin{matrix} & & & i & & j & \end{matrix} \\ \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & \dots & 1 & & \\ & & \vdots & \ddots & \vdots & & \\ & & 1 & \dots & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix} \end{array};$

$$\text{(E3)}\quad E_3(d) = \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & i & & j & & \end{array} \\ \begin{bmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & \cdots & q(d) & & & \\ & & & \ddots & \vdots & & & \\ & & & & 1 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \end{bmatrix} \end{array}, q(d) \in \mathbb{F}[d].$$

In fact, the elementary row (column) operation O1 performed on $P(d)$ corresponds to pre-multiplication (post-multiplication) of $P(d)$ by $E_1(d)$. Application of elementary row (column) operation O2 on $P(d)$ is achieved pre-multiplying (post-multiplying) $P(d)$ by $E_2(d)$. Finally, elementary row operation O3 corresponds to pre-multiplication of $P(d)$ by $E_3(d)$, while the application of elementary column operation O3 is obtained by post-multiplication of $P(d)$ by $E_3(d)^T$.

The inverse of an elementary matrix is another elementary matrix of the same type.

More generally, let consider polynomial matrices which inverse is also polynomial, i.e., the units of the noncommutative ring of square polynomial matrices.

Definition 2.1.1 *A matrix $U(d) \in \mathbb{F}[d]^{q\times q}$ is unimodular if is invertible in $\mathbb{F}[d]^{q\times q}$.*

Proposition 2.1.1 *[19, 26] Let $U(d) \in \mathbb{F}[d]^{q\times q}$. The following are equivalent:*

(i) $U(d)$ is unimodular;

(ii) det $U(d) \in \mathbb{F}\backslash\{0\}$*;*

(iii) $U(d)$ can be written as a product of elementary matrices.

Obviously, elementary matrices are also unimodular.

Example 2.1.1 The matrices

$$V(d) = \begin{bmatrix} d & d^2+d+1 \\ 1 & d+1 \end{bmatrix} \in \mathbb{F}[d]^{2\times 2},$$

$$W(d) = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & d \\ d^2 & 1 & d+1 \end{bmatrix} \in \mathbb{F}[d]^{3\times 3}$$

and

$$U(d) = \begin{bmatrix} \frac{2}{3}d+\frac{1}{3} & d^2+d+1 & 0 \\ \frac{4}{3} & 2d+1 & -d \\ 0 & 0 & 1 \end{bmatrix} \in \mathbb{F}[d]^{3\times 3},$$

are unimodular matrices, with polynomial inverses,

$$V(d)^{-1} = \begin{bmatrix} -d-1 & d^2+d+1 \\ 1 & -d \end{bmatrix} \in \mathbb{F}[d]^{2\times 2},$$

$$W(d)^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ d^3+d+1 & d+1 & -d \\ -d^2-1 & -1 & 1 \end{bmatrix} \in \mathbb{F}[d]^{3\times 3}$$

and

$$U(d)^{-1} = \begin{bmatrix} -2d-1 & d^2+d+1 & d^3+d^2+d \\ \frac{4}{3} & -\frac{2}{3}d-\frac{1}{3} & -\frac{2}{3}d^2-\frac{1}{3}d \\ 0 & 0 & 1 \end{bmatrix} \in \mathbb{F}[d]^{3\times 3},$$

respectively. ♢

The above results on polynomial matrices can be extended to the ring of square Laurent polynomial matrices. In fact, they can be extended to any domain.

The most important difference comes from the fact that the units of $\mathbb{F}[d, d^{-1}]$ are the monomials αd^n, $\alpha \in \mathbb{F}\backslash\{0\}$ and $n \in \mathbb{Z}$, while the units of $\mathbb{F}[d]$ are the nonzero elements of $\mathbb{F}$.

We will only present some results on unimodular matrices over $\mathbb{F}[d, d^{-1}]$ that will be needed. To see more about about matrices with entries in a ring, i.e. integral matrices, see [39].

Definition 2.1.2 *A matrix $U(d) \in \mathbb{F}[d, d^{-1}]^{q\times q}$ is unimodular if is invertible in $\mathbb{F}[d, d^{-1}]^{q\times q}$.*

Proposition 2.1.2 *Let $U(d) \in \mathbb{F}[d, d^{-1}]^{q\times q}$. The following are equivalent:*

(i) $U(d)$ *is unimodular;*

(ii) $\det\ U(d) = \alpha d^n,\ \ \alpha \in \mathbb{F}\backslash\{0\},\ \ n \in \mathbb{Z}$.

Unimodular matrices have the same role as the nonzero constants on polynomial factorization, and allow to define an equivalence relation on $\mathbb{F}[d]^{m\times p}$.

Definition 2.1.3 *Given two matrices $P(d)$ and $Q(d)$ of $\mathbb{F}[d]^{m\times p}$, we say that $P(d)$ and $Q(d)$ are:*

(i) right-equivalent,

(ii) left-equivalent,

(iii) equivalent,

if

(I) $P(d) = Q(d)U(d)$, *i.e., $P(d)$ can be obtained from $Q(d)$ (and vice-versa) by means of elementary column operations,*

(II) $P(d) = V(d)Q(d)$, *i.e., $P(d)$ can be obtained from $Q(d)$ (and vice-versa) by means of elementary row operations,*

(III) $P(d) = \tilde{U}(d)Q(d)\tilde{V}(d)$, *i.e., $P(d)$ can be obtained from $Q(d)$ (and vice-versa) by means of elementary row and/or column operations,*

respectively, for some unimodular matrices $U(d)$, $V(d)$, $\tilde{U}(d)$ and $\tilde{V}(d)$ of suitable dimensions.

As the set of unimodular matrices of the same order with matrix multiplication is a group, the relations (i), (ii) and (iii) on $\mathbb{F}[d]^{m\times p}$ of Definition 2.1.3 are equivalence relations. Canonical forms for these equivalence relations are the *row Hermite form*, the *column Hermite form* and the *Smith form*, respectively.

Theorem 2.1.1 *[19, 26] Let $P(d)$ be an $m\times p$ polynomial matrix. There exists a unimodular matrix $U(d) \in \mathbb{F}[d]^{p\times p}$ such that*

(i) if $p \geq m$,

$$\begin{aligned} H(d) &= P(d)U(d) \\ &= \left[\begin{array}{cccc|c} h_{11}(d) & & & 0 & \\ h_{21}(d) & h_{22}(d) & & & \\ \vdots & \vdots & \ddots & & 0 \\ h_{m1}(d) & h_{m2}(d) & \dots & h_{mm}(d) & \end{array}\right] \end{aligned}$$

where $h_{ii}(d),\ i = 1,\dots,m$ are monic polynomials such that $\deg h_{ii} > \deg h_{ij},\ j < i$,

(ii) if $p < m$,

$$\begin{aligned} H(d) &= P(d)U(d) \\ &= \left[\begin{array}{cccc} h_{11}(d) & & & 0 \\ h_{21}(d) & h_{22}(d) & & \\ \vdots & \vdots & \ddots & \\ h_{p1}(d) & h_{p2}(d) & \dots & h_{pp}(d) \\ \hline h_{p+1,1}(d) & h_{p+1,2}(d) & \dots & h_{p+1,p}(d) \\ \vdots & \vdots & & \vdots \\ h_{m1}(d) & h_{m2}(d) & \dots & h_{mp}(d) \end{array}\right] \end{aligned}$$

where $h_{ii}(d),\ i = 1,\dots,p$ are monic polynomials such that $\deg h_{ii} > \deg h_{ij},\ j < i$, and no particular statements can be made about $h_{ij}(d),\ i = p+1,\dots,m,\ j = 1,\dots,p$.

$H(d)$ is the (unique) row Hermite form of $P(d)$.

Theorem 2.1.2 *[19, 26] Let $P(d)$ be an $m \times p$ polynomial matrix. There exists a unimodular matrix $U(d) \in \mathbb{F}[d]^{m \times m}$ such that*

(i) if $p \leq m$,

$$\begin{aligned} H(d) &= U(d)P(d) \\ &= \left[\begin{array}{cccc} h_{11}(d) & h_{12}(d) & \dots & h_{1p}(d) \\ & h_{22}(d) & \dots & h_{2p}(d) \\ & & \ddots & \vdots \\ 0 & & & h_{pp}(d) \\ \hline & 0 & & \end{array}\right] \end{aligned}$$

where $h_{ii}(d),\ i = 1, \dots, p$ are monic polynomials such that $\deg h_{ii} > \deg h_{ji},\ j < i$,

(ii) if $p > m$,

$$\begin{aligned} H(d) &= U(d)P(d) \\ &= \left[\begin{array}{cccc|ccc} h_{11}(d) & h_{12}(d) & \dots & h_{1m}(d) & h_{1,m+1}(d) & \dots & h_{1p}(d) \\ & h_{22}(d) & \dots & h_{2m}(d) & h_{2,m+1}(d) & & h_{2p}(d) \\ & & \ddots & \vdots & \vdots & & \vdots \\ 0 & & & h_{mm}(d) & h_{m,m+1}(d) & \dots & h_{mp}(d) \end{array}\right] \end{aligned}$$

where $h_{ii}(d),\ i = 1, \dots, m$ are monic polynomials such that $\deg h_{ii} > \deg h_{ji},\ j < i$, and no particular statements can be made about $h_{ij}(d),\ i = 1, \dots, m,\ j = m+1, \dots, p$.

$H(d)$ is the (unique) column Hermite form of $P(d)$.

Theorem 2.1.3 *[19, 26] Every polynomial matrix $P(d) \in \mathbb{F}[d]^{m \times p}$ is equivalent to a matrix*

1. *if $p \geq m$,*

$$S(d) = \left[\begin{array}{ccc|c} \gamma_1(d) & & 0 & \\ & \gamma_2(d) & & \\ & & \ddots & 0 \\ 0 & & \gamma_m(d) & \end{array}\right],$$

where $\gamma_1(d), \gamma_2(d), \dots, \gamma_m(d)$ are monic polynomials satisfying $\gamma_{i+1}(d) | \gamma_i(d),\ i = 1, \dots, m-1$.

2. if $p < m$,

$$S(d) = \left[\begin{array}{ccc|c} \gamma_1(d) & & & 0 \\ & \gamma_2(d) & & \\ & & \ddots & \\ 0 & & & \gamma_p(d) \\ \hline & 0 & & \end{array}\right],$$

where $\gamma_1(d), \gamma_2(d), \ldots, \gamma_p(d)$ are monic polynomials satisfying $\gamma_{i+1}(d)|\gamma_i(d),\ i = 1, \ldots, p-1$.

These polynomials are uniquely determined by $P(d)$ and are called invariant polynomials of $P(d)$. $S(d)$ is the Smith form of $P(d)$.

Example 2.1.2 Let

$$P(d) = \begin{bmatrix} -2d-1 & d^2+d+1 & d^3+d^2+d \\ -2 & d+1 & d^2+d \end{bmatrix} \in \mathbb{F}[d]^{2\times 3}. \tag{2.1}$$

Its row Hermite form and Smith form are

$$H(d) = \begin{bmatrix} 1 & 0 & 0 \\ \frac{2}{3} & d-1 & 0 \end{bmatrix},$$

and

$$S(d) = \begin{bmatrix} d-1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

respectively, since $P(d)U(d) = H(d)$ and $P(d) = V(d)S(d)W(d)$, for the unimodular matrices defined on Example 2.1.1. ♢

Definition 2.1.4 *Let $P(d) \in \mathbb{F}[d]^{m\times p}$.*

(i) $\Delta(d) \in \mathbb{F}[d]^{m\times m}$ is a left divisor of $P(d)$ if

$$P(d) = \Delta(d)\bar{P}(d), \tag{2.2}$$

for some $\bar{P}(d) \in \mathbb{F}[d]^{m\times p}$.

(ii) $\Delta(d) \in \mathbb{F}[d]^{m\times m}$ *is called a left maximal divisor (lMD) of* $P(d)$ *if (2.2) holds and*

$$P(d) = \hat{\Delta}(d)\hat{P}(d), \hat{\Delta}(d) \in \mathbb{F}[d]^{m\times m}, \hat{P}(d) \in \mathbb{F}[d]^{m\times p} \Rightarrow$$
$$\Rightarrow \exists F(d) \in \mathbb{F}[d]^{m\times m} \Delta(d) = \hat{\Delta}(d)F(d).$$

Matrices without nontrivial (i.e., nonunimodular) factors play an important role on matrix factorization.

Definition 2.1.5 *A polynomial matrix* $P(d) \in \mathbb{F}[d]^{m\times p}$ *is left prime if in all factorizations*

$$P(d) = \Delta(d)\bar{P}(d), \quad \Delta(d) \in \mathbb{F}[d]^{m\times m}, \;\; \bar{P}(d) \in \mathbb{F}[d]^{m\times p},$$

the left factor $\Delta(d)$ *is unimodular.*

The next lemma is an immediate consequence of the previous definitions.

Lemma 2.1.1 *[26]*

1. $\Delta(d) \in \mathbb{F}[d]^{m\times m}$ *is a lMD of* $M(d) \in \mathbb{F}[d]^{m\times p}$ *if and only if* $M(d) = \Delta(d)\bar{M}(d)$*, for some left prime matrix* $\bar{M}(d) \in \mathbb{F}[d]^{m\times p}$*.*

2. *If* $P(d) = U(d)\bar{P}(d)$ *with* $U(d) \in \mathbb{F}[d]^{m\times m}$ *unimodular and* $\bar{P}(d) \in \mathbb{F}[d]^{m\times p}$ *left prime, then* $P(d)$ *is also left prime.*

3. *A left prime matrix* $P(d) \in \mathbb{F}[d]^{m\times p}$ *has full row rank.*

Therefore, if $P(d) \in \mathbb{F}[d]^{m\times p}$ is left prime, then $m \leq p$. There are several characterizations of left prime matrices, that will be given in the next Proposition 2.1.3. First we present the Binet-Cauchy formula that will be needed in the proof of the proposition.

Theorem 2.1.4 *(Binet-Cauchy Formula) [19] If* $F \in R^{m\times p}$ *and* $G \in R^{p\times m}$*,* $m \leq p$*, where* R *is a commutative ring, then*

$$\det(FG) = \sum_i \min_i(F)\min_i(G),$$

where i runs over all the m-tuples $(\nu_1, \ldots, \nu_m)$, with $1 \leq \nu_1 < \nu_2 < \ldots < \nu_m \leq p$, $\min_i(F)$ is the minor of F correspondent to the submatrix of F, F_i, constituted by the columns indicated by i, i.e., $\min_i(F) = \det(F_i)$, and $\min_i(G)$ is the minor of G correspondent to the submatrix of G, G_i, constituted by the rows in i, i.e., $\min_i(G) = \det(G_i)$.

Proposition 2.1.3 *[11, 26] Let $P(d) \in \mathbb{F}[d]^{m\times p}$. The following are equivalent:*

(i) $P(d)$ is left prime;

(ii) the Smith form of $P(d)$ is $[\, I_m \quad 0\,]$;

(iii) the row Hermite form of $P(d)$ is $[\, I_m \quad 0\,]$;

(iv) there exists $C(d) \in \mathbb{F}[d]^{(p-m)\times p}$ such that $\begin{bmatrix} P(d) \\ C(d) \end{bmatrix}$ is unimodular;

(v) $P(d)$ admits a polynomial right inverse;

(vi) the greatest common divisor (GCD) of the m-th order minors of $P(d)$ is 1;

(vii) for all $\hat{\mathbf{r}}(d) \in \mathbb{F}(d)^{1\times m}$, $\hat{\mathbf{r}}(d)P(d) \in \mathbb{F}[d]^{1\times p}$ implies $\hat{\mathbf{r}}(d) \in \mathbb{F}[d]^{1\times m}$;

(viii) $P(\alpha)$ has rank m, for all $\alpha \in \bar{\mathbb{F}}$, where $\bar{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$.

Proof: (i) $\Longrightarrow$ (ii) Let $P(d) = U(d)S(d)V(d)$, with $U(d)$ and $V(d)$ unimodular matrices of suitable dimensions, and

$$S(d) = \left[\begin{array}{ccc|c} \gamma_1(d) & & & \\ & \ddots & & 0 \\ & & \gamma_m(d) & \end{array}\right],$$

the Smith form of $P(d)$.

If

$$V(d) = \begin{bmatrix} V_1(d) \\ V_2(d) \end{bmatrix},\ V_1(d) \in \mathbb{F}[d]^{m\times p},\ V_2(d) \in \mathbb{F}[d]^{(p-m)\times p},$$

then

$$P(d) = \Delta(d)V_1(d),$$

where $\Delta(d) = U(d)\,\mathrm{diag}\{\gamma_1(d), \ldots, \gamma_m(d)\}$.

The left primeness of $P(d)$ implies that $\Delta(d)$ is unimodular, and, as $\det\ \Delta(d) = \det\ U(d) \times \gamma_1(d) \times \ldots \times \gamma_m(d) \in \mathbb{F}\backslash\{0\}$, the invariant polynomials of $P(d)$, $\gamma_i(d),\ i = 1, \ldots, m$, are monic polynomials of degree zero, and $S(d) = [I_m\ \ 0]$.

(ii) $\Longrightarrow$ (iii) From the assumption, we have that

$$U(d)P(d)V(d) = [I_m\ \ 0], \tag{2.3}$$

where $U(d) \in \mathbb{F}[d]^{m\times m}$ and $V(d) \in \mathbb{F}[d]^{p\times p}$ are unimodular. Pre-multiplying (2.3) by $U(d)^{-1}$ and post-multiplying (2.3) by the block-diagonal matrix $\mathrm{diag}\{U(d), I_{p-m}\}$, we obtain

$$P(d)\Delta(d) = [I_m\ \ 0],$$

where $\Delta(d) = V(d)\mathrm{diag}\{U(d), I_{p-m}\} \in \mathbb{F}[d]^{p\times p}$ is unimodular, and, therefore, $[I_m\ \ 0]$ is the row Hermite form of $P(d)$.

(iii) $\Longrightarrow$ (iv) From the assumption,

$$P(d) = [I_m\ \ 0]U(d),$$

for some unimodular matrix $U(d) \in \mathbb{F}[d]^{p\times p}$, i.e., $P(d)$ is the submatrix of $U(d)$ constituted by its first m rows.

(iv) $\Longrightarrow$ (v) Let $[X(d)\ Y(d)],\ X(d) \in \mathbb{F}[d]^{p\times m},\ Y(d) \in \mathbb{F}[d]^{p\times(p-m)}$, be the inverse of $\begin{bmatrix} P(d) \\ C(d) \end{bmatrix}$. Then $P(d)X(d) = I_m$.

(v) $\Longrightarrow$ (vi) Let $X(d) \in \mathbb{F}[d]^{p\times m}$ be the polynomial right inverse of $P(d)$, i.e.,

$$P(d)X(d) = I_m. \tag{2.4}$$

Applying the Binet-Cauchy formula to calculate the determinant of $P(d)X(d)$, (2.4) implies that

$$\sum_i \min_i(P)\min_i(X) = 1,$$

i.e., the greatest common divisor of the m-th order minors of $P(d)$ is 1.

(vi) $\Longrightarrow$ (vii) Let $\hat{\mathbf{y}}(d) = \hat{\mathbf{r}}(d)P(d) \in \mathbb{F}[d]^{1\times p}$. Let further i and $\min_i(P)$ be as in Theorem 2.1.4, and S_i be a matrix such that $P(d)\,S_i$ is the submatrix of $P(d)$ with columns in i.

Since

$$(P(d)S_i)^{-1} = \frac{\operatorname{adj}(P(d)S_i)}{\min_i(P)},$$

we have that

$$P(d)S_i \operatorname{adj}(P(d)S_i) = \min_i(P) I_m,$$

and, consequently,

$$\begin{aligned} \hat{\mathbf{y}}(d)S_i \operatorname{adj}(P(d)S_i) &= \hat{\mathbf{r}}(d)P(d)S_i \operatorname{adj}(P(d)S_i) \\ &= \hat{\mathbf{r}}(d)\min_i(P). \end{aligned}$$

From the assumption, there exist polynomials $h_i(d), \quad i = 1, \ldots, \binom{p}{m}$, such that $\sum_i \min_i(P)h_i(d) = 1$, which implies that

$$\begin{aligned} \sum_i \hat{\mathbf{y}}(d)S_i \operatorname{adj}(P(d)S_i)\, h_i(d) &= \sum_i \hat{\mathbf{r}}(d) \min_i(P)\, h_i(d) \\ &= \hat{\mathbf{r}}(d) \end{aligned}$$

is polynomial.

Next we will proof that (vii) $\Longrightarrow$ (i) and (vi) $\Longleftrightarrow$ (viii) instead of (vii) $\Longrightarrow$ (viii) and (viii) $\Longrightarrow$ (i), because the proof becomes much shorter.

(vii) $\Longrightarrow$ (i) Suppose that $P(d)$ is not left prime.

If $\operatorname{rank} P(d) < m$, there exists a nonpolynomial $\hat{\mathbf{u}}(d) \in \mathbb{F}(d)$ such that $\hat{\mathbf{u}}(d)P(d) = 0$, which contradicts (vii).

If $\operatorname{rank} P(d) = m$, then there exists a nonsingular and nonunimodular $\Delta(d) \in \mathbb{F}[d]^{m\times m}$ such that

$$P(d) = \Delta(d)\bar{P}(d),$$

for some $\bar{P}(d) \in \mathbb{F}[d]^{m\times p}$.

As $\Delta(d)$ is nonunimodular, there exists $i \in \{1, \ldots, m\}$ such that $\operatorname{row}_i(\Delta(d)^{-1})$ is not polynomial and

$$\operatorname{row}_i(\Delta(d)^{-1})P(d) = \operatorname{row}_i(\bar{P}(d)) \in \mathbb{F}[d]^p,$$

which contradicts (vii).

(vi) $\iff$ (viii) The GCD of the m-th order minors of $P(d)$, $m_i(P)$, $i = 1, \ldots, \binom{p}{m}$, is 1 if and only if they have no common zeros in $\bar{\mathbb{F}}$, i.e., if and only if $\operatorname{rank} P(\alpha) = m \; \forall \alpha \in \bar{\mathbb{F}}$. $\square$

From now on, let consider only full row rank matrices.

To obtain a left maximal divisor of a nonzero polynomial matrix $P(d) \in \mathbb{F}[d]^{m\times p}$ [26], consider its row Hermite form $[H(d) \;\; 0]$, $H(d) \in \mathbb{F}[d]^{m\times m}$, i.e.,

$$P(d) = [H(d) \;\; 0]U(d), \tag{2.5}$$

for some unimodular matrix

$$U(d) = \begin{bmatrix} U_1(d) \\ U_2(d) \end{bmatrix}, \; U_1(d) \in \mathbb{F}[d]^{m\times p}, \; U_2(d) \in \mathbb{F}[d]^{(p-m)\times p}.$$

Then,

$$P(d) = H(d)U_1(d), \tag{2.6}$$

with $U_1(d)$ left prime, by Proposition 2.1.3, and, consequently, $H(d)$ is a left maximal divisor of $P(d)$, by Lemma 2.1.1.

Furthermore, all left maximal divisors of a nonzero matrix differ by a right unimodular factor, and therefore

$$H(d)V(d),$$

where $V(d)$ sweeps over all $m \times m$ unimodular matrices, gives all lMD's of $P(d)$.

Example 2.1.3 From Example 2.1.2, it follows that

$$P(d) = \begin{bmatrix} 1 & 0 \\ \frac{2}{3} & d-1 \end{bmatrix} U_1(d),$$

where

$$U_1(d) = \begin{bmatrix} -2d-1 & d^2+d+1 & d^3+d^2+d \\ \frac{4}{3} & -\frac{2}{3}d - \frac{1}{3} & -\frac{2}{3}d^2 - \frac{1}{3}d \end{bmatrix}$$

is a left prime matrix, as it is formed by the first two rows of the unimodular matrix $U(d)^{-1}$ of Example 2.1.1. Therefore, any left maximal divisor of $P(d)$ is given by

$$\begin{bmatrix} 1 & 0 \\ \frac{2}{3} & d-1 \end{bmatrix} V(d),$$

where $V(d) \in \mathbb{F}[d]^{2\times 2}$ is a unimodular matrix. $\diamondsuit$

Definition 2.1.6 *Let $M_1(d) \in \mathbb{F}[d]^{m\times p_1}$ and $M_2(d) \in \mathbb{F}[d]^{m\times p_2}$.*

(i) $\Delta(d) \in \mathbb{F}[d]^{m\times m}$ is a left common divisor of $M_1(d)$ and $M_2(d)$ if

$$M_1(d) = \Delta(d)\bar{M}_1(d) \text{ and } M_2(d) = \Delta(d)\bar{M}_2(d), \tag{2.7}$$

for some $\bar{M}_1(d) \in \mathbb{F}[d]^{m\times p_1}$ and $\bar{M}_2(d) \in \mathbb{F}[d]^{m\times p_2}$.

(ii) $\Delta(d) \in \mathbb{F}[d]^{m\times m}$ is a left greatest common divisor of $M_1(d)$ and $M_2(d)$ if (2.7) holds and if $\bar{\Delta}(d) \in \mathbb{F}[d]^{m\times m}$ is any other left common divisor of $M_1(d)$ and $M_2(d)$,

$$\Delta(d) = \bar{\Delta}(d)F(d),$$

for some $F(d) \in \mathbb{F}[d]^{m\times m}$.

Clearly, $\Delta(d)$ is a left common divisor of $M_1(d)$ and $M_2(d)$ if and only if is a left divisor of $[M_1(d)\ M_2(d)]$, and is a left greatest common divisor of $M_1(d)$ and $M_2(d)$ if and only if is a left maximal divisor of $[M_1(d)\ M_2(d)]$.

Definition 2.1.7 *$M_1(d) \in \mathbb{F}[d]^{m\times p_1}$ and $M_2(d) \in \mathbb{F}[d]^{m\times p_2}$ are left coprime if all their left common factors are unimodular.*

Proposition 2.1.4 *[26] $M_1(d) \in \mathbb{F}[d]^{m\times p_1}$ and $M_2(d) \in \mathbb{F}[d]^{m\times p_2}$ are left coprime if and only if $[M_1(d)\ M_2(d)]$ is left prime, or equivalently, if there exist $X_1(d) \in \mathbb{F}[d]^{p_1\times m}$ and $X_2(d) \in \mathbb{F}[d]^{p_2\times m}$ such that the Bézout Equation,*

$$M_1(d)X_1(d) + M_2(d)X_2(d) = I_m,$$

holds.

Example 2.1.4

$$M_1(d) = \begin{bmatrix} 1 & d \\ 0 & d+1 \end{bmatrix} \in \mathbb{F}[d]^{2\times 2} \quad \text{and} \quad M_2(d) = \begin{bmatrix} d & 1 & 1 \\ 1 & d-1 & d+4 \end{bmatrix} \in \mathbb{F}[d]^{2\times 3}$$

are left coprime, since $M_1(d)X_1(d) + M_2(d)X_2(d) = I_2$, for

$$X_1(d) = \begin{bmatrix} 1 & -d \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad X_2(d) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

♢

Among equivalent polynomial matrices we can consider the ones that have least row degrees sum. We begin by considering some preliminary results.

The degree (resp. order) of a vector of Laurent polynomials is the maximum degree (resp. minimum order) of its components.

In the same manner, the degree of a row or column of a polynomial matrix can be defined as the maximum degree of its entries.

Definition 2.1.8 *Let $P(d) \in \mathbb{F}[d]^{m\times p}$ and $k_1, \ldots, k_m$ be the row degrees of $P(d)$.*

(i) The external degree of $P(d)$, $\text{extdeg}(P)$*, is the sum of its row degrees, i.e.,* $\text{extdeg}(P) = \sum_{i=1}^{m} k_i$*;*

(ii) The internal degree of $P(d)$, $\text{intdeg}(P)$*, is the maximum degree of its m-th order minors.*

Clearly, $\text{intdeg}(P) \leq \text{extdeg}(P)$, for any $P(d) \in \mathbb{F}[d]^{m\times p}$.

Definition 2.1.9 *An $m\times p$ polynomial matrix $P(d)$ is row reduced if* $\text{extdeg}(P) = \text{intdeg}(P)$.

If $P(d) \in \mathbb{F}[d]^{m\times p}$ has row degrees $k_1, k_2 \ldots, k_m$, it can be written as

$$P(d) = \begin{bmatrix} d^{k_1} & & & \\ & d^{k_2} & & \\ & & \ddots & \\ & & & d^{k_m} \end{bmatrix} P_{\text{hr}} + P_{\text{rem}}(d), \tag{2.8}$$

where $P_{\rm rem}(d)$ is a polynomial matrix that satisfies deg $\text{row}_i(P_{\rm rem}) < k_i,\ i = 1, \ldots, m$, and $P_{\rm hr} \in \mathbb{F}^{m\times p}$ is a matrix whose i-th row comprises the coefficients of d^{k_i} in the i-th row of $P(d)$. P_{hr} is called the *leading (or higher order) row coefficient matrix.*

Proposition 2.1.5 *[26, 14] Let $P(d) \in \mathbb{F}[d]^{m\times p}$ be a matrix with row degrees $k_1, k_2, \ldots, k_m$. The following are equivalent:*

(i) $P(d)$ is row reduced;

(ii) $P_{\rm hr}$ in (2.8) has rank m;

(iii) $P(d)$ exhibits the predictable degree property

$$\deg(\hat{\mathbf{v}}P) = \max_{i:\hat{v}_i(d)\neq 0} \{k_i + \deg \hat{v}_i\}, \tag{2.9}$$

for all nonzero polynomial vectors $\hat{\mathbf{v}}(d) \in \mathbb{F}[d]^m$. [1]

Some facts concerning row reduced matrices are listed below.

Proposition 2.1.6 *[26]*

(i) If $P_1(d), P_2(d) \in \mathbb{F}[d]^{m\times p}$ are row reduced, and $P_1(d) = U(d)P_2(d)$, $U(d) \in \mathbb{F}[d]^{m\times m}$ unimodular, then - modulo a permutation - the row degrees of $P_1(d)$ and $P_2(d)$ are the same.

(ii) If $P(d) \in \mathbb{F}[d]^{m\times p}$, there exists a unimodular matrix $U(d) \in \mathbb{F}[d]^{m\times m}$ such that $U(d)P(d)$ is row reduced, and, by (i), the row degrees of $U(d)P(d)$ are uniquely determined, up to a permutation.

The following example illustrates the procedure to obtain a left equivalent row reduced matrix of a given polynomial one, by successively reducing the individual row degrees until row-reducedness is achieved.

Example 2.1.5 Consider again the matrix (2.1).

$$P(d) = \begin{bmatrix} d^3 & 0 \\ 0 & d^2 \end{bmatrix} P_{hr} + P_{rem}(d),$$

[1] or, equivalently, for all nonzero Laurent polynomial vectors $\hat{\mathbf{v}}(d, d^{-1}) \in \mathbb{F}[d, d^{-1}]^m$.

where

$$P_{hr} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad P_{rem}(d) = \begin{bmatrix} -2d-1 & d^2+d+1 & d^2+d \\ -2 & d+1 & d \end{bmatrix}.$$

$P(d)$ is not row reduce as P_{hr} is not full row rank. Then, there exists a nonzero $\mathbf{u}_1 = [u_1^1 \;\; u_2^1] = [1 \;\; -1] \in \mathbb{F}^2$ such that $\mathbf{u}_1 P_{hr} = 0$. Let $I = \{i : u_i^1 \neq 0\} = \{1, 2\}$, and choose a greater degree row among the set $\{\text{row}_j(P(d)) : j \in I\} = \{\text{row}_1(P(d)), \text{row}_2(P(d))\}$. As $\text{row}_1(P(d))$ is such a row, consider

$$\begin{aligned} \hat{\mathbf{u}}_1(d) &= [u_1^1 \;\; u_2^1 \, d^{\deg \text{row}_1(P(d)) - \deg \text{row}_2(P(d))}] \\ &= [1 \;\; -d], \end{aligned}$$

which is a polynomial vector, and is such that pre-multiplication of $P(d)$ by the unimodular matrix

$$U_1(d) = \begin{bmatrix} \hat{\mathbf{u}}_1(d) \\ \mathbf{e_2} \end{bmatrix} = \begin{bmatrix} 1 & -d \\ 0 & 1 \end{bmatrix}$$

reduces the degree of the first row of $P(d)$, without changing the others. In fact,

$$\begin{aligned} P^1(d) &= U_1(d)P(d) \\ &= \begin{bmatrix} -1 & 1 & d \\ -2 & d+1 & d^2+d \end{bmatrix}. \end{aligned}$$

$P^1(d)$ is not row reduce, as $P_{hr}^1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$ is not full row rank.

Applying the above procedure to $P^1(d)$, we determine a unimodular matrix

$$U_2(d) = \begin{bmatrix} 1 & 0 \\ d & -1 \end{bmatrix}$$

such that

$$\begin{aligned} P^2(d) &= U_2(d)P^1(d) \\ &= \begin{bmatrix} -1 & 1 & d \\ -d+2 & -1 & -d \end{bmatrix}. \end{aligned}$$

Therefore, $P^2(d) = U(d)P(d)$, where $U(d) = U_2(d)U_1(d)$ is unimodular, and $P^2(d)$ is row reduce, as $P_{hr}^2 = \begin{bmatrix} 0 & 0 & 1 \\ -1 & 0 & -1 \end{bmatrix}$ is full row rank. $\diamondsuit$

If $P(d) \in \mathbb{F}[d]^{m\times m}$ is row reduced, with row degrees $k_1 \geq \ldots \geq k_m$ and invariant polynomials $\gamma_1(d), \ldots, \gamma_m(d)$, $\gamma_{i+1}|\gamma_i$, $i = 1, \ldots, m-1$, then we have

$$\begin{aligned} \deg(\gamma_1 \ldots \gamma_t) &\geq k_1 + \ldots + k_t, \quad t = 1, \ldots, m-1 \\ \deg(\gamma_1 \ldots \gamma_m) &= k_1 + \ldots + k_m. \end{aligned} \tag{2.10}$$

Vice-versa, a Smith form $\mathrm{diag}\{\gamma_1(d), \ldots, \gamma_m(d)\}_{m\times m}$ whose row degrees satisfy (2.10) is equivalent to a row reduced matrix with row degrees $k_1, \ldots, k_m$. This is part of the contents of a remarkable theorem due to Rosenbrock [43].

All statements on "row" and "left" factors can be couched in "column" and "right" terms, upon taking transposes.

2.2 Matrix fraction descriptions of rational matrices

In analogy with scalars, rational matrices can also be represented as the "ratio" of two polynomial matrices. However, as in general matrices do not commute, we must consider left and right denominators.

