

# 國立交通大學

應用數學系  
碩士論文

迴旋碼編碼器其非均等錯誤保護特性之研究

A Study on Convolutional Encoders for Unequal

Error Protection



研究生：吳偉帆

指導教授：王忠炫 教授

共同指導教授：傅恆霖 教授

中華民國九十八年十一月

迴旋碼編碼器其非均等錯誤保護特性之研究

A Study on Convolutional Encoders for Unequal  
Error Protection

研究生：吳偉帆

Student : Wei-Fan Wu

指導教授：王忠炫

Advisor : Chung-Hsuan Wang

共同指導教授：傅恆霖

Co-Advisor : Hung-Lin Fu

國立交通大學



A Thesis

Submitted to Department of Applied Mathematics  
College of Science

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master

in

Applied Mathematics

Nov. 2008

Hsinchu, Taiwan, Republic of China

中華民國九十七年十一月

# 迴旋碼編碼器其非均等錯誤保護特性之研究

研究生：吳偉帆

指導老師：王忠炫 教授

共同指導老師：傅恆霖 教授

國立交通大學

應用數學系

## 摘要

在很多通訊系統中，我們所傳送的訊息也許有某些部分是較為其它部分來的重要。因此當我們要傳送這個訊息進入通道前，我們希望這訊息中某些重要的部份能有更大的保護，進而在接收端所得到的資料裡重要的部份能夠更可靠。傳送訊息進通道前我們會對訊息使用非均等錯誤率編碼來給予不同程度的保護，傳送進入通道後，再將接收端所收到的向量透過解碼來取得訊息。擁有較大保護的訊息部份將有較高的錯誤更正能力，使得解碼出來的訊息能夠與原始傳送的訊息更為相近。早期大都是運用線性區塊碼來進行非均等錯誤率保護，漸漸的也開始發展使用迴旋碼來進行。文獻中已有研究指出，在任何的迴旋碼中，都會存在一個最佳編碼器來實行非均等錯誤率保護。很不幸地，並非所有迴旋碼都能有兼具最小延遲元件及最佳非均等錯誤率保護能力的最佳編碼器。因此給定任一迴旋碼，我們希望都能夠找到一個擁有最少延遲元件的最佳編碼器。利用我們提出的定理結果，可以直接算出實現一個迴旋碼編碼器所需要的最小延遲元件數，並且利用代數的方法來解釋出為什麼在一個 $(n,k)$ 迴旋碼的多項式編碼器中，所有 $k \times k$ 子矩陣其行列式之最大的度值不會超過實現此編碼器所需要最少的延遲元件數。最後，我們提出一個簡單的演算法來得到具有最少延遲元件數的最佳編碼器，並且保證此編碼器所產生出來的字碼，經過通道後，將接收端所接收到的向量解碼不會發生無窮項位元錯誤的情形。最後，我們亦證明了某一些迴旋碼皆會存在一個兼具最少延遲元件與最佳非均等錯誤率保護能力的最佳編碼器。

中華民國九十七年十一月

# A Study on Convolutional Encoders for Unequal Error Protection

Student: Wei-Fan Wu

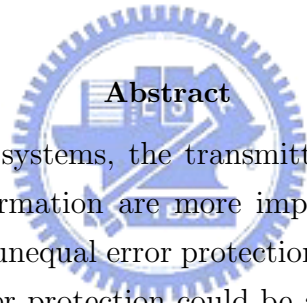
Advisor: Chung-Hsuan Wang

Co-Advisor: Hung-Lin Fu

*Department of Applied Mathematics*

*National Chiao Tung University*

*Hsinchu, Taiwan 30010*



In many communication systems, the transmitted data may have a structure that some parts of the information are more important than that in the other parts. Channel coding with unequal error protection (UEP) is usually employed in such systems so that stronger protection could be applied to the important parts to enhance the quality of communication. At the earliest, block codes were used to perform UEP mostly. Recently, studies of UEP have been expanded to convolutional codes. Previous results showed that there exists at least one UEP-optimal generator matrix with the greatest separation vector for every convolutional code. However, unfortunately, not all convolutional codes can have a UEP-optimal generator matrix which also keeps the minimal complexity for both of encoding and decoding. In this thesis, we show that we can calculate the McMillan degree of a generator matrix directly without decomposing it by using the Smith Algorithm. From this result, we also illustrate why the internal degree of a polynomial generator matrix is not greater than its McMillan degree. Besides, we provide a procedure for searching an optimal polynomial generator matrix with the lowest McMillan degree, and also we show that for some classes of convolutional codes there always exist generator matrices which are both optimal and minimal.

**Keywords:** Unequal error protection, optimal generator matrix, minimal generator matrix, noncatastrophic generator matrix, McMillan degree.

# 謝誌

能完成這篇論文，首先要謝謝傅恆霖老師。在我最徬徨的時候，傅老師給了我到外系去學習的想法。感謝電信系王忠炫老師，也就是我的指導教授，願意給我這樣的機會。剛開始幾乎是什麼都不懂，到現在能夠寫出一篇論文來，王老師讓我在這個學術領域中進步好多。在研究過程中，老師不厭其煩的教我好多東西，無論我遇到什麼樣的瓶頸，老師總是會給我不同的方向，並微笑的鼓勵我支持我。老師教學的態度嚴謹，但是私底下卻是個很風趣的人，也因為如此，跟著老師研究的這段期間幾乎沒什麼壓力。

剛進到實驗室，真是個氣氛很棒的地方。謝謝阿尼、小白、一哥、還有維庭。待在實驗室的這段期間，不論是課業、程式等方面都對我傾囊相授，也謝謝博士班的力仁學長，有時候我有好多問題都是學長幫我解決的。在這裡特別要感謝的是，博士班的健家學長。除了王老師之外，幫助我最大的就是學長了。在輔修電信所的時候，好多知識背景都是透過學長的指引，我才能夠順利完成。當我研究遇到問題，跑來求救時，學長總是抽空幫我解答，並給我一個正確的觀念。剛開始撰寫論文的時候懵懵懂懂的不知道怎麼著手，也是學長詳細的跟我解說清楚才有現在這篇。

感謝我在應數系 SA126 研究室的同學，耿松、子鴻、柏任、世忠。每次待在研究室的時候，總是會給我好心情。特別感謝耿松和子鴻，兩年來分別跟你們一起當微積分助教，每當我有困難的時候，你們總是願意幫我代班，幫我把事情做到好。感謝同學佩純，每次系辦有什麼事情通知，總是會收到妳的叮嚀交代。還有其他的應數所同學們，在這學習的期間，真的感到很溫暖。

最後要感謝我的家人、舅舅，以及小阿姨。有你們的支持，我才能在沒有壓力的環境下全心全意的做研究，有你們的鼓勵，我才能順利完成這篇論文。我願意與你們及週遭關心我的人一同分享完成這篇論文的榮耀與喜悅。

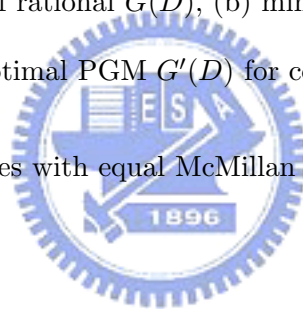
# Contents

Abstract (in Chinese) . . . . .	i
Abstract (in English) . . . . .	ii
Acknowledgement . . . . .	iii
Contents . . . . .	iv
List of Figures . . . . .	v
<b>1 Introduction</b>	<b>1</b>
<b>2 Preliminaries</b>	<b>4</b>
2.1 Basics of convolutional codes from an algebraic aspect . . . . .	4
2.2 Polynomial generator matrices and their properties . . . . .	8
2.3 Convolutional encoders for UEP . . . . .	17
<b>3 Lowest McMillan degree of polynomial encoders for UEP</b>	<b>24</b>
3.1 Smith decomposition on PGMs over the field $F[D^{-1}]$ . . . . .	25
3.2 Smith-McMillan decomposition on rational polynomial generator matrices over $F(D^{-1})$ . . . . .	34
3.3 The least degree encoder for UEP with the noncatastrophic property . . . . .	35
<b>4 Optimal PGMs with the lowest McMillan degree</b>	<b>39</b>
<b>5 Concluding remarks</b>	<b>50</b>



# List of Figures

2.1	Notations of the circuit elements. . . . .	7
2.2	The physical realization of $G(D)$ . . . . .	8
2.3	Two physical realizations of $G_1(D)$ . . . . .	12
2.4	Minimal realization of $G_1(D)$ , (b)Minimal realization of $G_2(D)$ . . . . .	15
3.1	(a) A physical realization of rational $G(D)$ , (b) minimal realization of rational $G(D)$ . . . . .	33
3.2	A minimal realization of optimal PGM $G'(D)$ for convolutional code $C$ . . . . .	38
4.1	Sets of all generator matrices with equal McMillan degree. . . . .	46



# Chapter 1

## Introduction

In many communication systems, the transmitted messages may have a structure that the information included in some parts of the message are more important than that in the other parts. Often these important parts of the message have to be received more reliably. Therefore, stronger protection should be applied to these parts than to the other parts. This requirement is called unequal error protection (UEP). For example, in packet transmission the header usually needs to be highly protected. Before transmitting messages to the channel, we use the UEP encoders to give different protection levels for different important level parts of the messages. At the earliest, block codes were mainly used to perform UEP. Dunning and Robbins [3] introduced a so-called separation vector to measure the error correction capability of a UEP block code, and in this sense they also proposed that given any linear block code, there exists an optimal generator matrix which has the greatest separation. For further researches on UEP block codes, we refer to [1][4][7][12][21].

Recently, more and more researches about UEP had been expanded to convolutional codes. Most of these researches concentrate on developing new UEP schemes [13][20]. Only few of them were about the UEP capabilities of ordinary convolutional codes [14][18]. Authors in [18] showed that for any convolutional code, there exists an optimal generator matrix which has the greatest separation vector, i.e., the best UEP capability. They also provided procedures to obtain some UEP generator matrices of special algebraic properties, such as basic



and optimal generator matrices, canonical generator matrices with the greatest separation vector, and systematic generator matrix with greatest separation vector. Unfortunately, not all convolutional codes have both the best UEP capability and the minimal property [18]. Although a procedure was provided in [18] to produce an optimal basic generator matrix with lowest external degree, it may not have the lowest McMillan degree.

The famous decoding scheme for convolutional codes is *Viterbi Algorithm* [11]. By the algorithm, we know that the number of delay elements in the convolutional encoder will determine the required decoding complexity. Hence we hope to obtain an optimal generator matrix with the lowest McMillan degree. In this thesis, we show that we can calculate the McMillan degree of a generator matrix without decomposing it by the Smith algorithm [15]. From this result, we also give a simple proof to illustrate why the internal degree of a polynomial generator matrix (PGM) is not greater than its McMillan degree. Also we provide a procedure to obtain an optimal polynomial generator matrix which guarantees the noncatastrophic property and has the lowest McMillan degree. Furthermore, we show that for all  $(n, 1)$ ,  $(n, 2)$  convolutional codes, and the  $(n, k)$  convolutional codes for  $k \geq 3$  which can be generated by the optimal generator matrices with single-value separations, there always exist generator matrices which are both optimal and minimal. And for the  $(n, k)$  convolutional codes with  $k \geq 3$  which can be generated by the optimal generator matrix  $G_b(D)$  with the separation vector of the form  $(\alpha, \alpha, \dots, \beta)$  where  $\alpha < \beta$  and  $G_b(D)$  is basic with the lowest external degree and every row of  $G_b(D)$  has only one row degree position, there exists an optimal PGM which has the lowest McMillan degree among all optimal generator matrices.

The rest of this thesis is organized as follows. In Chapter 2, we review some definitions and known results in the algebraic aspect of convolutional codes. Besides, UEP capabilities of convolutional codes are also described. In Chapter 3, we first show a theory so that we can understand the relations between the invariant factors of a polynomial generator matrix in finite field  $F[D]$  and in finite field  $F[D^{-1}]$ . And our work is started from this result. In

Chapter 4, we provide two procedures to obtain the optimal and noncatastrophic PGM with the lowest McMillan degree based on the different ideas. Finally, we conclude our work in Chapter 5.



# Chapter 2

## Preliminaries

### 2.1 Basics of convolutional codes from an algebraic aspect

We first review some definitions and properties of convolutional codes from an algebraic aspect. Let  $F$  be a finite field. The power series of the form  $\sum_{i \geq m} a_i D^i$  is called an one-sided Laurent series with indeterminate  $D$ , where  $a_i \in F$  for  $i \geq m$ , and  $m \in Z$ . The set of all one-sided Laurent series is denoted by  $F((D))$ . Laurent series of the form  $A(D) = a_0 + a_1 D + \dots + a_L D^L$  are called polynomials, where  $L$  is a positive integer. The set of all polynomials over  $F$  is denoted by  $F[D]$ . Let  $p(D), q(D) \in F[D]$  and  $q(D) \neq 0$ . It is well-known that the rational function  $p(D)/q(D)$  has a unique one-sided Laurent series expansion. For convenience, we call it a rational Laurent series. The set of all rational Laurent series forms the rational subfield of  $F((D))$ , denoted by  $F(D)$ . The number of nonzero coefficients of a polynomial  $y(D)$  is called the *weight* of  $y(D)$ , denoted by  $w(y(D))$ , and the weight of an one-sided Laurent series is infinite. The weight of a vector of laurent series  $\mathbf{y}(D) = (y_1(D), y_2(D), \dots, y_n(D))$  is defined to be the sum of  $w(y_i(D))$ , i.e.,  $w(\mathbf{y}(D)) = \sum_{i=1}^n w(y_i(D))$ .

We now introduce convolutional codes from a linear block codes aspect. Let  $\mathbf{C}$  be an  $(n, k)$  linear block code over a finite field  $F$ . Suppose  $\mathbf{C}$  is generated by the generator matrix  $\mathbf{G}$ , where  $\mathbf{G}$  is a  $k \times n$  matrix of rank  $k$  with entries from  $F$ . Hence  $\mathbf{G}$  maps a  $k$ -dimensional

information word  $\mathbf{x}$  into a  $n$ -dimension codeword  $\mathbf{y}'$  by way of  $\mathbf{y}' = \mathbf{x}\mathbf{G}$ . If  $\mathbf{G}$  is used not just one information word, but a sequence of information words, say  $\mathbf{x}(0), \mathbf{x}(1), \dots$ , hence the  $i$ -th codeword  $\mathbf{y}'(i)$  corresponding to the  $i$ -th information word  $\mathbf{x}(i)$  is  $\mathbf{y}'(i) = \mathbf{x}(i)\mathbf{G}$ , for all  $i$ . Let the sequence of information vectors  $\mathbf{x}(0), \mathbf{x}(1), \dots$  be the coefficients of the Laurent series form  $\mathbf{X}(D) = \sum_{i \geq 0} \mathbf{x}(i)D^i$ . For convenience, we call  $\mathbf{X}(D)$  the generating function of  $\mathbf{x}(0), \mathbf{x}(1), \dots$  with indeterminate  $D$ . We also use generating function on the codeword sequence, i.e., let Laurent series  $\mathbf{Y}'(D) = \sum_{i \geq 0} \mathbf{y}'(i)D^i$  be the codeword series. Then we get that  $\sum_{i \geq 0} \mathbf{y}'(i)D^i = (\sum_{i \geq 0} \mathbf{x}(i)D^i)\mathbf{G}$ , i.e.,  $\mathbf{Y}'(D) = \mathbf{X}(D)\mathbf{G}$  provided  $\mathbf{y}'(i) = \mathbf{x}'(i)\mathbf{G}$  for  $i \geq 0$ .

An  $(n, k)$  convolutional encoder is a linear device which maps a sequence of  $k$ -dimension information words  $\mathbf{u}(0), \mathbf{u}(1), \dots$ , into a sequence of  $n$ -dimension codewords  $\mathbf{y}(0), \mathbf{y}(1), \dots$ , respectively. The difference between convolutional encoder and linear block encoder is that convolutional encoder has an internal  $m$ -dimension state vector,  $\mathbf{s}(i)$ , and the  $i$ -th codeword  $\mathbf{y}(i)$  not only depends on the  $i$ -th input  $\mathbf{u}(i)$ , but also  $i$ -th state  $\mathbf{s}(i)$ . And the  $i$ -th state  $\mathbf{s}(i)$  may be affected by the state  $\mathbf{s}(i-1)$  and input  $\mathbf{u}(i-1)$  at time  $i-1$ . The formal description of the encoder is as follows:  $\mathbf{s}(0) = \mathbf{0}$  for  $i < 0$ , and for  $i \geq 0$ ,

$$\mathbf{s}(i+1) = \mathbf{s}(i)A + \mathbf{u}(i)B, \quad (1.1)$$

$$\mathbf{y}(i) = \mathbf{s}(i)C + \mathbf{u}(i)\bar{D}, \quad (1.2)$$

where matrices  $A, B, C, \bar{D}$  four matrices have dimensions  $m \times m, k \times m, m \times n, k \times n$ , respectively. The integer  $m$  is called the degree of the encoder. Also, the ordered quadruple  $(A, B, C, \bar{D})$  is called the *state space description* of a convolutional code. Let generating function  $\mathbf{S}(D) = \sum_{i \geq 0} \mathbf{s}(i)D^i$ , hence we multiply both sides of (1.1) and (1.2) by  $D^i$ , and sum over all  $i$ . It

follows that:

$$\begin{aligned}
& \sum_{i \geq 0} \mathbf{s}(i+1)D^i = \sum_{i \geq 0} \mathbf{s}(i)D^i A + \sum_{i \geq 0} \mathbf{s}(i)D^i B \\
\Rightarrow & \sum_{i \geq 1} \mathbf{s}(i)D^i D^{-1} = \sum_{i \geq 0} \mathbf{s}(i)D^i A + \sum_{i \geq 0} \mathbf{s}(i)D^i B, \\
\Rightarrow & \mathbf{S}(D)D^{-1} = \mathbf{S}(D)A + \mathbf{U}(D)B,
\end{aligned}$$

and

$$\begin{aligned}
& \sum_{i \geq 0} \mathbf{y}(i)D^i = \sum_{i \geq 0} \mathbf{s}(i)D^i C + \sum_{i \geq 0} \mathbf{u}(i)D^i \bar{D} \\
\Rightarrow & \mathbf{Y}(D) = \mathbf{S}(D)C + \mathbf{U}(D)\bar{D}.
\end{aligned}$$

Hence an explicit expression for  $\mathbf{S}(D)$  and  $\mathbf{Y}(D)$  in terms of  $\mathbf{U}(D)$  is as follows:

$$\mathbf{S}(D) = \mathbf{U}(D)E(D) = \mathbf{U}(D)B(D^{-1}I - A)^{-1}, \quad (1.3)$$

$$\mathbf{Y}(D) = \mathbf{U}(D)G(D) = \mathbf{U}(D)(\bar{D} + B(D^{-1}I - A)^{-1}C). \quad (1.4)$$

By (1.4), we call  $G(D)$  a generator matrix of a convolutional code. From [15], we know that an  $(n, k)$  convolutional code is a  $k$ -dimension subspace of  $F(D)^n$ . Hence, if a generator matrix  $G(D)$  generates a convolutional code  $C$ , then its  $k$  rows generate  $C$ . In linear algebra, we know that if a matrix  $M$  is multiplied by a nonsingular matrix  $U$  such that  $M' = UM$ , then row space of  $M =$  row space of  $M'$ . Hence  $T(D)G(D)$  will not change this code space if  $T(D)$  is a nonsingular matrix. For example, let two generator matrices  $G(D)$  and  $\hat{G}(D)$  as:

$$\begin{aligned}
G(D) &= \begin{pmatrix} 1 & 0 & D \\ 1+D & 1 & 0 \end{pmatrix}, \\
\hat{G}(D) = T(D)G(D) &= \begin{pmatrix} 1 & 0 \\ D & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & D \\ 1+D & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & D \\ 1 & 1 & D^2 \end{pmatrix}.
\end{aligned}$$

Since  $T(D)$  is nonsingular, the row spaces of  $G(D)$  and  $\hat{G}(D)$  are the same, and hence they generate the same convolutional code. We can use delay elements, adders, and multipliers with a shorthand notation for the circuit elements to realize generator matrices [12], which are described in Figure 2.1. Since we illustrate everything with respect to the field  $GF(2)$ , we

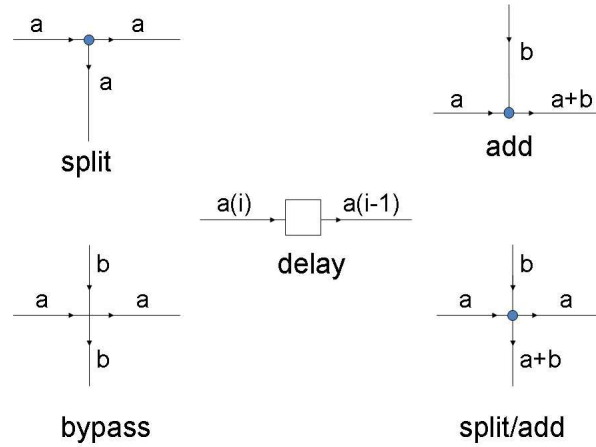


Figure 2.1: Notations of the circuit elements.

do not need multipliers. For example, suppose

$$G(D) = \begin{pmatrix} 1 & 0 & D \\ 1 + D & 1 & 0 \end{pmatrix}$$

is a  $2 \times 3$  generator matrix for a given convolutional code  $C$ , i.e., two information sequences are encoded to three codeword sequences. So we use two delay elements to realize  $G(D)$ , which is shown in Figure 2.2, where  $s_1$  and  $s_2$  means two delay elements,  $u_1$  and  $u_2$  means two information sequences, and  $y_1$ ,  $y_2$ , and  $y_3$  means three output sequences. Note that for a given convolutional code, there are distinct generator matrices which can encode the same code. Some of them are polynomial generator matrices (PGM), for which the entries are all polynomials. And the others are rational polynomial generator matrices, for which the entries are rational polynomials. For any rational polynomial generator matrix  $G(D)$ , let  $L(D)$  be the least common multiple (l.c.m) of all entries of  $G(D)$ . This implies that  $G(D) = \frac{1}{L(D)}G_p(D)$ , where  $G_p(D)$  is a polynomial matrix. Since each row of  $G_p(D)$  corresponds to a row of  $G(D)$  multiplied by  $L(D)$ ,  $G_p(D)$  is also a generator matrix. So, every convolutional code always has a polynomial generator matrix. Next, we review several properties of polynomial generator matrices.