Definition 2.2.1 *Let $(D_L(d), N_L(d))$ and $(N_R(d), D_R(d))$ be two pairs of polynomial matrices in $\mathbb{F}[d]^{m\times m} \times \mathbb{F}[d]^{m\times p}$ and $\mathbb{F}[d]^{m\times p} \times \mathbb{F}[d]^{p\times p}$, respectively, with $D_L(d)$ and $D_R(d)$ nonsingular,*

(i) we associate to the first one a left matrix fraction $D_L(d)^{-1}N_L(d)$ and to the second one a right matrix fraction $N_R(d)D_R(d)^{-1}$; furthermore

(a) $N_L(d), N_R(d)$ are called numerator matrices and $D_L(d), D_R(d)$ denominator matrices;

(b) $\deg\det D_L$ and $\deg\det D_R$ are said to be the determinantal degree of $D_L(d)^{-1}N_L(d)$ and $N_R(d)D_R(d)^{-1}$, respectively;

(ii) if

$$G(d) = D_L(d)^{-1}N_L(d) \in \mathbb{F}(d)^{m\times p} \quad \text{and} \quad \tilde{G}(d) = N_R(d)D_R(d)^{-1} \in \mathbb{F}(d)^{m\times p},$$

$D_L(d)^{-1}N_L(d)$ is said to be a left matrix fraction description (lMFD) of $G(d)$ and $N_R(d)D_R(d)^{-1}$ a right matrix fraction description (rMFD) of $\tilde{G}(d)$.

Any rational matrix $G(d) \in \mathbb{F}(d)^{m\times p}$ admits a left and a right matrix fraction description: if $g(d) \in \mathbb{F}[d]$ is the GCD of the denominators of the entries of $G(d)$, then $G(d) = [g(d)\, I_m]^{-1}M(d) = \tilde{M}(d)[g(d)\, I_p]^{-1}$ for suitable $M(d), \tilde{M}(d) \in \mathbb{F}[d]^{m\times p}$.

Definition 2.2.2 *$D_L(d)^{-1}N_L(d)$ is irreducible if $D_L(d)$ and $N_L(d)$ are left coprime.*

The construction described earlier (see (2.5),(2.6)) for finding a lMD of a polynomial matrix, permits to obtain an irreducible lMFD of a rational matrix $G(d) \in \mathbb{F}(d)^{m\times p}$.

In fact, consider any lMFD $D_L(d)^{-1}N_L(d)$ of $G(d)$, and apply the procedure (2.5),(2.6) to the polynomial matrix $[D_L(d) \quad N_L(d)]$ to obtain

$$[D_L(d) \quad N_L(d)] = H(d)[U_{11}(d) \quad U_{12}(d)], \tag{2.11}$$

with $H(d), U_{11}(d) \in \mathbb{F}[d]^{m\times m}$, $U_{12}(d) \in \mathbb{F}[d]^{m\times p}$ and $[U_{11}(d) \quad U_{12}(d)]$ left prime.

From (2.11), it follows that $U_{11}(d)$ is nonsingular as $D_L(d) = H(d)U_{11}(d)$ has full row rank, and that

$$G(d) = U_{11}(d)^{-1}U_{12}(d) \tag{2.12}$$

is irreducible.

The result of the above discussion is stated on the following proposition, together with some immediate consequences.

Proposition 2.2.1 *[26] Let $G(d) \in \mathbb{F}(d)^{m\times p}$.*

(i) $G(d)$ has an irreducible lMFD, $U_{11}(d)^{-1}U_{12}(d)$.

(ii) Any other irreducible lMFD of $G(d)$, $D_L(d)^{-1}N_L(d)$, is such that

$$[D_L(d) \quad N_L(d)] = V(d)\, [U_{11}(d) \quad U_{12}(d)], \tag{2.13}$$

where $V(d)$ is a suitable unimodular matrix.

(iii) Varying $V(d)$ on the group of nonsingular polynomial matrices, (2.13) allows to obtain all lMFD's of $G(d)$.

(iv) If $D_L(d)^{-1}N_L(d)$ is an irreducible lMFD of $G(d)$ with

$$[\, D_L(d) \quad N_L(d) \,] \tag{2.14}$$

row reduced, then the row degrees of (2.14) are unique, up to a permutation.

Corollary 2.2.1 *[26]*

(i) The determinant of all denominator matrices of irreducible lMFD's of $G(d) \in \mathbb{F}(d)^{m\times p}$ are associated polynomials. Therefore, irreducible lMFD's of $G(d)$ have the same determinantal degree.

(ii) The determinant of the denominator of any nonirreducible lMFD of $G(d) \in \mathbb{F}(d)^{m\times p}$ is a proper multiple of the determinant of an irreducible one. Therefore, the determinantal degree of a nonirreducible lMFD of $G(d)$ is greater than the determinantal degree of an irreducible one.

The results above are also valid for right MFD's, considering transposes and "right" and "column" terms instead of "left" and "row" ones, respectively.

Furthermore, it is possible to establish some connections between right and left MFD's of a rational matrix.

Proposition 2.2.2 *[26] Let $G(d) \in \mathbb{F}(d)^{m\times p}$ and $D_L(d)^{-1}N_L(d)$ and $N_R(d)D_R(d)^{-1}$ be irreducible MFD's of $G(d)$. Then $D_R(d)$ and $D_L(d)$ have the same nonunit invariant polynomials, and, up to nonzero constant factors, the same determinant.*

Proof: Consider the Hermite form of $[D_L(d) \quad N_L(d)]$

$$[D_L(d) \quad N_L(d)] = [H(d) \quad 0]U(d),$$

where

$$U(d) = \begin{bmatrix} U_{11}(d) & U_{12}(d) \\ U_{21}(d) & U_{22}(d) \end{bmatrix}$$

is unimodular and $U_{11}(d) \in \mathbb{F}[d]^{m\times m}$, $U_{12}(d) \in \mathbb{F}[d]^{m\times p}$, $U_{21}(d) \in \mathbb{F}[d]^{p\times m}$, $U_{22}(d) \in \mathbb{F}[d]^{p\times p}$, and $G(d) = U_{11}(d)^{-1}U_{12}(d)$ (see (2.11) and (2.12)).

Upon partitioning, accordingly, $U(d)^{-1}$,

$$U(d)^{-1} = \begin{bmatrix} V_{11}(d) & V_{12}(d) \\ V_{21}(d) & V_{22}(d) \end{bmatrix}$$

one gets

$$\begin{bmatrix} U_{11}(d) & U_{12}(d) \\ 0 & I_p \end{bmatrix} \begin{bmatrix} V_{11}(d) & V_{12}(d) \\ V_{21}(d) & V_{22}(d) \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ V_{21}(d) & V_{22}(d) \end{bmatrix}, \tag{2.15}$$

and, consequently, $V_{22}(d)$ is nonsingular.

From,

$$\begin{bmatrix} U_{11}(d) & U_{12}(d) \\ 0 & I_p \end{bmatrix} = \begin{bmatrix} I_m & U_{12}(d) \\ 0 & I_p \end{bmatrix} \begin{bmatrix} U_{11}(d) & 0 \\ 0 & I_p \end{bmatrix},$$

$$\begin{bmatrix} I_m & 0 \\ V_{21}(d) & V_{22}(d) \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ V_{21}(d) & I_p \end{bmatrix} \begin{bmatrix} I_m & 0 \\ 0 & V_{22}(d) \end{bmatrix}$$

and

$$\begin{bmatrix} I_m & 0 \\ V_{21}(d) & I_p \end{bmatrix}^{-1} = \begin{bmatrix} I_m & 0 \\ -V_{21}(d) & I_p \end{bmatrix},$$

it follows

$$\begin{bmatrix} I_m & 0 \\ -V_{21}(d) & I_p \end{bmatrix} \begin{bmatrix} I_m & U_{12}(d) \\ 0 & I_p \end{bmatrix} \begin{bmatrix} U_{11}(d) & 0 \\ 0 & I_p \end{bmatrix} \begin{bmatrix} V_{11}(d) & V_{12}(d) \\ V_{21}(d) & V_{22}(d) \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ 0 & V_{22}(d) \end{bmatrix}. \tag{2.16}$$

Since,

$$U_{11}(d)V_{12}(d) + U_{12}(d)V_{22}(d) = 0,$$

it follows that $-V_{12}(d)V_{22}(d)^{-1}$ is an irreducible rMFD of $G(d)$.

Equation (2.15) shows that $\det U_{11}$ and $\det V_{22}$ are associated polynomials, and consequently, so are $\det D_L$ and $\det D_R$.

Equation (2.16) shows that $U_{11}(d)$ and $V_{22}(d)$ (and consequently, also $D_L(d)$ and $D_R(d)$) have the same nonunit invariant polynomials. □

Example 2.2.1 Let

$$G(d) = \begin{bmatrix} \frac{d^2}{d+1} & \frac{-d^2+2d+1}{d+1} & \frac{-d^2-3d+1}{d+1} \\ \frac{1}{d+1} & \frac{d-1}{d+1} & \frac{d+4}{d+1} \end{bmatrix} \in \mathbb{F}(d)^{2\times 3}.$$

$G(d) = M_1(d)^{-1}M_2(d)$, where $M_1(d)$ and $M_2(d)$ are defined on Example 2.1.4. Since $M_1(d)$ and $M_2(d)$ are left coprime, $M_1(d)^{-1}M_2(d)$ is an irreducible lMFD of $G(d)$ and any other irreducible lMFD of $G(d)$, $D_L(d)^{-1}N_L(d)$, is such that

$$[D_L(d) \quad N_L(d)] = X(d)[M_1(d) \quad M_2(d)],$$

where $X(d) \in \mathbb{F}[d]^{2\times 2}$ is unimodular.

Furthermore, as

$$[M_1(d) \quad M_2(d)] = [I_2 \quad 0] \begin{bmatrix} 1 & d & d & 1 & 1 \\ 0 & d+1 & 1 & d-1 & d+4 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & d & d & 1 & 1 \\ 0 & d+1 & 1 & d-1 & d+4 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -d & d^2 & d^2-d-1 & d^2+4d-1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & -d-1 & -d+1 & -d-4 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

we have that

$$\begin{bmatrix} -d^2 & -d^2+d+1 & -d^2-4d+1 \\ -1 & 0 & 0 \end{bmatrix} \begin{bmatrix} -d-1 & -d+1 & -d-4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^{-1}$$

is an irreducible rMFD of $G(d)$. ♢

Lemma 2.2.1 (Generalized Bézout Identity) *[26] Let $N_R(d)D_R(d)^{-1}$ and $D_L(d)^{-1}N_L(d)$ be irreducible MFD's of $G(d) \in \mathbb{F}(d)^{m\times p}$. Then, there exist suitable polynomial matrices $X(d)$, $Y(d)$, $W(d)$ and $Z(d)$ such that the generalized Bézout identity*

$$\begin{bmatrix} X(d) & Y(d) \\ -N_L(d) & D_L(d) \end{bmatrix} \begin{bmatrix} D_R(d) & W(d) \\ N_R(d) & Z(d) \end{bmatrix} = \begin{bmatrix} I_p & 0 \\ 0 & I_m \end{bmatrix}, \tag{2.17}$$

holds. Moreover, the block matrices in (2.17) will be unimodular.

Proof: Since

$$G(d) = N_R(d)D_R(d)^{-1} = D_L(d)^{-1}N_L(d),$$

we have that

$$-N_L(d)D_R(d) + D_L(d)N_R(d) = 0. \tag{2.18}$$

As $N_R(d)$ and $D_R(d)$ are right coprime and $N_L(d)$ and $D_L(d)$ are left coprime, it follows, from Proposition 2.1.4, that there exist polynomial matrices $X(d) \in \mathbb{F}[d]^{p\times p}$, $Y(d) \in \mathbb{F}[d]^{p\times m}$, $\tilde{W}(d) \in \mathbb{F}[d]^{p\times m}$ and $\tilde{Z}(d) \in \mathbb{F}[d]^{m\times m}$ such that

$$X(d)D_R(d) + Y(d)N_R(d) = I_p$$

and

$$-N_L(d)\tilde{W}(d) + D_L(d)\tilde{Z}(d) = I_m,$$

which together with (2.18) implies that

$$\begin{bmatrix} X(d) & Y(d) \\ -N_L(d) & D_L(d) \end{bmatrix} \begin{bmatrix} D_R(d) & \tilde{W}(d) \\ N_R(d) & \tilde{Z}(d) \end{bmatrix} = \begin{bmatrix} I_p & V(d) \\ 0 & I_m \end{bmatrix}, \tag{2.19}$$

for some polynomial matrix $V(d) \in \mathbb{F}[d]^{p\times m}$.

If we multiply (2.19) on the right by

$$\begin{bmatrix} I_p & V(d) \\ 0 & I_m \end{bmatrix}^{-1} = \begin{bmatrix} I_p & -V(d) \\ 0 & I_m \end{bmatrix},$$

we obtain (2.17) with $W(d) := -D_R(d)V(d) + \tilde{W}(d) \in \mathbb{F}[d]^{p\times m}$ and $Z(d) := -N_R(d)V(d) + \tilde{Z}(d) \in \mathbb{F}[d]^{m\times m}$. □

Corollary 2.2.2 *[14] Let $N_R(d)D_R(d)^{-1}$ and $D_L(d)^{-1}N_L(d)$ be irreducible MFD's of $G(d) \in \mathbb{F}(d)^{m\times p}$. Then, $\begin{bmatrix} D_L(d) & N_L(d) \end{bmatrix}$ and $\begin{bmatrix} D_R(d) \\ N_R(d) \end{bmatrix}$ have the same internal degree.*

Proof: Substituting in (2.17) $[\, I_p \quad 0 \,] P$ for $[\, X(d) \quad Y(d) \,]$, P any $(p+m) \times (p+m)$ permutation matrix, shows that any two complementary maximal order minors in $[\, N_L(d) \quad D_L(d) \,]$ and in $\begin{bmatrix} D_R(d) \\ N_R(d) \end{bmatrix}$ are associate, and therefore the two matrices have the same internal degree. □

Chapter 3

Convolutional codes

Coding is the procedure of data protection against errors that can occur in a message during its transmission. Figure 3.1 shows in more detail the modifications that must be performed on the data to transmit it over a noisy channel.

The message $v(.)$, to be transmitted to destination by the information source, can be analog (eg. telephone, videocamera) or digital (eg. a computer sending a binary stream). The data $v(.)$ is first processed by a *source encoder* that eliminates unnecessary redundancy, and transforms $v(.)$ into a sequence $u(.)$ of symbols in a chosen alphabet $\mathcal{A}$. In practical implementations $\mathcal{A}$ is, usually, a finite field $\mathbb{F}$, with the binary field being the most used one.

As the transmission channel (or storage medium) is subject to noise, the transmitted message can be corrupted. To be able to recover the original message, the *information sequence* $u(.)$ is first injectively encoded into a *codeword* $w(.)$ by the *encoder*. This adds redundant information to $u(.)$ in a well-defined way, which, later, will permit to correct the errors introduced during the transmission.

Next, the *modulator* (or *writing unit*) transforms $w(.)$ into a waveform, converting each symbol of $w(.)$ into a corresponding analog symbol. The analog sequence obtained is transmitted through the transmission channel (or storage medium). The *demodulator* (or *reading unit*) converts the received analog sequence into a discrete one, $r(.)$, constituted by symbols in $\mathcal{A}$. The difference $e_t(.) = r(.) - w(.)$ is called the *transmission error* and, in general, is different from zero, due to noise corruption of $w(.)$ during the transmission.

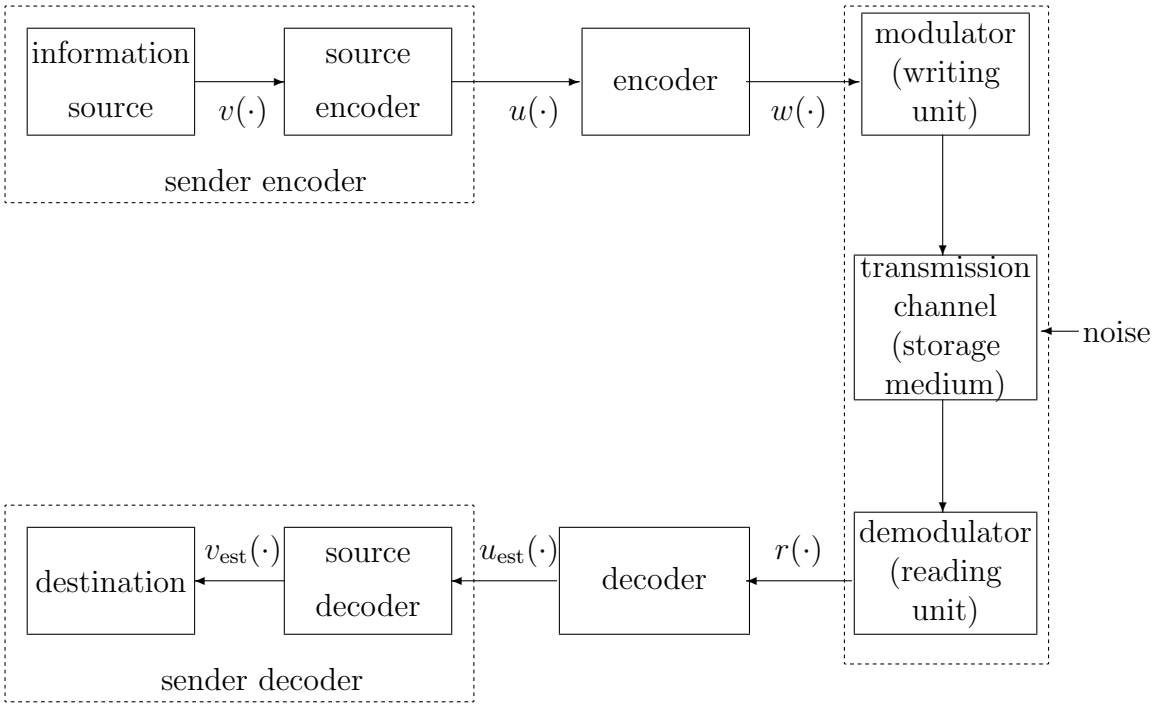

Figure 3.1 - Communication (storage) system (b)

The *decoder* uses the redundancy introduced by the encoder and the knowledge about the channel's noise, to guess which information sequence the received sequence $r(.)$ originates from. This guess is obtained by a two step operation, as shown in Figure 3.2. The *estimator* corrects the errors in $r(.)$ and produces an estimate $w_{est}(.)$ of the transmitted sequence $w(.)$. Next, the *information retriever* performs the inverse operation made by the encoder to obtain an estimate $u_{est}(.)$ of the original information sequence $u(.)$.

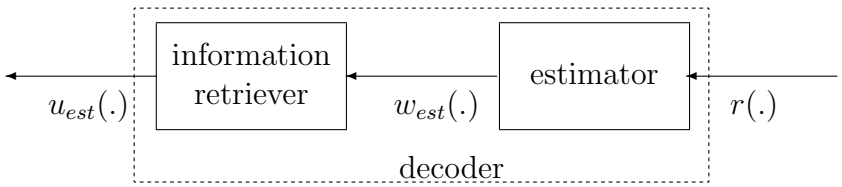

Figure 3.2 - Decoder

Finally, the *source decoder* reconstructs the original message, making the inverse operation of the source encoder, and delivers its output to the destination (see Figure 3.1).

In this chapter, we will concentrate on the encoders and on theirs output, i.e., the code. We will present a new definition of convolutional code, which is based on Willems's behavioral theory, that will be, briefly, presented next. Then, we will analyze the structure of the encoders of a code, taking into account theirs MFD's.

3.1 Behavioral approach

In Willems's behavioral theory [55, 56, 41], a *dynamical system*, $\Sigma = (\mathcal{T}, \mathcal{W}, \mathcal{B})$, models a phenomenon that evolves over the time set $\mathcal{T}$ and is described by *trajectories* that take values on the set $\mathcal{W}$, called the *alphabet*. The set of all trajectories $\mathbf{w} \in \mathcal{W}^{\mathcal{T}}$ compatible with the laws of the system is called the *behavior* and is represented by $\mathcal{B}$.

Let us restrict to discrete-time systems, i.e. $\mathcal{T} = \mathbb{Z}$, with trajectories taking values in $\mathbb{F}^p$, where $\mathbb{F}$ is a finite field. A discrete time trajectory $\mathbf{w}$ with values in $\mathbb{F}^p$ is a mapping from $\mathbb{Z}$ into $\mathbb{F}^p$,

$$\mathbf{w} : \mathbb{Z} \to \mathbb{F}^p : t \mapsto \mathbf{w}_t. \tag{3.1}$$

The trajectory $\mathbf{w} \in (\mathbb{F}^p)^{\mathbb{Z}}$ can be represented either as a bilateral sequence indexed by $\mathbb{Z}$, $\mathbf{w} = \ldots \mathbf{w}_{-1}\mathbf{w}_0\mathbf{w}_1 \ldots$ ($(\mathbb{F}^p)^{\mathbb{Z}} \simeq \ldots \times \mathbb{F}^p \times \mathbb{F}^p \times \ldots$) or as a bilateral formal power series, $\hat{\mathbf{w}}(d) := \sum_t \mathbf{w}_t d^t$, where d can be regarded merely as a placeholder, i.e. powers of d correspond to time instants. In the sequel we shall use the sequence and the corresponding series interchangeably, depending on the problem we are dealing with. For the sake of simplicity of notation we will also denote by $\mathcal{B}$ the set of the series corresponding to the sequences of a behavior $\mathcal{B}$.

If $\hat{\mathbf{w}}^{(1)}$ and $\hat{\mathbf{w}}^{(2)}$ are two bilateral formal power series, their sum is the bilateral formal power series

$$(\hat{\mathbf{w}}^{(1)} + \hat{\mathbf{w}}^{(2)})(d) := \sum_t (\mathbf{w}_t^{(1)} + \mathbf{w}_t^{(2)}) d^t, \tag{3.2}$$

and if $\hat{\mathbf{w}}(d)$ is a bilateral power series and $\alpha \in \mathbb{F}$, scalar multiplication of $\hat{\mathbf{w}}(d)$ by α produces the bilateral power series

$$(\alpha\hat{\mathbf{w}})(d) := \sum_t (\alpha \mathbf{w}_t) d^t. \tag{3.3}$$

The *support* and the *span* of a trajectory $\mathbf{w}$ (and of the corresponding series $\hat{\mathbf{w}}(d)$) are the subsets of $\mathbb{Z}$

$$\begin{aligned} \text{supp}(\mathbf{w}) &= \{t \in \mathbb{Z} : \mathbf{w}_t \neq 0\} \\ \text{span}(\mathbf{w}) &= [\inf \text{supp}(\mathbf{w}), \sup \text{supp}(\mathbf{w})], \end{aligned}$$

respectively.

The universe of all trajectories $(\mathbb{F}^p)^{\mathbb{Z}}$ is endowed with an $\mathbb{F}$-linear structure, with respect to operations (3.2) and (3.3). The imposition of these linearity properties also to the behavior, permits the application of standard mathematical structures to the system.

Definition 3.1.1 *The system $\Sigma = (\mathbb{Z}, \mathbb{F}^p, \mathcal{B})$ is linear if $\mathcal{B}$ is an $\mathbb{F}$-subspace of $(\mathbb{F}^p)^{\mathbb{Z}}$.*

The *one-step forward* (resp. *backward*) *shift* of a trajectory $\mathbf{w} \in (\mathbb{F}^p)^{\mathbb{Z}}$, $\sigma\mathbf{w}$ ($\sigma^{-1}\mathbf{w}$):

$$\begin{aligned} \sigma\mathbf{w} &: \mathbb{Z} \to \mathbb{F}^p : t \mapsto \mathbf{w}_{t-1} \\ \sigma^{-1}\mathbf{w} &: \mathbb{Z} \to \mathbb{F}^p : t \mapsto \mathbf{w}_{t+1} \end{aligned}$$

is obtained through the multiplication by d (resp. d^{-1}) of the corresponding series $\hat{\mathbf{w}}(d) = \sum \mathbf{w}_t\, d^t$:

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

Definition 3.1.2 *The system $\Sigma = (\mathbb{Z}, \mathbb{F}^p, \mathcal{B})$ is time-invariant if it is closed under forward and backward shift, i.e., if when $\mathbf{w} \in \mathcal{B}$ then $\sigma\mathbf{w}$ and $\sigma^{-1}\mathbf{w}$ are also in $\mathcal{B}$.*

Time-invariance is an important constraint because it implies that the behavior is described by laws that are constant over time.

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

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

The restriction of a sequence $\mathbf{w}$ to a certain time interval $I \subset \mathbb{Z}$, $\mathbf{w}|_I$, represents the function

$$\mathbf{w}|_I : I \to \mathbb{F}^p : t \mapsto \mathbf{w}_t, \tag{3.4}$$

and if $\mathcal{B} \subset (\mathbb{F}^p)^{\mathbb{Z}}$ and $I \subset \mathbb{Z}$,

$$\mathcal{B}|_I := \{\mathbf{w}|_I : \mathbf{w} \in \mathcal{B}\}.$$

In the classical approach, controllability and observability are properties of system representations, specifically of state space representations of the system. In Willems's theory, controllability and observability are defined as properties of the behavior of the system, and are somehow connected with the "memory" of the system.

Controllability of a behavior $\mathcal{B}$ is related with the "independence" of restrictions of $\mathcal{B}$ to time intervals that are sufficiently "separated", more concretely, the ("remote") past of a trajectory does not influence its future.

Observability is closely related with the memory of the system, as it depends on how long a trajectory must be observed before its past and future become independent.

Definition 3.1.3 *Let $\mathcal{B}$ be a subset of $(\mathbb{F}^p)^{\mathbb{Z}}$.*

(i) $\mathcal{B}$ is N-controllable (for some $N \in \mathbb{N}$) if, given any two trajectories $\mathbf{w}^{(1)}$ and $\mathbf{w}^{(2)}$ in $\mathcal{B}$ and an arbitrary time instant θ, there exists a suitable $\mathbf{r} \in \mathcal{B}$ such that

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

If there is an $N \in \mathbb{N}$ such that $\mathcal{B}$ is N-controllable then $\mathcal{B}$ is said to be strongly controllable.

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

$\mathcal{B}$ *is strongly observable if there is an* $L \in \mathbb{N}$ *such that* $\mathcal{B}$ *is L-observable.*

Remark: In Willems's behavioral theory a system $\Sigma = (\mathcal{T}, \mathcal{W}, \mathcal{B})$ is controllable if for any $\mathbf{w}^{(1)}$, $\mathbf{w}^{(2)} \in \mathcal{B}$ and an arbitrary time instant θ, there exists an $N \in \mathbb{N}$ and a suitable $\mathbf{r} \in \mathcal{B}$ such that

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

Observe that this definition is not the same as the definition of strong controllability presented in Definition 3.1.3 (i), which fixes a time interval length, N, to "connect" any two trajectories, while in Willems's theory, N depends of the considered trajectories.

On the other hand, a system $\Sigma = (\mathcal{T}, \mathcal{W}, \mathcal{B})$ whose behavior is L-observable (strong observable), as introduced in Definition 3.1.3 (ii), is said to have L-finite memory (finite memory) in Willems's theory.

We opted to consider these concepts as stated in Definition 3.1.3 because they were used by Loeliger and Mittelholzer [31] when they defined, the first time, a convolutional code using the behavioral approach.

A trajectory $\mathbf{w} \in (\mathbb{F}^p)^{\mathbb{Z}}$ is left compact if there exists $h \in \mathbb{Z}$ such that $\mathbf{w}_t = 0,\ \forall t < h$. In this case, its series representation,

$$\sum_{t=h}^{+\infty} \mathbf{w}_t d^t = \sum_{t=h}^{+\infty} \begin{bmatrix} w_{1t} \\ \vdots \\ w_{p_t} \end{bmatrix} d^t = \begin{bmatrix} \sum_{t=h}^{+\infty} w_{1t} d^t \\ \vdots \\ \sum_{t=h}^{+\infty} w_{p_t} d^t \end{bmatrix}$$

has components in the set of the *formal Laurent power series* in d over $\mathbb{F}$,

$$\mathbb{F}((d)) = \left\{ \sum_{t=h}^{+\infty} w_t d^t \in \mathbb{F}^{\mathbb{Z}},\ h \in \mathbb{Z} \right\}.$$

The sum of two formal Laurent power series, as defined in (3.2), is also a formal Laurent

power series. Moreover, if $\hat{w}_1(d) = \sum_{t=h_1}^{+\infty} w_{1t}d^t$ and $\hat{w}_2(d) = \sum_{t=h_2}^{+\infty} w_{2t}d^t$ belong to $\mathbb{F}((d))$, their (Cauchy) product

$$(\hat{w}_1.\hat{w}_2)(d) = \sum_{t=h_1+h_2}^{+\infty} \sum_{i+j=t} w_{1i}w_{2j}d^t$$

is also a formal Laurent power series, and $\mathbb{F}((d))$ is a field with respect to these sum and product operations.

Therefore, the $\mathbb{F}((d))$-vector space $\mathbb{F}((d))^p$ ($\cong$ $\mathbb{F}((d))^p$) represents all left compact trajectories of $(\mathbb{F}^p)^{\mathbb{Z}}$ and every $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$ is linear and time-invariant.

Given a nonzero formal Laurent power series $\hat{\mathbf{w}}(d) = \sum_{t=h}^{+\infty} \mathbf{w}_t d^t$, $\mathbf{w}_h \neq 0$, we call h the order of $\hat{\mathbf{w}}(d)$.

We say that a sequence $\mathbf{w}$ is *causal* if $\mathbf{w}_t = 0$, for $t < 0$. Obviously, polynomials in $\mathbb{F}[d]$ are causal sequences, and a rational function $\hat{w}(d) = \frac{p(d)}{q(d)}$ is causal if and only if $\deg q(d) \geq \deg p(d)$, or equivalently, in the case that $\frac{p(d)}{q(d)}$ is irreducible, if and only if $q(0) \neq 0$.

The restriction of $\mathbb{F}((d))$ to series of order greater or equal to zero, i.e. causal sequences, gives the set of *formal power series* and is represented by $\mathbb{F}[[d]]$.

When dealing with a family of left-compact trajectories $\mathcal{B}$ which corresponds to an $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$, strong controllability and strong observability are equivalent properties, as shown in the following proposition.

Proposition 3.1.1 *Let $\mathcal{B}$ be an $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$. The following are equivalent:*

(i) $\mathcal{B}$ is strongly observable.

(ii) $\mathcal{B}$ is strongly controllable.

(iii) $\mathcal{B}$ admits a polynomial basis.

Proof: $(i) \Rightarrow (ii)$ Suppose that $\mathcal{B}$ is N-observable, for some $N \in \mathbb{N}$. Denote by $\mathcal{B}^{(i)}$ the

$\mathbb{F}$-subspace of $\mathcal{B}$ constituted by all trajectories in $\mathcal{B}$ with support in $[i, +\infty)$. Clearly

$$\mathcal{B} \supseteq \ldots \supseteq \mathcal{B}^{(-2)} \supseteq \mathcal{B}^{(-1)} \supseteq \mathcal{B}^{(0)}$$

and consequently the same inclusions hold for the restriction subspaces

$$\mathcal{B}|_{[0,N)} \supseteq \ldots \supseteq \mathcal{B}^{(-2)}|_{[0,N)} \supseteq \mathcal{B}^{(-1)}|_{[0,N)} \supseteq \mathcal{B}^{(0)}|_{[0,N)}$$

As $\dim_{\mathbb{F}} \mathcal{B}|_{[0,N)} \leq Np$, the above inclusions imply that there exists $r \in \mathbb{N}$ such that $\mathcal{B}^{(-r)}|_{[0,N)} = \mathcal{B}^{(-r-1)}|_{[0,N)}$.

Let us see that $\mathcal{B}^{(-r)}|_{[0,N)} = \mathcal{B}^{(-r-1)}|_{[0,N)}$, implies $\mathcal{B}^{(-r)}|_{[0,N)} = \mathcal{B}^{(-k)}|_{[0,N)}$, for all $k \geq r$. Consider $s \in \mathcal{B}^{(-r-2)}|_{[0,N)}$, i.e., $s = \mathbf{w}|_{[0,N)}$ for some $\mathbf{w} \in \mathcal{B}^{(-r-2)}$. As $\sigma\mathbf{w} \in \mathcal{B}^{(-r-1)}$,

$$(\sigma\mathbf{w})|_{[0,N)} \in \mathcal{B}^{(-r-1)}|_{[0,N)} = \mathcal{B}^{(-r)}|_{[0,N)}$$

and we have that $(\sigma\mathbf{w})|_{[0,N)} = \tilde{\mathbf{w}}|_{[0,N)}$ for some $\tilde{\mathbf{w}} \in \mathcal{B}^{(-r)}$.

The N-observability of $\mathcal{B}$ implies that $\tilde{\mathbf{w}} \bigwedge_0 \sigma\mathbf{w} \in \mathcal{B}^{(-r)}$, consequently $\sigma^{-1}(\tilde{\mathbf{w}} \bigwedge_0 \sigma\mathbf{w}) \in \mathcal{B}^{(-r-1)}$ and

$$s = (\sigma^{-1}(\tilde{\mathbf{w}} \bigwedge_0 \sigma\mathbf{w}))|_{[0,N)} \in \mathcal{B}^{(-r-1)}|_{[0,N)}.$$

Therefore

$$\mathcal{B}^{(-r)}|_{[0,N)} = \mathcal{B}^{(-r-1)}|_{[0,N)} \Rightarrow \mathcal{B}^{(-r-1)}|_{[0,N)} = \mathcal{B}^{(-r-2)}|_{[0,N)}$$

and $\mathcal{B}^{(-r)}|_{[0,N)} = \mathcal{B}^{(-k)}|_{[0,N)} \ \ \forall\, k \geq r$.

On the other hand, note that if $\mathcal{B} \neq \{0\}$ [1] there exists a trajectory $\mathbf{w} \in \mathcal{B}^{(0)}$ that does not belong to $\mathcal{B}^{(1)}$, and

$$\mathbf{w}|_{[0,N)}, (\sigma\mathbf{w})|_{[0,N)}, \ldots, (\sigma^{N-1}\mathbf{w})|_{[0,N)} \in \mathcal{B}^{(0)}|_{[0,N)}$$

are linearly independent over $\mathbb{F}$, which implies that $\dim_{\mathbb{F}} \mathcal{B}^{(0)}|_{[0,N)} \geq N$. Thus

$$\mathcal{B}|_{[0,N)} = \mathcal{B}^{(-r)}|_{[0,N)} \supset \mathcal{B}^{(-r+1)}|_{[0,N)} \supset \ldots \supset \mathcal{B}^{(0)}|_{[0,N)}$$

[1] If $\mathcal{B} = \{0\}$, $\mathcal{B}$ is N-controllable and N-observable for any $N \in \mathbb{N}$, but it does not admit any basis, so the proposition restricts to the equivalence between (i) and (ii).

with $\dim_{\mathbb{F}}\mathcal{B}|_{[0,N)} \leq Np$ and $\dim_{\mathbb{F}}\mathcal{B}^{(0)}|_{[0,N)} \geq N$. Therefore $r \leq N(p-1)$ and

$$\mathcal{B}|_{[0,N)} = \mathcal{B}^{(-N(p-1))}|_{[0,N)}. \tag{3.5}$$

Finally, consider any two trajectories $\mathbf{w}^{(1)}$ and $\mathbf{w}^{(2)}$ in $\mathcal{B}$. Given any $k \in \mathbb{Z}$, time-invariance and linearity of $\mathcal{B}$ imply

$$\mathbf{w}^{(1)}|_{[k,k+N)} - \mathbf{w}^{(2)}|_{[k,k+N)} \in \mathcal{B}|_{[0,N)}$$

and, by (3.5) and time-invariance, there exists $\mathbf{w}^{(3)} \in \mathcal{B}$, with support in $[k-N(p-1), +\infty)$ such that

$$\mathbf{w}^{(3)}|_{[k,k+N)} = \mathbf{w}^{(1)}|_{[k,k+N)} - \mathbf{w}^{(2)}|_{[k,k+N)}$$

Since $\mathbf{w}^{(2)} + \mathbf{w}^{(3)}$ and $\mathbf{w}^{(1)}$ coincide on the interval $[k, k+N)$ and $\mathcal{B}$ is N-observable, the signal given by

$$\mathbf{w}_t = \begin{cases} (\mathbf{w}^{(2)} + \mathbf{w}^{(3)})_t & \text{if } t < k \\ \\ \mathbf{w}^{(1)}_t & \text{if } t \geq k \end{cases}$$

is a trajectory of $\mathcal{B}$. Moreover

$$(\mathbf{w}^{(2)} + \mathbf{w}^{(3)})|_{(-\infty,k-N(p-1))} = \mathbf{w}^{(2)}|_{(-\infty,k-N(p-1))}$$

gives

$$\mathbf{w} = \mathbf{w}^{(2)} \bigwedge_{k-N(p-1)} (\mathbf{w}^{(2)} + \mathbf{w}^{(3)}) \bigwedge_{k} \mathbf{w}^{(1)}$$

which proves that $\mathcal{B}$ is $N(p-1)$-controllable.