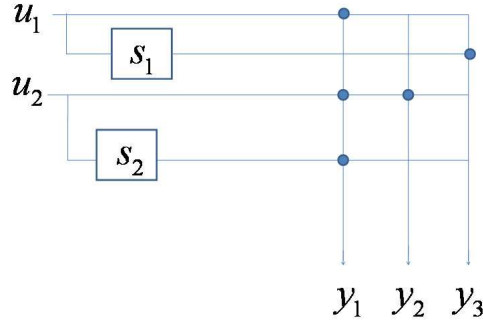


Figure 2.2: The physical realization of  $G(D)$ .

## 2.2 Polynomial generator matrices and their properties

Let  $G(D)$  be a  $k \times n$  polynomial generator matrix for a convolutional code  $C$  with entries  $g_{ij}(D)$ ,  $\forall 1 \leq i \leq k$ , and  $\forall 1 \leq j \leq n$ . Let the  $i$ -th row of  $G(D)$  be denoted by  $g_i(D)$ , i.e.,  $g_i(D) = (g_{i1}(D), g_{i2}(D), \dots, g_{in}(D))$ , and the row degree of  $g_i(D)$  be  $\max\{\deg(g_{ij}(D)) \mid j = 1, 2, \dots, n\}$ . Also, we define the *internal degree* and *external degree* [12] as follows:

$$\begin{aligned} \text{intdeg}(G(D)) &= \text{maximum degree of } k \times k \text{ minors of } G(D), \\ \text{extdeg}(G(D)) &= \text{sum of the row degrees of } G(D). \end{aligned}$$

Note that a  $k \times k$  minor of  $G(D)$  is the determinant of a  $k \times k$  submatrix of  $G(D)$ . The following theorem provides a useful fact about the internal degree of a PGM.

**Theorem 1** [12] *Let  $G(D)$  be a  $k \times n$  polynomial generator matrix. If  $T(D)$  is any non-singular  $k \times k$  polynomial matrix, then  $\text{intdeg}(T(D)G(D)) = \text{intdeg}(G(D)) + \deg(\det T(D))$ . In particular,  $\text{intdeg}(T(D)G(D)) \geq \text{intdeg}(G(D))$ , with equality holds if and only if  $T(D)$  is unimodular\*.*

By way of internal degree and external degree, we obtain two PGMs which are basic PGMs and reduced PGMs.

**Definition 1** *A  $k \times n$  PGM is called basic if among all polynomial generator matrices of the*

\*A polynomial matrix is called unimodular if its determinant is in  $F$

form  $T(D)G(D)$ , where  $T(D)$  is a nonsingular  $k \times k$  matrix over  $F(D)$ , it has the minimum internal degree.

**Definition 2** A  $k \times n$  PGM for a given convolutional code  $C$  is called reduced if among all polynomial generator matrices of the form  $U(D)G(D)$ , where  $U(D)$  is a unimodular,  $G(D)$  has the minimum external degree.

For a polynomial generator matrix, we can use nonsingular transformations to obtain an equivalent generator matrix, which generates the same code. We review here that a nonsingular transformation is a composition of *elementary matrices*, where an elementary matrix is defined as one of follows:

- Type 1. Interchange two rows (columns).
- Type 2. Multiply a row (column) with a rational polynomial  $\alpha(D)$ .
- Type 3. Add a rational polynomial multiple of a row (column) to another row (column).

We use  $3 \times 3$  elementary matrices for example, and are shown below, where Type 1 shows interchange 1st and 3rd rows, Type 2 shows multiply 2nd row with a rational polynomial  $\alpha(D)$ , and Type 3 means replace 3rd row with (row 3 +  $\beta(D)$   $\times$  row 1).

$$\text{Type 1: } \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \text{ Type 2: } \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha(D) & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ Type 3: } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \beta(D) & 0 & 1 \end{pmatrix}.$$

The following result is known as the *Invariant Theorem*:

**Theorem 2** [12] Let  $G(D)$  be a  $k \times n$  polynomial generator matrix. There exist finite number of elementary row and column operations which reduce  $G(D)$  into a diagonal polynomial matrix. That is,  $G(D) = W(D)\Gamma(D)V(D)$ , where  $W(D)$  and  $V(D)$  are unimodular and  $\Gamma(D)$  is of the form:

$$\Gamma(D) = \begin{pmatrix} \gamma_1(D) & \mathbf{0} & 0 & \dots & 0 \\ & \gamma_2(D) & \vdots & & \vdots \\ & & \ddots & & 0 \\ & \mathbf{0} & & \gamma_k(D) & 0 \\ & & & & 0 & \dots & 0 \end{pmatrix},$$



where  $\gamma_i(D) | \gamma_{i+1}(D)$ , for  $i=1, \dots, k-1$ , and  $\gamma_i(D) = \Delta_i(D)/\Delta_{i-1}(D)$ , where  $\Delta_i(D)$  is the greatest common divisor (g.c.d) of all  $i \times i$  minors of  $G(D)$  for  $i = 1, 2, \dots, n$ .

Here, the diagonal entries of  $\Gamma(D)$  are called the *invariant factors* of  $G(D)$ . We know that a basic generator matrix has the fewest internal degree among all polynomial generator matrices.

Therefore, we have:

**Theorem 3** [12] *A  $k \times n$  PGM  $G(D)$  is basic if and only if one of the following six conditions satisfies:*

- (1) *The invariant factors of  $G(D)$  are all 1.*
- (2) *The g.c.d of the  $k \times k$  minors of  $G(D)$  is 1.*
- (3)  *$G(\alpha)$  has rank  $k$  for any  $\alpha$  in the algebraic closure of  $F$ .*
- (4)  *$G(D)$  has a polynomial right inverse.*
- (5) *If  $\mathbf{y}(D) = \mathbf{x}(D)G(D)$ , and if  $\mathbf{x}(D) \in F[D]^n$ , then  $\mathbf{u}(D) \in F[D]^k$ .*
- (6)  *$G(D)$  is a submatrix of a unimodular matrix.*

For example, suppose a convolutional code  $C$  is generated by

$$G(D) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1+D & D & 1 \end{pmatrix}.$$

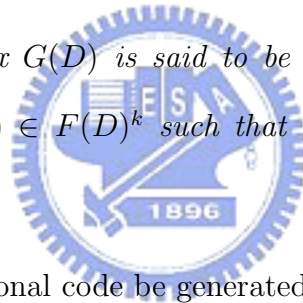
Then by the Smith decomposition on  $G(D)$ , we get that

$$G(D) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1+D & D & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Hence by (1) of Theorem 3, the invariant factors of  $G(D)$  are all 1. Hence  $G(D)$  is a basic generator matrix.

There is a special generator matrix which is called *noncatastrophic*, and now we illustrate what is the catastrophic phenomenon. Suppose an information word  $\mathbf{u}(D)$  is encoded by  $G(D)$  into codeword  $\mathbf{y}(D) = \mathbf{u}(D)G(D)$ . Let  $\mathbf{y}(D)$  be transmitted over a noisy channel and received as  $\mathbf{y}_r(D)$ . The decoder must make an estimate of  $\mathbf{u}(D)$ , based on  $\mathbf{y}_r(D)$ . The decoding job is to find a codeword  $\hat{\mathbf{y}}(D)$ , which is closest to  $\mathbf{y}_r(D)$ , and hope being that  $\hat{\mathbf{y}}(D) = \mathbf{y}(D)$ . Clearly, if the decoder's estimate of  $\mathbf{y}(D)$  is  $\hat{\mathbf{y}}(D)$ , its estimate of  $\mathbf{u}(D)$  will be  $\hat{\mathbf{u}}(D) = \hat{\mathbf{y}}(D)K(D)$ , where  $K(D)$  is an  $n \times k$  right inverse of  $G(D)$ . If we define codeword error by  $\mathbf{e}_c(D) = \mathbf{y}(D) - \hat{\mathbf{y}}(D)$ , and the information error by  $\mathbf{e}_I(D) = \mathbf{u}(D) - \hat{\mathbf{u}}(D)$ . Hence we got that  $\mathbf{e}_I(D) = \mathbf{e}_c(D)K(D)$ . A decoding catastrophic is said to have occurred if the codeword error has finite weight, but the corresponding information error has infinite weight. Since  $\mathbf{e}_c(D)$  is a difference of codewords, it is a codeword. Hence have the following definition.

**Definition 3** A generator matrix  $G(D)$  is said to be catastrophic if there is an information word of infinite weight  $\mathbf{u}(D) \in F(D)^k$  such that the corresponding codeword  $\mathbf{y}(D) = \mathbf{u}(D)G(D)$  has finite weight.



For example, let a  $(2, 3)$  convolutional code be generated by a generator matrix

$$G(D) = \begin{pmatrix} 1 & D & 1 \\ D & 1+D & 1+D^2 \end{pmatrix}.$$

We can find that  $G(D)$  is catastrophic since give a infinite weight input  $\mathbf{u}(D) = (\frac{D}{1+D+D^2}, \frac{1}{1+D+D^2})$ , we will get a finite weight output  $\mathbf{y}(D) = (0, 1, 1) = \mathbf{u}(D)G(D)$ . In 1968, Messey and Sain proved the following:

**Theorem 4** [14] If  $G(D)$  is a polynomial generator matrix for a convolutional code  $C$ , then the following three conditions are equivalent.

- (1) No infinite weight input  $\mathbf{u}(D)$  can produce a finite weight output  $\mathbf{y}(D) = \mathbf{u}(D)G(D)$ .
- (2) The g.c.d of all  $k \times k$  minors of  $G(D)$  is power of  $D$ .
- (3)  $G(D)$  has a right inverse  $K(D)$  whose entries are of finite weight.

A PGM is said to be noncatastrophic if it satisfied one of these properties. Otherwise, it is called catastrophic.

Let  $G_b(D)$  be a basic generator matrix of a given convolutional code  $C$ . By Theorem 3 and Theorem 4, the basic generator matrix  $G_b(D)$  has a property that the g.c.d of  $k \times k$  minors of  $G_b(D)$  is 1. Since  $1 = D^0$  which is a power of  $D$ . So  $G_b(D)$  is also a noncatastrophic generator matrix.

A generator matrix  $G(D)$  may have more than one physical realization. Among all of these realizations, the fewest number of delay elements is called McMillan degree of  $G(D)$ .

**Example 1** Let a  $(2, 3)$  convolutional code  $C$  be generated by:

$$G_1(D) = \begin{pmatrix} D & 0 & D \\ 1 + D^2 & 1 + D & D^2 \end{pmatrix}.$$

This implies that there are at least at least two distinct physical realizations of  $G_1(D)$ , see Figure 2.3.