(ii) $\Rightarrow$ *(iii)* Suppose $\mathcal{C}$ is N-controllable, and let $G(d) \in \mathbb{F}((d))^{m\times p}$ be a *generator matrix* of $\mathcal{C}$, i.e., a matrix which rows constitute a basis for $\mathcal{C}$. As premultiplication of $G(d)$ by a nonsingular $M(d) \in \mathbb{F}((d))^{m\times m}$ still gives a generator matrix, we can assume that each row of $G(d)$ includes only nonnegative powers of d and has nonzero constant term.

If $G(0)$ is not full rank, let $\hat{\mathbf{g}}_k(d),\ k > 1$, be the first row of $G(d)$ with the property that $\hat{\mathbf{g}}_k(0)$ linearly depends on the previous rows of $G(0)$ and consider the space $\mathcal{S}$ of $\mathbb{F}((d))$-linear combinations of the first $k-1$ rows of $G(d)$

$$\hat{\mathbf{c}}(d) = \sum_j \mathbf{c}_j d^j = \hat{\mathbf{a}}(d) \begin{bmatrix} \hat{\mathbf{g}}_1(d) \\ \vdots \\ \hat{\mathbf{g}}_{k-1}(d) \end{bmatrix},\ \hat{\mathbf{a}}(d) \in \mathbb{F}((d))^{k-1} \tag{3.6}$$

Because of the $\mathbb{F}$-linear independence of the first $k-1$ rows of $G(0)$, the order of the series $\hat{\mathbf{c}}(d)$ in (3.6) coincides with the order of $\hat{\mathbf{a}}(d)$. This implies that two series $\hat{\mathbf{c}}^{(1)}(d)$ and $\hat{\mathbf{c}}^{(2)}(d)$ in $\mathcal{S}$ coincide up to the degree ℓ if and only if the same holds for the corresponding $\hat{\mathbf{a}}^{(1)}(d)$ and $\hat{\mathbf{a}}^{(2)}(d)$.

Clearly $\mathcal{S}$ includes some power series in $\mathbb{F}[[d]]^p$ that fits at least the constant term of $\hat{\mathbf{g}}_k(d)$, and possibly its higher terms up to some finite degree ν. However, the value of ν is uniformly bounded, as $\hat{\mathbf{c}}(d)$ varies in $\mathcal{S}$. Otherwise, we could find an infinite sequence of polynomial combinators $\hat{\mathbf{a}}^{(1)}(d), \hat{\mathbf{a}}^{(2)}(d), \ldots$, with $\deg(\hat{\mathbf{a}}^{(i)}) = i$, such that the corresponding $\hat{\mathbf{c}}^{(i)}(d) \in \mathcal{S}$ fit $\hat{\mathbf{g}}_k(d)$ up to the degree i. As $\hat{\mathbf{a}}^{(i)}(d)$ and $\hat{\mathbf{a}}^{(i+1)}(d)$ agree up to the degree i, $i = 1, 2, \ldots$, we could define the series $\hat{\mathbf{a}}(d) := \lim_{i\to\infty} \hat{\mathbf{a}}^{(i)}(d) \in \mathbb{F}[[d]]^{k-1}$, which would allow to express $\hat{\mathbf{g}}_k(d)$ as a combination of the first $k-1$ rows of $G(d)$, yielding a contradiction.

If $\bar{\nu}$ denotes the maximum value of ν, corresponding to some $k-1$-tuple $\hat{\bar{a}}_1(d)$, $\ldots$, $\hat{\bar{a}}_{k-1}(d)$, in the generator matrix

$$G'(d) := \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ -[d^{-\bar{\nu}}\hat{\bar{a}}_1(d)] & \ldots & -[d^{-\bar{\nu}}\hat{\bar{a}}_{k-1}(d)] & d^{-\bar{\nu}} & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix} G(d)$$

the first k rows of $G'(0)$ are independent over the field $\mathbb{F}$. Upon iterating the above procedure, if further rows of $G'(0)$ linearly depend on the previous ones, we can ultimately assume that the generator matrix

$$G(d) = \begin{bmatrix} \hat{\mathbf{g}}_1(d) \\ \vdots \\ \hat{\mathbf{g}}_m(d) \end{bmatrix}$$

does not include negative powers, and $G(0)$ has rank m.

As $\mathcal{C}$ is N-controllable, there exist sequences $\mathbf{r}_1, \ldots, \mathbf{r}_m$ such that

$$\mathbf{p}_1 \quad = \quad \mathbf{g}_1 \underset{1}{\bigwedge} \mathbf{r}_1 \underset{N+1}{\bigwedge} \mathbf{0}$$

$$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$$

$$\mathbf{p}_m \quad = \quad \mathbf{g}_m \bigwedge_{1} \mathbf{r}_m \bigwedge_{N+1} \mathbf{0}$$

are finite support elements of $\mathcal{C}$, and the degrees of the corresponding polynomial vectors $\mathbf{p}_1(d), \ldots, \mathbf{p}_m(d)$ in $\mathbb{F}[d]^p$ do not exceed N. As

$$P(d) := \begin{bmatrix} \mathbf{p}_1(d) \\ \vdots \\ \mathbf{p}_m(d) \end{bmatrix}$$

satisfies $P(0) = G(0)$, the polynomial matrix $P(d)$ is full row rank and, hence, a generator matrix of $\mathcal{C}$.

$(iii) \Rightarrow (i)$ The hypothesis implies that there exists an $m \times p$ polynomial generator matrix, $G(d)$, of $\mathcal{B}$, such that

$$\mathcal{B} = \{\hat{\mathbf{w}}(d) \in \mathbb{F}((d))^p : \hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G(d),\ \hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m\}.$$

Consider two unimodular matrices $U(d)$ and $V(d)$ such that

$$S(d) = U(d)G(d)V(d)$$

where $S(d) = [\tilde{S}(d) \quad 0]$ is the Smith form of $G(d)$. Clearly, the polynomial matrix $\tilde{G}(d) := U(d)G(d)$ is a generator matrix of $\mathcal{B}$, too.

From

$$\hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)\tilde{G}(d)$$

it follows that

$$\begin{aligned} \hat{\mathbf{w}}(d)V(d) &= \hat{\mathbf{u}}(d)\tilde{G}(d)V(d) \\ &= \hat{\mathbf{u}}(d)S(d) \\ &= \hat{\mathbf{v}}(d)[\tilde{S}(d) \quad 0]. \end{aligned}$$

Upon partitioning $V(d)$ into $[\,V^{(1)}(d) \quad V^{(2)}(d)\,]$, where $V^{(1)}(d) \in \mathbb{F}[d]^{p\times m}$ and $V^{(2)}(d) \in \mathbb{F}[d]^{p\times(p-m)}$, we have that

$$\hat{\mathbf{w}}(d) \in \mathcal{B} \Leftrightarrow \hat{\mathbf{w}}(d)V^{(2)}(d) = 0. \tag{3.7}$$

The polynomial matrix $V^{(2)}(d)$ can be expressed as

$$V^{(2)}(d) = V_0 + V_1 d + \cdots + V_N d^N,$$

$V_i \in \mathbb{F}^{p\times(p-m)}$ and $N \in \mathbb{N}$, and therefore we have

$$\hat{\mathbf{w}}(d) \in \mathcal{B} \Leftrightarrow \sum_{i=0}^{N} \mathbf{w}_{t-i} V_i = 0 \quad \forall t \tag{3.8}$$

If $\mathbf{w}^{(1)}$ and $\mathbf{w}^{(2)}$ are any two trajectories of $\mathcal{B}$ such that

$$\mathbf{w}^{(1)}|_{[k,k+N]} = \mathbf{w}^{(2)}|_{[k,k+N]}$$

for some $k \in \mathbb{Z}$, the trajectory $\mathbf{w}^{(1)} \bigwedge_k \mathbf{w}^{(2)} \in \mathbb{F}((d))^p$ satisfies

$$(\mathbf{w}^{(1)} \bigwedge_k \mathbf{w}^{(2)})_t := \begin{cases} \mathbf{w}_t^{(1)} & \text{if } t < k \\ \mathbf{w}_t^{(1)} = \mathbf{w}_t^{(2)} & \text{if } k \le t \le k+N \\ \mathbf{w}_t^{(2)} & \text{if } t > k+N \end{cases},$$

and consequently,

$$\sum_{i=0}^{N} (\mathbf{w}^{(1)} \bigwedge_k \mathbf{w}^{(2)})_{t-i} V_i = 0 \quad \forall t.$$

This implies $\mathbf{w}^{(1)} \bigwedge_k \mathbf{w}^{(2)} \in \mathcal{B}$, i.e. $\mathcal{B}$ is $(N+1)$-observable.

□

Corollary 3.1.1 *If $\mathcal{C} \subseteq \mathbb{F}((d))^p$ is an $\mathbb{F}((d))$-subspace, N-controllable but not $(N-1)$-controllable, then $\mathcal{C}$ admits a polynomial basis of degree N, but it does not admit any one of degree $N-1$.*

Proof: From the proof of Proposition 3.1.1, follows that the N-controllability of $\mathcal{C}$ implies that $\mathcal{C}$ admits a polynomial basis of degree N. To see that it does not admit a polynomial basis of degree $N-1$, suppose that $P(d) \in \mathbb{F}[d]^{m\times p}$ is a polynomial generator matrix for $\mathcal{C}$, with row degrees not greater than $N-1$, and consider two arbitrary elements of $\mathcal{C}$, say $\mathbf{w}^{(1)}, \mathbf{w}^{(2)}$. Then $\hat{\mathbf{w}}^{(1)}(d) = \hat{\mathbf{u}}^{(1)}(d)P(d)$ and $\hat{\mathbf{w}}^{(2)}(d) = \hat{\mathbf{u}}^{(2)}(d)P(d)$, for suitable $\hat{\mathbf{u}}^{(1)}(d)$ and $\hat{\mathbf{u}}^{(2)}(d)$ in $\mathbb{F}((d))^m$. Defining $\mathbf{u} := \mathbf{u}^{(1)} \bigwedge_\theta \mathbf{u}^{(2)}$, it follows that $\hat{\mathbf{w}}(d) := \hat{\mathbf{u}}(d)P(d)$ is in $\mathcal{C}$ and, for all $\theta \in \mathbb{Z}$, $\mathbf{w}$ satisfies $\mathbf{w} = \mathbf{w}^{(1)} \bigwedge_\theta \mathbf{r} \bigwedge_{N-1+\theta} \mathbf{w}^{(2)}$ for a suitable $\mathbf{r}$, i.e., $\mathcal{C}$ is $(N-1)$ -controllable. □

Remark: The equivalence between strong observability and strong controllability stated in Proposition 3.1.1 does not hold anymore in Willems's behavioral theory [55, 56], where bilateral signals (i.e., signals whose support can be any subset of $\mathbb{Z}$) are considered. If we restrict to Willems's "complete" behaviors, i.e., to families of trajectories that can be described as kernels of polynomial matrices, controllable behaviors are kernels of right prime matrices (or, equivalently, images of polynomial matrices) while all complete behaviors are observable. So, for complete bilateral behaviors, controllability always implies observability, but the converse does not hold. This situation is illustrated in the next example, where we present a complete behavior constituted by bilateral sequences, which is strongly observable, but not strongly controllable.

Example 3.1.1 Consider $\mathcal{B} = \operatorname{Ker} M(d) = \{\hat{\mathbf{x}}(d) \in (\mathbb{F}^3)^{\mathbb{Z}} : \hat{\mathbf{x}}(d)M(d) = 0\} \subseteq (\mathbb{F}^3)^{\mathbb{Z}}$, with

$$M(d) = \begin{bmatrix} -2d^2 - d + 4 & -2d - 5 \\ d^3 + d^2 - d - 1 & d^2 + 3d + 2 \\ d^4 + d^3 - d^2 - d & d^3 + 3d^2 + 2d \end{bmatrix}.$$

Factorize $M(d) = \bar{M}(d)X(d)$, where

$$\bar{M}(d) = \begin{bmatrix} -2d - 1 & \frac{4}{3} \\ d^2 + d + 1 & -\frac{2}{3}d - \frac{1}{3} \\ d^3 + d^2 + d & \frac{-2}{3}d^2 - \frac{1}{3}d \end{bmatrix} \text{ and } X(d) = \begin{bmatrix} d & 1 \\ 3 & -3 \end{bmatrix}.$$

Observe that $\bar{M}(d)$ is the transpose of the left prime matrix $U_1(d)$ of Example 2.1.3, and consequently is right prime.

$\mathcal{B}$ is L-observable for L equal to the greater degree of the entries of $M(d)$ plus 1, i.e., to $L = 5$. In fact, write

$$M(d) = M_4d^4 + M_3d^3 + M_2d^2 + M_1d + M_0,$$

where $M_i \in \mathbb{F}^{3\times 2}$, $i = 0, \ldots, 4$. Then,

$$\begin{aligned} \hat{\mathbf{w}}(d) \in \mathcal{B} &\Leftrightarrow \hat{\mathbf{w}}(d)M(d) = 0 \\ &\Leftrightarrow \sum_{i=0}^{4} M_i \mathbf{w}_{j+(4-i)} = 0, \ \forall\, j \in \mathbb{Z}. \end{aligned} \tag{3.9}$$

Thus, if $\mathbf{w}_1$ and $\mathbf{w}_2$ are any trajectories of $\mathcal{B}$ such that $\mathbf{w}_1|_{[0,5)} = \mathbf{w}_2|_{[0,5)}$, it follows that $\mathbf{w}_1 \underset{0}{\wedge} \mathbf{w} \underset{5}{\wedge} \mathbf{w}_2 \in \mathcal{B}$, for $\mathbf{w} = \mathbf{w}_1$ and $\mathbf{w} = \mathbf{w}_2$, because $(\mathbf{w}_1 \underset{0}{\wedge} \mathbf{w} \underset{5}{\wedge} \mathbf{w}_2)|_{[j,j+5)}$ is equal to $\mathbf{w}_1|_{[j,j+5)}$ or $\mathbf{w}_2|_{[j,j+5)}$ for all j in $\mathbb{Z}$, and therefore satisfies (3.9).

On the other hand, as

$$X(d) = \begin{bmatrix} d & 1 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1+d \end{bmatrix},$$

with $U(d) := \begin{bmatrix} d & 1 \\ 3 & 0 \end{bmatrix}$ unimodular, we have that $[\hat{\mathbf{y}}_1(d) \quad \hat{\mathbf{y}}_2(d)] \in \operatorname{Ker} X(d)$ has infinite support in both directions of $\mathbb{Z}$ if and only if $[\hat{\mathbf{z}}_1(d) \quad \hat{\mathbf{z}}_2(d)] := [\hat{\mathbf{y}}_1(d) \quad \hat{\mathbf{y}}_2(d)]U(d) \in \operatorname{Ker} \begin{bmatrix} 1 & -1 \\ 0 & 1+d \end{bmatrix}$ has also infinite support in both directions of $\mathbb{Z}$. Furthermore,

$$[\hat{\mathbf{z}}_1(d) \;\; \hat{\mathbf{z}}_2(d)] \begin{bmatrix} 1 & -1 \\ 0 & 1+d \end{bmatrix} = [0 \quad 0] \Leftrightarrow \begin{cases} \hat{\mathbf{z}}_1(d) = 0 \\ \hat{\mathbf{z}}_2(d)(1+d) = 0 \end{cases}$$

As $\hat{\mathbf{z}}_2(d)(1+d) = 0$ implies that either $\hat{\mathbf{z}}_2(d) = 0$ or $\hat{\mathbf{z}}_2(d)$ has infinite support in both directions of $\mathbb{Z}$, it follows that if $[\hat{\mathbf{y}}_1(d) \;\; \hat{\mathbf{y}}_2(d)]$ is a nonzero vector of $\operatorname{Ker} X(d)$, it must have infinite support in both directions of $\mathbb{Z}$.

Let

$$\hat{\mathbf{u}}(d) = \left[\sum_{i=-\infty}^{+\infty} 3(-1)^i d^i \quad \sum_{i=-\infty}^{+\infty} (-1)^i d^i \right] \in \operatorname{Ker} X(d).$$

The trajectory $\hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)\bar{M}(d)^{-1} \in (\mathbb{F}^3)^{\mathbb{Z}}$ is in $\mathcal{B}$ as $\hat{\mathbf{w}}(d)M(d) = \hat{\mathbf{u}}(d)X(d) = 0$.

Let $N \in \mathbb{N}$ and suppose there exists $\mathbf{r} \in \mathcal{B}$ such that $\bar{\mathbf{w}} := \mathbf{w} \underset{0}{\wedge} \mathbf{r} \underset{N}{\wedge} 0 \in \mathcal{B}$. Then $\hat{\bar{\mathbf{w}}}(d)\bar{M}(d)X(d) = \hat{\bar{\mathbf{w}}}(d)M(d) = 0$, i.e., $\hat{\bar{\mathbf{w}}}(d)\bar{M}(d) \in \operatorname{Ker} X(d)$, which implies that either $\hat{\bar{\mathbf{w}}}(d)\bar{M}(d)$ has infinite support in both directions of $\mathbb{Z}$ or $\hat{\bar{\mathbf{w}}}(d)\bar{M}(d) = 0$, which is impossible because $\bar{\mathbf{w}}|_{[N,+\infty)} = 0$ and there exists $\tau < 0$ such that $(\bar{\mathbf{w}}\bar{M})|_{(-\infty,\tau]} = (\mathbf{w}\bar{M})|_{(-\infty,\tau]} = \mathbf{u}|_{(-\infty,\tau]}$ which is different from zero, as $\hat{\mathbf{u}}$ has infinite support in both directions of $\mathbb{Z}$ and $\bar{M}(d)^{-1}$ is left prime. So, $\mathcal{B}$ is not strongly controllable. $\diamondsuit$

3.2 Convolutional codes and their encoders

Loeliger and Mittelholzer [31] studied convolutional codes over groups and defined a convolutional code over a group $\mathcal{G}$ as a time-invariant, strongly controllable and strongly observable subgroup of $\mathcal{G}^{\mathbb{Z}}$ ($\mathcal{G}^{\mathbb{Z}} \simeq \ldots \times \mathcal{G} \times \mathcal{G} \times \ldots$ is a group considering the operation of $\mathcal{G}$ componentwise).

As we have proven on Proposition 3.1.1, strong controllability and strong observability are equivalent properties for $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$, which leads to our definition of convolutional code.

Definition 3.2.1 *A $[p, m]$-convolutional code $\mathcal{C}$ is a strongly controllable (or, equivalently, a strongly observable) m-dimensional $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$.*

Some basic properties a convolutional code is endowed with are an immediate consequence of the above definition. First of all, being closed under scalar multiplication by elements of $\mathbb{F}((d))$, $\mathcal{C}$ is closed under forward and backward shifts (i.e. if $\hat{\mathbf{w}}(d)$ is a codeword of $\mathcal{C}$, $d^{-1}\hat{\mathbf{w}}(d)$ and $d\,\hat{\mathbf{w}}(d)$ are codewords too), and is an $\mathbb{F}[d]$ and an $\mathbb{F}[d^{-1}]$-module as well. Moreover, as shown in Proposition 3.1.1 above, $\mathcal{C}$ admits a polynomial basis, and consequently all codewords can be viewed as outputs of some moving average linear model. In fact, the term 'convolutional' comes from the observation that the codewords can be viewed as a convolutional of the information sequence and certain generator sequences.

Definition 3.2.2 *Any $m \times p$ rational (in particular, polynomial) matrix $G(d)$ whose rows provide an $\mathbb{F}((d))$-basis for a $[p, m]$-convolutional code $\mathcal{C}$ is called an encoder of $\mathcal{C}$. $\mathcal{C}$ is the image of $G(d)$, in the sense that*

$$\mathcal{C} = \{\hat{\mathbf{w}}(d) : \hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G(d),\ \hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m\}.$$

Therefore an encoder of a $[p, m]$-convolutional code $\mathcal{C}$ is an $m \times p$ matrix that provides all the codewords of $\mathcal{C}$ (i.e. generates $\mathcal{C}$), and allows to unambiguously recover the information sequence $\hat{\mathbf{u}}(d)$ from the codeword (i.e. is a full row rank matrix), which is an elementary condition for a code to be useful.

Definition 3.2.3 *[35] Two encoders are equivalent encoders if the codes they generate are the same.*

Therefore, equivalent encoders are full row rank matrices of the same type that are related by a nonsingular rational factor.

Proposition 3.2.1 *[40]* $G_1(d), G_2(d) \in \mathbb{F}(d)^{m\times p}$ *are equivalent encoders if and only if*

$$G_2(d) = T(d)G_1(d) \tag{3.10}$$

for some $m \times m$ *nonsingular rational matrix* $T(d)$*.*

Consequently if $G_1(d)$ is any encoder of a convolutional code $\mathcal{C}$, (3.10) parametrizes all the encoders of $\mathcal{C}$, as $T(d)$ ranges over the linear group $GL(m, \mathbb{F}(d))$ of nonsingular rational $m \times m$ matrices.

Among its polynomial encoders, a convolutional code always admits left prime and row reduced ones (see Definition 2.1.5 and Proposition 2.1.6). In coding theory, such encoders have specific names [14, 38, 17]:

- *basic encoders*, i.e. left prime encoders; they are related each other via (3.10), where $T(d)$ describes the group of $m \times m$ polynomial unimodular matrices;
- *row reduced encoders*;
- *canonical encoders*, i.e, encoders that are both left prime and row reduced.

Since canonical encoders are also basic, two equivalent canonical encoders differ by a left unimodular factor $T(d)$, which implies, by Proposition 2.1.6, that they have the same row degrees, up to a permutation, and so row degrees constitute a set of invariants of the code.

Remark: It was Forney [14] who studied canonical encoders and understood their important role in convolutional coding. In his paper [16], he related the row degrees of canonical encoders with the controllability and observability indices of a controllable and observable system. In the Handbook of Coding Theory [38], McEliece calls these indices *Forney indices*, and this is the nomenclature that we will adopt.

Definition 3.2.4 *The Forney indices of $\mathcal{C}$ are the row degrees, $\phi_1, \ldots, \phi_m$, of any canonical encoder of $\mathcal{C}$, and their sum is the degree of the code,* $\deg \mathcal{C} = \sum_{i=1}^{m} \phi_i$.

Basic and row reduced polynomial encoders realize some particular connections between the spans of the information sequences and the corresponding codewords, as we shall see in the following.

Proposition 3.2.2 *A polynomial encoder $G(d)$ is basic if and only if the following facts simultaneously hold:*

(i) for any information signal $\hat{\mathbf{u}}(d)$, the supports of $\hat{\mathbf{u}}(d)$ and of $\hat{\mathbf{u}}(d)G(d)$ have the same minimum point,

(ii) there exists a positive integer δ, such that, for all $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$

$$\sup \operatorname{span}(\hat{\mathbf{u}}) \leq \sup \operatorname{span}(\hat{\mathbf{u}}G) + \delta \tag{3.11}$$

Proof: Assume that $G(d)$ is basic and consider its right polynomial inverse $Q(d) = [q_{ij}(d)]$. $\hat{\mathbf{u}}(d) = [\hat{\mathbf{u}}(d)G(d)]Q(d)$ implies (3.11), with $\delta = \max_{i,j:q_{ij}(d)\neq 0} \{\deg q_{ij}\}$.

Moreover, since $G(0)$ has full row rank (due to the left-primeness of $G(d)$), the minimum points of the support of $\hat{\mathbf{u}}(d)$ and $\hat{\mathbf{u}}(d)G(d)$ coincide.

Vice-versa, suppose that $G(d)$ is not basic and consider its Smith form

$$G(d) = V(d) \left[\begin{array}{ccc|c} \gamma_1(d) & & & \\ & \ddots & & 0 \\ & & \gamma_m(d) & \end{array}\right] W(d),$$

where $V(d)$ and $W(d)$ are unimodular matrices and $\deg \gamma_1 > 0$.

If $\gamma_1(d) = d^k \gamma(d),\ k > 0$ and $\gamma(d) \in \mathbb{F}[d]$ such that $\gamma(0) \neq 0$, the minimum point of the support of $[\,1 \quad \ldots \quad 0\,]V(d)^{-1}$ is 0, but the corresponding codeword starts at $t = k$.

If $\gamma_1(0) \neq 0$, the information signal $\hat{\mathbf{u}}(d) = \left[\,\frac{1}{\gamma_1(d)} \quad 0 \quad \ldots \quad 0\,\right] V^{-1}(d)$ has infinite support while the corresponding codeword has not. □

On the other hand, when $G(d)$ is row reduced, with row degrees $k_1, k_2, \ldots, k_m$, a precise estimate of the maximum point of the support of $\hat{\mathbf{u}}(d)G(d)$ can be obtained via the *predictable degree property* (2.9), as we have

$$\deg(\hat{\mathbf{u}}G) = \max_{i:\hat{u}_i(d)\neq 0} \{k_i + \deg \hat{u}_i\}, \tag{3.12}$$

and a finite support information signal $\hat{\mathbf{u}}(d, d^{-1}) = [\, \hat{u}_1(d, d^{-1}) \quad \ldots \quad \hat{u}_m(d, d^{-1}) \,] \in \mathbb{F}[d, d^{-1}]^m$ produces a codeword $\hat{\mathbf{u}}(d, d^{-1})G(d)$ with support in $(-\infty, 0]$ if and only if $\deg \hat{u}_i \leq -k_i,\ i = 1, \ldots, m$.

In the analysis of rational encoders, it is quite useful to consider their (left) matrix fraction descriptions

$$G(d) = D(d)^{-1}N(d), \tag{3.13}$$

where $D(d) \in \mathbb{F}[d]^{m\times m}$ and $N(d) \in \mathbb{F}[d]^{m\times p}$. Note that the numerator matrix $N(d)$ is again an encoder of $\mathcal{C}$, because (3.10) holds with $T(d) = D(d)$.

Remark: Matrix fraction descriptions of the encoders are strongly connected to controllability system matrices considered by Forney in [16]. Every input/output pair $[\hat{\mathbf{w}}(d) \ \ \hat{\mathbf{u}}(d)] \in \mathbb{F}((d))^{p+m}$ satisfies

$$[\hat{\mathbf{w}}(d) \ \ \hat{\mathbf{u}}(d)] = \hat{\mathbf{u}}(d)[G(d) \ \ I_m] = \hat{\mathbf{u}}(d)D(d)^{-1}[N(d) \ \ D(d)] = \hat{\mathbf{v}}(d)[N(d) \ \ D(d)]$$

and vice-versa, given $\hat{\mathbf{v}}(d) \in \mathbb{F}((d))^m$, $\hat{\mathbf{v}}(d)[N(d) \ \ D(d)]$ is an input/output pair. In case $[N(d) \ \ D(d)]$ is left prime, $[\hat{\mathbf{w}}(d) \ \ \hat{\mathbf{u}}(d)]$ is polynomial if and only if $\hat{\mathbf{v}}(d)$ is polynomial, and the rows $[\hat{\mathbf{n}}_i(d) \quad \hat{\mathbf{d}}_i(d)],\ i = 1, \ldots, m$, of $[N(d) \ \ D(d)]$ provide a basis for the $\mathbb{F}[d]$-module of all polynomial input/output pairs.

Obviously, the most important class of encoders are the ones that can be realized by a physical device: the *causal* encoders. Many authors [14, 25] consider this restriction as part of the definition of encoder.

Given any formal Laurent power series $\hat{A}(d) = \sum_t A_t d^t \in \mathbb{F}^{m\times p}((d))$ and an integer

$T \in \mathbb{Z}$, define the truncation operator $\mathcal{P}_T$ at time T:

$$\mathcal{P}_T : \mathbb{F}^{m\times p}((d)) \to \mathbb{F}^{m\times p}((d)) : \sum_t A_t d^t \mapsto \sum_{t<T} A_t d^t \tag{3.14}$$

Definition 3.2.5 *A series* $G(d) = \sum_{t=k}^{+\infty} G_t d^t \in \mathbb{F}((d))^{m\times p}$ *is causal if* $k \geq 0$.

Proposition 3.2.3 *[5, 38] Let* $G(d) \in \mathbb{F}(d)^{m\times p}$. *The following are equivalent:*

(i) $G(d)$ *is causal;*

(ii) in any irreducible lMFD $G(d) = D(d)^{-1}N(d)$ *the matrix* $D(0)$ *is nonsingular;*

(iii) for all $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$,

$$\mathcal{P}_0(\hat{\mathbf{u}}G) = \mathcal{P}_0\Big((\mathcal{P}_0\hat{\mathbf{u}})G\Big).$$

All encoders of a $[p, m]$-convolutional code $\mathcal{C}$ admit a left MFD, $D(d)^{-1}N(d)$, whose numerator $N(d)$ is the product of a nonsingular $m \times m$ polynomial matrix $\Delta(d)$ and a given basic encoder of $\mathcal{C}$. Moreover, the irreducibility of $D(d)^{-1}N(d)$ is closely connected with the irreducibility of $D(d)^{-1}\Delta(d)$.

Proposition 3.2.4 *Given a basic encoder* $G_b(d) \in \mathbb{F}[d]^{m\times p}$, *all equivalent encoders of* $\mathcal{C}$ *have MFD's*

$$G(d) = [D(d)]^{-1}[\Delta(d)G_b(d)] \tag{3.15}$$

where $\Delta(d)$ *and* $D(d)$ *are nonsingular* $m \times m$ *polynomial matrices.*

Furthermore, (3.15) is irreducible if and only if $D(d)^{-1}\Delta(d)$ *is irreducible too.*

Proof: Let $G(d)$ be an equivalent encoder to $G_b(d)$. By (3.10) there exists an $m \times m$ nonsingular rational matrix $T(d)$ such that

$$G(d) = T(d)G_b(d),$$

and (3.15) holds for any left MFD $D(d)^{-1}\Delta(d)$ of $T(d)$. The nonsingularity of $T(d)$ implies that both $D(d)$ and $\Delta(d)$ are also nonsingular.

By Proposition 2.1.3 a polynomial matrix is left prime if and only if has a right polynomial inverse. Therefore, as

$$[D(d) \;\; \Delta(d)G_b(d)] = [D(d) \;\; \Delta(d)] \begin{bmatrix} I_m & 0 \\ 0 & G_b(d) \end{bmatrix}$$

and

$$\begin{bmatrix} I_m & 0 \\ 0 & G_b(d) \end{bmatrix} \begin{bmatrix} I_m & 0 \\ 0 & X(d) \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ 0 & I_m \end{bmatrix},$$

where $X(d) \in \mathbb{F}[d]^{p\times m}$ is a right polynomial inverse of $G_b(d)$, we have that $[D(d) \;\; \Delta(d)]$ has a right polynomial inverse if and only if $[D(d) \;\; \Delta(d)G_b(d)]$ has a right polynomial inverse, and consequently (3.15) is irreducible if and only if $D(d)^{-1}\Delta(d)$ is irreducible too. □

Corollary 3.2.1 *All causal encoders of $\mathcal{C}$ are represented by (3.15), with $D(d)^{-1}\Delta(d)$ irreducible and $D(0)$ nonsingular.*

Massey and Sain [36] defined the *catastrophic encoders* of a code as the encoders that can encode an infinite support information sequence into a finite support codeword.

This situation allows that a finite number of errors on the codeword possibly lead to an infinite number of errors on the information sequence, i.e. to a *catastrophic error propagation*, which is strongly undesirable.

In fact, suppose that $G(d)$ is a catastrophic encoder, $\hat{\mathbf{u}}(d)$ an information sequence, $\hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G(d)$ the corresponding codeword transmitted over the channel (see Figure 3.1), $\hat{\mathbf{w}}_{est}(d)$ the codeword estimate generated by the estimator and $\hat{\mathbf{u}}_{est}(d)$ the information sequence estimate produced by the information retriever (see Figure 3.2).

If we denote

$$\hat{\mathbf{e}}_{\mathbf{w}}(d) = \hat{\mathbf{w}}(d) - \hat{\mathbf{w}}_{est}(d) \quad \text{and} \quad \hat{\mathbf{e}}_{\mathbf{u}}(d) = \hat{\mathbf{u}}(d) - \hat{\mathbf{u}}_{est}(d),$$

we have that $\hat{\mathbf{e}}_{\mathbf{w}}(d) = \hat{\mathbf{e}}_{\mathbf{u}}(d)G(d)$. Therefore, if $\hat{\mathbf{e}}_{\mathbf{w}}(d)$ is a finite support sequence and $\hat{\mathbf{e}}_{\mathbf{u}}(d)$ is an infinite support sequence, it follows that a finite number of errors, $\hat{\mathbf{e}}_{\mathbf{w}}(d)$, on the estimate

$\hat{\mathbf{w}}_{est}(d)$, have generated an infinite number of errors, $\hat{\mathbf{e}}_{\mathbf{u}}(d)$, on the produced information sequence estimate $\hat{\mathbf{u}}_{est}(d)$.

Definition 3.2.6 *An encoder $G(d)$ of a $[p, m]$-convolutional code $\mathcal{C}$ is noncatastrophic if it maps every infinite support information series $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$ into an infinite support codeword $\hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G(d)$.*

Proposition 3.2.5 *[14] Taking into account only causal encoders of $\mathcal{C}$, the following are equivalent:*

(i) $G(d)$ is noncatastrophic;

(ii) in any irreducible left MFD $G(d) = D(d)^{-1}N(d)$ the numerator matrix $N(d)$ factorizes into $N(d) = \Delta(d)\bar{N}(d)$, where $\bar{N}(d)$ is a basic encoder and $\det \Delta(d) = \alpha d^k$, $0 \neq \alpha \in \mathbb{F}$ and $k \in \mathbb{N}$.

(iii) $G(d)$ admits a right inverse $A(d)B(d)^{-1} \in \mathbb{F}(d)^{p\times m}$, with $\det B(d) = \beta d^h$, $0 \neq \beta \in \mathbb{F}$ and $h \in \mathbb{N}$, or, equivalently, there exists a polynomial matrix $M(d) \in \mathbb{F}[d]^{p\times m}$ such that $G(d)M(d) = d^s I_m$, $s \in \mathbb{N}$.