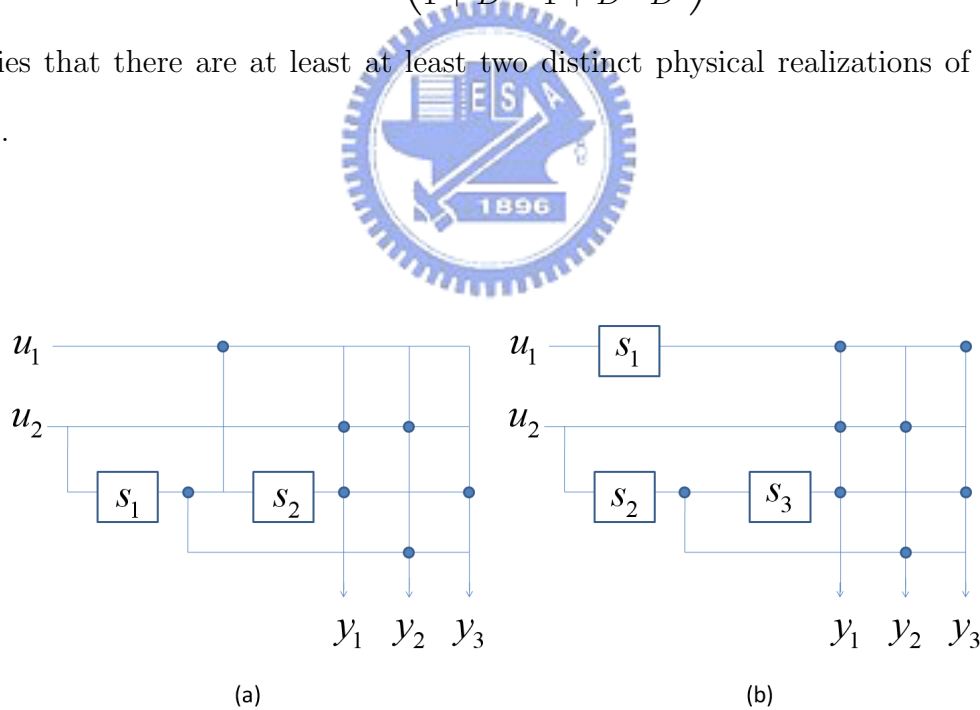


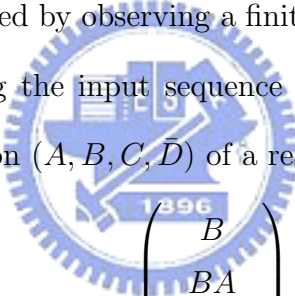
Figure 2.3: Two physical realizations of  $G_1(D)$ .

Also, we call the realization of  $G(D)$  is a *minimal realization* if it contains the minimum degree among all realizations. A realization of  $G(D)$  is called the *direct-form realization* if it is realized by realizing every row of  $G(D)$  directly and combine them into a circuit. Suppose

$G(D)$  has a realization with degree  $m$ . So dimension of  $A$  is  $m$  in the state space description  $(A, B, C, \bar{D})$ . Let  $T$  be an  $m \times m$  nonsingular matrix, and let

$$A_1 = TAT^{-1}, B_1 = BT^{-1}, C_1 = TC, \text{ and } D_1 = \bar{D}.$$

This implies that  $G(D) = \bar{D} + B(D^{-1}I - A)^{-1}C = D_1 + BT^{-1}T(D^{-1}I - A)^{-1}T^{-1}TC = D_1 + C_1(D^{-1}I - A_1)^{-1}B_1$ . So,  $(A_1, B_1, C_1, D_1)$  is also a state space description of  $G(D)$ , and from  $(A_1, B_1, C_1, D_1)$  we get another physical realization since we know the relations of the input, the output, and the state. Note that  $T$  is called the *similar transformation* matrix. Consider a realization for a generator matrix  $G(D)$ . The realization is called *reachable* if we can reach any specified final state  $\mathbf{s}_f$  starting from any arbitrary initial state  $\mathbf{s}_i$  by applying an appropriate finite length input sequence; and the realization is called *observable* if the state  $\mathbf{s}_t$  at time  $t$  can be uniquely determined by observing a finite length segment of output sequence starting from time  $t$ , and knowing the input sequence for the corresponding set of sample values. For a state space description  $(A, B, C, \bar{D})$  of a realization with  $m$  delay elements, let



$$\mathcal{R}_{AB} = \begin{pmatrix} B \\ BA \\ BA^2 \\ \vdots \\ BA^{m-1} \end{pmatrix}$$

be a matrix which is obtained by using  $A$  and  $B$ . By [17], this realization is reachable if and only if  $\mathcal{R}_{AB}$  has full rank  $m$ . Also, let

$$\mathcal{S}_{CA} = \begin{pmatrix} C & AC & A^2C & \dots & A^{m-1}C \end{pmatrix}$$

be a matrix which is obtained by using  $A$  and  $C$ . Again by [17], this realization is observable if and only if  $\mathcal{S}_{CA}$  has full rank  $m$ . Since a realization is a minimal realization if and only if it is reachable and observable [17]. We can use similar transformation to obtain a realization which is reachable and observable, and thus is a minimal realization. For example, Figure 2.3(b) is the direct-form realization of  $G(D)$ , and we can get its relations of input state and

output state:

$$\begin{aligned} (s_1(i+1), s_2(i+1), s_3(i+1)) &= (s_1(i), s_2(i), s_3(i)) \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} + (u_1(i), u_2(i)) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \\ (y_1(i), y_2(i), y_3(i)) &= (s_1(i), s_2(i), s_3(i)) \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} + (u_1(i), u_2(i)) \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}. \end{aligned}$$

Hence we have a state space description

$$(A, B, C, \bar{D}) = \left( \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \right).$$

Let the similar transformation matrix be

$$T(D) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

By using a similar transformation  $T$ , we obtain another state space description  $(A_1, B_1, C_1, D_1)$  as

$$\begin{aligned} A_1 = TAT^{-1} &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, B_1 = BT^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \\ C_1 = TC &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, D_1 = \bar{D} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}. \end{aligned}$$

This implies that the input state and output state are

$$\begin{aligned} (s_1(i+1), s_2(i+1), s_3(i+1)) &= (s_1(i), s_2(i), s_3(i)) \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} + (u_1(i), u_2(i)) \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \\ (y_1(i), y_2(i), y_3(i)) &= (s_1(i), s_2(i), s_3(i)) \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} + (u_1(i), u_2(i)) \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}. \end{aligned}$$

By above, we find that at any time  $i$  the output  $(y_1(i), y_2(i), y_3(i))$  is independent of the first state value  $s_1(i)$ . So we can rewrite the equalities without  $s_1$  as:

$$\begin{aligned} (s_2(i+1), s_3(i+1)) &= (s_2(i), s_3(i)) \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + (u_1(i), u_2(i)) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ (y_1(i), y_2(i), y_3(i)) &= (s_2(i), s_3(i)) \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} + (u_1(i), u_2(i)) \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}. \end{aligned}$$

Using the notation of state vector  $(s_1, s_2)$  to replace  $(s_2, s_3)$ , we can realize this circuit which is shown in Figure 2.3(a). Since it is reachable and observable, hence it is a minimal realization.

So every generator matrix  $G(D)$  has a minimal realization, and the degree of minimal realization is called McMillan degree of  $G(D)$ , denoted by  $\text{Mcdeg}(G(D))$ . Although there are so many generator matrices can generate the same convolutional code, their McMillan degree may not equal. For example, suppose a  $(2, 4)$  convolutional code  $C$  can be generated by two PGMs as follows:

$$\begin{aligned} G_1(D) &= \begin{pmatrix} 1 & 1+D+D^2 & 1+D^2 & 1+D \\ D & 1+D+D^2 & D^2 & 1 \end{pmatrix}, \\ G_2(D) &= \begin{pmatrix} 1 & D & 1+D & 0 \\ 0 & 1+D & D & 1 \end{pmatrix}. \end{aligned}$$

Thus we realize this two PGMs with their minimal realizations, as shown in Figure 2.4. We find

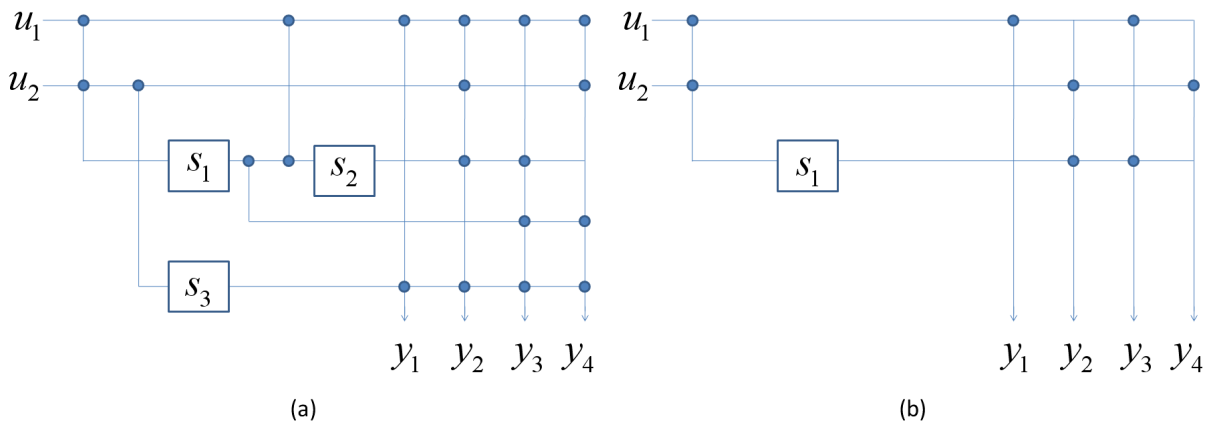


Figure 2.4: Minimal realization of  $G_1(D)$ , (b)Minimal realization of  $G_2(D)$ .

that although  $G_1(D)$  and  $G_2(D)$  generate the same convolutional code,  $G_1(D)$  has McMillan degree 3 and  $G_2(D)$  has McMillan degree 1, hence they have different McMillan degree. For

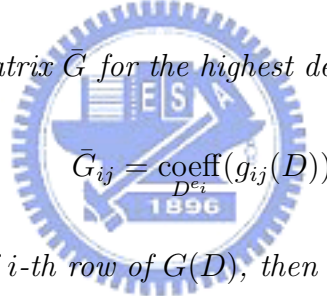
a given convolutional code  $C$ , there are so many generator matrices can generate  $C$ , and each of them have different McMillan degree. We call  $G(D)$  is a minimal generator matrix if  $\text{Mcdeg}(G(D))$  is not greater than all the others. Hence we give a definition as follows:

**Definition 4** For a given convolutional code  $C$ , generator matrix  $G_m(D)$  is called minimal if among all possible generator matrices,  $G_m(D)$  has the fewest McMillan degree.

From Definition 2, we know that a reduced generator matrix has the fewest external degree among all polynomial generator matrices. With this definition, the reduced generator matrix is proved to have some equivalent conditions as follows:

**Theorem 5** [15] A  $k \times n$  PGM  $G(D)$  is reduced if and only if one of the following three conditions satisfies:

(1) If we define the indicator matrix  $\bar{G}$  for the highest degree terms in each row of  $G(D)$  by



$$\bar{G}_{ij} = \text{coeff}_{D^{e_i}}(g_{ij}(D)),$$

where  $e_i$  is the row degree of  $i$ -th row of  $G(D)$ , then  $\bar{G}$  has rank  $k$ .