Proof:

(ii) $\Rightarrow$ (i) Since $\det \Delta(d) = \alpha d^k$, $0 \neq \alpha \in \mathbb{F}, k \in \mathbb{N}$, it follows that (see Proposition 2.1.2) $\Delta(d)$ is a Laurent unimodular matrix, and consequently, its inverse, $\Delta(d)^{-1}$, is also Laurent polynomial. As $\bar{N}(d)$ is left prime, it admits a polynomial right inverse, $L(d)$.

Let $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$ and suppose that $\hat{\mathbf{u}}(d)G(d)$ has finite support. Then, $\hat{\mathbf{u}}(d)D(d)^{-1} = \hat{\mathbf{u}}(d)G(d)L(d)\Delta(d)^{-1}$ has also finite support and hence so has $\hat{\mathbf{u}}(d)$, which permits to conclude that $G(d)$ is noncatastrophic.

(i) $\Rightarrow$ (ii) Factorize $N(d) = \Delta(d)\bar{N}(d)$, with $\bar{N}(d)$ left prime, $\Delta(d)$ nonsingular and suppose that $\det \Delta(d) \neq \alpha d^k$. Since $\Delta(d)^{-1}$ is not (Laurent) polynomial, there exists $\mathbf{c} \in \mathbb{F}^m$ such that $\hat{\mathbf{v}}(d) := \mathbf{c}\Delta(d)^{-1} \notin \mathbb{F}[d, d^{-1}]^m$.

As left factors of $[D(d) \;\; \Delta(d)]$ are also left factors of $[D(d) \;\; N(d)]$, the irreducibility of $D(d)^{-1}N(d)$ implies that $[D(d) \;\; \Delta(d)]$ is left prime. Consequently, from $\hat{\mathbf{v}}(d) \notin \mathbb{F}[d, d^{-1}]^m$ it

follows that $\hat{\mathbf{v}}(d)[D(d)\ \Delta(d)]$ has infinite support too, which, together with $\hat{\mathbf{v}}(d)\Delta(d) = \mathbf{c} \in \mathbb{F}^m$, implies that $\hat{\mathbf{v}}(d)D(d) \notin \mathbb{F}[d, d^{-1}]^m$.

Thus the infinite support information sequence $\hat{\mathbf{u}}(d) := \hat{\mathbf{v}}(d)D(d)$ produces the codeword,

$$\hat{\mathbf{u}}(d)G(d) = \hat{\mathbf{v}}(d)D(d)D(d)^{-1}\Delta(d)\bar{N}(d) = \mathbf{c}\bar{N}(d),$$

which has finite support, i.e., $G(d)$ is catastrophic.

(ii) $\Rightarrow$ (iii) Consider a polynomial right inverse $\bar{L}(d)$ of $\bar{N}(d)$, so that $G(d)\bar{L}(d)\Delta(d)^{-1}D(d) = I_m$. If $\bar{A}(d)B(d)^{-1}$ denotes any right MFD of $\Delta(d)^{-1}D(d)$, just assume $A(d) := \bar{L}(d)\bar{A}(d)$.

(iii) $\Rightarrow$ (ii) Taking into account that $D(d)^{-1}N(d)$ is irreducible, from

$$D(d)^{-1}\Delta(d)\bar{N}(d)A(d)B(d)^{-1} = I_m$$

we get an irreducible left MFD $\Delta(d)^{-1}D(d)$ of $\bar{N}(d)A(d)B(d)^{-1}$. Consequently, $\det\Delta$ divides $\det B = \beta d^h$. □

As a consequence of the above proposition, a noncatastrophic encoder $G(d)$ has the characteristic property that the span of each information sequence does not exceed "too much" that of the corresponding codeword. In fact, part (iii) is equivalent to the existence of a right Laurent polynomial inverse $L(d, d^{-1}) = \sum_{m \le i \le M} P_i d^i,\ P_m \neq 0,\ P_M \neq 0$ of $G(d)$ and

$$\text{span}(\hat{\mathbf{u}}) \subset [\inf\ \text{span}(\hat{\mathbf{u}}G) + m, \sup\ \text{span}(\hat{\mathbf{u}}G) + M].$$

Encoders that generate codewords that permit to obtain the corresponding information sequences through a projection operation (in simpler terms, up to a bit permutation, the information sequences can be obtained by elimination of some components of the corresponding codewords) are called *systematic*.

Definition 3.2.7 *Systematic encoders are rational matrices that reduce to the following structure*

$$G(d) = [I_m\ \ G_2(d)]$$

up to a column permutation.

Costello [4] was the first to notice that every code admits a systematic encoder. In fact, take a basic encoder $G_b(d)$ of $\mathcal{C}$, select any $m \times m$ submatrix $D(d)$ of $G_b(d)$ with nonsingular $D(0)$, and consider the equivalent encoder $G(d) = D(d)^{-1}G_b(d)$; this is a (causal) systematic encoder. In general, however, such encoders fail to be polynomial. The next proposition characterizes the existence of (Laurent) polynomial systematic encoders.

Proposition 3.2.6 *[11] Let $\mathcal{C}$ be a $[p, m]$-convolutional code. The following are equivalent:*

(i) there exists a Laurent polynomial systematic encoder of $\mathcal{C}$;

(ii) all basic encoders of $\mathcal{C}$ have an m-th order minor which is a nonzero monomial of $\mathbb{F}[d]$;

(iii) there exist $i_1, i_2, \ldots, i_m \in \{1, \ldots, p\}$ such that if the codeword $\hat{\mathbf{w}}(d)$ has finite support components $\hat{w}_{i_1}(d), \hat{w}_{i_2}(d), \ldots, \hat{w}_{i_m}(d)$, then $\hat{\mathbf{w}}(d)$ has finite support.

Proof: (i) $\Rightarrow$ (ii) Let $G(d, d^{-1})$ be a Laurent polynomial systematic encoder of $\mathcal{C}$. Then, up to a column permutation,

$$G(d, d^{-1}) = [I_m \quad P(d, d^{-1})],$$

where $P(d, d^{-1}) \in \mathbb{F}[d, d^{-1}]^{m\times(p-m)}$.

Let $\nu_1, \nu_2, \ldots, \nu_m$ be nonnegative integers such that

$$\tilde{G}(d) = \begin{bmatrix} d^{\nu_1} & & \\ & \ddots & \\ & & d^{\nu_m} \end{bmatrix} G(d, d^{-1}) \tag{3.16}$$

$$= \begin{bmatrix} d^{\nu_1} & & & \\ & \ddots & & \tilde{P}(d) \\ & & d^{\nu_m} & \end{bmatrix}, \tag{3.17}$$

where $\tilde{P}(d) \in \mathbb{F}[d]^{m\times(p-m)}$. As $\mathrm{diag}\{d^{\nu_1}, \ldots, d^{\nu_m}\}$ is nonsingular, (3.10) implies that $\tilde{G}(d)$ is an equivalent encoder of $G(d, d^{-1})$.

Let $\Delta(d) \in \mathbb{F}[d]^{m\times m}$ be such that

$$\tilde{G}(d) = \Delta(d)G_b(d),$$

where $G_b(d) \in \mathbb{F}[d]^{m\times p}$ is left prime. As $\tilde{G}(d)$ and $G_b(d)$ are full row rank, we have that $\Delta(d)$ is nonsingular, and by (3.10), $G_b(d)$ is a (basic) encoder of $\mathcal{C}$, whose minor formed by its first m columns is a nonzero monomial in $\mathbb{F}[d]$. Moreover, as any basic encoder of $\mathcal{C}$ differs from $G_b(d)$ by a left unimodular factor, it follows that any basic encoder of $\mathcal{C}$ has the same property.

(ii) $\Rightarrow$ (iii) Let $G(d)$ be a basic encoder of $\mathcal{C}$ such that, up to a column permutation,

$$G(d) = [V(d) \;\; P(d)],$$

where $V(d) \in \mathbb{F}[d]^{m\times m}$ is unimodular over $\mathbb{F}[d, d^{-1}]$, and $P(d) \in \mathbb{F}[d]^{m\times(p-m)}$.

Partition the codeword $\hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G(d)$ into

$$\hat{\mathbf{w}}(d) = [\hat{\mathbf{w}}_1(d) \quad \hat{\mathbf{w}}_2(d)],$$

where $\hat{\mathbf{w}}_1(d) = \hat{\mathbf{u}}(d)V(d) \in \mathbb{F}((d))^m$ and $\hat{\mathbf{w}}_2(d) = \hat{\mathbf{u}}(d)P(d) \in \mathbb{F}((d))^{p-m}$.

If $\hat{\mathbf{w}}_1(d)$ has finite support, then $\hat{\mathbf{u}}(d) = \hat{\mathbf{w}}_1(d)V(d)^{-1} \in \mathbb{F}[d, d^{-1}]^m$, which implies that $\hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G(d)$ has also finite support.

(iii) $\Rightarrow$ (i) We can assume, without loss of generality, that $\{i_1, i_2, \ldots, i_m\} = \{1, 2, \ldots, m\}$. Consider

$$G(d) = [V(d) \;\; P(d)],\; V(d) \in \mathbb{F}[d]^{m\times m},\; P(d) \in \mathbb{F}[d]^{m\times(p-m)},$$

a basic encoder of $\mathcal{C}$. Let us see that $V(d)$ is a Laurent unimodular matrix.

Suppose that $V(d)$ is not a Laurent unimodular matrix, i.e., $\det V(d) = p(d) \neq \alpha d^n$, for all $\alpha \in \mathbb{F}\backslash\{0\}$ and $n \in \mathbb{Z}$ (see Proposition 2.1.2).

If $p(d) = 0$, there exists an infinite support rational information sequence $\hat{\mathbf{u}}(d)$ such that $\hat{\mathbf{u}}(d)V(d) = 0$.

If $p(d) \neq 0$ and $S(d) = \mathrm{diag}\{\gamma_1(d), \ldots, \gamma_m(d)\}$ is the Smith form of $V(d)$, then $\hat{\mathbf{u}}(d) = [\frac{1}{\gamma_1(d)} \; 0 \ldots 0]$ has infinite support, while $\hat{\mathbf{w}}_1(d) = \hat{\mathbf{u}}(d)V(d)$ has not. The proof of this fact is similar to the one of Proposition 3.2.2.

So, there exists an infinite support rational information sequence $\hat{\mathbf{u}}(d)$ such that the corresponding codeword $\hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G(d)$ has also infinite support, since $G(d)$ is left prime (Proposition 2.1.3), but its first m components $\hat{\mathbf{w}}_1(d) = \hat{\mathbf{u}}(d)V(d)$ have finite support, which contradicts the hypothesis.

Therefore, $V(d)$ is a Laurent unimodular matrix, which implies that $V(d)^{-1}P(d) \in \mathbb{F}[d, d^{-1}]^{m\times(p-m)}$, and by (3.10),

$$\begin{aligned} \tilde{G}(d) &= V(d)^{-1}G(d) \\ &= [I_m \quad V(d)^{-1}P(d)] \end{aligned}$$

is a systematic Laurent polynomial encoder of $\mathcal{C}$. □

Clearly, systematic encoders constitute a special class of noncatastrophic encoders: if $G(d) = [I_m \;\; G_2(d)]P$, with P a permutation matrix, is a systematic encoder, $P \begin{bmatrix} I_m \\ 0 \end{bmatrix}$ is a right inverse of $G(d)$, which, by Proposition 3.2.5, implies that $G(d)$ is noncatastrophic.

Systematic encoders constitute a standard (i.e., canonical) class for linear block codes. Besides the security they offer by preserving the information sequences in the codewords, they also present the advantage of having trivial right inverses and are simpler to implement.

Systematic encoders can also be regarded as a standard class for convolutional codes, but are, in general, not polynomial, as shown in Proposition 3.2.6. The main virtue of the standard class of encoders of a code considered by Forney [14], the canonical encoders, is that they constitute a standard basis for the set of all polynomial codewords of the code. Systematic encoders are preferred for code searches, while canonical encoders are usually preferred for analysis. For a comparison of canonical and systematic encoders see ([14]).

Another advantage of systematic encoders is their simplicity, which can be very useful in many situations as in code decomposition, as we will see next.

3.3 Code decomposition

In this chapter the decomposition of a code into smaller codes is going to be studied. This is directly connected with the existence of encoders in block diagonal form, called *decoupled encoders*.

Definition 3.3.1 *Let $G(d)$ be an encoder of a $[p, m]$-convolutional code $\mathcal{C}$ and $p_1, \ldots, p_k$ be positive integers such that $\sum_{i=1}^{k} p_i = p$. $G(d)$ is $(p_1, \ldots, p_k)$-decoupled if there exist positive integers $m_1, \ldots, m_k$ with $\sum_{i=1}^{k} m_i = m$ such that, possibly up to a column permutation,*

$$G(d) = \operatorname{diag}\{G_1(d), \ldots, G_k(d)\}, \;\; G_i(d) \in \mathbb{F}(d)^{m_i \times p_i}, \; i = 1, \ldots, k.$$

The existence of a decoupled encoder of $\mathcal{C}$ is equivalent to the possibility of representing $\mathcal{C}$ as a direct sum of smaller convolutional codes $\mathcal{C}_i$. Upon partitioning an information sequence $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$ into $[\hat{\mathbf{u}}_1(d) \ldots \hat{\mathbf{u}}_k(d)]$, $\hat{\mathbf{u}}_i(d) \in \mathbb{F}((d))^{m_i}$, we have

$$\hat{\mathbf{u}}(d)G(d) = [\hat{\mathbf{w}}_1(d) \ldots \hat{\mathbf{w}}_k(d)], \; \hat{\mathbf{w}}_i(d) = \hat{\mathbf{u}}_i(d)G_i(d), \; i = 1, \ldots, k,$$

and therefore

$$\mathcal{C} = \mathcal{C}_1 \times \ldots \times \mathcal{C}_k \tag{3.18}$$

where $\mathcal{C}_i$ is the $[p_i, m_i]$-convolutional code generated by $G_i(d)$.

The purpose of this section is to investigate the structure of the decoupled encoders of $\mathcal{C}$ and to develop appropriate algorithms to compute the direct summands appearing in (3.18), starting from a set of generators of $\mathcal{C}$. This is closely connected with the partition of the columns of an encoder of $\mathcal{C}$ into independent sets.

Definition 3.3.2 *If $S_1, \ldots, S_k$ are $\mathbb{F}((d))-$subspaces of $\mathbb{F}((d))^m$, they are called independent if for every k-tuple*

$$(\hat{\mathbf{w}}^{(1)}(d), \ldots, \hat{\mathbf{w}}^{(k)}(d)) \in S_1 \times \ldots \times S_k, \;\; \text{with} \;\; \hat{\mathbf{w}}^{(i)}(d) \neq 0, \; i = 1, \ldots, k,$$

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

As any encoder of $\mathcal{C}$ is a full row rank matrix, its columns constitute a generator set of $\mathbb{F}((d))^m$.

If $G(d)$ is an encoder of $\mathcal{C}$ such that $\mathrm{col}_i(G) = 0$, then any other encoder of $\mathcal{C}$, $\tilde{G}(d) = T(d)G(d)$, for some $T(d) \in GL(m, \mathbb{F}((d)))$, has also the i-th column equal to zero. Furthermore, the i-th component of all codewords of $\mathcal{C}$ is zero, and consequently it is sufficient to consider the convolutional code constituted by the codewords of $\mathcal{C}$ without the i-th component, whose encoders are the submatrices of the encoders of $\mathcal{C}$ with the i-th column deleted. Therefore, we will consider encoders with nonzero columns, i.e., whose columns constitute a set of nonzero generators of $\mathbb{F}((d))^m$.

Definition 3.3.3 *A set of nonzero generators of* $\mathbb{F}((d))^m$, $\mathcal{G} = \{\hat{\mathbf{v}}_1(d), \hat{\mathbf{v}}_2(d), \ldots, \hat{\mathbf{v}}_p(d)\}$ *and a decomposition of* $\mathbb{F}((d))^m$ *in direct sum*

$$\mathbb{F}((d))^m = V_1 \oplus V_2 \oplus \ldots \oplus V_k, \tag{3.19}$$

are compatible if every vector of $\mathcal{G}$ *belongs to a summand of (3.19) (and, obviously, to only one).*

In the following, $\mathcal{G} = \{\hat{\mathbf{v}}_1(d), \hat{\mathbf{v}}_2(d), \ldots, \hat{\mathbf{v}}_p(d)\}$ will represent a set of nonzero generators of $\mathbb{F}((d))^m$. If $\mathcal{G}$ is compatible with (3.19), it follows immediately that

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

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

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

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

(iii) there exists a unique finest direct sum decomposition

$$\mathbb{F}((d))^m = \bar{V}_1 \oplus \bar{V}_2 \oplus \ldots \oplus \bar{V}_h \tag{3.20}$$

compatible with $\mathcal{G}$. Each summand of any other compatible decomposition of $\mathbb{F}((d))^m$ can be expressed as a suitable sum of some $\bar{V}_i$s in (3.20).

In order to obtain a partition of $\mathcal{G}$ associated with the finest decomposition (3.20), we introduce on $\mathcal{G}$ the following relation.

Definition 3.3.4 *Let $B \subset \mathcal{G}$ be a basis of $\mathbb{F}((d))^m$ and denote by $\mathcal{M}_\nu$ the smallest subset of B such that $\hat{\mathbf{v}}_\nu(d) \in \text{span } \mathcal{M}_\nu$. If $\hat{\mathbf{v}}_i(d), \hat{\mathbf{v}}_j(d) \in \mathcal{G}$, let*

$$\hat{\mathbf{v}}_i(d) \sim_B \hat{\mathbf{v}}_j(d) \tag{3.21}$$

if there exists a chain $\mathcal{M}_i = \mathcal{M}_{\nu_1}, \mathcal{M}_{\nu_2}, \ldots, \mathcal{M}_{\nu_h} = \mathcal{M}_j$ such that $\mathcal{M}_{\nu_l} \cap \mathcal{M}_{\nu_{l+1}} \neq \emptyset,\ l = 1, \ldots, h-1$.

Proposition 3.3.1 *Let B and $\tilde{B}$ be two subsets of $\mathcal{G}$ that constitute a basis of $\mathbb{F}((d))^m$ and $\hat{\mathbf{v}}_i(d), \hat{\mathbf{v}}_j(d) \in \mathcal{G}$. Then:*

(i) $\sim_B$ is an equivalence relation on $\mathcal{G}$.

(ii) $\hat{\mathbf{v}}_i(d) \sim_B \hat{\mathbf{v}}_j(d)$ if and only if $\hat{\mathbf{v}}_i(d)$ and $\hat{\mathbf{v}}_j(d)$ belong to the same subspace in the finest compatible direct sum decomposition (3.20).

(iii) $\hat{\mathbf{v}}_i(d) \sim_B \hat{\mathbf{v}}_j(d)$ if and only if $\hat{\mathbf{v}}_i(d) \sim_{\tilde{B}} \hat{\mathbf{v}}_j(d)$.

Proof: (i) Obvious.

(ii) If $\mathcal{M}_\nu \cap \mathcal{M}_\mu \neq \emptyset$, $\nu, \mu \in \{1, \ldots, p\}$, then span $\mathcal{M}_\nu$ and span $\mathcal{M}_\mu$ are not independent, and therefore $\mathcal{M}_\nu$ and $\mathcal{M}_\mu$ belong to the same summand in (3.20). Consequently, if $\hat{\mathbf{v}}_i(d) \in$ span $\mathcal{M}_i$ and $\hat{\mathbf{v}}_j(d) \in$ span $\mathcal{M}_j$ are such that $\hat{\mathbf{v}}_i(d) \sim_B \hat{\mathbf{v}}_j(d)$, there exists, by definition, a chain $\mathcal{M}_i = \mathcal{M}_{\nu_1}, \mathcal{M}_{\nu_2}, \ldots, \mathcal{M}_{\nu_h} = \mathcal{M}_j$ with $\mathcal{M}_{\nu_l} \cap \mathcal{M}_{\nu_{l+1}} \neq \emptyset,\ l = 1, \ldots, h-1$ such that $\mathcal{M}_i = \mathcal{M}_{\nu_1}, \mathcal{M}_{\nu_2}, \ldots, \mathcal{M}_{\nu_h} = \mathcal{M}_j$, and consequently also $\hat{\mathbf{v}}_i(d)$ and $\hat{\mathbf{v}}_j(d)$, belong to the same summand in (3.20).

Vice-versa, assume that $\hat{\mathbf{v}}_i(d) \not\sim_B \hat{\mathbf{v}}_j(d)$ and let $\mathcal{N}_i$ be the subset of B defined by

$$\mathcal{N}_i = \bigcup_{\{\nu \in \{1,\ldots,p\}: \hat{\mathbf{v}}_i(d) \sim_B \hat{\mathbf{v}}_\nu(d)\}} \mathcal{M}_\nu.$$

$\mathcal{N}_i \neq \emptyset$, as $\mathcal{M}_i \subset \mathcal{N}_i$. $\mathcal{M}_j \cap \mathcal{N}_i = \emptyset$ because otherwise $\exists \hat{\mathbf{v}}_r(d) \in B\ \ \hat{\mathbf{v}}_r(d) \in \mathcal{M}_j \wedge \hat{\mathbf{v}}_r(d) \in \mathcal{N}_i$, i.e., there exists $\hat{\mathbf{v}}_r(d) \in B$ such that $\hat{\mathbf{v}}_r(d) \sim_B \hat{\mathbf{v}}_j(d)$ and $\hat{\mathbf{v}}_r(d) \sim_B \hat{\mathbf{v}}_i(d)$, which contradicts the assumption.

Therefore, $\mathcal{N}_i$ and $B\backslash\mathcal{N}_i$ are nonempty disjoint subsets of B, which implies that

$$\operatorname{span}\mathcal{N}_i \oplus \operatorname{span} B\backslash\mathcal{N}_i = \mathbb{F}((d))^m,$$

and therefore $\hat{\mathbf{v}}_i(d) \in \operatorname{span}\mathcal{N}_i$ and $\hat{\mathbf{v}}_j(d) \in \operatorname{span} B\backslash\mathcal{N}_i$ do not belong to the same summand in (3.20).

(iii) follows directly from (ii). □

From Proposition 3.3.1, (iii), it follows that the relation defined in (3.21) is independent from the basis, and from now on it will be simply represented by $\sim$. The proposition also shows that to find the partition of $\mathcal{G}$ associated with (3.20), it is sufficient to determine the equivalence classes of $\sim$, which is done by the following algorithm.

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

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

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

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

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

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

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

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

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

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

Proposition 3.3.2 *Let $\mathcal{G} = \{\hat{\mathbf{v}}_1(d), \ldots, \hat{\mathbf{v}}_p(d)\}$ be a set of nonzero generators of $\mathbb{F}((d))^m$. The above algorithm provides the partition of $\mathcal{G}$ associated with the finest compatible decomposition of $\mathbb{F}((d))^m$.*

Proof: We prove first that

$$\hat{\mathbf{v}}_i(d) \sim \hat{\mathbf{v}}_j(d) \Longleftrightarrow (A^T A)^{p-1}_{ij} = 1. \tag{3.22}$$

Observe that

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

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

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

and, more generally, for all $n \in \mathbb{N}$

$$\begin{aligned} (A^T A)^n_{ij} = 1 &\iff \exists \nu_2, \ldots, \nu_n \ : \ (A^T A)_{i\nu_2} = (A^T A)_{\nu_2\nu_3} = \ldots = (A^T A)_{\nu_n j} = 1 \\ &\iff \exists \nu_1 = i, \nu_2, \ldots, \nu_n, \nu_{n+1} = j \ : \ \mathcal{M}_{\nu_l} \cap \mathcal{M}_{\nu_{l+1}} \neq \emptyset, \ \ l = 1, \ldots, n. \end{aligned}$$

Consequently,

$$\hat{\mathbf{v}}_i(d) \sim \hat{\mathbf{v}}_j(d) \Longleftrightarrow \exists k \quad (A^T A)^k_{ij} = 1. \tag{3.23}$$

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

$$(A^T A)^n_{ij} = 1 \Longrightarrow (A^T A)^{n+1}_{ij} = 1, \ \ \forall n \in \mathbb{N}, \ \ \forall i, j. \tag{3.24}$$

On the other hand

$$(A^T A)^n_{ij} = 1 \Longrightarrow (A^T A)^{n-1}_{ij} = 1, \ \forall\, i, j \in \{1, \ldots, p\}, \ \forall n \geq p. \tag{3.25}$$

In fact, if $(A^T A)^n_{ij} = 1$, there exist $\mathcal{M}_i = \mathcal{M}_{\nu_1}, \mathcal{M}_{\nu_2}, \ldots, \mathcal{M}_{\nu_{n+1}} = \mathcal{M}_j$ with $\mathcal{M}_{\nu_l} \cap \mathcal{M}_{\nu_{l+1}} \neq \emptyset, \ l = 1, \ldots, n$. As $|\mathcal{G}| = p$, there exist $k_1 < k_2$ such that $\nu_{k_1} = \nu_{k_2}$, and $\mathcal{M}_i = \mathcal{M}_{\nu_1}, \mathcal{M}_{\nu_2}, \ldots, \mathcal{M}_{\nu_{k_1}} = \mathcal{M}_{\nu_{k_2}}, \ldots, \mathcal{M}_{\nu_{n+1}} = \mathcal{M}_j$ satisfies $\mathcal{M}_{\nu_l} \cap \mathcal{M}_{\nu_{l+1}} \neq \emptyset, \ l = 1, \ldots, k_1 - 1, \ l = k_2, \ldots, n$. This, together with (3.24), implies $(A^T A)^{n-1}_{ij} = 1$.

(3.22) follows immediately from (3.23) and (3.25).

It is now clear that a permutation matrix $P \in \mathbb{F}^{p\times p}$ sorts the columns of $[\hat{\mathbf{v}}_1(d)\dots\hat{\mathbf{v}}_p(d)]$ according to the equivalence classes of $\sim$ if and only if

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

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

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

□

The partition of the columns of an encoder of $\mathcal{C}$, associated with the finest decomposition (3.20) of $\mathbb{F}((d))^m$, is a code property, in the sense that is the same for every encoder of $\mathcal{C}$. In fact, let $G(d)$ and $\tilde{G}(d)$ be two encoders of $\mathcal{C}$, $P \in \mathbb{F}^{p\times p}$ a permutation matrix, $p_1,\dots,p_k$ positive integers such that $\sum_{i=1}^k p_i = p$, and consider the column partitions

$$G(d)P = [G_1(d)|\dots|G_k(d)],\ G_i(d)\in\mathbb{F}(d)^{m\times p_i},\ i=1,\dots,k,$$

$$\tilde{G}(d)P = [\tilde{G}_1(d)|\dots|\tilde{G}_k(d)],\ \tilde{G}_i(d)\in\mathbb{F}(d)^{m\times p_i},\ i=1,\dots,k.$$

Since

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

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

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

if and only if

$$\mathbb{F}((d))^m = \text{span } \tilde{G}_1(d)\oplus\dots\oplus\text{span } \tilde{G}_k(d).$$

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

Step 1 in the above algorithm produces a systematic encoder. Therefore, in order to find a column partition associated with (3.20) we can always consider a systematic encoder, and apply the algorithm, starting on Step 2.

Systematic encoders are naturally decoupled encoders. In fact, if $S(d)$ is a systematic encoder and P the permutation matrix obtained by the algorithm above,

$$S(d)P = \text{diag}\{S_1(d), \ldots, S_h(d)\},\ S_i(d) \in \mathbb{F}(d)^{m_i \times p_i},\ i = 1, \ldots, h.$$

Example 3.3.1 Let us find the partition of the columns of the encoder of $\mathcal{C}$,

$$G(d) = \begin{bmatrix} d & \frac{1}{d} & d-1 & \frac{d^4+1}{d^2} & d+1 & d^2-1 \\ d+1 & 0 & d^2+d+2 & d^2+d & 0 & 2+3d+2d^2+d^3 \\ 1 & d^2+1 & \frac{1}{d-1} & \frac{2d^2+1}{d} & 0 & \frac{d+1}{d-1} \\ 0 & 1 & 0 & \frac{1}{d} & 1 & 0 \end{bmatrix},$$

associated with the finest decomposition(3.20) of $\mathbb{F}((d))^4$, by applying the algorithm above.

The first columns of $G(d)$ that form a nonsingular matrix are the first, second, third and fifth. Consider the 4×4 nonsingular submatrix $M(d)$ of $G(d)$ formed by these columns, i.e.,

$$M(d) = \begin{bmatrix} d & \frac{1}{d} & d-1 & d+1 \\ d+1 & 0 & d^2+d+2 & 0 \\ 1 & d^2+1 & \frac{1}{d-1} & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

and define

$$\begin{aligned} V(d) &= M(d)^{-1}G(d) \\ &= \begin{bmatrix} 1 & 0 & 0 & d & 0 & 0 \\ 0 & 1 & 0 & \frac{1}{d} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1+d \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \end{aligned}$$

which is a systematic encoder of $\mathcal{C}$.

The corresponding boolean matrix is

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

and $(A^T A)^5$ is such that

$$P^T (A^T A)^5 P = \text{diag} \left\{ \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad , \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \quad , \quad [1] \right\},$$

where $P = [e_1 \; e_2 \; e_4 \; e_3 \; e_6 \; e_5]$ and e_i is the column vector with the i-th entry equal to 1 and the others entries equal to zero, $i = 1, \ldots 6$.

Post-multiplying $G(d)$ by the permutation matrix P, we obtain the desired partition,

$$G(d)P = \left[\begin{array}{ccc|cc|c} d & \frac{1}{d} & \frac{d^4+1}{d^2} & d-1 & d^2-1 & d+1 \\ d+1 & 0 & d^2+d & 2+d+d^2 & 2+3d+2d^2+d^3 & 0 \\ 1 & d^2+1 & \frac{2d^2+1}{d} & \frac{1}{d-1} & \frac{d+1}{d-1} & 0 \\ 0 & 1 & \frac{1}{d} & 0 & 0 & 1 \end{array}\right].$$

♢

3.4 Conclusion

In this chapter we defined a convolutional code and analyzed its encoders. We started by introducing the behavioral approach to systems theory, considering discrete time systems constituted by bilateral sequences over $\mathbb{F}^p$, where $\mathbb{F}$ is a finite field. Next, we restricted ourselves to left compact sequences and showed that for linear, time-invariant behaviors, strong controllability and strong observability are equivalent properties. Considering this fact, we defined a convolutional code as a behavior which is strongly controllable (or strongly observable).

In the study of the encoders of a convolutional code we used MFD's and have obtained new proofs of some known results, as well as new results. In particular, we have considered

the decoupled encoders of a code, which permit to "decompose" the code as a sum of smaller codes.

Chapter 4

Minimal encoders

Concerning encoders that can be physically implemented, i.e. the causal encoders, a natural problem is that of characterizing the ones that can be realized by linear sequential circuits with minimum number of delay elements, or equivalently, which have realizations of minimal dimension. These encoders are called minimal.

In this chapter we are going to study the minimal encoders of a convolutional code, and in particular the decoupled ones. We will characterize them in terms of their abstract state space, and obtain two parametrizations of the minimal encoders of a code: one in terms of their MFD's and the other considering a realization procedure.

4.1 State space realization and minimal encoders

State space models for convolutional encoders have been considered since many years [35], and provide a neat framework for classifying encoders complexity by resorting to the dimension of their minimal state space realizations.

A linear, discrete time, dynamical system $\Sigma = (A, B, C, J)$ [16, 26, 43]

$$\begin{aligned} \mathbf{x}_{t+1} &= \mathbf{x}_t A + \mathbf{u}_t B \\ \mathbf{w}_t &= \mathbf{x}_t C + \mathbf{u}_t J \end{aligned} \tag{4.1}$$

$A \in \mathbb{F}^{n\times n},\ B \in \mathbb{F}^{m\times n}, C \in \mathbb{F}^{n\times p}, J \in \mathbb{F}^{m\times p}$ is an *n-dimensional realization* of a causal encoder $G(d)$ of $\mathcal{C}$ if, starting from zero initial conditions, Σ encodes every information series

$\hat{\mathbf{u}}(d) = \sum_t \mathbf{u}_t d^t$ into the corresponding codeword produced by $G(d)$, namely

$$\hat{\mathbf{w}}(d) := \sum_t \mathbf{w}_t d^t = \hat{\mathbf{u}}(d)G(d).$$

This happens if and only if

$$G(d) = J + Bd(I - dA)^{-1}C.$$

Every causal encoder $G(d)$ can be realized by a linear dynamical system (4.1). Moreover, every causal encoder has infinitely many realizations, and the realizations of $G(d)$ with least dimension are called *minimal realizations* of $G(d)$.

Definition 4.1.1 *Let $G(d)$ be an encoder of $\mathcal{C}$. The minimal dimension, $\mu(G)$, of a state realization of $G(d)$ is called the "McMillan degree of $G(d)$". Realizations with dimension $\mu(G)$ are said to be minimal.*

The McMillan degree of an encoder $G(d)$ is a measure of the complexity of a physical implementation of $G(d)$, as it gives the minimum number of delay elements necessary to physically implement the encoder.

The above notation is not widely used in convolutional coding. We have opted to use it as it is the notation adopted in systems theory, and there is no equivalent term in convolutional coding. Moreover, it is also used by some well known authors [38, 17], in the area of convolutional coding.

The following procedure for obtaining a minimal realization of a given $G(d)$, is an adaptation of similar algorithms available in the literature [16, 46, 45].

1. Consider any left MFD $\bar{D}_L(d)^{-1}\bar{N}_L(d)$ of $G(d)$ such that $\bar{D}_L(0)$ is nonsingular.

   Pre-multiply both $\bar{D}_L(d)$ and $\bar{N}_L(d)$ by a suitable unimodular matrix $U(d)$, in order to produce a left MFD

   $$D_L(d)^{-1}N'_L(d) = G(d)$$

   with

   $$P'(d) := [\, D_L(d) \quad N'_L(d) \,] \tag{4.2}$$

   row reduced, with row degrees $k_1, k_2, \ldots k_m$. $D_L(0) = U(0)\bar{D}_L(0)$ is still nonsingular.

2. Rewrite $G(d)$ as

$$\begin{aligned} G(d) &= D_L(0)^{-1}N'_L(0) + D_L(d)^{-1}[N'_L(d) - D_L(d)D_L(0)^{-1}N'_L(0)] \\ &= D_L(0)^{-1}N'_L(0) + D_L(d)^{-1}N_L(d), \end{aligned}$$

with $N_L(d) = N'_L(d) - D_L(d)D_L(0)^{-1}N'_L(0)$.

Then, $D_L(d)^{-1}N_L(d)$ is strictly causal, as $N_L(0) = 0$, and

$$P(d) = [\, D_L(d) \quad N_L(d) \,] \tag{4.3}$$

is row reduced, with the same row degrees $k_1, k_2, \ldots k_m$, as the leading (row) coefficient matrices $P_{\rm hr}$ and $P'_{\rm hr}$ satisfy

$$P_{\rm hr} = P'_{\rm hr} \begin{bmatrix} I_m & -D_L(0)^{-1}N'_L(0) \\ 0 & I_p \end{bmatrix}.$$

In order to obtain a realization (A, B, C, J) for $G(d)$, we take

$$J = D_L(0)^{-1}N'_L(0), \tag{4.4}$$

and reduce the problem to finding a realization (A, B, C) for the strictly causal matrix $G_{\rm sc}(d) = D_L(d)^{-1}N_L(d)$.

3. Suppose for the moment that all row degrees $k_1, k_2, \ldots, k_m$ are strictly positive and let $n := \sum_{i=1}^{m} k_i$.