(2)  $\text{extdeg}(G(D)) = \text{intdeg}(G(D))$ .

(3) For any  $k$ -dimension polynomial vector  $\mathbf{u}(D) = (u_1(D), \dots, u_k(D))$ ,

$$\deg(\mathbf{u}(D)G(D)) = \max_{1 \leq i \leq k} (\deg(u_i(D)) + \deg(g_i(D))).$$

**Example 2** Suppose a given convolutional code  $C$  can be generated by

$$G(D) = \begin{pmatrix} 1 & 0 & D \\ 1+D & 1 & 0 \end{pmatrix}.$$

Then from Theorem 2, we get that

$$G(D) = \begin{pmatrix} 1 & 0 \\ 1+D & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & D \\ 0 & 1 & D+D^2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence we know that all invariant factors of  $G(D)$  are all 1; so it is basic and hence noncatastrophic. Also, since

$$\bar{G} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

has full rank, hence  $G(D)$  is also reduced.

A PGM  $G_c(D)$  is called *canonical* generator matrix if among all polynomial generator matrices,  $G_c(D)$  has the lowest possible external degree. It is proved that a PGM is canonical if and only if it is basic and reduced [15]. Hence in Example 2,  $G(D)$  is canonical since it is basic and reduced. External degree of a PGM corresponds to the degree of its direct-form realization, i.e., we can realize every row of a PGM directly with correspondent row degree and combine them into a circuit. So we know that McMillan degree is smaller than external degree. And latter, we will illustrate that internal degree is smaller than McMillan degree. Hence every PGM  $G(D)$  has the degree property as follows [15]:

$$\text{intdeg}(G(D)) \leq \text{Mcdeg}(G(D)) \leq \text{extdeg}(G(D)). \quad (2.5)$$

By (2.5), we know that a canonical generator matrix  $G(D)$  is basic, so  $\text{intdeg}(G(D))$  is the lowest, also it is reduced, so  $\text{extdeg}(G(D)) = \text{intdeg}(G(D))$ . Hence it follows that  $\text{Mcdeg}(G(D))$  is the lowest, i.e.,  $G(D)$  is minimal.

## 2.3 Convolutional encoders for UEP

For a convolutional code  $C$ , we define that *free distance* of  $C$  is the minimum distance between codewords of  $C$ , denoted by  $d_{free}$ . Since a convolutional code is a linear code, hence if  $c_1$  and  $c_2$  are two codewords in  $C$ , then  $c_1 + c_2$  is also a codeword in  $C$ . Suppose a generator matrix  $G(D)$  generate a convolutional code, and let two information vector  $u_1(D)$  and  $u_2(D)$  is encoded by  $G(D)$  such that  $u_1(D)G(D) = y_1(D)$ , and  $u_2(D)G(D) = y_2(D)$ , where  $y_1(D)$



and  $y_2(D)$  are correspondent codeword vectors. So we find that :

$$\begin{aligned}
d_{free} &= \min_{u_1(D), u_2(D)} (w(y_1(D) + y_2(D)) : u_1(D) \neq u_2(D)) \\
&= \min_{u(D)} (w(y(D)) : u(D) \neq 0) \\
&= \min_{u(D)} (w(u(D)G(D)) : u(D) \neq 0),
\end{aligned}$$

where  $w(y_1(D) + y_2(D))$  means weight of  $y_1(D) + y_2(D)$ . So  $d_{free}$  is the minimum weight of nonzero codewords. Similarly to the free distance, the UEP capability of a convolutional code can be described by the separation vector defined as follows:

**Definition 5** Let  $C$  be an  $(n, k)$  convolutional code over finite field  $F$ . The separation vector of  $G(D)$  is defined as  $s(G(D)) = (s(G(D))_1, s(G(D))_2, \dots, s(G(D))_k)$ , where

$$s(G(D))_i = \min_{I(D)} \{w(I(D)G(D)) | I_i(D) \neq 0\},$$

$\forall 1 \leq i \leq k$  and  $I(D) = (I_1(D), I_2(D), \dots, I_k(D))$  is the input information bits with  $I_l(D) \in F(D), \forall 1 \leq l \leq k$ .

By above definition, the minimum of  $s(G(D))_i, \forall 1 \leq i \leq k$ , is the free distance of the convolutional code. Besides, let the  $i$ -th information sequence  $I_i(D)$  fed into the  $i$ -th input of the encoder, at high signal-to-noise ratios (SNR) a large value of  $s(G(D))_i$  implies a small bit-error-rate (BER) [14]. Hence different values of  $s(G(D))_i$  will make the different BER. Hence we can use  $G(D)$  for UEP as long as the data of distinct BER requirements are fed into  $G(D)$ .

We define two vectors  $\mathbf{a} = (a_1, a_2, \dots, a_k)$  and  $\mathbf{b} = (b_1, b_2, \dots, b_k)$  are comparable if  $a_i \geq b_i$  or  $a_i \leq b_i$  for  $i = 1, \dots, n$ , denoted by  $\mathbf{a} \geq \mathbf{b}$  or  $\mathbf{a} \leq \mathbf{b}$ . For an  $(n, k)$  convolutional code  $C$ , if  $G(D)$  has the greatest separation vector among all generator matrices, then we call  $G(D)$  is an *optimal* generator matrix. So we give a formal definition of the optimal generator matrices as follows:

**Definition 6** For a convolutional code  $C$ ,  $G(D)$  is called an optimal generator matrix if and only if for any other generator matrix  $G'(D)$ , there exists a permutation  $\psi$  such that  $s(G(D)) \geq \psi(s(G'(D)))$ .

Consider a set of vectors  $\mathbf{X} = \{\mathbf{x}_1(D), \mathbf{x}_2(D), \dots\}$ , where  $\mathbf{x}_i(D) \in F(D)^n$  for all  $i$ , we denote

$$\langle \mathbf{X} \rangle = \left\{ \sum_i a_i(D) \mathbf{x}_i(D) : a_i(D) \in F(D) \right\}$$

as the vectors space of all linear combinations of elements in  $\mathbf{X}$ . Given a convolutional code  $C$  with a generator matrix  $G(D)$ . Also we denote  $C^\rho = \{c(D) : \forall c(D) \in C, w(c(D)) < \rho\}$ . There is a theorem about the necessary and sufficient conditions for optimal generator matrices as follows:

**Theorem 6** [18] For a convolutional code  $C$ , define  $w(C) = \{w(c(D)) : \forall c(D) \in C\}$ . A generator matrix  $G(D)$  is optimal if and only if

$$\forall \rho \in w(C), \exists X(D) \subseteq G(D) \text{ such that } \langle C^\rho \rangle = \langle X(D) \rangle,$$

where  $X(D) \subseteq G(D)$  means that all rows of  $X(D)$  are contained in  $G(D)$ .

Authors in [18] proved that for every convolutional code, there always exists an optimal generator matrix to generate the code. To find an optimal generator matrix, we define a class of generator matrices, which are called *monotonically weight retaining* matrices below.

**Definition 7** A generator matrix  $G(D)$  for an  $(n, k)$  convolutional code  $C$  is said to be *monotonically weight retaining* matrix if and only if

$$w[\langle g_i(D) \rangle] = w[C \setminus \langle g_1(D), g_2(D), \dots, g_{i-1}(D) \rangle], \text{ for } 1 \leq i \leq k.$$

Also from this definition we define a generator matrix to be weight retaining if it is contained from a monotonically weight retaining matrix. The weight retaining matrices have been proved to have some properties, which are shown in Theorem 7.

**Theorem 7** [18] *Let  $G(D)$  be a generator matrix for an  $(n, k)$  convolutional code  $C$ . Then the following statements are equivalent.*

(1)  $G(D)$  is a weight retaining matrix for  $C$ .

(2) Given any other generator matrix  $A(D)$  with rows  $\{a_1(D), a_2(D), \dots, a_k(D)\}$  for  $C$ ,

$$\sum_{i=1}^k w[\langle g_i(D) \rangle] \leq \sum_{i=1}^k w[\langle a_i(D) \rangle].$$

(3)  $s(G(D)) = (w[\langle g_1(D) \rangle], w[\langle g_2(D) \rangle], \dots, w[\langle g_k(D) \rangle])$ .

Hence by Theorem 7, we can find that an optimal generator matrix is also a weight retaining generator matrix. Authors in [18] also proved that every retaining matrix for an  $(n, k)$  convolutional code  $C$  is an optimal generator matrix for  $C$ . Hence by this property, they provide Procedure 1 to obtain a weight retaining matrix PGM for a given convolutional code, and hence is optimal.



**Procedure 1** [18]

**Step 1** Given an  $(n, k)$  convolutional code  $C$ .

**Step 2** Choose a polynomial codeword  $c(D) \in C \setminus \langle g_1(D), g_2(D), \dots, g_{i-1}(D) \rangle$  such that

$$w(c(D)) = w[C \setminus \langle g_1(D), g_2(D), \dots, g_{i-1}(D) \rangle].$$

**Step 3** Set  $g_i(D) = c(D)$ .

**Step 4** If  $i < k$ , then replace  $i = i + 1$  and go to Step 2, else go to next step.

**Step 5** Set  $G(D)$  be the generator matrix with rows  $g_1(D), g_2(D), \dots, g_k(D)$ , which will be the desired optimal generator matrix of  $C$ .

In order to achieve UEP performance, we should use optimal generator for encoding. It is proved that two optimal generator matrices are related by *effectively lower-triangular* matrix, which is defined as:

**Definition 8** Let  $G(D)$  be a generator matrix of an  $(n, k)$  convolutional code  $C$ . Without loss of generality (W.L.O.G), suppose  $s(G(D))$  is in the nondecreasing order and has  $\alpha$  different component values, each with  $\beta_i$  repetitions for  $1 \leq i \leq \alpha$ . For a  $k \times k$  matrix  $T(D)$  over  $F(D)$ , let  $t_{u,v}(D)$  be the entry in the position  $(u,v)$  of  $T(D)$  for all  $1 \leq u, v \leq k$ .  $T(D)$  is called effectively lower-triangular with respect to  $G(D)$  if and only if  $t_{u,v}(D) = 0$  for all  $\sum_{l=1}^{i-1} \beta_l < u \leq \sum_{l=1}^i \beta_l$ ,  $v > \sum_{l=1}^i \beta_l$ , and  $1 \leq i \leq \alpha$ .

For example, if  $s(G(D)) = (1, 2, 2, 2, 3, 3)$ , then the effectively lower - triangular matrix with respect to  $G(D)$  is of the form:

$$T(D) = \begin{pmatrix} \times & & & & & & \\ \times & \times & \times & & & & \\ \times & \times & \times & & & & \\ \times & \times & \times & & & & \\ \times & \times & \times & \times & \times & \times & \\ \times & \times & \times & \times & \times & \times & \times \end{pmatrix}.$$

So from above, we introduced this theorem as follows:

**Theorem 8** [18] Given an  $(n, k)$  convolutional code  $C$ , W.L.O.G, let  $G(D)$  be an optimal generator matrix of nondecreasing separation vector. For any  $k \times k$  nonsingular matrix  $T(D)$ ,  $T(D)G(D)$  is optimal if and only if  $T(D)$  is effectively lower - triangular with respect to  $G(D)$ .