Denote by M_i the $k_i \times k_i$ nilpotent Jordan block

$$M_i = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ & & & 0 \end{bmatrix}, \tag{4.5}$$

and introduce the following matrices

$$\bar{M} := \mathrm{diag}\{M_{k_1}, M_{k_2}, \ldots, M_{k_m}\}, \qquad \bar{B} := \begin{bmatrix} \mathbf{e}_1 \\ \mathbf{e}_{1+k_1} \\ \cdots \\ \mathbf{e}_{1+k_1+\ldots+k_{m-1}} \end{bmatrix},$$

of dimension $n \times n$ and $m \times n$, respectively. It is clear that

$$X(d) := d\bar{B}(I_n - \bar{M}d)^{-1} = \begin{bmatrix} d & d^2 & \dots & d^{k_1} & & & & & & \\ & & & & d & d^2 & \dots & d^{k_2} & & \\ & & & & & & & & \ddots & \\ & & & & & & & & d & d^2 & \dots & d^{k_m} \end{bmatrix},$$

and, consequently, there exists $C \in \mathbb{F}^{n \times p}$ such that

$$N_L(d) = X(d)C. \tag{4.6}$$

4. Rewrite $D_L(d)$ as $(I_m - X(d)\bar{A})D_L(0)$, for a suitable $\bar{A} \in \mathbb{F}^{n \times m}$. This is always possible since the row degrees of $D_L(d)$ are less or equal than $k_1, \dots, k_m$, and $D_L(0)$ is nonsingular. As $D_L(d)$ is nonsingular it follows that $I_m - X(d)\bar{A}$ is also nonsingular.

   Upon defining

$$A := \bar{M} + \bar{A}\bar{B}, \quad B := D_L(0)^{-1}\bar{B}, \tag{4.7}$$

   we have that

$$\begin{aligned} X(d)(I_n - dA) &= d\bar{B}(I_n - \bar{M}d)^{-1}(I_n - d(\bar{M} + \bar{A}\bar{B})) \\ &= d\bar{B}(I_n - (I_n - \bar{M}d)^{-1}\bar{A}\bar{B}d) \\ &= (I_m - d\bar{B}(I_n - \bar{M}d)^{-1}\bar{A})\bar{B}d \\ &= (I_m - X(d)\bar{A})\bar{B}d, \end{aligned}$$

   or, equivalently,

$$(I_m - X(d)\bar{A})^{-1}X(d) = \bar{B}d(I_n - dA)^{-1},$$

   which in turn, together with (4.7), implies

$$\begin{aligned} D_L(d)^{-1}N_L(d) &= D_L(0)^{-1}(I_m - X(d)\bar{A})^{-1}X(d)C \\ &= D_L(0)^{-1}\bar{B}d(I_n - dA)^{-1}C \\ &= Bd(I_n - dA)^{-1}C. \end{aligned}$$

   Thus (4.4), (4.6) and (4.7) provide an n-dimensional state space realization (A, B, C, J) of the encoder $G(d)$.

5. In case $k_i = 0$ for some i, the procedure is the same as above; however the i-th row in $\bar{B}$ and in $X(d)$ has to be zero, and the i-th diagonal block M_{k_i} is empty.

In case we start from an irreducible left MFD $D_L(d)^{-1}N_L(d)$ of $G_{\rm sc}(d)$, the above procedure provides a *minimal realization*, in the sense that any other state space realization of the encoder has dimension greater than or equal to n. The converse is also true, as it can be seen in the following proposition.

Proposition 4.1.1 *Let $G_{sc}(d) \in \mathbb{F}(d)^{m\times p}$ be strictly causal and $D_L(d)^{-1}N_L(d)$ a lMFD of $G_{sc}(d)$, such that*

$$[D(d) \;\; N_L(d)]$$

is row reduced, with row degrees $k_1, \ldots, k_m$.

The above realization algorithm gives a minimal realization of $G_{sc}(d)$ if and only if $D_L(d)^{-1}N_L(d)$ is irreducible.

Proof:

Let $\Sigma = (A, B, C)$ be the realization of dimension $n := \sum_{i=1}^{m} k_i$ obtained by application of the above realization algorithm to $D_L(d)^{-1}N_L(d)$.

Assume that $D_L(d)^{-1}N_L(d)$ is not irreducible, and let $\tilde{D}_L(d)^{-1}\tilde{N}_L(d)$ be an irreducible left MFD of $G_{sc}(d)$ such that

$$[\tilde{D}_L(d) \quad \tilde{N}_L(d)]$$

is row reduced, with row degrees $\tilde{k}_1, \ldots, \tilde{k}_m$.

Since

$$[D_L(d) \quad N_L(d)] = F(d)[\tilde{D}_L(d) \quad \tilde{N}_L(d)],$$

for some nonunimodular matrix $F(d) \in \mathbb{F}(d)^{m\times m}$ (see Proposition 2.2.1), it follows that

$$\begin{aligned} \tilde{n} \;\; &:= \;\; \sum_{i=1}^{m} \tilde{k}_i = \text{extdeg}([\tilde{D}_L \;\; \tilde{N}_L]) = \text{intdeg}([\tilde{D}_L \;\; \tilde{N}_L]) < \\ &< \;\; \text{intdeg}([D_L \;\; N_L]) = \text{extdeg}([D_L \;\; N_L]) = n. \end{aligned}$$

The application of the above algorithm to $\tilde{D}_L(d)^{-1}\tilde{N}_L(d)$ provides a realization of $G_{sc}(d)$ of dimension $\tilde{n} < n$, and, consequently, Σ is not minimal.

Vice-versa, assume that $D_L(d)^{-1}N_L(d)$ is irreducible and suppose that $\tilde{\Sigma} = (\tilde{A}, \tilde{B}, \tilde{C})$ is a realization of $G_{\rm sc}(d)$, with dimension $\tilde{n}$, where $\tilde{A} \in \mathbb{F}^{\tilde{n}\times\tilde{n}}$, $\tilde{B} \in \mathbb{F}^{m\times\tilde{n}}$ and $\tilde{C} \in \mathbb{F}^{\tilde{n}\times p}$.

Then $G_{\rm sc}(d)$ can be represented as

$$\tilde{B}d(I_{\tilde{n}} - \tilde{A}d)^{-1}\tilde{C} = R(d)Q(d)^{-1}\tilde{C} = \tilde{D}(d)^{-1}\tilde{N}(d)\tilde{C} = D_L(d)^{-1}N_L(d),$$

where $R(d)Q(d)^{-1}$ and $\tilde{D}(d)^{-1}\tilde{N}(d)$ are irreducible MFD's of $\tilde{B}d(I_{\tilde{n}} - \tilde{A}d)^{-1}$ with

$$\begin{bmatrix} Q(d) \\ R(d) \end{bmatrix} \text{ and } [\,\tilde{D}(d) \quad \tilde{N}(d)\,] \tag{4.8}$$

column and row reduced, respectively.

From Corollary 2.2.2, it follows that both matrices in (4.8) have the same internal degree, and therefore their external degrees coincide, too.

Consequently,

$$\begin{aligned} \tilde{n} &\geq \text{extdeg}\left(\begin{bmatrix} d\tilde{B} \\ I_{\tilde{n}} - \tilde{A}d \end{bmatrix}\right) \geq \text{intdeg}\left(\begin{bmatrix} d\tilde{B} \\ I_{\tilde{n}} - \tilde{A}d \end{bmatrix}\right) \geq \\ &\geq \text{intdeg}\left(\begin{bmatrix} R \\ Q \end{bmatrix}\right) = \text{intdeg}([\tilde{D} \quad \tilde{N}]). \end{aligned} \tag{4.9}$$

On the other hand, as

$$[\tilde{D}(d) \quad \tilde{N}(d)\tilde{C}] = [\tilde{D}(d) \quad \tilde{N}(d)] \begin{bmatrix} I_m & 0 \\ 0 & \tilde{C} \end{bmatrix},$$

it follows that

$$\text{intdeg}([\tilde{D}(d) \quad \tilde{N}(d)\tilde{C}]) \leq \text{intdeg}([\tilde{D}(d) \quad \tilde{N}(d)]). \tag{4.10}$$

Furthermore, since $D_L(d)^{-1}N_L(d) = \tilde{D}(d)^{-1}\tilde{N}(d)\tilde{C} = G_{sc}(d)$ and $D_L(d)^{-1}N_L(d)$ is irreducible, we have that (see Proposition 2.2.1)

$$\text{intdeg}([\tilde{D}(d) \quad \tilde{N}(d)\tilde{C}]) \geq \text{intdeg}([D_L(d) \quad N_L(d)]). \tag{4.11}$$

From (4.9), (4.10) and (4.11) we conclude that

$$\tilde{n} \geq \text{intdeg}([D_L(d) \quad N_L(d)]) = \text{extdeg}([D_L(d) \quad N_L(d)]) = n.$$

□

As a corollary, the McMillan degree of a causal encoder $G(d)$ can be determined considering a special kind of left MFD's of $G(d)$, as it is summarized below.

Corollary 4.1.1 *Suppose that $D(d)^{-1}N(d)$ is an irreducible left MFD of a causal encoder $G(d)$ such that*

$$[\, D(d) \quad N(d)\,]$$

is row reduced, with row degrees $k_1, k_2, \ldots k_m$. Then, the McMillan degree of $G(d)$ is given by $n = \sum_{i=1}^{m} k_i$.

Corollary 4.1.2 *[14] The McMillan degree of a canonical encoder $G_c(d)$ coincides with the degree of its code $\mathcal{C}$.*

Proof: $I_m^{-1}G_c(d)$ is an irreducible MFD of $G_c(d)$ and $[I_m \;\; G_c(d)]$ is row reduced, the row degrees being the Forney indices $\phi_1, \ldots, \phi_m$ of $\mathcal{C}$, (cf. Definition 3.2.4). □

A convolutional code $\mathcal{C}$ admits infinitely many different encoders. So a natural problem is that of characterizing which encoders of $\mathcal{C}$ have minimal McMillan degree, and hence can be realized by linear sequential circuits with minimum number of delay elements. They are called *minimal encoders (of $\mathcal{C}$).*

Proposition 4.1.2 *[14] A causal encoder $G(d)$ of $\mathcal{C}$ is minimal if and only if its McMillan degree coincides with* $\deg \mathcal{C}$.

Proof: Let $G_c(d)$ be a canonical encoder of $\mathcal{C}$ and $G(d)$ any other causal encoder of $\mathcal{C}$. $G(d)$ admits an irreducible left MFD

$$G(d) = D(d)^{-1}[\Delta(d)G_c(d)]$$

with $D(0)$ invertible and $\Delta(d)$ nonsingular (see Proposition 3.2.4).

Moreover, in case $[D(d) \quad \Delta(d)G_c(d)]$ is not row reduced, left multiplication by a suitable unimodular $V(d)$ produces a row reduced matrix

$$[V(d)D(d) \quad V(d)\Delta(d)G_c(d)]$$

with row degrees $k_1, k_2, \ldots, k_m$ and $(V(d)D(d))^{-1}[V(d)\Delta(d)G_c(d)]$ is still an irreducible MFD of $G(d)$. Consequently

$$\begin{aligned}\mu(G) = \sum_{i=1}^{m} k_i &= \text{extdeg}\,[\,VD \quad V\Delta G_c\,] \geq \text{extdeg}(V\Delta G_c) \geq \text{intdeg}(V\Delta G_c) \\ &\geq \text{intdeg}(G_c) = \text{extdeg}(G_c) = \sum_{i=1}^{m} \phi_i\end{aligned}$$

and $\deg \mathcal{C} = \sum_{i=1}^{m} \phi_i$ provides the minimum McMillan degree of all causal encoders of $\mathcal{C}$. □

Corollary 4.1.3 *1. Canonical encoders are minimal.*

2. Minimal polynomial encoders are basic.

Proof: If $G(d)$ is polynomial and nonbasic, there exists a nonunimodular left factor $\Delta(d)$ such that $G(d) = \Delta(d)G_c(d)$, with $G_c(d)$ a canonical encoder (see Lemma 2.1.1 and Proposition 2.1.6). Moreover, if $[I_m \quad G(d)]$ fails to be row reduced, there exists a unimodular matrix $V(d)$ (see Proposition 2.1.6) such that $[V(d) \quad V(d)G(d)]$ is row reduced. Then

$$\begin{aligned}\mu(G) &= \text{extdeg}[V \quad VG] = \text{intdeg}[V \quad VG] \geq \text{intdeg}(VG) = \text{intdeg}(G) \\ &= \text{intdeg}(\Delta G_c) > \text{intdeg}(G_c) = \sum_{i=1}^{m} \phi_i\end{aligned}$$

□

The above corollary provides inclusions between different classes of encoders, that cannot be reversed, as shown by the following examples.

Example 4.1.1 The canonical encoder

$$G_c(d) = \begin{bmatrix} d^4+1 & d^4 & d \\ d^3 & 1 & d+1 \end{bmatrix}$$

has McMillan degree 7. Considering the unimodular matrix

$$U(d) = \begin{bmatrix} d^2+1 & d^2 \\ d^2 & d^2-1 \end{bmatrix},$$

$U(d)^{-1}G_c(d)$ is an irreducible left MFD of the polynomial encoder

$$G_b(d) = \begin{bmatrix} -d^6+d^5+d^4-d^2+1 & -d^6+d^4+d^2 & d^2+d \\ d^6-d^5-d^3+d^2 & d^6-d^2-1 & -d^2-d-1 \end{bmatrix}. \tag{4.12}$$

Clearly $G_b(d)$ is basic, noncanonical, since (4.12) fails to be row reduced, and minimal, since $[U(d)\ G_c(d)]$ is row reduced with external row degree 7. ♢

Example 4.1.2 The canonical encoder

$$G_c(d) = \begin{bmatrix} d+1 & d & d \\ -d & -d+1 & 1 \end{bmatrix}$$

has McMillan degree 2. The equivalent encoder

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

is basic, as $U(d)$ is unimodular, and nonminimal. In fact

$$[U(d)\ G_c(d)] = \begin{bmatrix} d^2+1 & d^2 & d+1 & d & d \\ -1 & -1 & -d & -d+1 & 1 \end{bmatrix}$$

is row reduced and the sum of the row degrees is 3, so that $\mu(G) = 3 > \mu(G_c)$. ♢

4.2 Structure of minimal encoders

The purpose of this section is to characterize the structure of all minimal encoders of a code $\mathcal{C}$, and to provide a complete parametrization based on their MFD's. The first proposition, and the subsequent corollary, are based on a result on polynomial invertibility that traces back to a classical paper [14] by Forney.

Proposition 4.2.1 *Let $G(d) \in \mathbb{F}(d)^{m\times p}$ be a causal encoder of $\mathcal{C}$. The following are equivalent:*

(i) $G(d)$ is a minimal encoder;

(ii) $G(d)$ admits a left MFD

$$G(d) = D(d)^{-1}G_c(d) \tag{4.13}$$

where $G_c(d)$ is a canonical encoder and $D(d)$ an $m \times m$ polynomial matrix with $D(0)$ nonsingular and $\deg \text{row}_i\, D \leq \deg \text{row}_i\, G_c,\ i = 1, \ldots, m$;

(iii) $G(d)$ has a right polynomial inverse $X(d) \in \mathbb{F}[d]^{p\times m}$ and a right polynomial inverse $Y(d^{-1}) \in \mathbb{F}[d^{-1}]^{p\times m}$.

Proof: $(i) \Rightarrow (ii)$ Consider an irreducible left MFD $D(d)^{-1}N(d)$ of $G(d)$ with $[\, D(d) \quad N(d)\,]$ row reduced and $D(0)$ nonsingular (cf. Proposition 3.2.3). $N(d) \in \mathbb{F}[d]^{m\times p}$ is also an encoder of $\mathcal{C}$ and it can be factorized into

$$N(d) = \Delta(d)\bar{N}(d),$$

where $\Delta(d) \in \mathbb{F}[d]^{m\times m}$ and $\bar{N}(d) \in \mathbb{F}[d]^{m\times p}$ is row reduced and left prime (see Lemma 2.1.1 and Proposition 2.1.6). Then $\bar{N}(d)$ is a canonical encoder of $\mathcal{C}$, and

$$\deg \mathcal{C} = \mu(\bar{N}) = \text{extdeg}(\bar{N}) = \text{intdeg}(\bar{N}) \leq \text{intdeg}(N) \leq \text{extdeg}(N),$$

and, therefore, by Corollary 4.1.1,

$$deg\, \mathcal{C} = \mu(G) = \text{extdeg}\,[\, D \quad N\,] \geq \text{extdeg}(N) \geq \deg \mathcal{C}. \tag{4.14}$$

As all terms in (4.14) coincide, $N(d)$ is a canonical encoder of $\mathcal{C}$ and the row degrees in $N(d)$ are the same as in $[D(d) \quad N(d)]$. Consequently the row degrees of $D(d)$ can not exceed the corresponding ones in $N(d)$. This shows that (ii) holds with $G_c(d) = N(d)$.

$(ii) \Rightarrow (iii)$ If $R(d)$ denotes a right polynomial inverse of $G_c(d)$ (see Proposition 2.1.3), we have that

$$X(d) := R(d)D(d)$$

is an inverse of $G(d)$ with entries in $\mathbb{F}[d]$.

On the other hand, if $\phi_1, \ldots, \phi_m$ are the row degrees of $G_c(d)$,

$$\begin{aligned} G(d) &= [\mathrm{diag}\{d^{-\phi_1}, \ldots, d^{-\phi_m}\} D(d)]^{-1} [\mathrm{diag}\{d^{-\phi_1}, \ldots, d^{-\phi_m}\} G_c(d)] \\ &=: \tilde{D}(d^{-1})^{-1} \tilde{N}(d^{-1}) \end{aligned}$$

is a left MFD of $G(d)$ in $\mathbb{F}[d^{-1}]$. Since $G_c(d)$ is left prime and row reduced, $\tilde{N}(d^{-1})$ is full rank for every $d^{-1} \in \bar{\mathbb{F}}$, where $\bar{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$, and $\tilde{N}(0) = (G_c)_{\mathrm{hr}}$ is full rank too. This implies that $\tilde{N}(d^{-1})$ is left prime and has a right inverse $\tilde{R}(d^{-1})$ in $\mathbb{F}[d^{-1}]$ (see Propositions 2.1.3 and 2.1.5). So,

$$Y(d^{-1}) := \tilde{R}(d^{-1}) \tilde{D}(d^{-1})$$

provides an $\mathbb{F}[d^{-1}]$ polynomial right inverse of $G(d)$.

$(iii) \Rightarrow (i)$ Suppose that $D(d)^{-1}N(d)$ is an irreducible left MFD of $G(d)$, and $[\, D(d) \quad N(d)\,]$ is row reduced with row degrees $k_1, \ldots, k_m$. Upon defining

$$[\tilde{D}(d^{-1}) \quad \tilde{N}(d^{-1})] := \mathrm{diag}\{d^{-k_1}, \ldots, d^{-k_m}\} \, [\, D(d) \quad N(d)\,],$$

consider also $\tilde{D}(d^{-1})^{-1}\tilde{N}(d^{-1})$, a left MFD of $G(d)$ over the ring $\mathbb{F}[d^{-1}]$, with $\tilde{D}(d^{-1})$ row reduced, as $(\tilde{D})_{\mathrm{hr}} = D(0)$ is invertible (see Propositions 3.2.3 and 2.1.5). Since $[D(d) \quad N(d)]$ is left prime and row reduced, it follows that $[\tilde{D}(d^{-1}) \quad \tilde{N}(d^{-1})]$ is also left prime (see Proof of $(ii) \Rightarrow (iii)$ above).

Let $M(d)$ be a polynomial right inverse of $[\, D(d) \quad N(d)\,]$ and note that the equation

$$D(d)^{-1}N(d)X(d) = I_m$$

implies

$$I_m = N(d) \, [\, X(d) \quad I_p\,] \, M(d),$$

showing that $N(d)$ is left prime.

By a similar argument one sees that $\tilde{N}(d^{-1})$ is left prime. This guarantees that $\tilde{N}(0)$ is full rank, and, as

$$N(d) = \mathrm{diag}\{d^{k_1}, \ldots, d^{k_m}\} \tilde{N}(d^{-1}),$$

$N_{hr} = \tilde{N}(0)$ has rank m, which implies that $N(d)$ is row reduced (cf. Proposition 2.1.5), with row degrees $k_1, \ldots, k_m$. So, $N(d)$ is a canonical encoder of $\mathcal{C}$, and

$$\mu(G) = \text{extdeg}([D \quad N]) = \sum_{i=1}^{m} k_i = \text{extdeg}(N) = \mu(N) = \deg\mathcal{C},$$

i.e., $G(d)$ is a minimal encoder. □

The next corollary follows immediately from the condition (iii) of the above proposition, taking Definition 3.2.7 and Proposition 3.2.5 into account.

Corollary 4.2.1 *A systematic causal encoder is minimal, and a minimal encoder is non-catastrophic.*

Proposition 4.2.2 below shows that all minimal encoders of $\mathcal{C}$, and in particular all canonical and systematic encoders, can be represented as MFD's whose numerator is a *fixed* canonical encoder $G_c(d)$. This gives a neat parametrization of minimal, canonical and systematic encoders of $\mathcal{C}$. The proof depends on the following technical lemma.

Lemma 4.2.1 *Suppose that both* $[\, D(d) \quad N(d) \,]$ *and its block* $N(d)$ *are row reduced, with same row degrees* $k_1, \ldots, k_m$*. Suppose, moreover, that* $V(d)$ *is unimodular, and let*

$$[\, \tilde{D}(d) \quad \tilde{N}(d) \,] = V(d) \, [\, D(d) \quad N(d) \,] \, .$$

If $\tilde{N}(d)$ *is row reduced, the same holds true for* $[\, \tilde{D}(d) \quad \tilde{N}(d) \,]$*, and both matrices have row degrees* $k_1, \ldots, k_m$*, up to a permutation.*

Proof: As $N(d)$ and $\tilde{N}(d)$ are row reduced and differ each other by a left unimodular factor $V(d)$, the row degrees k_i of $N(d)$ and $\tilde{k}_i$ of $\tilde{N}(d)$ coincide, up to a permutation (cf. Proposition 2.1.6). So, possibly after multiplying $V(d)$ on the left by a permutation matrix, we shall assume $k_i = \tilde{k}_i$, $i = 1, \ldots, m$.

The predictable degree property (see Proposition 2.1.5) for $N(d)$ and $\tilde{N}(d)$ implies that

$$k_i = \deg \ \text{row}_i \tilde{N} = \max_{j : V_{ij}(d) \neq 0} \{ \deg \ \text{row}_j N + \deg V_{ij} \} = \max_{j : V_{ij}(d) \neq 0} \{ k_j + \deg V_{ij} \},$$

and therefore, as $\tilde{D}(d) = V(d)D(d)$, it follows that

$$\deg\ \mathrm{row}_i \tilde{D} \leq \max_{j:V_{ij}(d)\neq 0} \{\deg\ \mathrm{row}_j D + \deg V_{ij}\} \leq \max_{j:V_{ij}(d)\neq 0} \{k_j + \deg V_{ij}\} = k_i.$$

Thus $k_i, i = 1, \ldots, m$, are the row degrees of $[\,\tilde{D}(d) \quad \tilde{N}(d)\,]$, which is row reduced. □

Proposition 4.2.2 *Let $G_c(d)$ be a canonical encoder of $\mathcal{C}$.*

(i) All minimal encoders of $\mathcal{C}$ can be represented as

$$G(d) = D(d)^{-1} G_c(d),$$

upon varying the denominator in the set of $m \times m$ polynomial matrices $D(d)$ with $D(0)$ nonsingular and $\deg\ \mathrm{row}_i\, D \leq \deg\ \mathrm{row}_i\, G_c,\ i = 1, \ldots, m$.

(ii) All polynomial minimal encoders of $\mathcal{C}$ are obtained by restricting the denominators $D(d)$ to unimodular matrices.

(iii) All systematic causal encoders of $\mathcal{C}$ are given by

$$G(d) = D(d)^{-1} G_c(d)$$

where $D(d)$ is any $m \times m$ submatrix of $G_c(d)$ with $D(0)$ nonsingular.

(iv) Suppose that the row degrees of $G_c(d)$ are non decreasing, and that the Forney indices assume $q \leq m$ distinct values $\phi'_1 < \phi'_2 < \cdots < \phi'_q$, with multiplicity d_h, $h = 1, \ldots, q$.

Any other canonical encoder of $\mathcal{C}$, with non decreasing row degrees, is given by

$$\tilde{G}_c(d) = D(d)^{-1} G_c(d) \tag{4.15}$$

as $D(d)$ varies in the group of block polynomial matrices of the form

$$\begin{bmatrix} D_{11} & & & 0 \\ D_{21}(d) & D_{22} & & \\ \vdots & \vdots & \ddots & \\ D_{q1}(d) & D_{q2}(d) & \cdots & D_{qq} \end{bmatrix}, \tag{4.16}$$

where $D_{hh} \in \mathbb{F}^{d_h \times d_h}$ is non singular, $h = 1, \ldots, q$, and the degree of each entry in $D_{hk}(d)$, $h > k$, does not exceed $\phi'_h - \phi'_k$.

Proof: (i) By Proposition 4.2.1, any minimal encoder $G(d)$ can be expressed as $G(d) = \tilde{D}(d)^{-1}\tilde{G}_c(d)$, where $\tilde{G}_c(d)$ is a canonical encoder and $\tilde{D}(d)$ is a polynomial matrix whose row degrees do not exceed the corresponding ones in $\tilde{G}_c(d)$, and $\tilde{D}(0)$ nonsingular.

Let $V(d)$ be an unimodular matrix such that $V(d)\tilde{G}_c(d) = G_c(d)$, and let $D(d) := V(d)\tilde{D}(d)$. Clearly $G(d)$ can be represented as $D(d)^{-1}G_c(d)$ and $D(0)$ is nonsingular; moreover, by Lemma 4.2.1, $[D(d) \quad G_c(d)]$ is row reduced with row degrees $\phi_1, \ldots, \phi_m$ and $\deg \text{row}_i\, D \leq \deg \text{row}_i\, G_c,\ i = 1, \ldots, m$.

Conversely, if $G(d) = D(d)^{-1}G_c(d)$, where $D(d) \in \mathbb{F}[d]^{m\times m}$ with $D(0)$ invertible and $\deg \text{row}_i D \leq \deg \text{row}_i G_c,\ i = 1, \ldots, m$, then, as $G_c(d)$ is left prime and row reduced,

$$[D(d) \quad G_c(d)]$$

is also left prime and row reduced, with the same row degrees as $G_c(d)$. Therefore,

$$\mu(G) = \text{extdeg}([D \quad G_c]) = \text{extdeg}(G_c),$$

which implies that $G(d)$ is minimal.

(ii) Since $G_c(d)$ is left prime, $D(d)^{-1}G_c(d)$ is polynomial if and only if $D(d)^{-1}$ is polynomial, as $G_c(d)$ has a right polynomial inverse (see Proposition 2.1.3), which amounts to say that $D(d)$ is unimodular.

(iii) Every systematic encoder $G(d)$ of $\mathcal{C}$ satisfies $G(d)P = [I_m \quad \tilde{G}_2(d)]$, where P is a suitable column permutation matrix. If $G(d)$ is causal, by Corollary 4.2.1 it has to be minimal, and consequently, by (i), it can be expressed by a left MFD

$$[I_m \quad \tilde{G}_2(d)]P^{-1} = D(d)^{-1}G_c(d),$$

with $D(0)$ nonsingular. So

$$D(d)[I_m \quad \tilde{G}_2(d)] = G_c(d)P$$

shows that $D(d)$ is an $m \times m$ submatrix of $G_c(d)$.

Conversely, assume that $D(d)$ is an $m \times m$ submatrix of $G_c(d)$ with $D(0)$ nonsingular. Then there exists a permutation matrix P such that $G_c(d)P = [D(d) \quad M(d)]$ and consequently

$$D(d)^{-1}G_c(d) = [I_m \quad D(d)^{-1}M(d)]P^{-1}$$

is systematic.

(iv) Suppose that the row degrees $\phi_1, \ldots, \phi_m$ of two canonical encoders $\tilde{G}_c(d)$ and $G_c(d)$ are non decreasing and consider a unimodular matrix $D(d)$ such that $G_c(d) = D(d)\tilde{G}_c(d)$. As both $\tilde{G}_c(d)$ and $G_c(d)$ are row reduced, the predictable degree property (see Proposition 2.1.5) implies that

$$\phi_i = \deg \operatorname{row}_i(D\tilde{G}_c) = \max_{j:D_{ij}(d)\neq 0} \{\phi_j + \deg(D_{ij})\} \tag{4.17}$$

and therefore

$$\begin{aligned} \deg(D_{ij}) \leq \phi_i - \phi_j \text{ or } D_{ij}(d) = 0 \quad &\text{if} \quad \phi_i > \phi_j, \\ \deg(D_{ij}) = 0 \text{ or } D_{ij}(d) = 0 \quad &\text{if} \quad \phi_i = \phi_j \\ D_{ij}(d) = 0 \quad &\text{if} \quad \phi_i < \phi_j \end{aligned}$$

Clearly $D(d)$ is block triangular, with constant and nonsingular diagonal blocks as $D(d)$ is unimodular, and the block matrices $D_{ij}(d)$, such that $\phi_i > \phi_j$, satisfying the degree constraints specified in (iv). Therefore $\tilde{G}_c(d) = D(d)^{-1}G_c(d)$ can be represented as in (4.15).

Conversely, any $D(d)$ as given in (4.16) is unimodular, with inverse of the same form (4.16) satisfying the degree constraints specified in (iv). Applying the predictable degree property (see Proposition 2.1.5) we obtain

$$\deg \operatorname{row}_i(G_c) = \deg \operatorname{row}_i(D^{-1}G_c),\ i = 1, \ldots, m,$$

which implies that $D(d)^{-1}G_c(d)$ is canonical. □

A particular choice of matrix $D(d)$ in (4.16) is described by Forney in [16], that allows to obtain a canonical encoder in *echelon form*. This designation is due to its resemblance to the echelon form [3] for the left-equivalence relation on $\mathbb{F}[d]^{m\times p}$ given in Definition 2.1.3.

A convolutional code has infinitely many canonical encoders. A canonical encoder in echelon form is unique, and the code can be uniquely identified with it.

Definition 4.2.1 *Let $G_c(d)$ be a canonical encoder of $\mathcal{C}$ with row degrees in nondecreasing order $\phi_1 \leq \phi_2 \leq \cdots \leq \phi_m$. The i-th pivot γ_i of $G_c(d)$ is the least integer such that the submatrix of $G_c[[.], [\gamma_1, \gamma_2, \ldots, \gamma_i]]$[1] constituted by the rows of degree $\leq \phi_i$ has higher order coefficient matrix of rank i.*

It can be easily proved that all canonical encoders, with ordered row degrees, have the same pivot indices [16].

Definition 4.2.2 *A canonical encoder $G_c(d)$ is in echelon form if*

1. *its row degrees are in nondecreasing order, i.e., $\phi_1 \leq \phi_2 \leq \ldots \leq \phi_m$;*
2. *$(G_c)_{i,\gamma_i}, i = 1, \ldots, m$ are monic polynomials of degree ϕ_i, where γ_i is the i-th pivot index;*
3. *for any i and i' such that $\phi_i \leq \phi_{i'}$, $\deg(G_c)_{i',\gamma_i} < \phi_i$.*

These conditions imply that the higher order coefficient matrix of a canonical encoder in echelon form, $G_c(d)$, verifies some conditions. Suppose that $G_c(d)$ has nondecreasing row degrees, $\phi_1, \ldots, \phi_m$, that assume $q \leq m$ distinct values $\phi'_1 < \phi'_2 < \ldots < \phi'_q$ with multiplicity $d_h,\ h = 1, \ldots, q$, and let $G_1(d), G_2(d), \ldots, G_q(d)$ be the submatrices of $G_c(d)$ constituted by the rows 1 to d_1, d_1+1 to d_1+d_2, ..., $d_1+d_2+\cdots+d_{q-1}+1$ to $d_1+d_2+\cdots+d_q$, respectively, then

1. $(G_1)_{hr}[[.], [\gamma_1, \ldots, \gamma_{d_1}]]$, $(G_2)_{hr}[[.], [\gamma_{d_1+1}, \ldots, \gamma_{d_1+d_2}]]$, ...,

   $(G_q)_{hr}[[.], [\gamma_{d_1+\cdots+d_{q-1}+1}, \ldots, \gamma_{d_1+\cdots+d_{q-1}+d_q}]]$ are identity matrices;

2. $(G_1)_{hr}, (G_2)_{hr}, \ldots, (G_q)_{hr}$ have zeros in all positions (j, γ_i) such that $\phi_j > \phi_i$.

[1] $M[[.], [j_1, \ldots, j_l]]$ denotes the submatrix of M constituted by the columns $j_1, \ldots, j_l$.

The following algorithm allows to obtain a canonical encoder in echelon form:

Let $G_c(d)$ be a canonical encoder of $\mathcal{C}$ with nondecreasing row degrees that assume $q \leq m$ distinct values ϕ'_i with multiplicity $d_i,\ i = 1, \ldots, q$, and $G_i(d) \in \mathbb{F}[d]^{d_i \times p},\ i = 1, \ldots, q$, be the submatrices of $G_c(d)$ such that

$$G_c(d) = \begin{bmatrix} G_1(d) \\ G_2(d) \\ \vdots \\ G_q(d) \end{bmatrix}.$$

1. Apply the following procedure to compute the pivot indices of $G_c(d)$ and let γ be an empty vector that will keep the pivot indices by order of computation.

   For $i = 1, \ldots, q$ do: {

   (a) Delete the columns of $G_i(d)$ with index in γ and call $\bar{G}_i(d)$ the obtained matrix.

   (b) Find the lowest index columns $\gamma_{i_1}, \ldots, \gamma_{i_{d_i}}$ of $(\bar{G}_i)_{hr}$ such that

   $$D_{ii} := (\bar{G}_i)_{hr}[[.], [\gamma_{i_1}, \ldots, \gamma_{i_{d_i}}]]$$

   is nonsingular. Add $\gamma_{i_1}, \ldots, \gamma_{i_{d_i}}$ to γ.

   }

2. Let $\tilde{D} := \text{diag}\{D_{11}, \ldots, D_{qq}\}$, and let $\bar{G}_c(d) := \tilde{D}^{-1} G_c(d)$.

   Partitionate γ into $\gamma^{(1)}, \ldots, \gamma^{(q)}$ where $\gamma^{(1)}$ contains the first d_1 pivot indices of γ, $\gamma^{(2)}$ contains the pivot indices $d_1 + 1$ to $d_1 + d_2$,..., $\gamma^{(q)}$ contains the pivot indices $d_1 + d_2 + \cdots + d_{q-1} + 1$ to $d_1 + d_2 + \cdots + d_q$.