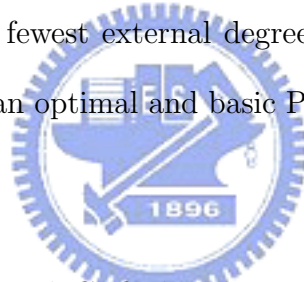
From this result, we can produce many optimal generator matrices if we can get any one optimal generator matrix. Among all of them, we will focus on a special optimal generator matrix for our study, which is optimal and basic. Suppose a convolutional code  $C$  is generated by a polynomial optimal generator matrix  $G(D)$ , and let separation vector  $s(G(D))$  be in decreasing order. From Theorem 2, we know that it can be decomposed by the Smith-Algorithm such that  $G(D) = W(D)\Gamma(D)V(D)$ . Let  $W(D)\Gamma(D) = \Psi(D)$ , we can find that

$$G(D) = \Psi(D)V(D) = \begin{pmatrix} \gamma_{11}(D) & 0 & \dots & 0 & 0 & \dots & 0 \\ \gamma_{21}(D) & \gamma_{22}(D) & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ \gamma_{k1}(D) & \gamma_{k2}(D) & \dots & \gamma_{kk}(D) & 0 & \dots & 0 \end{pmatrix} V(D),$$

where  $\gamma_{ij} \in F[D]$  for  $1 \leq i \leq k$  and  $1 \leq j \leq i$ . And we denote that  $G_b(D)$  is the first  $k$  rows of  $V(D)$ , hence we find that  $G(D) = \Psi_k(D)G_b(D)$ , where  $\Psi_k(D)$  is the first  $k$  columns of  $\Psi(D)$ . Since  $\Psi_k(D)$  is a lower triangular matrix hence  $\Psi_k^{-1}(D)$  is also a lower triangular matrix. Hence  $G_b(D) = \Psi_k^{-1}(D)G(D)$ , and by Theorem 8, we can get that  $G_b(D)$  and  $G(D)$  have the same separation vector, so  $G_b(D)$  is also optimal. Since they generate the same convolutional code  $C$ , and since  $V(D)$  is unimodular, we know that there exists a polynomial matrix  $V^{-1}(D)$  such that  $V(D)V^{-1}(D) = I$ . Hence there exist a polynomial right inverse  $G_b^{-1}(D)$  which is formed as the  $k$  columns of  $V^{-1}(D)$ , such that  $G_b(D)G_b^{-1}(D) = I$ . So  $G_b(D)$  is basic and optimal. By this property, we can obtain a basic and optimal generator matrix.

Since external degree of a generator matrix  $G(D)$  is the degree of its direct-form realizations. Hence reducing the external degree as smallest as possible will makes the circuits easier. To get an optimal generator with fewest external degree and guarantee noncatastrophic, we can use Procedure 2 to obtaining an optimal and basic PGM with the lowest external degree.

**Procedure 2** [18]



**Step 1** Give an  $(n, k)$ convolutional  $C$ , find a generator matrix  $G(D)$  which is basic and optimal. Suppose  $g_i(D)$  is the rows of  $G(D)$  for  $1 \leq i \leq k$ , and separation  $s(G(D))$  is in nondecreasing order of  $\alpha$  distinct component value, each has  $\beta_i$  repetitions for all  $1 \leq i \leq \alpha$ .

**Step 2** Set  $l = 1$ ,  $C^* = \emptyset$ , and  $\hat{C}$  be the collection of all codewords whose degree is not more then  $\text{extdeg}(G(D))$ .

**Step 3** Choose  $\beta_l$  independent codewords, say  $c_1(D), c_2(D), \dots, c_{\beta_l}(D)$ , of the smallest sum of degree from  $\hat{C}$  which are independent to all codewords in  $C^*$  and satisfy the

following constraints:

$$\begin{pmatrix} c_1(D) \\ c_2(D) \\ \vdots \\ c_{\beta_i}(D) \end{pmatrix} = [\Gamma_{l,1}(D), \Gamma_{l,2}(D), \dots, \Gamma_{l,l}(D)] \begin{pmatrix} g_1(D) \\ g_2(D) \\ \vdots \\ g_{\sum_{r=1}^l \beta_r}(D) \end{pmatrix}$$

where  $\Gamma_{l,j}(D)$  is a  $\beta_i \times \beta_j$  matrix over  $F[D]$  for all  $1 \leq j \leq l$  and  $\Gamma_{l,l}(D)$  is unimodular.

**Step 4** Set  $C^* = C^* \cup \{c_1(D), c_2(D), \dots, c_{\beta_i}(D)\}$  and  $\hat{C} = \hat{C} \setminus \{c_1(D), c_2(D), \dots, c_{\beta_i}(D)\}$ .

**Step 5** If  $l < \alpha$ , then replace  $l$  by  $l + 1$  and go to Step 3; else go to the next step.

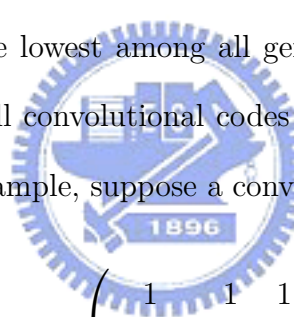
**Step 6** Set  $G^*(D)$  to be the generator matrix whose rows consist of all codewords in  $C^*$ , which will be the desired basic and optimal PGM of the smallest external degree.



## Chapter 3

# Lowest McMillan degree of polynomial encoders for UEP

In Chapter 2, we know that for a convolutional code  $C$ , there exists a generate matrix for which the  $\text{Mcdeg}(G(D))$  is the lowest among all generator matrices. But unfortunately, authors in [18] showed that not all convolutional codes can be generated by an optimal and minimal generator matrix. For example, suppose a convolutional code  $C$  can be generated by the canonical PGM


$$G_c(D) = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & D & 0 \\ 1+D & D & 0 & 0 \end{pmatrix},$$

which has  $s(G_c(D)) = (2, 2, 2)$  and  $\text{Mcdeg}(G_c(D)) = 2$ . By Procedure 1, we obtain an optimal PGM

$$G_o(D) = \begin{pmatrix} 0 & 1 & D & 0 \\ 1 & 0 & 0 & D^2 \\ 0 & 0 & 1 & 1+D \end{pmatrix},$$

which has  $s(G_o(D)) = (2, 2, 3)$ . As the result of [16], there are a finite number of minimal generator matrices for a given convolutional code. Hence calculating the separation vectors of all minimal generator matrices for  $C$ , we find that there are no minimal generator matrices that have separation vectors equal to  $(2, 2, 3)$ . So there are no minimal and optimal generator matrices which can generate  $C$ . In the following we based on some theorems to find an optimal PGM with the lowest  $\text{Mcdeg}(G(D))$ .

### 3.1 Smith decomposition on PGMs over the field $F[D^{-1}]$

Similar to the definition of polynomials, a Laurent series has the form  $A(D^{-1}) = a_{-m}D^{-m} + a_{-m+1}D^{-m+1} + \dots + a_0$  is called an anti-polynomial and has degree  $m$ , denoted by  $\deg(A(D^{-1}))$ . The set of all anti-polynomials is denoted by  $F[D^{-1}]$ . Hence an anti-polynomial series is just a polynomial series in  $D^{-1}$ . We denote  $F((D^{-1}))$  to be a field with all one-sided anti-Laurent series, which are one-sided Laurent series in  $D^{-1}$ . The rational subfield of  $F((D^{-1}))$  consists of all rational anti-Laurent series, which are rational Laurent series in  $D^{-1}$ , and is denoted by  $F(D^{-1})$ . For two anti-polynomials  $A(D^{-1})$  and  $B(D^{-1})$ , we say that  $A(D^{-1})$  is divisible by  $B(D^{-1})$  if there exists an anti-polynomial  $C(D^{-1})$  such that  $A(D^{-1})C(D^{-1}) = B(D^{-1})$ , and denoted by  $A(D^{-1}) \mid B(D^{-1})$ . For example,  $D^{-2}$  is divisible by  $D^{-5}$  since  $D^{-2} \cdot D^{-3} = D^{-5}$ , so we have  $D^{-2} \mid D^{-5}$ .

We will introduce two types of given generator matrix. Let  $G(D)$  be a PGM for a given  $(n, k)$  convolutional code  $C$ . Suppose  $\rho =$  the maximum degree of  $g_{ij}(D)$ , where  $g_{ij}(D)$  means the  $i$ -th row and the  $j$ -th column entry of  $G(D)$ . We write  $G(D)$  as a matrix over  $F(D^{-1})$  as follows:

$$G(D) = (g_{ij}(D))_{i,j} = (D^\rho \left( \frac{g_{ij}(D)}{D^\rho} \right))_{i,j} = D^\rho G_{-1}(D^{-1}) \quad (1.1)$$

where

$$G_{-1}(D^{-1}) = (D^{-\rho} g_{ij}(D))_{i,j} \quad (1.2)$$

is a matrix of polynomial in  $D^{-1}$ ,  $\forall 1 \leq i \leq k$ , and  $\forall 1 \leq j \leq n$ . If we use  $z^{-1}$  to replace  $D$  in (1.1), then we get a matrix like the transfer function form as follows:

$$G(z^{-1}) = (z^{-\rho} \left( \frac{g_{ij}(z^{-1})}{z^{-\rho}} \right))_{i,j} = z^{-\rho} P(z) \quad (1.3)$$

where  $P(z)$  is a polynomial matrix in  $z$ . By the Smith-Algorithm on  $P(z)$ , we can decompose  $P(z)$  as  $P(z) = V(z)\Phi(z)W(z)$ , where  $V(z)$  and  $W(z)$  are  $k \times k$  and  $n \times n$  unimodular matrices, respectively, and  $\Phi(z)$  is a  $k \times n$  diagonal matrix whose diagonal entries are invariant factors of  $P(z)$ . So we can decompose  $G(z^{-1})$  as  $G(z^{-1}) = V(z)z^{-\rho}\Phi(z)W(z) = V(z)\Lambda(z)W(z)$ , where



$\Lambda(z)$  is a diagonal matrix with the  $i$ -th diagonal entry  $\lambda_i(z) = \alpha_i(z)/\beta_i(z)$ , and

$$(\alpha_i(z), \beta_i(z)) = 1, \text{ and } \alpha_i(z) | \alpha_{i+1}(z), \beta_{i+1}(z) | \beta_i(z), \text{ for } \forall 1 \leq i \leq k, \quad (1.4)$$

where  $(\alpha_i(z), \beta_i(z))$  is g.c.d of  $\alpha_i(z)$  and  $\beta_i(z)$ . It is the so-called *Smith-McMillan* decomposition, and it is proved that the McMillan degree  $\mu$  of  $G(z^{-1})$  is  $\sum_{i=1}^k \deg(\beta_i(z))$  [17], i.e., the sum of denominator polynomial degree of invariant factors. Replace  $z$  by  $D^{-1}$  in  $G(z^{-1})$ ; then we have generator matrix of the form as (1.1). Similar way we use the Smith-Algorithm on  $G_{-1}(D^{-1})$  with field  $F(D^{-1})$  to decompose  $G_{-1}(D^{-1}) = V_{-1}(D^{-1})\Phi_{-1}(D^{-1})W_{-1}(D^{-1})$ , where

$$V_{-1}(D^{-1}) = V(z)|_{z=D^{-1}}, \quad \Phi_{-1}(D^{-1}) = \Phi(z)|_{z=D^{-1}}, \quad W_{-1}(D^{-1}) = W(z)|_{z=D^{-1}}.$$