   For $i = 1, \ldots, q-1$ do: {

   Let $\bar{G}_i(d)$ be the submatrix of $\bar{G}_c(d)$ constituted by the columns of index in $\gamma^{(i)}$, and partitionate

   $$\bar{G}_i(d) = \begin{bmatrix} \underline{\bar{G}_{i1}(d)} \\ \underline{\bar{G}_{i2}(d)} \\ \bar{G}_{i3}(d) \end{bmatrix},$$

   where $\bar{G}_{i1}(d)$ is constituted by the first $d_1 + \cdots + d_{i-1}$ rows of $\bar{G}_i(d)$, which have degrees less than ϕ'_i, $\bar{G}_{i2}(d)$ is constituted by the rows $d_1 + \cdots + d_{i-1} + 1$ to $d_1 + \cdots + d_i$, and

is such that $(\bar{G}_{i2})_{hr} = I_{d_i}$, and $\bar{G}_{i3}(d)$ is constituted by the remaining rows of $\bar{G}_i(d)$, which can have degree greater than ϕ'_i.

Obtain a left-equivalent matrix

$$\tilde{G}_i(d) = \begin{bmatrix} \underline{\bar{G}_{i1}(d)} \\ \underline{\bar{G}_{i2}(d)} \\ \tilde{G}_{i3}(d) \end{bmatrix},$$

such that $\tilde{G}_{i3}(d)$ has row degrees less than ϕ'_i, and let $U_i(d)$ be the unimodular matrix such that $\tilde{G}_i(d) = U_i(d)\bar{G}_i(d)$.

}

Observe that for $i = 1, \ldots, q-1$,

$$U_i(d) = \begin{bmatrix} I_{d_1+\cdots+d_{i-1}} & 0 & 0 \\ 0 & I_{d_i} & 0 \\ 0 & D_i(d) & I_{d_{i+1}+\cdots+d_q} \end{bmatrix},$$

with

$$D_i(d) = \begin{bmatrix} D_{i+1,i}(d) \\ \vdots \\ D_{qi}(d) \end{bmatrix},$$

where each entry in $D_{hi},\ h > i$ has degree that does not exceed $\phi'_h - \phi'_i$.

3. Let $D(d)^{-1} := U_{q-1}(d) \cdots U_1(d)\tilde{D}^{-1}$. Then

$$D(d) = \begin{bmatrix} D_{11} & & & 0 \\ D_{21}(d) & D_{22} & & \\ \vdots & \vdots & \ddots & \\ D_{q1}(d) & D_{q2}(d) & \cdots & D_{qq} \end{bmatrix},$$

where $D_{hh} \in \mathbb{F}^{d_h \times d_h}$ is nonsingular, $h = 1, \ldots, q$, and the degree of each entry in $D_{hk}(d)$, $h > k$, does not exceed $\phi'_h - \phi'_k$, as $D(d)^{-1}$ satisfies the same conditions.

The canonical encoder

$$D(d)^{-1}G_c(d)$$

is in echelon form.

In the following example we apply the above algorithm to a canonical encoder, to obtain an equivalent canonical encoder in echelon form.

Example 4.2.1 [16] Consider the canonical encoder

$$G_c(d) = \begin{bmatrix} 1 & d & d-1 & d-2 \\ 1 & 0 & d+1 & 1 \\ d^2 & d^2-1 & 0 & 0 \end{bmatrix}.$$

$\phi'_1 = 1$ and $\phi'_2 = 2$ with multiplicity $d_1 = 2$ and $d_2 = 1$, respectively.

1. From the higher order coefficient matrix

$$(G_c)_{hr} = \left[\begin{array}{cccc} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ \hline 1 & 1 & 0 & 0 \end{array}\right],$$

we see that the pivot indices are $\gamma = (2, 3, 1)$ and that $D_{11} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $D_{22} = [1]$.

2. $\tilde{D} := \text{diag}\{D_{11}, D_{22}\}$, $\gamma^{(1)} = (2, 3)$, $\gamma^{(2)} = (1)$ and

$$\begin{aligned} \bar{G}_c(d) &= \tilde{D}^{-1} G_c(d) \\ &= \begin{bmatrix} 0 & d & -2 & d-3 \\ 1 & 0 & d+1 & 1 \\ d^2 & d^2-1 & 0 & 0 \end{bmatrix}. \end{aligned}$$

So, $\bar{G}_1(d) = \left[\begin{array}{cc} d & -2 \\ 0 & d+1 \\ \hline d^2-1 & 0 \end{array}\right]$ and $\bar{G}_2(d) = \left[\begin{array}{c} 0 \\ 1 \\ \hline d^2 \end{array}\right]$.

To get $\deg(\bar{G}_1)_{31} < 1 = \phi'_1$ left multiply $\bar{G}_1(d)$ by $U_1(d) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -d & 0 & 1 \end{bmatrix}$ and let

$$\bar{G}'_1(d) = U_1(d)\bar{G}_1(d) = \begin{bmatrix} d & -2 \\ 0 & d+1 \\ -1 & 2d \end{bmatrix}.$$

To get $\deg(\bar{G}'_1)_{32} < 1 = \phi'_1$ left-multiply $\bar{G}'_1(d)$ by $U_2(d) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix}$.

3. $D(d)^{-1} := U_2 U_1 \tilde{D}^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ -d & d-2 & 1 \end{bmatrix}$, i.e., $D(d) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & -d+3 & 1 \end{bmatrix}$, and the canonical encoder

$$D(d)^{-1} G_c(d) = \begin{bmatrix} 0 & d & -2 & d-3 \\ 1 & 0 & d+1 & 1 \\ d^2-2 & -1 & -2 & -d^2-2 \end{bmatrix},$$

is in echelon form.

♢

In case the code admits $(p_1, \ldots, p_k)$-decoupled encoders, it also has canonical $(p_1, \ldots, p_k)$-decoupled encoders. Furthermore, a parametrization, similar to the one of Proposition 4.2.2, of the canonical and minimal $(p_1, \ldots, p_k)$-decoupled encoders can be done.

Proposition 4.2.3 *Let $G_c(d)$ be a canonical encoder of $\mathcal{C}$, and consider the partition*

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

$G_i(d) \in \mathbb{F}[d]^{m \times p_i}$ with rank m_i *$i = 1, \ldots, k$, $\sum_{i=1}^{k} m_i = m$, $\sum_{i=1}^{k} p_i = p$, compatible with the finest sum decomposition of $\mathbb{F}((d))^m$ (see Definition 3.3.3 and (3.20)), where $P \in \mathbb{F}^{p \times p}$ is a permutation matrix.*

(i) Then there exists a unimodular matrix $X(d) = [X_1(d)|\ldots|X_k(d)]$, $X_i(d) \in \mathbb{F}[d]^{m \times m_i}$, $i = 1, \ldots, k$, such that

$$X(d)^{-1} G_c(d) = \begin{bmatrix} \bar{G}_1(d) & & \\ & \ddots & \\ & & \bar{G}_k(d) \end{bmatrix} P^{-1},\ \bar{G}_i(d) \in \mathbb{F}[d]^{m_i \times p_i}, i = 1, \ldots, k, \quad (4.18)$$

is a canonical $(p_1, \ldots, p_k)$-decoupled encoder of $\mathcal{C}$.

(ii) Suppose that the row degrees of $\bar{G}_i(d)$ are non decreasing, and assume $q_i \leq m_i$ distinct values $\phi_1^i < \phi_2^i < \ldots < \phi_{q_i}^i$, with multiplicity d_h^i, $h = 1, \ldots, q_i$, $i = 1, \ldots, k$.

Any other canonical $(p_1, \ldots, p_k)$-decoupled encoder, with diagonal blocks having row degrees in non decreasing order, is given by

$$\tilde{G}_c(d) = [X_1(d)D_1(d)| \ldots |X_k(d)D_k(d)]^{-1} G_c(d)$$

as $D_i(d)$, $i = 1, \ldots, k$, varies in the group of block diagonal matrices of the form

$$\begin{bmatrix} D_{11}^i & & & 0 \\ D_{21}^i(d) & D_{22}^i & & \\ \vdots & & \ddots & \\ D_{q_i 1}^i(d) & D_{q_i 2}^i(d) & \ldots & D_{q_i q_i}^i \end{bmatrix}, \tag{4.19}$$

where $D_{hh}^i \in \mathbb{F}^{d_h^i \times d_h^i}$ is non singular, $h = 1, \ldots, q_i$, and the degree of each entry in D_{hk}^i, $h > k$, does not exceed $\phi_h^i - \phi_k^i$.

(iii) All minimal $(p_1, \ldots, p_k)$-decoupled encoders of $\mathcal{C}$ are obtained by

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

by varying $D_i(d)$ in the set of the $m_i \times m_i$ polynomial matrices, whose row degrees do not exceed the corresponding ones of $\bar{G}_i(d)$ in (4.18) and $D_i(0)$ is nonsingular, $i = 1, \ldots, k$.

Proof: (i) Select an $m_i \times p_i$ full rank submatrix of $G_i(d)$, $\tilde{G}_i(d)$, $i = 1, \ldots, k$, and factorize it into

$$\tilde{G}_i(d) = M_i(d)\bar{G}_i(d)$$

where $\bar{G}_i(d) \in \mathbb{F}[d]^{m_i \times p_i}$ is left prime, and $M_i(d) \in \mathbb{F}[d]^{m_i \times m_i}$ is a left maximal divisor of $\tilde{G}_i(d)$.

If $\hat{\mathbf{r}}(d) \in \mathbb{F}[d]^{1 \times p_i}$ is any row of $G_i(d)$, there exists a rational row vector $\hat{\mathbf{x}}(d) \in \mathbb{F}(d)^{1 \times m_i}$ such that

$$\hat{\mathbf{r}}(d) = \hat{\mathbf{x}}(d)\bar{G}_i(d),$$

and the left primeness of $\bar{G}_i(d)$ implies that $\hat{\mathbf{x}}(d)$ is polynomial too (see Proposition 2.1.3). Consequently,

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

and we have

$$G_c(d)P = [X_1(d)|\dots|X_k(d)]\text{diag}\{\bar{G}_1(d),\dots,\bar{G}_k(d)\}.$$

As $G_c(d)$ and $\bar{G}_i(d),\ i=1,\dots,k$, are left prime, so are $G_c(d)P$ and $\text{diag}\{\bar{G}_1(d),\dots,\bar{G}_k(d)\}$, which implies that $[X_1(d)|\dots|X_k(d)]$ is unimodular.

For a suitable choice of $X_i(d)$, the submatrices $\bar{G}_i(d),\ i=1,\dots,k$, are row reduced, and consequently $\text{diag}\{\bar{G}_1(d),\dots,\bar{G}_k(d)\}$ is also row reduced. Thus,

$$\text{diag}\{\bar{G}_1(d),\dots,\bar{G}_k(d)\}P^{-1} = [X_1(d)|\dots|X_k(d)]^{-1}G_c(d) \tag{4.20}$$

is a canonical $(p_1,\dots,p_k)$-decoupled encoder of $\mathcal{C}$.

(ii) Let $\tilde{G}_c(d)$ be another canonical $(p_1,\dots,p_k)$-decoupled encoder of $\mathcal{C}$. Then,

$$\tilde{G}_c(d)P = \begin{bmatrix} \tilde{G}_1(d) & & \\ & \ddots & \\ & & \tilde{G}_k(d) \end{bmatrix},\ \tilde{G}_i(d) \in \mathbb{F}[d]^{m_i\times p_i},\ i=1,\dots,k.$$

It is easy to see that $\text{diag}\{\tilde{G}_1(d),\dots,\tilde{G}_k(d)\}$ is left prime and row reduced if and only if $\tilde{G}_i(d),\ i=1,\dots,k$, are also left prime and row reduced.

From (i),

$$D(d)\tilde{G}_c(d)P = [X_1(d)|\dots|X_k(d)]^{-1}G_c(d)P,$$

for some unimodular matrix $D(d)\in\mathbb{F}[d]^{m\times m}$, i.e.,

$$D(d)\begin{bmatrix} \tilde{G}_1(d) & & \\ & \ddots & \\ & & \tilde{G}_k(d) \end{bmatrix} = \begin{bmatrix} \bar{G}_1(d) & & \\ & \ddots & \\ & & \bar{G}_k(d) \end{bmatrix},$$

which implies that

$$D(d) = \text{diag}\{D_1(d),\dots,D_k(d)\},$$

with $D_i(d)\in\mathbb{F}[d]^{m_i\times m_i}$ unimodular, $i=1,\dots,k$. Consequently, as

$$D_i(d)\tilde{G}_i(d) = \bar{G}_i(d),\ i=1,\dots,k,$$

the row degrees of $\tilde{G}_i(d)$ and $\bar{G}_i(d)$ are the same, up to a row permutation.

Suppose that the row degrees of $\tilde{G}_i(d),\ i = 1, \ldots, k$, are also in non decreasing order. Then, from Proposition 4.2.2, (iv), it follows that

$$D_i(d) = \begin{bmatrix} D^i_{11} & & & 0 \\ D^i_{21}(d) & D^i_{22} & & \\ \vdots & & \ddots & \\ D^i_{q_i1}(d) & D^i_{q_i2}(d) & \ldots & D^i_{q_iq_i} \end{bmatrix}$$

where $D^i_{hh} \in \mathbb{F}^{d^i_h \times d^i_h}$ is nonsingular, $h = 1, \ldots, q_i$, and the degree of each entry in $D^i_{hk}(d),\ h > k$, does not exceed $\phi^i_h - \phi^i_k,\ \ i = 1, \ldots, k$.

Therefore,

$$\tilde{G}_c(d) = [X_1(d)D_1(d)| \ldots |X_k(d)D_k(d)]^{-1} G_c(d)$$

with $D_i(d),\ i = 1, \ldots, k$, given by (4.19).

Conversely, let

$$\begin{aligned} \tilde{G}_c(d) &= [X_1(d)D_1(d)| \ldots |X_k(d)D_k(d)]^{-1} G_c(d) \\ &= \begin{bmatrix} D_1(d) & & \\ & \ddots & \\ & & D_k(d) \end{bmatrix}^{-1} \begin{bmatrix} \bar{G}_1(d) & & \\ & \ddots & \\ & & \bar{G}_k(d) \end{bmatrix} P^{-1}, \end{aligned} \tag{4.21}$$

where $D_i(d),\ i = 1, \ldots, k$, are of the form (4.19).

Then,

$$\tilde{G}_c(d)P = \begin{bmatrix} D_1(d)^{-1}\bar{G}_1(d) & & \\ & \ddots & \\ & & D_k(d)^{-1}\bar{G}_k(d) \end{bmatrix}$$

is a $(p_1, \ldots, p_k)$-decoupled encoder of $\mathcal{C}$.

From Proposition 4.2.2 (iv), $D_i(d)^{-1}\bar{G}_i(d)$ is left prime and row reduced, $i = 1, \ldots, k$, which implies that also $\mathrm{diag}\{D_1(d)^{-1}\bar{G}_1(d), \ldots, D_k(d)^{-1}\bar{G}_k(d)\}$ is left prime and row reduced, and consequently, $\tilde{G}_c(d)$ is a canonical $(p_1, \ldots, p_k)$-decoupled encoder of $\mathcal{C}$.

(iii) If $G(d)$ is a minimal $(p_1, \ldots, p_k)$-decoupled encoder of $\mathcal{C}$, then

$$G(d)P = \begin{bmatrix} G_1(d) & & \\ & \ddots & \\ & & G_k(d) \end{bmatrix}, \; G_i(d) \in \mathbb{F}(d)^{m_i \times p_i}, \; i = 1, \ldots, k,$$

and, from Proposition 4.2.2 (i),

$$\begin{aligned} G(d)P &= D(d)^{-1}[X_1(d)| \ldots |X_k(d)]^{-1} G_c(d)P \\ &= D(d)^{-1} \begin{bmatrix} \bar{G}_1(d) & & \\ & \ddots & \\ & & \bar{G}_k(d) \end{bmatrix}, \end{aligned}$$

for some $D(d) \in \mathbb{F}[d]^{m \times m}$, with $D(0)$ nonsingular, and row degrees not greater than the corresponding ones of the canonical encoder $[X_1(d)| \ldots |X_k(d)]^{-1} G_c(d)$, and, obviously, also of $\mathrm{diag}\{\bar{G}_1(d), \ldots, \bar{G}_k(d)\}$.

Therefore,

$$\begin{bmatrix} G_1(d) & & \\ & \ddots & \\ & & G_k(d) \end{bmatrix} = D(d)^{-1} \begin{bmatrix} \bar{G}_1(d) & & \\ & \ddots & \\ & & \bar{G}_k(d) \end{bmatrix},$$

which implies that $D(d) = \mathrm{diag}\{D_1(d), \ldots, D_k(d)\}$, where $D_i(d) \in \mathbb{F}[d]^{m_i \times m_i}, \; i = 1, \ldots, k$, have row degrees that do not exceed the corresponding ones of $\bar{G}_i(d)$, with $D_i(0)$ invertible, and such that

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

Conversely, let

$$\begin{aligned} G(d) &= [X_1(d)D_1(d)| \ldots \; |X_k(d)D_k(d)]^{-1} G_c(d) \\ &= \begin{bmatrix} D_1(d) & & \\ & \ddots & \\ & & D_k(d) \end{bmatrix}^{-1} \begin{bmatrix} \bar{G}_1(d) & & \\ & \ddots & \\ & & \bar{G}_k(d) \end{bmatrix} P^{-1}, \end{aligned}$$

where $D_i(d) \in \mathbb{F}^{m_i \times m_i}$ with $D_i(0)$ invertible, and $\deg \text{row}_j D_i \leq \deg \text{row}_j \bar{G}_i$, $j = 1, \ldots, m_i$, $i = 1, \ldots, k$. Then,

$$D(d) := \text{diag}\{D_1(d), \ldots, D_k(d)\}$$

is such that $D(0)$ is nonsingular, and has row degrees that do not exceed the corresponding ones of the canonical encoder $\text{diag}\{\bar{G}_1(d), \ldots, \bar{G}_k(d)\}P^{-1}$, and, therefore, by Proposition 4.2.1, $G(d)$ is a minimal encoder of $\mathcal{C}$. □

4.3 Abstract states

Given a causal (polynomial or rational) encoder $G(d)$, consider the homomorphism between the $\mathbb{F}$-vector spaces $\mathbb{F}[d^{-1}]^m$ and $d\,\mathbb{F}[[d]]^p$, given by

$$\mathcal{S}_G : \mathbb{F}[d^{-1}]^m \to d\,\mathbb{F}[[d]]^p : \hat{\mathbf{u}}(d^{-1}) \mapsto (\text{id} - \mathcal{P}_1)(\hat{\mathbf{u}}G), \tag{4.22}$$

where $\mathcal{P}_1$ is the truncation operator at time 1 defined in (3.14), that associates to an information signal $\hat{\mathbf{u}}(d^{-1})$ with support in $(-\infty, 0]$ the restriction to $[1, +\infty)$ of the corresponding codeword $\hat{\mathbf{u}}(d^{-1})G(d)$. The elements of the image of $\mathcal{S}_G$, i.e, the free evolutions of the encoder output on $[1, +\infty)$ are called the *abstract states* of the encoder [14, 25]. An information signal $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$ induces, after time $t = 0$, an abstract state given by the codeword restriction $(\text{id} - \mathcal{P}_1)((\mathcal{P}_1\hat{\mathbf{u}})G)$ in $d\,\mathbb{F}[[d]]^p$. The image of $\mathcal{S}_G$ will be called *abstract state space* associated to $G(d)$.

In [27] Kalman considered an unusual definition of input/output map, in order to express the outcome of an "experiment" which results from the application of an input sequence of finite duration that terminates at time t_0, and the observation of the output sequence only after the input is terminated, that is, for $t > t_0$.

Definition 4.3.1 *A linear, zero-state, input-output map over* $\mathbb{F}$ *is an homomorphism*

$$f : \mathbb{F}[d^{-1}]^m \to d\,\mathbb{F}[[d]]^p,$$

which is invariant under translation with respect to time in the following sense:

the diagram

$$\begin{array}{ccc} \mathbb{F}[d^{-1}]^m & \xrightarrow{\quad f \quad} & d\,\mathbb{F}[[d]]^p \\ \Big\downarrow \tilde{\sigma}_{\mathbb{F}[d^{-1}]^m} & & \Big\downarrow \tilde{\sigma}_{d\,\mathbb{F}[[d]]^p} \\ \mathbb{F}[d^{-1}]^m & \xrightarrow[\quad f \quad]{} & d\,\mathbb{F}[[d]]^p \end{array}$$

commutes, with the shift operators $\tilde{\sigma}_{\mathbb{F}[d^{-1}]^m}$ *and* $\tilde{\sigma}_{d\,\mathbb{F}[[d]]^p}$ *defined as*

$$\tilde{\sigma}_{\mathbb{F}[d^{-1}]^m}(\sum_{i=k}^{0} \mathbf{u}_i d^i) = \sum_{i=k-1}^{-1} \mathbf{u}_{i+1} d^i, \quad k \leq 0,$$

and

$$\tilde{\sigma}_{d\,\mathbb{F}[[d]]^p}(\sum_{i=1}^{+\infty} \mathbf{w}_i d^i) = \sum_{i=1}^{+\infty} \mathbf{w}_{i+1} d^i.$$

Remark:

- f is causal as the output starts always after the end of the input; the output starts at time $i \geq 1$, and the input ends at time $j \leq 0$.
- $\tilde{\sigma}_{\mathbb{F}[d^{-1}]^m}(\sum_{i=k}^{0} \mathbf{u}_i d^i)$ shifts to the left the sequence $\mathbf{u}$ corresponding to $\hat{\mathbf{u}}(d) = \sum_{i=k}^{0} \mathbf{u}_i\, d^i$.
- $\tilde{\sigma}_{d\,\mathbb{F}[[d]]^p}(\sum_{i=1}^{+\infty} \mathbf{w}_i d^i)$ shifts to the left the sequence $\mathbf{w}$ represented by $\hat{\mathbf{w}}(d) = \sum_{i=1}^{+\infty} \mathbf{w}_i\, d^i$, and discards $\mathbf{w}_1$.

Given such an input-output map, an equivalence relation can be defined, called *Nerode equivalence*, which states that two inputs, that terminate at some time t_0, are equivalent if the output, after t_0, is the same.

Definition 4.3.2 *(Nerode equivalence) Given an input/output map over* $\mathbb{F}$, $f : \mathbb{F}[d^{-1}]^m \to d\mathbb{F}[[d]]^p$, *the Nerode equivalence relation on* $\mathbb{F}[d^{-1}]^m$ *induced by* f *is*

$$\hat{\mathbf{u}}_1(d) \sim \hat{\mathbf{u}}_2(d) \text{ if } f(\hat{\mathbf{u}}_1(d) \circ \hat{\mathbf{x}}(d)) = f(\hat{\mathbf{u}}_2(d) \circ \hat{\mathbf{x}}(d)) \ \forall \hat{\mathbf{x}}(d) \in \mathbb{F}[d^{-1}]^m,$$

where $\hat{\mathbf{u}}(d) \circ \hat{\mathbf{x}}(d) = \hat{\mathbf{u}}(d)d^{-k} + \hat{\mathbf{x}}(d)$, *with* k *being the difference between the order of* $\hat{\mathbf{x}}(d)$ *and the degree of* $\hat{\mathbf{u}}(d)$, *if* $\hat{\mathbf{x}}(d)$ *is not the zero sequence, and* $\hat{\mathbf{u}}(d) \circ \hat{\mathbf{x}}(d) = \hat{\mathbf{u}}(d)$, *if* $\hat{\mathbf{x}}(d) = 0$.

It can be easily proved that $\hat{\mathbf{u}}_1(d)$ and $\hat{\mathbf{u}}_2(d)$ in $\mathbb{F}[d^{-1}]^m$ are Nerode equivalent with respect to an input/output map f if and only if $f(\hat{\mathbf{u}}_1(d)) = f(\hat{\mathbf{u}}_2(d))$ [27].

Definition 4.3.2 means that two inputs $\hat{\mathbf{u}}_1(d)$ and $\hat{\mathbf{u}}_2(d)$ in $\mathbb{F}[d^{-1}]^m$ are Nerode equivalent if the output sequences they induce on $[1, +\infty)$ are the same and remain the same whenever both $\hat{\mathbf{u}}_1(d)$ and $\hat{\mathbf{u}}_2(d)$ are followed by an arbitrary input $\hat{\mathbf{v}}(d) \in \mathbb{F}[[d]]^m$. Consequently, the Nerode equivalence classes associated to an input/output map can be viewed as the states of f. Indeed, observe that $\mathcal{S}_G$ defined in (4.22) is a linear, zero-state input-output map. Since $\operatorname{Im} \mathcal{S}_G$ is canonically isomorphic to $\mathbb{F}[d^{-1}]^m / \ker \mathcal{S}_G$, the Nerode equivalence classes are the elements of $\mathbb{F}[d^{-1}]^m / \ker \mathcal{S}_G$ and each abstract state of an encoder can be viewed as a Nerode equivalence class on the information sequences ending at time 0, or equivalently as the coset $\mathcal{P}_1\hat{\mathbf{u}} + \ker \mathcal{S}_G$ in $\mathbb{F}[d^{-1}]^m$.

If $\Sigma = (A, B, C, J)$ is an n-dimensional realization of the encoder $G(d)$, the *physical states* induced by Σ are the contents of its memory elements, at some time t [15]. By time-invariance, it is enough to consider $t = 1$. The set of physical states, $\Gamma_{(A,B,C,J)}$, is an $\mathbb{F}$-vector space, called the *physical state space*, and its elements, i.e., the physical states induced by Σ, will be denoted by ρ. $\Gamma_{(A,B,C,J)}$ has dimension n if and only if Σ is reachable [26, 12].

Let us restrict to reachable realizations of $G(d)$. If $\hat{\mathbf{a}}_G(d)$ is the abstract state of $G(d)$ induced by $\hat{\mathbf{u}}(d) \in \mathbb{F}[d^{-1}]^m$, i.e., $\hat{\mathbf{a}}_G(d) = \mathcal{S}_G(\hat{\mathbf{u}}(d))$, and $\hat{\mathbf{x}}(d)$ the forced state evolution of Σ corresponding to the input $\hat{\mathbf{u}}(d)$, we have that

$$\hat{\mathbf{a}}_G(d) = \rho(I - Ad)^{-1}Cd \tag{4.23}$$

where $\rho = \mathbf{x}_1$. So, $\dim \Gamma_{(A,B,C,J)} \geq \dim \operatorname{Im} \mathcal{S}_G$, and the equality is satisfied if and only if the epimorphism between $\Gamma_{(A,B,C,J)}$ and $\operatorname{Im} \mathcal{S}_G$ defined by (4.23) is injective, i.e., if and only if the realization Σ is observable, or equivalently, minimal [26, 12]. So, an n-dimensional

realization $\Sigma = (A, B, C, J)$ of $G(d)$ is minimal if and only if $n = \dim \Gamma_{(A,B,C,J)} = \dim \operatorname{Im} \mathcal{S}_G$, and the next proposition follows immediately.

Proposition 4.3.1 *[25] An encoder is minimal if the associated abstract state space has minimal dimension among all equivalent encoders.*

In this section, we shall investigate how some properties of an encoder do reflect into the structure of its abstract state space, the final goal being a classical characterization of minimal encoders [14]. In our discussion, we provide in advance a fairly complete account of different inclusions between the span of an information sequence and that of the corresponding codeword, and show how they are related to a nontrivial intersection between the code $\mathcal{C}$ and the space of the abstract states of the encoder.

In the following discussion $D(d)^{-1}N(d)$ denotes an irreducible left MFD of a causal encoder $G(d)$, with $N(d)$ row reduced and $\deg \operatorname{row}_i(N) = k_i,\ i = 1, \ldots, m$. Moreover $N(d) = \Delta(d)\bar{N}(d)$ is a factorization of $N(d)$ with $\bar{N}(d)$ left prime.

Lemma 4.3.1 *Consider the following inclusion relations*

$$(I) \quad \inf \operatorname{span}(\hat{\mathbf{v}}) \geq \inf \operatorname{span}(\hat{\mathbf{v}}G),\ \forall\, \hat{\mathbf{v}}(d) \in \mathbb{F}((d))^m,$$

$$(S_{fin}) \quad \sup \operatorname{span}(\hat{\mathbf{v}}) \leq \sup \operatorname{span}(\hat{\mathbf{v}}G),\ \forall\, \hat{\mathbf{v}}(d) \in \mathbb{F}[d, d^{-1}]^m,$$

$$(S_\infty) \quad \sup \operatorname{span}(\hat{\mathbf{v}}) = \infty \Longrightarrow \sup \operatorname{span}(\hat{\mathbf{v}}G) = \infty,\ \forall\, \hat{\mathbf{v}}(d) \in \mathbb{F}((d))^m,$$

$$(B_{fin}) \quad \operatorname{span}(\hat{\mathbf{v}}) \subseteq \operatorname{span}(\hat{\mathbf{v}}G),\ \forall\, \hat{\mathbf{v}}(d) \in \mathbb{F}[d, d^{-1}]^m,$$

$$(B) \quad \operatorname{span}(\hat{\mathbf{v}}) \subseteq \operatorname{span}(\hat{\mathbf{v}}G),\ \forall\, \hat{\mathbf{v}}(d) \in \mathbb{F}((d))^m.$$

Then we have the equivalences:

$$(I)\ \wedge\ (S_{fin}) \Longleftrightarrow (B_{fin}) \tag{4.24}$$

$$(I)\ \wedge\ (S_{fin})\ \wedge\ (S_\infty) \Longleftrightarrow (B) \tag{4.25}$$

Moreover

(a) (I) *holds if and only if* $\operatorname{rank} N(0) = m$,

(b) (S_{fin}) *holds if and only if* $\deg \operatorname{row}_i(D) \leq \deg \operatorname{row}_i(N),\ i = 1, \ldots, m$,

(c) (S_∞) *holds if and only if* $\det(\Delta) = \alpha\, d^k,\ \alpha \in \mathbb{F}\backslash\{0\},\ k \geq 0$.

Proof: (4.24) and (4.25) are obvious.

(a) $\operatorname{rank} N(0) = m$ is equivalent to $\operatorname{rank} G(0) = m$, which is clearly equivalent to (I).

(b) Let $\deg \operatorname{row}_i(D) \leq \deg \operatorname{row}_i(N) = k_i,\ i = 1, \ldots, m$. Given $\hat{\mathbf{v}}(d) \in \mathbb{F}[d, d^{-1}]^m$, suppose $\sup \operatorname{span}(\hat{\mathbf{v}}G) = \ell \in \mathbb{N}$. Then $\hat{\mathbf{u}}(d) := \hat{\mathbf{v}}(d)D(d)^{-1}$ is Laurent polynomial, as

$$\hat{\mathbf{u}}(d)[D(d)\ \ N(d)] = [\hat{\mathbf{v}}(d)\ \ \hat{\mathbf{v}}(d)G(d)]$$

is Laurent polynomial and $[D(d)\ N(d)]$ is left prime. Furthermore, since $N(d)$ is row reduced,

$$\deg(\hat{\mathbf{u}}N) = \deg(\hat{\mathbf{v}}G) = \ell \Longrightarrow \deg \hat{u}_i \leq \ell - k_i,\ i = 1, \ldots, m$$

and

$$\hat{v}_i(d) = \hat{\mathbf{u}}(d)\operatorname{col}_i(D),\ i = 1, \ldots, m$$

implies

$$\deg \hat{v}_i \leq \max_{0 \leq i \leq m} \{\deg \hat{u}_i + k_i\} \leq \ell.$$

We therefore have $\sup \operatorname{span}(\hat{\mathbf{v}}) \leq \sup \operatorname{span}(\hat{\mathbf{v}}G)$.

Vice-versa, suppose that there exists $i \in \{1, \ldots, m\}$ such that $\deg \operatorname{row}_i(D) > k_i$. The information sequence $\hat{\mathbf{v}}(d) := [0 \ldots d^{-k_i} \ \ldots \ 0]D(d) = d^{-k_i}\ \operatorname{row}_i(D)$, is polynomial with degree greater than zero, and the corresponding codeword,

$$\hat{\mathbf{v}}(d)G(d) = \hat{\mathbf{v}}(d)D(d)^{-1}N(d) = d^{-k_i}\ \operatorname{row}_i(N)$$

has degree zero, i.e., $\sup \operatorname{span}(\hat{\mathbf{v}}) > \sup \operatorname{span}(\hat{\mathbf{v}}G)$.

(c) has been already proved in Proposition 3.2.5. □

Proposition 4.3.2 *The code* $\mathcal{C}$ *does not include nonzero abstract states of the encoder* $G(d)$*, i.e.* $(\operatorname{Im} \mathcal{S}_G) \cap \mathcal{C} = \{0\}$*, if and only if* (I)*,* (S_{fin}) *and* (S_∞) *in Lemma 4.3.1 simultaneously hold.*

Proof: If (I) does not hold, there exists $\hat{\mathbf{v}}(d) \in \mathbb{F}((d))^m$ such that $\inf \operatorname{span}(\hat{\mathbf{v}}) \leq 0$ and $\inf \operatorname{span}(\hat{\mathbf{v}}G) > 0$. By the causality of $G(d)$,

$$0 = \mathcal{P}_1(\hat{\mathbf{v}}G) = \mathcal{P}_1\Big((\mathcal{P}_1\hat{\mathbf{v}})G\Big),$$

which implies that the nonzero codeword $(\mathcal{P}_1\hat{\mathbf{v}})G = (\mathrm{id} - \mathcal{P}_1)\Big((\mathcal{P}_1\hat{\mathbf{v}})G\Big)$ is an abstract state of $G(d)$.

If (S_{fin}) or (S_∞) do not hold, there exists $\hat{\mathbf{v}}(d) \in \mathbb{F}((d))^m$ such that $\sup \operatorname{span}(\hat{\mathbf{v}}) > 0$ or $\sup \operatorname{span}(\hat{\mathbf{v}}) = \infty$ and $\sup \operatorname{span}(\hat{\mathbf{v}}G) \leq 0$. Therefore

$$0 = (\mathrm{id} - \mathcal{P}_1)(\hat{\mathbf{v}}G) = (\mathrm{id} - \mathcal{P}_1)\Big((\mathcal{P}_1\hat{\mathbf{v}})G\Big) + (\mathrm{id} - \mathcal{P}_1)\Big([(\mathrm{id} - \mathcal{P}_1)\hat{\mathbf{v}}]G\Big)$$

and by causality, $(\mathrm{id} - \mathcal{P}_1)\Big((\mathcal{P}_1\hat{\mathbf{v}})G\Big) = -\Big((\mathrm{id} - \mathcal{P}_1)\hat{\mathbf{v}}\Big)G \neq 0$ belongs to $(\operatorname{Im} \mathcal{S}_G) \cap \mathcal{C}$.

Vice-versa, assume that (I), (S_{fin}) and (S_∞) hold and suppose that the abstract state of $\hat{\mathbf{u}}(d^{-1}) \in \mathbb{F}[d^{-1}]^m$ is a codeword, i.e.,

$$\mathcal{S}_G(\hat{\mathbf{u}}(d^{-1})) = (\mathrm{id} - \mathcal{P}_1)(\hat{\mathbf{u}}G) = \hat{\mathbf{v}}(d)G(d) \tag{4.26}$$

for some $\hat{\mathbf{v}}(d) \in \mathbb{F}((d))^m$. As $\inf \operatorname{span}(\hat{\mathbf{v}}G) > 0$, (I) implies $\inf \operatorname{span}(\hat{\mathbf{v}}) > 0$, and, by (4.26), the codeword

$$(\hat{\mathbf{u}}(d^{-1}) - \hat{\mathbf{v}}(d))G(d) = \mathcal{P}_1(\hat{\mathbf{u}}G) + (\mathrm{id} - \mathcal{P}_1)(\hat{\mathbf{u}}G) - \hat{\mathbf{v}}(d)G(d) = \mathcal{P}_1(\hat{\mathbf{u}}G)$$

has support in $(-\infty, 0]$. Thus by (S_{fin}) and (S_∞), we have $\operatorname{span}(\hat{\mathbf{u}}(d^{-1}) - \hat{\mathbf{v}}(d)) \subseteq (-\infty, 0]$ and therefore $\hat{\mathbf{v}}(d) = (\mathrm{id} - \mathcal{P}_1)(\hat{\mathbf{u}} - \hat{\mathbf{v}}) = 0$, i.e, $\mathcal{S}_G(\hat{\mathbf{u}}(d^{-1})) = 0$. □

The following proposition is now an immediate consequence of Proposition 4.3.2 above, and constitutes a generalization of results obtained in [14, 25, 17].