Hence  $G(D)$  has a Smith-McMillan decomposition as  $G(D) = V_{-1}(D^{-1})D^\rho\Phi_{-1}(D^{-1})W_{-1}(D^{-1}) = V_{-1}(D^{-1})\Lambda_{-1}(D^{-1})W_{-1}(D^{-1})$ , where  $\Lambda_{-1}(D^{-1})$  is a  $k \times k$  diagonal matrix with diagonal entries  $\lambda_i(D^{-1}) = \alpha_i(D^{-1})/\beta_i(D^{-1})$ , and

$$(\alpha_i(D^{-1}), \beta_i(D^{-1})) = 1, \text{ and } \alpha_i(D^{-1}) | \alpha_{i+1}(D^{-1}), \beta_{i+1}(D^{-1}) | \beta_i(D^{-1}), \text{ for } \forall 1 \leq i \leq k. \quad (1.5)$$

So we can calculate McMillan degree  $\mu$  of  $G(D)$  as  $\mu = \sum_{i=1}^k \deg(\beta_i(D^{-1}))$ , and we conclude it as follows :

**Theorem 9** [5] *Let  $G(D)$  be a  $k \times n$  generator matrix, and have invariant factors  $\lambda_i(D^{-1})$  with respect to  $F(D^{-1})$ , for  $i = 1, \dots, k$ . Assume that  $\lambda_i(D^{-1}) = \alpha_i(D^{-1})/\beta_i(D^{-1})$  with no common factors, where  $\alpha_i(D^{-1})$  and  $\beta_i(D^{-1})$  are polynomials in  $D^{-1}$ . Then McMillan degree  $\mu = \sum_{i=1}^k \deg(\beta_i(D^{-1}))$ .*

**Example 3** Suppose

$$G(D) = \begin{pmatrix} D & 0 & D \\ 1 & 1+D & 1 \end{pmatrix}.$$

Since maximum degree of entries is 1, we can get

$$G(D) = \frac{1}{D^{-1}} \begin{pmatrix} 1 & 0 & 1 \\ D^{-1} & 1+D^{-1} & D^{-1} \end{pmatrix}.$$

Hence by the Smith-McMillan decomposition with respect to the field  $F(D^{-1})$ , we get

$$G(D) = \begin{pmatrix} 1 & 0 \\ D^{-1} & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{D^{-1}} & 0 & 0 \\ 0 & \frac{1+D^{-1}}{D^{-1}} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We use  $z^{-1}$  to replace  $D$  in  $G(D)$ , so we get

$$G(z^{-1}) = \begin{pmatrix} z^{-1} & 0 & z^{-1} \\ 1 & 1+z^{-1} & 1 \end{pmatrix}.$$

Again use the Smith-McMillan decomposition with respect to the field  $F(z)$  we can get

$$G(z^{-1}) = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{z} & 0 & 0 \\ 0 & \frac{1+z}{z} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Comparing this two types generator matrices, we can find that this is only different from the choice of indeterminate. Hence we get that McMillan degree of  $G(D)$  is 2.

In [9], Johannesson and Wan proved some degree properties as listed in Lemma 1 and Theorem 10:



**Lemma 1** [9] *Let the finite field  $F = GF(2)$ , and let  $f_1(D), f_2(D), \dots, f_l(D) \in F[D]$  with  $\text{g.c.d}(f_1(D), f_2(D), \dots, f_l(D)) = 1$ . Suppose  $f = \max\{\deg(f_i(D)) \mid i = 1, 2, \dots, l\}$ . Then for  $m \geq f$ ,  $D^{-m}f_1(D), D^{-m}f_2(D), \dots, D^{-m}f_l(D) \in F[D^{-1}]$  and*

$$(D^{-m}f_1(D), D^{-m}f_2(D), \dots, D^{-m}f_l(D)) = D^{-(m-f)}.$$

**Theorem 10** [9] *Let  $G(D)$  be a basic encoding matrix and let  $r$  and  $s$  be maximum degree of its  $k \times k$  minors and  $(k-1) \times (k-1)$  minors, respectively. Then the  $k$ -th invariant factor of  $G(D)$  regarded as a matrix over  $F(D^{-1})$  is  $\frac{1}{D^{-(r-s)}}$ , where the finite field  $F = GF(2)$ .*

We will generalize this lemma and theorem and give proofs; then use this result to get  $\Lambda_{-1}(D^{-1})$  by invariant form of  $G(D)$ , and then we can calculate  $\text{Mcdeg}(G(D))$  directly without decompose them by the Smith-McMillan decomposition.

**Lemma 2** Let  $F$  be a finite field, and let  $f_1(D), f_2(D), \dots, f_l(D) \in F[D]$  with  $\text{g.c.d}(f_1(D), f_2(D), \dots, f_l(D)) = \Delta(D)$ . Suppose  $f = \max\{\deg(f_i(D)) \mid i = 1, 2, \dots, l\}$ , and let  $f_i(D) = D^{\omega_i} g_i(D)$ ,  $i = 1, \dots, l$ , where  $g_i(D)$  is a delay-free polynomial. Also let

$$\omega = \min(\omega_1, \omega_2, \dots, \omega_l), \quad \eta = \min\{\deg(g_i(D)) \mid i = 1, 2, \dots, l\}.$$

Then for  $m \geq f$ ,  $D^{-m} f_1(D), D^{-m} f_2(D), \dots, D^{-m} f_l(D) \in F[D^{-1}]$ , and

$$(D^{-m} f_1(D), D^{-m} f_2(D), \dots, D^{-m} f_l(D)) = D^{-(m-f)} D^{-\eta} \Delta(D) D^{-\omega}.$$

**Proof:** Since  $f_i(D) = D^{\omega_i} g_i(D)$ ,  $\forall 1 \leq i \leq l$ , it follows that  $(g_1(D), g_2(D), \dots, g_l(D)) = \Delta(D)/D^\omega$ . Hence for  $m \geq f$ ,

$$\begin{aligned} D^{-m} f_i(D) &= D^{-m} D^{\omega_i} g_i(D) \\ &= D^{-(m-\omega_i-\deg(g_i(D)))} (D^{-\deg(g_i(D))} g_i(D)) \\ &= D^{-(m-\deg(f_i(D)))} (D^{-\deg(g_i(D))} g_i(D)), \end{aligned}$$

where the last equation follows from the fact that  $\deg(f_i(D)) = \omega_i + \deg(g_i(D))$ ,  $i=1, 2, \dots, l$ .

Since  $g_1(D), g_2(D), \dots, g_l(D)$  are delay-free polynomials, it follows that

$$\begin{aligned} (D^{-\deg(g_1(D))} g_1(D), D^{-\deg(g_2(D))} g_2(D), \dots, D^{-\deg(g_l(D))} g_l(D)) &= D^{-\eta} (g_1(D), g_2(D), \dots, g_l(D)) \\ &= D^{-\eta} \Delta(D) / D^\omega \\ &= D^{-\eta} \Delta(D) D^{-\omega}. \end{aligned}$$

Therefore, we get that

$$\begin{aligned} &(D^{-m} f_1(D), D^{-m} f_2(D), \dots, D^{-m} f_l(D)) \\ &= (D^{-(m-\deg(f_1(D)))} (D^{-\deg(g_1(D))} g_1(D)), \dots, D^{-(m-\deg(f_l(D)))} (D^{-\deg(g_l(D))} g_l(D))) \\ &= D^{-(m-f)} (D^{-\deg(g_1(D))} g_1(D), \dots, D^{-\deg(g_l(D))} g_l(D)) \\ &= D^{-(m-f)} D^{-\eta} \Delta(D) D^{-\omega}, \end{aligned}$$

and the proof is completed. ■

**Example 4** Let  $f_1(D) = D^2 + D^3 + D^5$ ,  $f_2(D) = D^3 + D^4 + D^6$ ,  $f_3(D) = D^3 + D^5 + D^6 + D^7$ . Hence we know that  $(f_1(D), f_2(D), f_3(D)) = D^2 + D^3 + D^5 = D^2(1 + D + D^3)$ , and  $\max(\deg(f_1(D)), \deg(f_2(D)), \deg(f_3(D))) = 7$ . Suppose  $f_1(D) = D^2(1 + D + D^3) = D^{\omega_1}g_1(D)$ ,  $f_2(D) = D^3(1 + D + D^3) = D^{\omega_2}g_2(D)$ , and  $f_3(D) = D^3(1 + D)(1 + D + D^3) = D^{\omega_3}g_3(D)$ . We can find that  $\min(\omega_1, \omega_2, \omega_3) = 2$ , and  $\min(\deg(g_1), \deg(g_2), \deg(g_3)) = 3$ . Therefore, for any  $m \geq 7$ , W.L.O.G, let  $m = 8$ , it follows that

$$\begin{aligned}
& (D^{-8}f_1(D), D^{-8}f_2(D), D^{-8}f_3(D)) \\
&= (D^{-3} + D^{-5} + D^{-6}, D^{-2} + D^{-4} + D^{-5}, D^{-1} + D^{-2} + D^{-3} + D^{-5}) \\
&= D^{-1}(1 + D^{-2} + D^{-3}) \\
&= D^{-(8-7)}D^{-3}(D^2 + D^3 + D^5)D^{-2}.
\end{aligned}$$

**Theorem 11** Let  $F$  be a finite field. Suppose  $G(D)$  be a  $k \times n$  polynomial encoding matrix and let  $m_i$  be the maximum degree of  $i \times i$  minors of  $G(D)$ ,  $\forall 1 \leq i \leq k$ . Suppose  $i$ -th invariant factor of  $G(D)$  is  $\gamma_i(D)$ , and  $d_i$  is the number makes  $\gamma_i(D)$  become delay-free, that is,  $\gamma_i(D) = D^{d_i}\gamma'_i(D)$ ,  $\gamma'_i(D) \neq 0$ , and let  $\theta_i = \deg(\gamma'_i(D))$ . Then the  $i$ -th invariant factor of  $G(D)$  regarded as a matrix over  $F(D^{-1})$  is  $D^{-\theta_i}\gamma_i(D)D^{-d_i}/D^{-(m_i-m_{i-1})}$ .

**Proof:** Let  $G(D)$  has entries  $g_{ij}(D)$ , for  $\forall 1 \leq i \leq k, \forall 1 \leq j \leq n$ , and  $w = \max(\deg(g_{ij}(D)))$ .