Proposition 4.3.3 *The following are equivalent*

(i) $(\operatorname{Im} \mathcal{S}_G) \cap \mathcal{C} = \{0\}$,

(ii) $G(d)$ *is a minimal encoder,*

(iii) $\operatorname{span}(\hat{\mathbf{v}}) \subseteq \operatorname{span}(\hat{\mathbf{v}}G)$, $\forall\, \hat{\mathbf{v}}(d) \in \mathbb{F}((d))^m$.

Proof: Both (i) and (iii) are equivalent to assumption $(I) \wedge (S_{fin}) \wedge (S_\infty)$ of Lemma 4.3.1.

On the other hand, represent $G(d)$ as $D(d)^{-1}N(d)$, with $N(d)$ row reduced, and write $N(d) = \Delta(d)\bar{N}(d)$, with $\bar{N}(d)$ left prime.

By (a) and (c) of Lemma 4.3.1, conditions (I) and (S_∞) are equivalent to assume that $\det(\Delta) = \alpha d^k,\ \alpha \in \mathbb{F}\backslash\{0\},\ k \geq 0$, and $\operatorname{rank} N(0) = m$.

If $\det(\Delta) = \alpha d^k,\ \alpha \in \mathbb{F}\backslash\{0\},\ k \geq 0$, and $\operatorname{rank} N(0) = m$ hold, we have that $\operatorname{rank} \Delta(0) = m$, as $N(0) = \Delta(0)\bar{N}(0)$, and therefore, $\det(\Delta) = \alpha,\ \alpha \in \mathbb{F}\backslash\{0\}$. Vice-versa, if $\det(\Delta) = \alpha,\ \alpha \in \mathbb{F}\backslash\{0\}$, as $\operatorname{rank} \bar{N}(0) = m$ (because $\bar{N}(d)$ is left prime), $N(0) = \Delta(0)\bar{N}(0)$ implies that $\operatorname{rank} N(0) = m$. Therefore, conditions (I) and (S_∞) are equivalent to assume that $\Delta(d)$ is unimodular, which is equivalent to assume that $N(d)$ is left prime, i.e., that $N(d)$ is a canonical encoder. So, by Proposition 4.2.1 and Lemma 4.3.1 (b), we conclude that $(I) \wedge (S_{fin}) \wedge (S_\infty)$ altogether imply and are implied by the minimality of $G(d)$. □

We restrict now our analysis to the abstract state structure of two classes of encoders, i.e., minimal encoders and polynomial reduced encoders.

Referring to the representation (4.13), let $G(d) = D(d)^{-1}G_c(d)$ be a minimal encoder, and $k_i \leq \phi_i$ be the row degrees of $D(d)$. The abstract zero state of the encoder, viewed as a coset in $\mathbb{F}[d^{-1}]^m/\ker \mathcal{S}_G$,

$$\ker \mathcal{S}_G = \{\hat{\mathbf{u}}(d^{-1}) \in \mathbb{F}[d^{-1}]^m : \hat{\mathbf{u}}(d^{-1})D(d)^{-1}G_c(d) \in \mathbb{F}[d^{-1}]^p\}, \tag{4.27}$$

can be computed as follows. If $\hat{\mathbf{u}}(d^{-1}) \in \ker \mathcal{S}_G$, then $\hat{\mathbf{v}}(d, d^{-1}) := \hat{\mathbf{u}}(d^{-1})D(d)^{-1}$ must be a Laurent polynomial vector, otherwise the upper bound of the support of $\hat{\mathbf{v}}(d, d^{-1})G_c(d)$ would not be finite because of the left primeness of $G_c(d)$. Substituting $\hat{\mathbf{u}}(d^{-1}) = \hat{\mathbf{v}}(d, d^{-1})D(d)$ into (4.27), gives $\deg \hat{v}_i \leq -\phi_i,\ i = 1, \ldots, m$ and, consequently,

$$\begin{aligned} \ker \mathcal{S}_G &= \{\hat{\mathbf{u}}(d^{-1}) = \hat{\mathbf{w}}(d^{-1})\operatorname{diag}\{d^{-\phi_1}, \ldots, d^{-\phi_m}\}D(d),\ \hat{\mathbf{w}}(d^{-1}) \in \mathbb{F}[d^{-1}]^m\} \\ &= \{\hat{\mathbf{u}}(d^{-1}) = \hat{\mathbf{w}}(d^{-1})\tilde{D}(d^{-1}),\ \hat{\mathbf{w}}(d^{-1}) \in \mathbb{F}[d^{-1}]^m\}, \end{aligned}$$

where $\tilde{D}(d^{-1}) = \operatorname{diag}\{d^{-\phi_1}, \ldots, d^{-\phi_m}\}D(d)$. Taking the Smith form of $\tilde{D}(d^{-1})$

$$\tilde{D}(d^{-1}) = \tilde{W}(d^{-1})\operatorname{diag}\{\tilde{\gamma}_1(d^{-1}), \ldots, \tilde{\gamma}_m(d^{-1})\}\tilde{V}(d^{-1}),$$

with $\tilde{V}(d^{-1})$ and $\tilde{W}(d^{-1})$ unimodular matrices, we have also

$$\ker \mathcal{S}_G = \left\{ \hat{\mathbf{u}}(d^{-1}) = \hat{\mathbf{m}}(d^{-1})\mathrm{diag}\{\tilde{\gamma}_1(d^{-1}), \ldots, \tilde{\gamma}_m(d^{-1})\}\tilde{V}(d^{-1}),\ \hat{\mathbf{m}}(d^{-1}) \in \mathbb{F}[d^{-1}]^m \right\}.$$

So, the abstract states of $G(d)$ are the cosets, modulo $\ker \mathcal{S}_{\mathrm{G}}$, of the $\mathbb{F}$-linear combinations of the independent vectors $d^{-i}\mathbf{e}_j\tilde{V}(d^{-1}),\ j = 1, \ldots, m,\ 0 \leq i < \deg \tilde{\gamma}_j(d^{-1})$.

Moreover, letting $\tilde{N}(d^{-1}) := \mathrm{diag}\{d^{-\phi_1}, \ldots, d^{-\phi_m}\}G_c(d)$, $G(d) = \tilde{D}(d^{-1})^{-1}\tilde{N}(d^{-1})$, and the codeword induced by any information signal $\hat{\mathbf{u}}(d^{-1}) \in \mathbb{F}[d^{-1}]^m$ satisfies

$$\tilde{\gamma}_1(d^{-1})\hat{\mathbf{u}}(d^{-1})G(d) = \hat{\mathbf{u}}(d^{-1})\tilde{V}(d^{-1})^{-1} \begin{bmatrix} 1 & & \\ & \ddots & \\ & & \dfrac{\tilde{\gamma}_1(d^{-1})}{\tilde{\gamma}_m(d^{-1})} \end{bmatrix} \tilde{W}(d^{-1})^{-1}\tilde{N}(d^{-1}) \in\ \mathbb{F}[d^{-1}]^p$$

which implies that $\tilde{\gamma}_1(d^{-1})\hat{\mathbf{u}}(d^{-1}) \in \ker \mathcal{S}_G$.

If $G(d)$ is a row reduced polynomial encoder with row degrees $k_1, \ldots, k_m$, the zero state $\ker \mathcal{S}_G$ consists of all input signals $\hat{\mathbf{u}}(d^{-1})$ satisfying $\deg \hat{u}_i \leq -k_i,\ i = 1, \ldots, m$, and, vice-versa, this condition implies that $G(d)$ is row reduced. So, the restriction to $[1, +\infty)$ of the codeword induced by $\hat{\mathbf{u}}(d^{-1}) \in \mathbb{F}[d^{-1}]^m$ provides a complete information on the restriction of $\hat{u}_i(d)$ to $(-k_i, 0]$, $i = 1, 2, \ldots, m$, and no information on the remaining coefficients of $\hat{u}_i(d)$.

4.4 State feedback and parametrization of minimal encoders

In this section it will be shown that all minimal encoders of $\mathcal{C}$ can be obtained from a minimal one, by applying static feedback and static precompensation to a minimal state space realization of a canonical encoder $G_c(d)$.

Suppose that $\Sigma = (A, B, C, J)$ is the minimal realization of $G_c(d) = I_m^{-1}G_c(d)$, given by (4.4), (4.6) and (4.7) in section 4.1. As we have seen, the dimension n of the realization coincides with the degree $\sum_{i=1}^{m} \phi_i$ of $\mathcal{C}$. If the state $\mathbf{x}$ is fed-back into the system via a matrix $K \in \mathbb{F}^{n \times m}$ (see Figure 4.1), the input sequence becomes the sum of the information sequence $\{\mathbf{u}_t\}$ and the feedback sequence $\{\mathbf{x}_t K\}$, and the state model Σ modifies into $\Sigma^{(K)} =$

$(A + KB, B, C + KJ, J)$, as we have

$$\begin{aligned} \mathbf{x}_{t+1} &= \mathbf{x}_t A + [\mathbf{u}_t + \mathbf{x}_t K]B = \mathbf{x}_t[A + KB] + \mathbf{u}_t B \\ \mathbf{w}_t &= \mathbf{x}_t C + [\mathbf{u}_t + \mathbf{x}_t K]J = \mathbf{x}_t[C + KJ] + \mathbf{u}_t J \end{aligned} \tag{4.28}$$

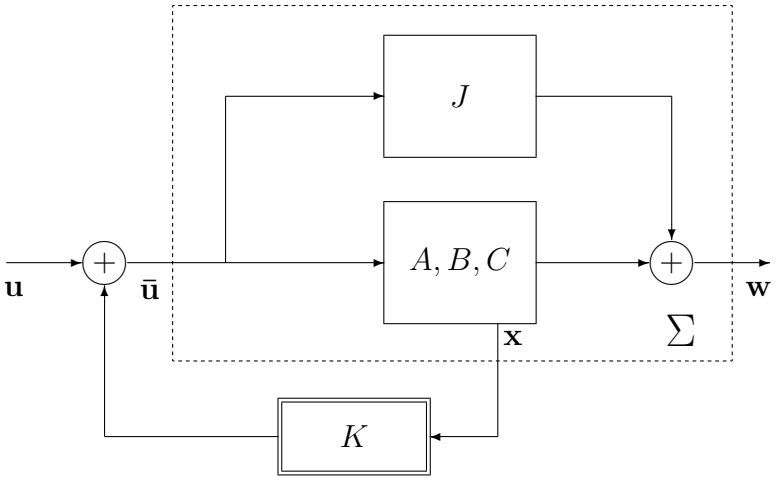

Figure 4.1 - Application of static feedback to Σ

From (4.28), it follows that the series $\hat{\mathbf{x}}(d) := \sum_t \mathbf{x}_t d^t$, corresponding to the forced state evolution of $\Sigma^{(K)}$, and the information series $\hat{\mathbf{u}}(d) := \sum_t \mathbf{u}_t d^t$ are connected by

$$\begin{aligned} & d^{-1}\hat{\mathbf{x}}(d) = \hat{\mathbf{x}}(d)(A + KB) + \hat{\mathbf{u}}(d)B \\ \Leftrightarrow\ & \hat{\mathbf{x}}(d)(I_n - dA) = (\hat{\mathbf{u}}(d) + \hat{\mathbf{x}}(d)K)Bd \\ \Leftrightarrow\ & \hat{\mathbf{x}}(d) = (\hat{\mathbf{u}}(d) + \hat{\mathbf{x}}(d)K)Bd(I_n - Ad)^{-1} \\ \Leftrightarrow\ & \hat{\mathbf{x}}(d)(I_n - KBd(I_n - Ad)^{-1}) = \hat{\mathbf{u}}(d)Bd(I_n - Ad)^{-1} \\ \Leftrightarrow\ & \hat{\mathbf{x}}(d) = \hat{\mathbf{u}}(d)Bd(I_n - Ad)^{-1}(I_n - KBd(I_n - Ad)^{-1})^{-1}. \end{aligned} \tag{4.29}$$

Observe that, if M and L are matrices of dimension $m \times n$ and $n \times m$, respectively, such that $I_n - LM$ is invertible, then as $(I_m - ML)M = M(I_n - LM)$, it follows that

$$M(I_n - LM)^{-1} = (I_m - ML)^{-1}M. \tag{4.30}$$

Therefore,

$$Bd(I_n - Ad)^{-1}(I_n - KBd(I_n - Ad)^{-1})^{-1} = (I_m - Bd(I_n - Ad)^{-1}K)^{-1}Bd(I_n - Ad)^{-1},$$

which, together with (4.29), implies that

$$\hat{\mathbf{x}}(d) = \hat{\mathbf{u}}(d)[I_m - Bd(I_n - dA)^{-1}K]^{-1}Bd(I_n - dA)^{-1}.$$

As the output $\hat{\mathbf{w}}(d) := \sum_t \mathbf{w}_t d^t$ is given by $\hat{\mathbf{x}}(d)(C + KJ) + \hat{\mathbf{u}}(d)J$, it follows that

$$\begin{aligned}
\hat{\mathbf{w}}(d) &= \hat{\mathbf{u}}(d)[(I_m - Bd(I_n - dA)^{-1}K)^{-1}Bd(I_n - dA)^{-1}(C + KJ) + J] \\
&= \hat{\mathbf{u}}(d)(I_m - Bd(I_n - dA)^{-1}K)^{-1} \times \\
&\qquad \times [Bd(I_n - dA)^{-1}C + Bd(I_n - dA)^{-1}KJ + (I_m - Bd(I_n - dA)^{-1}K)J] \\
&= \hat{\mathbf{u}}(d)(I_m - Bd(I_n - dA)^{-1}K)^{-1}[Bd(I_n - dA)^{-1}C + J],
\end{aligned}$$

and so, the transfer matrix of $\Sigma^{(K)}$ is represented by the left MFD

$$G^{(K)}(d) = [I_m - Bd(I_n - dA)^{-1}K]^{-1}[J + Bd(I_n - dA)^{-1}C].$$

Observe that since the left MFD $I_m^{-1}G_c(d)$ considered to construct Σ has denominator I_m, we obtain

$$X(d) = dB(I_n - Ad)^{-1} = \begin{bmatrix} d & d^2 & \dots & d^{\phi_1} & & & & & & & & \\ & & & & d & d^2 & \dots & d^{\phi_2} & & & & \\ & & & & & & & & \ddots & & & \\ & & & & & & & & & d & d^2 & \dots & d^{\phi_m} \end{bmatrix},$$

which implies that

$$G^{(K)}(d) = [I_m - X(d)K]^{-1}G_c(d).$$

As K varies in $\mathbb{F}^{n\times m}$, the matrix $I_m - X(d)K$ describes all polynomial matrices in $\mathbb{F}^{m\times m}$ having I_m as constant term and i-th row degree not greater than ϕ_i, $i = 1, 2, \dots, m$.

If the input of $\Sigma^{(K)}$ is filtered through an invertible static precompensator $M \in \mathbb{F}^{m\times m}$ (see Figure 4.2), the equations of the resulting state model become

$$\begin{aligned}
\mathbf{x}_{t+1} &= \mathbf{x}_t[A + KB] + \mathbf{u}_t MB \\
\mathbf{w}_t &= \mathbf{x}_t[C + KJ] + \mathbf{u}_t MJ
\end{aligned}$$

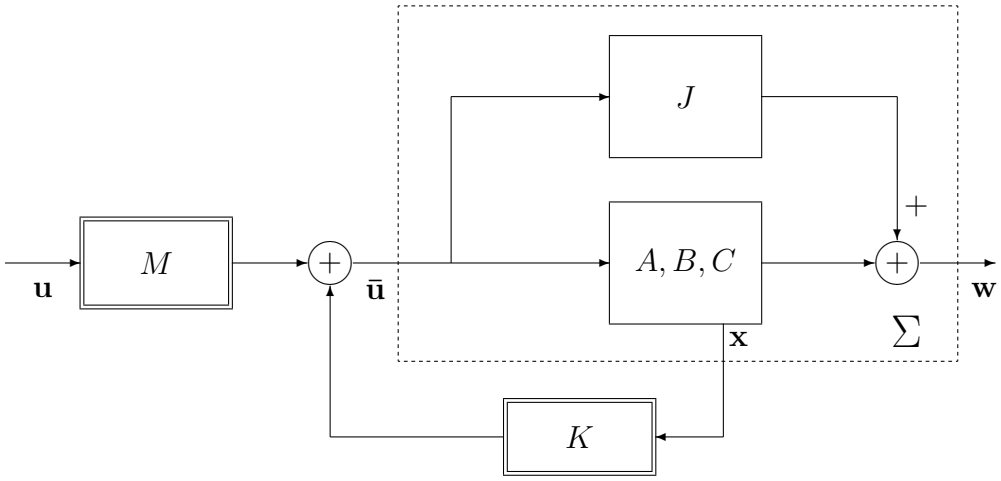

Figure 4.2 - Application of static precompensation to $\Sigma^{(K)}$

and the transfer matrix of the resulting system $\Sigma^{(K,M)} = (A + KB, MB, C + KJ, MJ)$ is equal to $MG^{(K)}(d)$, and so has the following left MFD

$$\begin{aligned} G^{(K,M)}(d) &= [M^{-1} - Bd(I_n - dA)^{-1}KM^{-1}]^{-1}[J + Bd(I_n - dA)^{-1}C] \\ &= [M^{-1} - X(d)KM^{-1}]^{-1}G_c(d). \end{aligned}$$

As each minimal encoder of $\mathcal{C}$ can be represented as $G(d) = D(d)^{-1}G_c(d)$, with $D(0)$ invertible and deg $\text{row}_i D \leq$ deg $\text{row}_i G_c$, $i = 1, \ldots, m$, it is possible to determine a unique precompensator $M = D(0)^{-1}$ and a unique state feedback matrix K such that $D(d) = M^{-1} - X(d)KM^{-1}$. We summarize the above discussion in the following proposition.

Proposition 4.4.1 *Let $G_c(d)$ be a canonical encoder of a $[p, m]$-convolutional code $\mathcal{C}$ of degree n. The set $\mathcal{M}$ of all minimal encoders of $\mathcal{C}$ is constituted by the transfer matrices of all systems $\Sigma^{(K,M)} = (A + KB, MB, C + KJ, MJ)$, obtained by application of static feedback and (nonsingular) precompensation to a minimal realization $\Sigma = (A, B, C, J)$ of $G_c(d)$. Therefore, the set of the pairs $(K, M) \in \mathbb{F}^{n\times m} \times \text{Gl}(m, \mathbb{F})$ biuniquely parametrizes $\mathcal{M}$.*

If the encoders are represented as MFD's in the indeterminate d^{-1}, minimal encoders of

$\mathcal{C}$ are MFD's with the following structure

$$G(d) = \tilde{D}(d^{-1})^{-1}\tilde{N}(d^{-1}) := \Big[\mathrm{diag}\{d^{-\phi_1}, \ldots, d^{-\phi_m}\}D(d)\Big]^{-1}\Big[\mathrm{diag}\{d^{-\phi_1}, \ldots, d^{-\phi_m}\}G_c(d)\Big],$$

where $\tilde{D}(d^{-1})$ runs over the set of all $m \times m$ row reduced polynomial matrices with row degrees $\phi_1, \ldots, \phi_m$, and $\tilde{N}(d^{-1})$ is a fixed left prime row reduced polynomial matrix in d^{-1} (see Proof of Proposition 4.2.1). Rosenbrock's theorem [43], quoted in section 2.1, shows that the Smith forms of the denominator matrices $\tilde{D}(d^{-1})$ of minimal encoders comprise all strings of m monic polynomials $\gamma_1(d^{-1}), \ldots, \gamma_m(d^{-1})$ satisfying

$$\begin{aligned}
&\gamma_{i+1}|\gamma_i \\
&\deg(\gamma_1 \cdots \gamma_t) \geq \phi_1 + \ldots + \phi_t \\
&\deg(\gamma_1 \cdots \gamma_m) = \phi_1 + \ldots + \phi_m = \deg \mathcal{C}.
\end{aligned}$$

Note that the Smith form of $\tilde{D}(d^{-1})$ provides also the invariant polynomials - and in particular the minimal polynomial - of the matrix A in any minimal state space realization of $\tilde{D}(d^{-1})^{-1}\tilde{N}(d^{-1})$.

4.5 Conclusion

In this chapter we focused on the minimal encoders of a convolutional code. Two procedures to determine all minimal encoders, given a canonical one, were obtained. The first one allows to obtain the minimal encoders of the code by pre-multiplying the canonical encoder by the inverse of a polynomial matrix that fulfills certain characteristics, i.e., it provides the minimal encoders of the code in terms of their MFD's. The second one is a realization procedure, which obtains all minimal encoders by applying static feedback and precompensation to a realization of the canonical encoder.

A well-known characterization of the minimal encoders of a convolutional code is formulated in terms of their abstract state spaces and of the relation between the span of the information sequences and the span of the corresponding codewords, when we confine to rational codewords. We considered all codewords of the code and showed how the latter relation is connected with the properties of an irreducible left MFD of the encoder. This permitted to extend the above characterization of the minimal encoders to the set of all

codewords of the code. Finally, we analyzed the abstract state space of a polynomial reduced encoder and of a minimal encoder of a convolutional code, considering in the last case, a special kind of left MFD of the encoder.

Chapter 5

Syndrome formers

Besides encoders, we can consider another kind of matrices associated with a linear code (block or convolutional), called the *parity-check* [1] matrices.

If $\mathcal{C}$ is a linear code over $\mathbb{F}^p$, a *parity-check* for $\mathcal{C}$ is an equation of the form

$$\hat{a}_1(d)\,\hat{w}_1(d) + \hat{a}_2(d)\,\hat{w}_2(d) + \cdots + \hat{a}_p(d)\,\hat{w}_p(d) = 0, \tag{5.1}$$

$\hat{a}_i(d) \in \mathbb{F}((d)),\ i = 1, \ldots, p$, which is satisfied for all $\hat{\mathbf{w}}(d) = (\hat{w}_1(d), \hat{w}_2(d), \ldots, \hat{w}_p(d)) \in \mathcal{C}$.

As we will see, the set of all p-tuples $(\hat{a}_1(d), \hat{a}_2(d), \ldots, \hat{a}_p(d))$ that satisfy (5.1) constitutes the dual code of $\mathcal{C}$. Full rank matrices whose columns generate the dual code are called parity-check matrices.

In convolutional codes, parity-check matrices are also called *syndrome formers*. In this chapter we will focus on the analysis of the syndrome formers of a convolutional code.

[1] The name comes from the binary case, where, in a sequence of bits, a parity-check is an extra bit that denotes if the sequence has an even number or an odd number of 1's.

5.1 Dual code

Let $\mathcal{C}$ be a $[p, m]$-convolutional code. As $\mathcal{C}$ is an m-dimensional $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$, we can consider the orthogonal of $\mathcal{C}$,

$$\mathcal{C}_\perp := \{\hat{\mathbf{v}}_\perp(d) \in \mathbb{F}((d))^p : \hat{\mathbf{v}}_\perp(d)\hat{\mathbf{w}}(d)^T = 0,\ \forall \hat{\mathbf{w}}(d) \in \mathcal{C}\},$$

which is a $(p-m)$-dimensional $\mathbb{F}((d))$-subspace of $\mathbb{F}((d))^p$ [33].

Let us see that $\mathcal{C}_\perp$ admits a polynomial basis [14]. Consider $G_b(d)$, a basic encoder of $\mathcal{C}$. From Proposition 2.1.3, there exists $C(d) \in \mathbb{F}[d]^{(p-m)\times p}$ such that $U(d) = \begin{bmatrix} G_b(d) \\ C(d) \end{bmatrix}$ is unimodular. Consequently, $C(d)$ is also left prime. If $G_b(d)^{-1} \in \mathbb{F}[d]^{p\times m}$ and $C(d)^{-1} \in \mathbb{F}[d]^{p\times(p-m)}$ represent the polynomial right inverses of $G_b(d)$ and $C(d)$, respectively, the inverse of $U(d)$ is the polynomial matrix

$$U(d)^{-1} = [\, G_b(d)^{-1} \quad C(d)^{-1} \,].$$

Let $\hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G_b(d)$ be a codeword of $\mathcal{C}$. Then

$$\begin{aligned} \hat{\mathbf{w}}(d)\,[\, G_b(d)^{-1} \quad C(d)^{-1} \,] &= \hat{\mathbf{u}}(d)G_b(d)\,[\, G_b(d)^{-1} \quad C(d)^{-1} \,] \\ &= [\, \hat{\mathbf{u}}(d) \quad 0 \,], \end{aligned}$$

i.e., $\hat{\mathbf{w}}(d)C(d)^{-1} = 0$.

So, the columns of $C(d)^{-1}$ are $p-m$ linearly independent vectors of $\mathcal{C}_\perp$, and therefore constitute a polynomial basis of $\mathcal{C}_\perp$. Consequently, by Proposition 3.1.1, $\mathcal{C}_\perp$ is strongly controllable and strongly observable, and, therefore, by Definition 3.2.1, $\mathcal{C}_\perp$ is a $[p, p-m]$-convolutional code.

As the orthogonal of any subspace of a vector space is unique [33], $\mathcal{C}_\perp$ is uniquely determined by $\mathcal{C}$, and vice-versa.

Definition 5.1.1 *Let $\mathcal{C}$ be a $[p, m]$-convolutional code. The dual code of $\mathcal{C}$ is the $[p, p-m]$-convolutional code*

$$\mathcal{C}_\perp := \{\hat{\mathbf{v}}_\perp(d) \in \mathbb{F}((d))^p : \hat{\mathbf{v}}_\perp(d)\hat{\mathbf{w}}(d)^T = 0,\ \forall \hat{\mathbf{w}}(d) \in \mathcal{C}\}.$$

5.2 Syndrome formers

In Chapter 3, an encoder $G(d)$ of a convolutional code $\mathcal{C}$, was defined as a matrix whose image is $\mathcal{C}$. Thus, the encoders provide representations of a code as an image (image representations).

As we have seen in Section 5.1, $\mathcal{C}_\perp$ uniquely determines $\mathcal{C}$, i.e. if $G_\perp(d) \in \mathbb{F}(d)^{(p-m)\times p}$ is any encoder of $\mathcal{C}_\perp$, then

$$\hat{\mathbf{w}}(d)G_\perp(d)^T = 0 \Leftrightarrow \hat{\mathbf{w}}(d) \in \mathcal{C}. \tag{5.2}$$

Therefore, a convolutional code can also be viewed as kernel, i.e., admits kernel representations.

Definition 5.2.1 *Any $p \times (p-m)$ full column rank rational matrix $S(d)$ such that*

$$\operatorname{Ker} S(d) = \{\hat{\mathbf{w}}(d) : \hat{\mathbf{w}}(d)S(d) = 0\} = \mathcal{C},$$

is called a syndrome former of $\mathcal{C}$.

From (5.2) it follows that the syndrome formers of $\mathcal{C}$ are the transpose of the encoders of its dual code $\mathcal{C}_\perp$ [15].

Definition 5.2.2 *Let $S(d) \in \mathbb{F}(d)^{p\times(p-m)}$ be a syndrome former of $\mathcal{C}$. The syndrome of a series $\hat{\mathbf{r}}(d) \in \mathbb{F}((d))^p$ induced by $S(d)$ is given by $\hat{\mathbf{s}}(d) := \hat{\mathbf{r}}(d)S(d)$.*

Consequently, if $S(d) \in \mathbb{F}(d)^{p\times(p-m)}$ is a syndrome former of $\mathcal{C}$, a series $\hat{\mathbf{r}}(d) \in \mathbb{F}((d))^p$ is in $\mathcal{C}$ if and only if its syndrome, $\hat{\mathbf{s}}(d) := \hat{\mathbf{r}}(d)S(d)$, is zero. Furthermore, the syndrome depends only on the errors introduced during the channel transmission [2]. If $\mathbf{w}$ is the transmitted codeword, over the transmission channel, and $\mathbf{r}$ the received sequence (see Figure 3.1), the error introduced is $\mathbf{e} = \mathbf{r} - \mathbf{w}$. Then, if $\mathbf{s}_r$ and $\mathbf{s}_e$ represent the syndromes of $\mathbf{r}$ and $\mathbf{e}$,

[2]The term "syndrome" was introduced by Hagelbarger [6, 37] as an analogy to "syndrome" used in medical terminology, where it means a number of symptoms of a disease. In our context, the disease consists in the introduced errors, and the symptom is the syndrome.

respectively, it follows that

$$\begin{aligned}\hat{\mathbf{s}}_r(d) &= \hat{\mathbf{r}}(d)S(d)\\ &= \hat{\mathbf{w}}(d)S(d) + \hat{\mathbf{e}}(d)S(d)\\ &= \hat{\mathbf{s}}_e(d).\end{aligned}$$

So, if $\mathbf{w}$ and $\mathbf{r}$ are the transmitted and received signals, respectively, it follows that if the syndrome of $\mathbf{r}$ is different from zero we can conclude that a transmission error has occurred. But the converse is not true. In fact, it can happen that $\mathbf{e} = \mathbf{r} - \mathbf{w}$ is a nonzero element of $\mathcal{C}$, and, in this case, the syndrome of $\mathbf{r}$ will be zero, but the transmission error not. If we consider the *syndrome map* induced by the syndrome former $S(d)$,

$$\mathbf{S} : \mathbb{F}((d))^p \to \mathbb{F}((d))^{p-m}, \;\; \hat{\mathbf{r}}(d) \mapsto \hat{\mathbf{s}}(d) = \hat{\mathbf{r}}(d)S(d),$$

the cosets of $\mathbb{F}((d))^p/\mathcal{C}$ are constituted by all sequences that produce the same syndrome. So, the syndrome of the received signal permits to verify if the signal is in $\mathcal{C}$, and, if not, to which coset of $\mathbb{F}((d))^p/\mathcal{C}$ it belongs.

As the syndrome formers of $\mathcal{C}$ are exactly the transpose of the encoders of $\mathcal{C}_\perp$, we may expect that a discussion on syndrome formers structure could mirror that on the encoders of $\mathcal{C}$.

The next proposition is an immediate consequence of Proposition 3.2.1.

Proposition 5.2.1 *If $S(d) \in \mathbb{F}(d)^{p\times(p-m)}$ is a syndrome former of $\mathcal{C}$, then*

$$S(d)T(d)$$

provides all syndrome formers of $\mathcal{C}$ as $T(d)$ varies on the group of nonsingular $(p-m)\times(p-m)$ rational matrices.

Analogously to encoders, a convolutional code admits (right) prime, (column) reduced and causal syndrome formers.

- The transpose of any basic encoder $G_{b_\perp}(d)$ of $\mathcal{C}_\perp$,

  $$S_b(d) := G_{b_\perp}(d)^T$$

  is a right prime polynomial syndrome former of $\mathcal{C}$, that will be called *basic*.

- The transpose of any canonical encoder $G_{c_\perp}(d)$ of $\mathcal{C}_\perp$,

$$S_c(d) := G_{c_\perp}(d)^T$$

is a polynomial syndrome former of $\mathcal{C}$, right prime and column reduced, with column degrees $\psi_1, \ldots, \psi_{p-m}$, that will be called *canonical*. Furthermore, any canonical syndrome former of $\mathcal{C}$ has the same column degrees, up to a permutation.

- The transpose of any causal encoder $G_\perp(d)$ of $\mathcal{C}_\perp$,

$$S(d) := G_\perp(d)^T$$

is also causal, and if $P(d)Q(d)^{-1}$ is an irreducible right MFD of $S(d)$ then $S(d)$ is causal if and only if $Q(0)$ is nonsingular [5, 38].

A preliminary, fundamental connection between basic syndrome formers and basic encoders of $\mathcal{C}$ is provided by the following lemma, which is an immediate consequence of Corollary 2.2.2.

Lemma 5.2.1 *[15] Suppose that $G_b(d) \in \mathbb{F}[d]^{m\times p}$ is a basic encoder of $\mathcal{C}$. Select $C(d)$ in $\mathbb{F}^{(p-m)\times p}[d]$ so that $\begin{bmatrix} G_b(d) \\ C(d) \end{bmatrix}$ is unimodular, and $D(d) \in \mathbb{F}[d]^{p\times m}$ and $S(d) \in \mathbb{F}[d]^{p\times(p-m)}$ so that*

$$\begin{bmatrix} G_b(d) \\ C(d) \end{bmatrix} [\, D(d) \mid S(d) \,] = I_p.$$

Then $S(d)$ is a basic *syndrome former of $\mathcal{C}$, and its maximal order minors are equal, up to units, to the complementary maximal order minors of $G_b(d)$.*

As the degree of a code is equal to the internal degree of any basic encoder of the code, the next corollary follows immediately from the above lemma.

Corollary 5.2.1 *[14] The degree of $\mathcal{C}_\perp$ is equal to the degree of $\mathcal{C}$, and row degrees $\psi_1, \ldots, \psi_{p-m}$ of any canonical encoder of $\mathcal{C}_\perp$ satisfy*

$$\sum_{i=1}^{p-m} \psi_i = \sum_{i=1}^{m} \phi_i = \deg \mathcal{C}.$$

Remark: As the rows of a canonical encoder of $\mathcal{C}$ constitute a polynomial basis of $\mathcal{C}$ of least degree, it follows that the N-controllability of a convolutional code $\mathcal{C}$ is connected with the greatest Forney index of the code. In fact, from the proof of Proposition 3.1.1 and from Corollary 3.1.1 we have that $\mathcal{C}$ is N-controllable if and only if it admits a polynomial basis of degree N.

On the other hand, the L-observability of $\mathcal{C}$ is related with the greatest column degree of a canonical syndrome former of $\mathcal{C}$, in the sense that if L is the greatest degree of the columns of a canonical syndrome former of $\mathcal{C}$, then $\mathcal{C}$ is L-observable (see Example 3.1.1).

When considering the way of operating of a syndrome former $S(d)$, we may ask whether its finite support syndromes are all induced by sequences $\mathbf{v}$ that differ in a finite number of positions from some codeword $\mathbf{w}$ of $\mathcal{C}$. In other terms, is there any condition on $S(d)$ guaranteeing that finite support syndromes imply finite support errors?

This problem is quite similar to (non)catastrophic error generation, and the structural condition on the syndrome former is dual with respect to the condition on (non) catastrophic encoders.

Proposition 5.2.2 *Let $P(d)Q(d)^{-1}$ be an irreducible right MFD of a causal syndrome former $S(d) \in \mathbb{F}(d)^{p\times(p-m)}$ of $\mathcal{C}$. The following are equivalent:*

(i) for all $\hat{\mathbf{v}}(d)$ in $\mathbb{F}((d))^p$, if the syndrome $\hat{\mathbf{v}}(d)S(d)$ has finite support, then $\hat{\mathbf{v}}(d) - \hat{\mathbf{w}}(d)$ has finite support, for some codeword $\hat{\mathbf{w}}(d) \in \mathcal{C}$;

(ii) $P(d)$ factorizes into $P(d) = \bar{P}(d)\Delta(d)$, where $\bar{P}(d)$ is right prime and $\det \Delta(d) = \alpha d^k$, $0 \neq \alpha \in \mathbb{F}$, $k \in \mathbb{N}$.

Proof: (ii) $\Rightarrow$ (i) Note that $\bar{P}(d) \in \mathbb{F}[d]^{p\times(p-m)}$ has a polynomial left inverse $L(d) \in \mathbb{F}[d]^{(p-m)\times p}$ and $\Delta(d) \in \mathbb{F}[d]^{(p-m)\times(p-m)}$ has a Laurent polynomial inverse (see Propositions 2.1.3 and 2.1.2). So, if $\hat{\mathbf{s}}(d) := \hat{\mathbf{v}}(d)S(d)$ has finite support, $\hat{\mathbf{s}}(d)Q(d)\Delta(d)^{-1}L(d)$ has finite support too, and

$$[\hat{\mathbf{v}}(d) - \hat{\mathbf{s}}(d)Q(d)\Delta(d)^{-1}L(d)]S(d) = 0$$

This implies that $\hat{\mathbf{w}}(d) := \hat{\mathbf{v}}(d) - \hat{\mathbf{s}}(d)Q(d)\Delta(d)^{-1}L(d)$ is a codeword, and $\hat{\mathbf{v}}(d) - \hat{\mathbf{w}}(d)$ has finite support.

(i) $\Rightarrow$ (ii) Suppose that $P(d) \in \mathbb{F}[d]^{p\times(p-m)}$ factorizes into $P(d) = \bar{P}(d)\Delta(d)$, with $\bar{P}(d) \in \mathbb{F}[d]^{p\times(p-m)}$ right prime and $\Delta(d) \in \mathbb{F}[d]^{(p-m)\times(p-m)}$ nonsingular, with $\det\Delta \neq \alpha d^k$. The right MFD $\Delta(d)Q(d)^{-1}$ is irreducible, as any right common factor of $\Delta(d)$ and $Q(d)$ is also a right common factor of $P(d)$ and $Q(d)$ and $P(d)Q(d)^{-1}$ is irreducible. So, if $X(d)^{-1}Y(d)$, $X(d), Y(d) \in \mathbb{F}[d]^{(p-m)\times(p-m)}$, is an irreducible left MFD of $\Delta(d)Q(d)^{-1}$, then $\det Y = \det\Delta \neq \alpha d^k$ (see Proposition 2.2.1), i.e. $Y(d)$ is not Laurent unimodular (see Proposition 2.1.2). Consequently, the expansion of $Y(d)^{-1}$ includes some series with infinite support, and therefore, there exists $\mathbf{c} \in \mathbb{F}^m$ such that $\hat{\mathbf{q}}(d) := \mathbf{c}Y(d)^{-1}$ has infinite support and $\hat{\mathbf{q}}(d)Y(d)$ is polynomial. On the other hand,

$$\hat{\mathbf{b}}(d) := \hat{\mathbf{q}}(d)X(d)$$

has infinite support, otherwise $\hat{\mathbf{q}}(d)\,[\,X(d) \quad Y(d)\,]$ would have finite support, which is inconsistent with the left primeness of $[\,X(d) \quad Y(d)\,]$.

As $\bar{P}(d)$ is right prime, it admits a polynomial left inverse $L(d) \in \mathbb{F}[d]^{(p-m)\times p}$, which is left prime, and therefore, the signal

$$\hat{\mathbf{v}}(d) := \hat{\mathbf{b}}(d)L(d) \in \mathbb{F}((d))^p$$

has infinite support.

The corresponding syndrome is given by

$$\hat{\mathbf{s}}(d) = \hat{\mathbf{v}}(d)S(d) = \hat{\mathbf{b}}(d)L(d)\bar{P}(d)X(d)^{-1}Y(d) = \hat{\mathbf{b}}X(d)^{-1}Y(d) = \hat{\mathbf{q}}(d)Y(d)$$

and therefore has finite support.

Finally, suppose that $\hat{\mathbf{w}}(d)$ is any codeword of $\mathcal{C}$, and consider a basic encoder $G(d) \in \mathbb{F}[d]^{m\times p}$ of $\mathcal{C}$, with polynomial right inverse $C(d) \in \mathbb{F}[d]^{p\times m}$. Then, as $G(d)S(d) = G(d)\bar{P}(d)Q(d)^{-1} = 0$ implies that $G(d)\bar{P}(d) = 0$, we have

$$\begin{bmatrix} L(d) \\ G(d) \end{bmatrix} [\,\bar{P}(d) \quad C(d)\,] = \begin{bmatrix} I_{p-m} & * \\ 0 & I_m \end{bmatrix},$$

which implies that $\begin{bmatrix} L(d) \\ G(d) \end{bmatrix}$ is unimodular, and the difference

$$\hat{\mathbf{v}}(d) - \hat{\mathbf{w}}(d) = \hat{\mathbf{b}}(d)L(d) - \hat{\mathbf{u}}(d)G(d) = [\,\hat{\mathbf{b}}(d) \quad -\hat{\mathbf{u}}(d)\,] \begin{bmatrix} L(d) \\ G(d) \end{bmatrix}$$

cannot be finite support, as $[\,\hat{\mathbf{b}}(d) \quad -\hat{\mathbf{u}}(d)\,]$ is not. □

5.3 Minimal syndrome formers

Let us restrict to causal syndrome formers of $\mathcal{C}$, i.e., to the syndrome formers of $\mathcal{C}$ that can be realized by a linear dynamical system.

It is easy to see that if $\Sigma = (A, B, C, J)$ is a state space realization of $G(d) \in \mathbb{F}(d)^{q\times p}$, then $\Sigma^{(T)} = (A^T, C^T, B^T, J^T)$ is a state space realization of $G(d)^T$ with the same dimension of Σ. So, the realization algorithm described in section 4.1 can be used to obtain a realization of a causal syndrome former of $\mathcal{C}$. First we construct a state space realization Σ of the encoder $S(d)^T$ of $\mathcal{C}_\perp$, and then determine the realization $\Sigma^{(T)}$ of $S(d)$.

Definition 5.3.1 *Let $S(d)$ be a syndrome former of $\mathcal{C}$. The McMillan degree of $S(d)$ is the minimum of the dimensions of the state realizations of $S(d)$. A realization of $S(d)$ is said to be minimal if its dimension is equal to the McMillan degree of $S(d)$.*

In the same way as it was done for the encoders of $\mathcal{C}$, we can define minimal syndrome former of the code.

Definition 5.3.2 *A causal syndrome former of $\mathcal{C}$, $S(d) \in \mathbb{F}(d)^{p\times(p-m)}$, is said to be minimal if it has minimal McMillan degree among all causal syndrome formers of $\mathcal{C}$.*

The minimal syndrome formers of $\mathcal{C}$ are exactly the transposes of the minimal encoders of $\mathcal{C}_\perp$, and therefore, from Corollary 5.2.1 it follows that all minimal syndrome formers of $\mathcal{C}$ have McMillan degree $\sum_{i=1}^{p-m} \psi_i$, where $\psi_1, \psi_2, \ldots, \psi_m$ are the column degrees of any canonical

syndrome former of $\mathcal{C}$ [15].

A similar parametrization as the one done for minimal encoders in Proposition 4.2.2, can be done for minimal syndrome formers.

Proposition 5.3.1 *Let $S_c(d) \in \mathbb{F}[d]^{p\times(p-m)}$ be a canonical syndrome former of $\mathcal{C}$. Then the minimal syndrome formers of $\mathcal{C}$ are biuniquely parametrized by the right MFD's*

$$S_c(d)Q(d)^{-1},$$

as $Q(d)$ sweeps over all $(p-m)\times(p-m)$ polynomial matrices with $\deg \mathrm{col}_i(Q) \leq \deg \mathrm{col}_i(S_c)$, $i = 1, \ldots, p-m$ and $Q(0)$ nonsingular.

In section 4.4 we have shown that all minimal encoders of $\mathcal{C}$ can be obtained by application of static feedback and static precompensation to a minimal state space realization of a canonical encoder. The same can be done for minimal syndrome formers, by application of output injection and static output compensation to a minimal state space realization of a canonical syndrome former $S_c(d)$ of $\mathcal{C}$.

Suppose that $\Sigma_\perp = (A_\perp, B_\perp, C_\perp, J_\perp)$ is a minimal n-dimensional realization of the canonical encoder $S_c(d)^T$ of $\mathcal{C}_\perp$ obtained via the procedure of section 4.1. Then the dual system $\Sigma = (A_\perp^T, C_\perp^T, B_\perp^T, J_\perp^T)$

$$\begin{aligned} \mathbf{x}_{t+1} &= \mathbf{x}_t\, A_\perp^T + \mathbf{w}_t\, C_\perp^T \\ \mathbf{s}_t &= \mathbf{x}_t\, B_\perp^T + \mathbf{w}_t\, J_\perp^T \end{aligned}$$

provides a minimal realization of $S_c(d) = C_\perp^T d(I_n - A_\perp^T)^{-1}B_\perp^T + J_\perp^T$.

An output injection $\mathbf{s}_t L$, $L \in \mathbb{F}^{(p-m)\times n}$, (see Figure 5.1), modifies the above equations as follows

$$\begin{aligned} \mathbf{x}_{t+1} &= \mathbf{x}_t\, A_\perp^T + \mathbf{w}_t\, C_\perp^T + \mathbf{s}_t L \\ &= \mathbf{x}_t(A_\perp^T + B_\perp^T L) + \mathbf{w}_t(C_\perp^T + J_\perp^T L) \\ \mathbf{s}_t &= \mathbf{x}_t\, B_\perp^T + \mathbf{w}_t\, J_\perp^T \end{aligned} \tag{5.3}$$

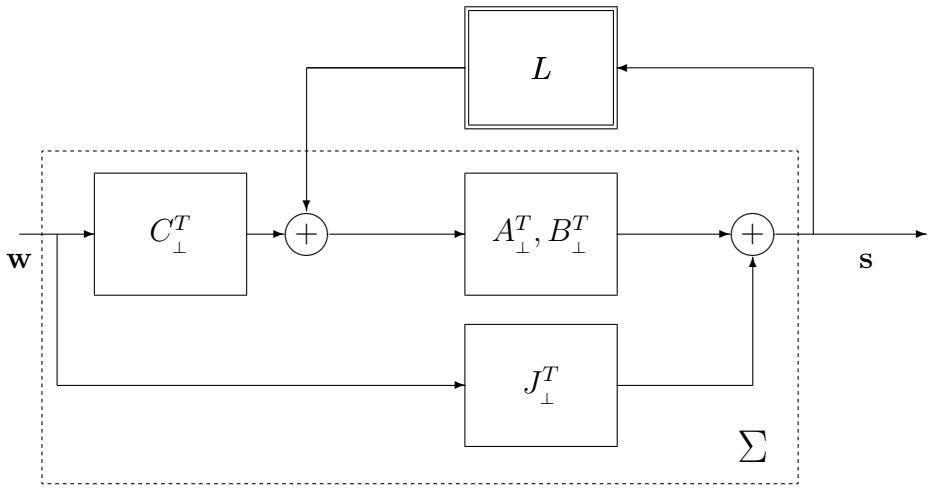

Figure 5.1 - Application of output injection to Σ

Therefore the series $\hat{\mathbf{x}}(d) := \sum_t \mathbf{x}_t d^t$ and $\hat{\mathbf{w}}(d) := \sum_t \mathbf{w}_t d^t$ are connected by

$$\begin{aligned}
& d^{-1}\hat{\mathbf{x}}(d) = \hat{\mathbf{x}}(d)(A_\perp^T + B_\perp^T L) + \hat{\mathbf{w}}(d)(C_\perp^T + J_\perp^T L) \\
\Leftrightarrow\ & \hat{\mathbf{x}}(d) = [\hat{\mathbf{x}}(d)B_\perp^T Ld + \hat{\mathbf{w}}(d)(C_\perp^T d + J_\perp^T Ld)](I_n - A_\perp^T d)^{-1} \\
\Leftrightarrow\ & \hat{\mathbf{x}}(d)(I_n - B_\perp^T Ld(I_n - A_\perp^T d)^{-1}) = \hat{\mathbf{w}}(d)(C_\perp^T d + J_\perp^T Ld)(I_n - A_\perp^T d)^{-1} \\
\Leftrightarrow\ & \hat{\mathbf{x}}(d) = \hat{\mathbf{w}}(d)(C_\perp^T d + J_\perp^T Ld)(I_n - A_\perp^T d)^{-1}(I_n - B_\perp^T Ld(I_n - A_\perp^T d)^{-1})^{-1}. \qquad (5.4)
\end{aligned}$$

From (5.3) and (5.4), it follows that the output $\hat{\mathbf{s}}(d)$ is given by

$$\hat{\mathbf{s}}(d) = \hat{\mathbf{w}}(d)[(C_\perp^T d + J_\perp^T Ld)(I_n - A_\perp^T d)^{-1}(I_n - B_\perp^T Ld(I_n - A_\perp^T d)^{-1})^{-1}B_\perp^T + J_\perp^T].$$

Applying (4.30), we have that $\hat{\mathbf{s}}(d)$ is obtained by $\hat{\mathbf{w}}(d)$ as follows

$$\begin{aligned}
\hat{\mathbf{s}}(d) &= \hat{\mathbf{w}}(d)[(C_\perp^T d + J_\perp^T Ld)(I_n - A_\perp^T d)^{-1}B_\perp^T(I_{p-m} - Ld(I_n - A_\perp^T d)^{-1}B_\perp^T)^{-1} + J_\perp^T] \\
&= \hat{\mathbf{w}}(d)[C_\perp^T d(I_n - A_\perp^T d)^{-1}B_\perp^T + J_\perp^T(Ld(I_n - A_\perp^T d)^{-1}B_\perp^T + I_{p-m} - Ld(I_n - A_\perp^T d)^{-1}B_\perp^T)] \times \\
&\qquad \times(I_{p-m} - Ld(I_n - A_\perp^T d)^{-1}B_\perp^T)^{-1} \\
&= \hat{\mathbf{w}}(d)[C_\perp^T d(I_n - dA_\perp^T)^{-1}B_\perp^T + J_\perp^T][I_{p-m} - Ld(I_n - dA_\perp^T)^{-1}B_\perp^T]^{-1}
\end{aligned}$$

and so the transfer matrix of the resulting system $\Sigma^{(L)} = (A_\perp^T + B_\perp^T L,\, C_\perp^T + J_\perp^T L,\, B_\perp^T, J_\perp^T)$ is given by

$$\begin{aligned} S^{(L)}(d) &= [C_\perp^T d(I_n - dA_\perp^T)^{-1}B_\perp^T + J_\perp^T][I_{p-m} - Ld(I_n - dA_\perp^T)^{-1}B_\perp^T]^{-1} \\ &= S_c(d)[I_{p-m} - LX(d)]^{-1}, \end{aligned}$$

where

$$X(d)^T = d(I_n - dA_\perp^T)^{-1}B_\perp^T = \begin{bmatrix} d & d^2 & \dots & d^{\psi_1} & & & & & & & & \\ & & & & d & d^2 & \dots & d^{\psi_2} & & & & \\ & & & & & & & & \ddots & & & \\ & & & & & & & & & d & d^2 & \dots & d^{\psi_m} \end{bmatrix},$$

and, consequently, the matrix $I_{p-m} - LX(d)$ describes all $(p-m)\times(p-m)$ polynomial matrices with constant term I_{p-m} and ith -column degree not greater than $\psi_i,\ i = 1, \dots, p-m$, as L varies in $\mathbb{F}^{(p-m)\times n}$.

Finally, if the output of $\Sigma^{(L)}$ is filtered through an invertible nondynamical system $N \in \mathbb{F}^{(p-m)\times(p-m)}$ (see Figure 5.2), we end up with a state space model $\Sigma^{(L,N)} = (A_\perp^T + B_\perp^T L,\, C_\perp^T + J_\perp^T L,\, B_\perp^T N, J_\perp^T N)$ of a new syndrome former, with equations

$$\begin{aligned} \mathbf{x}_{t+1} &= \mathbf{x}_t(A_\perp^T + B_\perp^T L) + \mathbf{w}_t(C_\perp^T + J_\perp^T L) \\ \mathbf{s}_t &= \mathbf{x}_t\, B_\perp^T N + \mathbf{w}_t\, J_\perp^T N. \end{aligned}$$

and transfer matrix $S^{(L,N)}(d) = S^{(L)}(d)N$, i.e.,

$$\begin{aligned} S^{(L,N)}(d) &= [C_\perp^T d(I_n - dA_\perp^T)^{-1}B_\perp^T + J_\perp^T][N^{-1} - N^{-1}Ld(I_n - dA_\perp^T)^{-1}B_\perp^T]^{-1} \\ &= S_c(d)[N^{-1} - N^{-1}LX(d)]^{-1}. \end{aligned} \tag{5.5}$$

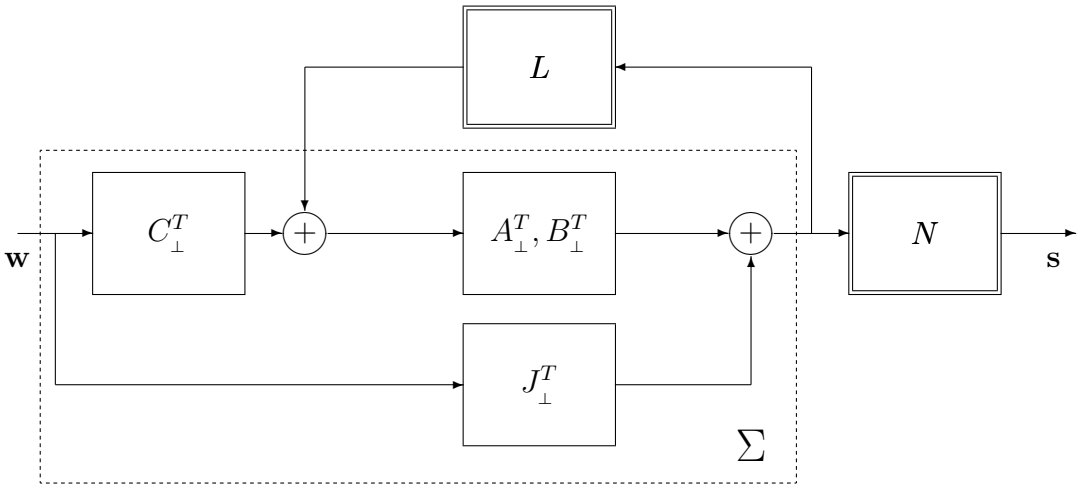

Figure 5.2 - Application of static postcompensation to $\Sigma^{(L)}$

Varying N in $Gl(p-m, \mathbb{F})$ and L in $\mathbb{F}^{(p-m)\times n}$, the denominator matrices $N^{-1} - N^{-1}LX(d)$ in (5.5) biuniquely represent all $(p-m) \times (p-m)$ matrices $Q(d)$ with invertible constant term $Q(0)$ and column degrees not greater than the corresponding ones in $S_c(d)$. Hence (5.5) provides all minimal syndrome formers of $\mathcal{C}$.

5.4 Decoupled syndrome formers

We will now study the existence of decoupled syndrome formers of a $[p, m]$-convolutional code $\mathcal{C}$.

Definition 5.4.1 *Let $p_1, \ldots, p_k$ be positive integers such that $\sum_{i=1}^k p_i = p$. $S(d) \in \mathbb{F}(d)^{p\times(p-m)}$ is a $(p_1, \ldots, p_k)$-decoupled syndrome former of $\mathcal{C}$ if there exist positive integers $m_1, \ldots, m_k$ satisfying $\sum_{i=1}^k m_i = m$, such that, up to a row permutation*

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

Decoupled syndrome formers permit to more efficiently verify if a series $\hat{\mathbf{r}}(d) \in \mathbb{F}((d))^p$ belongs to $\mathcal{C}$. In fact, if $S(d)$ is a $(p_1, \ldots, p_k)$-decoupled syndrome former as defined above,

then $\hat{\mathbf{r}}(d) = [\hat{\mathbf{r}}_1(d) \cdots \hat{\mathbf{r}}_k(d)]$, $\hat{\mathbf{r}}_i(d) \in \mathbb{F}((d))^{p_i},\ i = 1, \ldots, k$, is in $\mathcal{C}$ if and only if $\hat{\mathbf{r}}_i(d)S_i(d) = 0$, $i = 1, \ldots, k$.

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

Proposition 5.4.1 *A $[p, m]$-convolutional code $\mathcal{C}$ admits a $(p_1, \ldots, p_k)$-decoupled encoder if and only if admits a $(p_1, \ldots, p_k)$-decoupled syndrome former.*

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

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

with P a permutation matrix, be a canonical $(p_1, \ldots, p_k)$-decoupled encoder of $\mathcal{C}$ (see Proposition 4.2.3).

Consider a syndrome former $S_i(d) \in \mathbb{F}(d)^{p_i \times (p_i - m_i)}$ of the $[p_i, m_i]$-convolutional code $\mathcal{C}_i$ generated by $G_i(d)$, $i = 1, \ldots, k$. [3] Then

$$S(d) = P\text{diag}\{S_1(d), \ldots, S_k(d)\}$$

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

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

Conversely, suppose that

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

is a syndrome former of $\mathcal{C}$ and $G(d)$ is an encoder of $\mathcal{C}$. To see that $\mathcal{C}$ admits a $(p_1, \ldots, p_k)$-decoupled encoder it is enough to prove (see the algorithm on section 3.3) that if we consider the partition

$$G(d)P = [G_1(d)| \ldots |G_k(d)],\ G_i(d) \in \mathbb{F}(d)^{m \times p_i},\ i = 1, \ldots, k,$$

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

then

$$\operatorname{span} G_1(d) \oplus \ldots \oplus \operatorname{span} G_k(d) = \mathbb{F}((d))^m.$$

Observe that $0 = G(d)S(d) = [G_1(d)|\ldots|G_k(d)]\mathrm{diag}\{S_1(d), ..., S_k(d)\}$, which implies that $G_i(d)S_i(d) = 0, \;\; i = 1, \ldots, k$.

Let $0 \neq \hat{\mathbf{w}}_i(d) \in \operatorname{span} G_i(d)$, i.e, $\hat{\mathbf{w}}_i(d) = G_i(d)\hat{\mathbf{a}}_i(d)$ for some $\hat{\mathbf{a}}_i(d) \in \mathbb{F}((d))^{p_i} \backslash \{0\}$, and $\alpha_i(d) \in \mathbb{F}((d)),\ i = 1, \ldots, k$. Since

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

we have that

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

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

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

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

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

which is equivalent to $\alpha_i(d)\hat{\mathbf{a}}_i(d) = S_i(d)\hat{\mathbf{b}}_i(d),\ \ i = 1, \dots k.$

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

Example 5.4.1 Consider the encoder $G(d)$ considered on Example 3.3.1 and the column partition of $G(d)$ compatible with the finest decomposition (3.20) of $\mathbb{F}((d))^4$,

$$G(d)P = [G_1(d) \,|\, G_2(d) \,|\, G_3(d)],$$

where $G_1(d) \in \mathbb{F}[d]^{4\times 3}$, $G_2(d) \in \mathbb{F}[d]^{4\times 2}$ and $G_3(d) \in \mathbb{F}[d]^{4\times 1}$, with rank $G_1(d) = 2$, rank $G_2(d) = 1$ and rank $G_3(d) = 1$. So, there exists a $(3, 2, 1)$-decoupled syndrome former of $\mathcal{C}$.

$$S(d) = P \begin{bmatrix} S_1(d) & 0 \\ 0 & S_2(d) \\ 0_{1\times 1} & 0_{1\times 1} \end{bmatrix},$$

with

$$S_1(d) = \begin{bmatrix} d^2 \\ 1 \\ -1 \end{bmatrix},\ S_2(d) = \begin{bmatrix} -1-d \\ 1 \end{bmatrix},$$

is such a syndrome former. ♢

5.5 Conclusion

The syndrome formers of a convolutional code can be computed by calculation of the transposes of the encoders of the dual code. So, similar results to the ones obtained in Chapters 3 and 4 for the encoders of the code, can also be considered for syndrome formers, using duality methods. In this chapter we presented the results that we have considered most important. In particular, the parametrization of the minimal syndrome formers in terms of their MFD's, a realization procedure to obtain all minimal syndrome formers applying output injection and postcompensation to a realization of a canonical syndrome former, and the study of the existence of decoupled syndrome formers of the code.

Chapter 6

Conclusions

Since its appearance, in 1955, much research has been carried out in convolutional coding. The interaction between convolutional coding and systems theory, started in 1967/68 with the work [35, 36] of Massey and Sain, has enriched this research with the self-knowledge of systems theorists. Specifically, since a convolutional code is the output of an input/output map, and its (causal) encoders are the transfer functions (matrices) that represent such maps, techniques used in systems theory were introduced in the study of convolutional codes and theirs encoders. However, MFD's techniques, that play an important role in the analysis of multivariable systems, have not been widely used in convolutional coding.

In this thesis, we have used MFD's in the investigation of the structure of a convolutional code and the family of its encoders and syndrome formers, and realized that MFD's constitute a powerful tool in the study of convolutional codes.

In Chapter 3, a new definition of convolutional code was introduced. The behavioral approach, introduced by Willems, seems to be a more natural setting to define a convolutional code, since it uses only properties (strong controllability and strong observability) of the code itself, in opposition to the classical definition that resorts to the characteristics of its encoders.

In the study of the encoders of a convolutional code, we considered MFD's in their representations, and we have obtained new proofs of some classical results.

Concerning code decomposition (i.e., when we obtain a code as a sum of smaller codes),

we have studied encoders that exhibit some degree of decoupling between inputs and outputs, called decoupled encoders.

In Chapter 4, we have concentrated in the study of the minimal encoders of a convolutional code. We have determined a simple parametrization, via MFD's, of such encoders, in particular of the decoupled ones. Taking into account this parametrization, we have shown that all minimal encoders can be obtained from a realization of a canonical encoder, by application of feedback and static precompensation.

Minimal encoders of a convolutional code can also be characterized using their abstract state space. In fact, Forney, Johannesson and Wan [14, 17], have shown that two necessary and sufficient conditions for the minimality of an encoder, are that the intersection between the abstract state space of the encoder and the code must be the null space, and moreover that restricting to the rational codewords of the code, the span of the information sequences must be contained in the span of the corresponding codewords. We have generalized such characterization to the set of all sequences of the code. We also have shown how the structure of an MFD of an encoder influences the relation between the span of the information sequences and the corresponding codewords.

Since syndrome formers of a convolutional code are the transposes of the encoders of its dual, we have obtained results for syndrome formers similar to the ones presented for encoders. These results are collected on Chapter 5, where, in particular, we have given an MFD parametrization of the minimal syndrome formers of a convolutional code and have obtained all minimal syndrome formers of the code, by application of output injection and static output compensation to a realization of a canonical one. We have also defined and parametrized the decoupled syndrome formers of the code.

The realization procedures presented in Chapters 4 and 5, to obtain the minimal encoders and syndrome formers of a convolutional code, seem to provide a good "tool" to be used in future investigations, in order to evaluate the performance of the encoders and syndrome formers of a code, and consequently also in the search for good codes.

In the future, another challenging work to be done, is the extension of the obtained results to convolutional codes constituted by bilateral sequences.

More interesting, but more difficult, is the extension of these results to multidimensional coding theory [13, 54]. In fact, in this thesis, we have used polynomial methods that do not hold anymore when we consider matrices whose entries are polynomials in two or more variables. Another problem to be solved concernes the minimality characterization via McMillan degree of encoders and syndrome formers, which is not available when we consider multidimensional systems. Perhaps a different concept of minimality should be devised, which seems to be a hard task.

References

[1] R. Blahut. *Theory and Practice of Error Control Codes*. Addison-Wesley Publishing Company, Inc., MA, 1983.

[2] R. Bose and D. Ray-Chaudhuri. On a Class of Error Correcting Binary Group Codes. *Information and Control*, 3:68–79, 1960.

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

[4] D. Costello. Construction of Convolutional Codes for Sequential Decoding. *Tech. Rpt. EE-692*, 1969.

[5] C. Desoer and M. Vidyasagar. *Feedback Systems: Input-Output Properties*. Academic Press, Inc., New York, 1975.

[6] A. Dholakia. *Introduction to Convolutional Codes with Applications*. Kluwer Academic, Boston, 1994.

[7] P. Elias. Coding for Noisy Channels. *IRE Conv. Record*, part 4:37–47, 1955.

[8] F. Fagnani and S. Zampieri. Dynamical Systems and Convolutional Codes over Finite Abelian Groups. *IEEE Trans. Inform. Theory*, 42(6):1892–1912, 1996.

[9] R. Fano. A Heuristic Discussion of Probabilistic Decoding. *IEEE Trans. Inform. Theory*, IT-9:64–74, 1963.

[10] J. Feigenbaum, G. Forney, B. Marcus, R. McEliece, and A. Vardy. Introduction to the Special Issue on Codes and Complexity. *IEEE Trans. Inform. Theory*, 42(6):1649–1659, 1996.

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

[12] E. Fornasini and G. Marchesini. *Appunti di Teoria dei Sistemi*. Edizioni Libreria Progetto, Padua, 1994.

[13] E. Fornasini and M. Valcher. Algebraic Aspects of 2D Convolutional Codes. *IEEE Trans. Inform. Theory*, 40:1068–1082, 1994.

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

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

[16] G. Forney. Minimal Bases of Rational Vector Spaces, with Applications to Multivariable Systems. *SIAM J.Control*, 13(3):493–520, 1975.

[17] G. Forney, R. Johannesson, and Z. Wan. Minimal and Canonical Rational Generator Matrices for Convolutional Codes. *IEEE Trans. Inform. Theory*, 42(6):1865–1880, 1996.

[18] G. Forney and M. Trott. The Dynamics of Group Codes: State Spaces, Trellis Diagrams, and Canonical Encoders. *IEEE Trans. Inform. Theory*, 39(9):1491–1513, 1993.

[19] F. Gantmacher. *The Theory of Matrices, vol.I*. Chelsea Publishing Company, New York, 1977.

[20] M. Golay. Notes on Digital Coding. *Proceedings of the IRE*, 37:657, 1949.

[21] R. Hamming. Error Detecting and Error Correcting Codes. *Bell System Technical Journal*, 29:147–160, 1950.

[22] A. Hocquenghem. Codes Correcteurs d'Errors. *Chiffres (Paris)*, 2:147–156, 1959.

[23] C. Huffman and V. Pless. *Handbook of Coding Theory, volumes 1,2*. Elsevier Sciences, North-Holland, 1998.

[24] F. Jelinek. A Fast Sequential Decoding Algorithm Using a Stack. *IBM J. Res. and Dev.*, 13:675–685, 1969.

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

[26] T. Kailath. *Linear Systems*. Englewood Cliffs, N.J.:Prentice Hall, 1980.

[27] R. Kalman, P. Falb, and M. Arbib. *Topics in Mathematical System Theory*. McGraw-Hill, New York, 1969.

[28] S. Lang. *Algebra*. Springer-Verlag, New York, 2002.

[29] S. Lin and D. Costello. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, Inc, Englewood Cliffs, New Jersey, 1983.

[30] H. Loeliger, G. Forney, T. Mittelholzer, and M. Trott. Minimality and Observability of Group Systems. *Linear Algebra Appl.*, 205/206:937–963, 1994.

[31] H. Loeliger and T. Mittelholzer. Convolutional Codes over Groups. *IEEE Trans. Inform. Theory*, 42:1660–1686, 1996.

[32] F. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes*. Elsevier Science, North-Holland, 1977.

[33] M. Marcus and H. Minc. *Introduction to Linear Algebra*. Dover Publications, Inc., New York, 1965.

[34] J. Massey. *Threshold Decoding*. MIT Press, Cambridge, Mass., 1963.

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

[36] J. Massey and M. Sain. Inverses of Linear Sequential Circuits. *IEEE Trans. on Computers*, 17:330–337, 1968.

[37] R. McEliece. The Theory of Information and Coding. *Encyclopedia of Mathematics and Its Applications*, volume 3, 1977.

[38] R. McEliece. *The Algebraic Theory of Convolutional Codes*. in Handbook of Coding Theory, vol. 1, V.S.Pless, W.C.Huffman, R.A.Brualdi eds., North Holland, Amsterdam, 1998.

[39] M. Newman. *Integral Matrices.* Academic Press, New York and London, 1972.

[40] P. Piret. *Convolutional Codes: an Algebraic Approach.* Cambridge, Mass.: MIT Press, 1988.

[41] J. Polderman and J. Willems. *Introduction to Mathematical Systems Theory - A Behavioral Approach.* Springer-Verlag, New York, 1998.

[42] I. Reed and G. Solomon. Polynomial Codes over Certain Finite Fields. *J. SIAM*, 8:300–304, 1960.

[43] H. Rosenbrock. *State Space and Multivariable Theory.* John Wiley & Sons, New York, 1970.

[44] J. Rosenthal. Connections Between Systems and Convolutional Codes. In J. R. B. Marcus, editor, *Codes, Systems, and Graphical Models*, pages 39–66. Springer-Verlag, New York, 2001.

[45] J. Rosenthal and J. Schumacher. Realization by Inspection. *IEEE Trans. Autom. Control*, 42(9):1257–1263, 1997.

[46] J. Rosenthal, J. Schumacher, and E. York. On Behaviors and Convolutional Codes. *IEEE Trans. Inform. Theory*, 42(6, part 1):1881–1891, 1996.

[47] C. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, 27:379–423,623–656, 1948.

[48] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions of MDS- Convolutional Codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, 2001.

[49] M. Sudan. Coding Theory: Tutorial and Survey. *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science,* 36-53, Las Vegas, Nevada, 2001.

[50] M. Sudan. *Essential Coding Theory.* Available from http://theory.lcs.mit.edu/∼madhu/FT02, 2002.

[51] M. Valcher and E. Fornasini. On 2D Finite Support Convolutional Codes: an Algebraic Approach. *Multidim. Sys. and Sign. Proc.*, 5:231–243, 1994.

[52] J. van Lint. *Introduction to Coding Theory.* Springer-Verlag, Berlin, 1999.

[53] A. Viterbi. Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm. *IEEE Trans. Inform. Theory,* 13:260-269, 1967.

[54] P. Weiner. *Multidimensional Convolutional Codes.* Ph.D. dissertation, University of Notre Dame, 1998.

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

[56] J. Willems. Paradigms and Puzzles in the Theory of Dynamical Systems. *IEEE Trans. Automat. Control*, 36:259–294, 1991.

[57] J. Wozencraft. Sequential Decoding for Reliable Communication. *IRE Nat. Conv. Rec.*, 5, pt. 2:11–25, 1957.

[58] E. York. *Algebraic Description and Construction of Error Correcting Codes: A Linear Systems Point of View.* Ph.D. dissertation, University of Notre Dame, 1997.

[59] K. Zigangirov. Some Sequential Decoding Procedures. *Probl. Peredachi Inf.*, 2:13–25, 1966.