Write  $G(D)$  as a matrix over  $F[D^{-1}]$  as follows:

$$G(D) = D^w G_{-1}(D^{-1}), \quad (1.6)$$

where  $G_{-1}(D^{-1})$  is a matrix of polynomial in  $D^{-1}$  as we mentioned in (1.1). Suppose all  $i \times i$  minors of  $G(D)$  are  $f_1(D), f_2(D), \dots, f_l(D) \in F[D]$ , and let the g.c.d of  $i \times i$  minors is  $\Delta_i(D)$ , in other words,  $\Delta_i(D) = (f_1(D), f_2(D), \dots, f_l(D))$ . Similarly,  $\Delta_{i-1}(D) = (q_1(D), q_2(D), \dots, q_t(D))$ , where  $q_i(D) \in F[D]$  are all  $(i-1) \times (i-1)$  minors of  $G(D)$ ,  $\forall 1 \leq i \leq t$ , and  $\Delta_{i-1}(D)$  is the g.c.d of  $(i-1) \times (i-1)$  minors of  $G(D)$ . Also, let  $d_i$  and  $d_t$  be

the numbers that make  $\Delta_i(D)$  and  $\Delta_{i-1}(D)$  delay-free, respectively, i.e.,

$$\begin{cases} \Delta_i(D) &= D^{d_i} \Delta'_i(D), \\ \Delta_{i-1}(D) &= D^{d_{i-1}} \Delta'_{i-1}(D), \end{cases}$$

where  $\Delta'_i(D)$  and  $\Delta'_{i-1}(D)$  are delay-free polynomials. Let  $\theta_i = \deg(\Delta'_i(D))$  and  $\theta_{i-1} = \deg(\Delta'_{i-1}(D))$ .

Since an  $i \times i$  minor of  $G_{-1}(D^{-1})$  is equal to the corresponding  $i \times i$  minor of  $G(D)$  multiplied by  $D^{-wi}$ . It is trivial that any degree of  $i \times i$  minor of  $G(D)$  is less or equal than  $w \cdot i$ . Hence we get that  $w \cdot i \geq m_i$ , by Lemma 2, we have

$$\begin{aligned} \Delta_i(G_{-1}(D^{-1})) &= (D^{-wi} f_1(D), D^{-wi} f_2(D), \dots, D^{-wi} f_l(D)) \\ &= D^{-(wi-m_i)} D^{-\theta_i} \Delta_i(D) D^{-d_i}, \end{aligned}$$

where  $\Delta_i(G_{-1}(D^{-1}))$  means g.c.d of  $i \times i$  minor of  $G_{-1}(D^{-1})$ . Similarly,  $\Delta_{i-1}(G_{-1}(D^{-1})) = D^{-(w(i-1)-m_{i-1})} D^{-\theta_{i-1}} \Delta_{i-1}(D) D^{-d_{i-1}}$ . Thus the  $i$ -th invariant of  $G_{-1}(D^{-1})$  is

$$\frac{\Delta_i(G_{-1}(D^{-1}))}{\Delta_{i-1}(G_{-1}(D^{-1}))} = \frac{D^{-(wi-m_i)} D^{-\theta_i} \Delta_i(D) D^{-d_i}}{D^{-(w(i-1)-m_{i-1})} D^{-\theta_{i-1}} \Delta_{i-1}(D) D^{-d_{i-1}}} = \frac{D^{-w}}{D^{-(m_i-m_{i-1})}} D^{-\theta_i} \gamma_i(D) D^{-d_i}, \quad (1.7)$$

where  $d_i$  is the integer making  $\gamma_i(D)$  delay-free, i.e.,  $D^{-d_i} \gamma_i(D) = \gamma'_i(D)$  and  $\theta_i = \deg(\gamma'_i(D))$ .

From (1.6) and (1.7), it follows that the  $i$ -th invariant factor of  $G(D)$  regarded as a matrix over  $F(D^{-1})$  is

$$D^w \cdot \frac{D^{-w}}{D^{-(m_i-m_{i-1})}} D^{-\theta_i} \gamma_i(D) D^{-d_i} = \frac{D^{-\theta_i} \gamma_i(D) D^{-d_i}}{D^{-(m_i-m_{i-1})}}. \quad (1.8)$$

■

By Theorem 11, suppose a  $k \times n$  PGM  $G(D)$  with the  $i$ -th invariant factor  $\gamma_i(D)$ ,  $\forall 1 \leq i \leq k$ ; then it can be decomposed by the Smith-Algorithm over field  $F(D^{-1})$  as  $G(D) =$

$$V_{-1}(D^{-1}) \Gamma_{-1}(D^{-1})$$

$W_{-1}(D^{-1})$ , where  $\Gamma_{-1}(D^{-1})$  is of the form:

$$\begin{bmatrix} \frac{D^{-\theta_1} \gamma_1(D) D^{-d_1}}{D^{-(m_1)}} & & & 0 & \dots & 0 \\ & \frac{D^{-\theta_2} \gamma_2(D) D^{-d_2}}{D^{-(m_2-m_1)}} & & \vdots & & \vdots \\ & & \ddots & & & \\ & & & & & 0 \dots 0 \\ & & & & \frac{D^{-\theta_k} \gamma_k(D) D^{-d_k}}{D^{-(m_k-m_{k-1})}} & 0 \dots 0 \end{bmatrix}.$$

Note that  $m_0 = 0$ , and  $d_i$  is the number makes  $\gamma_i(D)$  become delay-free and  $\theta_i = \deg(D^{-d_i}\gamma_i(D))$ ,  $\forall 1 \leq i \leq k$ . Also, degree of denominator of  $\Gamma_{-1}(D^{-1})$ 's entries only depends on  $m_i - m_{i-1}$ ,  $\forall 1 \leq i \leq k$ . By Theorem 9, we know that McMillan degree of  $G(D) = (m_0 - m_1) + (m_2 - m_1) + \cdots + (m_k - m_{k-1})$ . If  $m_i - m_{i-1} < 0$ , for some index  $i$ ,  $D^{-(m_i - m_{i-1})}$  will have positive degree in denominator of  $\Gamma_{-1}(D^{-1})$ 's entries, and hence we will not add it when calculating McMillan degree of  $G(D)$ . So it follows that

**Corollary 1** Suppose  $G(D)$  is a  $k \times n$  PGM for a convolutional code  $C$ , then we can get its McMillan degree  $\mu$  as  $\mu = \sum_{i=1}^k (m_i - m_{i-1})^+$  without decomposing by the Smith-McMillan algorithm where

$$(m_i - m_{i-1})^+ = \max\{m_i - m_{i-1}, 0\}$$

From Corollary 1, we can prove the first inequality of degree equation (2.5).

**Corollary 2** Let  $G(D)$  be a polynomial generator matrix for a given convolutional code  $C$ . Suppose  $\text{Mcdeg}(G(D))$  is  $\mu$ , then  $\text{intdeg}(G(D)) \leq \mu \leq \text{extdeg}(G(D))$ .

**Proof:** We have explained about the last inequality, and now we give proof for the first inequality. By (1.5), we can find that for any  $k \times n$  PGM  $G(D)$  with the maximum degree of  $i \times i$  minors  $m_i$ ,  $\forall 1 \leq i \leq k$ ,

$$D^{m_k - m_{k-1}} | D^{m_{k-1} - m_{k-2}}, D^{m_{k-1} - m_{k-2}} | D^{m_{k-2} - m_{k-3}}, \dots, D^{m_2 - m_1} | D^{m_1}. \quad (1.9)$$

Hence we know that

$$m_1 \geq m_2 - m_1 \geq \cdots \geq m_{k-1} - m_{k-2} \geq m_k - m_{k-1}. \quad (1.10)$$

Let  $\mu - m_k = m_1 + (m_2 - m_1)^+ + \cdots + (m_k - m_{k-1})^+ - m_k$ , where  $m_k$  is the maximum degree of  $k \times k$  minors of  $G(D)$ , that is, internal degree of  $G(D)$ . So

**Case 1.** If  $m_k - m_{k-1} \geq 0$ . Hence from (1.10) we know that  $m_i - m_{i-1} \geq 0$ ,  $\forall 1 \leq i \leq k$ . So

$$\mu - m_k = m_k - m_k = 0, \text{ we get that } \mu = m_k.$$

**Case 2.** If  $m_j - m_{j-1} < 0$  and  $m_i - m_{i-1} \geq 0, \forall 1 \leq i \leq j - 1, \forall 2 \leq j \leq k$ . Hence from

$$(1.10) \text{ we know that } m_t - m_{t-1} < 0, \forall j \leq t \leq k. \text{ So we have } \mu - m_k = m_{j-1} - m_k = (m_{j-1} - m_j) + (m_j - m_{j+1}) + \cdots + (m_{k-1} - m_k) > 0. \text{ Hence, we get that } \mu > m_k.$$

By above, we conclude that for a PGM  $G(D)$ ,  $\text{intdeg}(G(D)) \leq$  McMillan degree  $\mu$ , the equality holds only if  $m_k \geq m_{k-1}$ . ■

By Corollary 2, we know that if  $m_k - m_{k-1} \geq 0$ , then  $m_1, (m_2 - m_1), \dots, (m_k - m_{k-1})$  will be non-negative integers, and hence McMillan degree

$$\mu = \sum_{i=1}^k (m_i - m_{i-1})^+ = m_1 + (m_2 - m_1)^+ + \cdots + (m_k - m_{k-1})^+ = m_k = \text{intdeg}(G(D)). \quad (1.11)$$

We know that when we realize every  $k \times n$  generator matrix, we can describe this circuit with the so-called state space description, W.L.O.G,  $(A, B, C, \bar{D})$ , where the four matrices  $A, B, C$ , and  $\bar{D}$  have entries in  $F$  and has dimensions  $m \times m, k \times m, m \times n$ , and  $k \times n$ , respectively, and the integer  $m$  is the degree of the realization. For a convolutional code  $C$ , there are so many generator matrices can generate  $C$ , and all of them have a minimal realization. Since we work with finite field  $F$ , we can find that among these minimal realization, state matrices  $A$  with dimension  $m$  are finite. It follows that minimal realizations with degree  $m$  are finite. From (2.5), we know that all PGM  $G(D)$  can be realized with the fewest degree equal to  $\text{intdeg}(G(D))$ . By Theorem 1, if  $G(D)$  is a  $k \times n$  basic polynomial generator matrix with  $\text{intdeg}(G(D)) = a$ , then  $T(D)G(D)$  has  $\text{intdeg}(T(D)G(D)) = a + b$  where  $T(D)$  is any nonsingular  $k \times k$  matrix with  $\det(T(D))$  has degree  $b$ . Hence by (1.11), if  $U(D)$  is a unimodular matrix such that  $U(D)T(D)G(D)$  has  $m_k \geq m_{k-1}$ , where  $m_k$  and  $m_{k-1}$  means maximum degree of  $k \times k$  and  $(k-1) \times (k-1)$  minors of  $U(D)T(D)G(D)$ , then we can realize  $U(D)T(D)G(D)$  with delay elements  $a + b$ . Hence we conclude below:

**Corollary 3** *Suppose  $G(D)$  is a basic generator matrix of a convolutional code  $C$ , and let  $\text{intdeg}(G(D)) = a$ . Suppose a nonsingular matrix  $T(D)$  with determinant has degree  $b$ . If*

there is a unimodular matrix  $U(D)$  such that  $U(D)T(D)G(D)$  has  $m_k \geq m_{k-1}$ , where  $m_k$  and  $m_{k-1}$  means the maximum degrees of  $k \times k$  and  $(k-1) \times (k-1)$  minors of  $U(D)T(D)G(D)$ , then there exists a realization with  $a + b$  delay elements.

A rational polynomial generator matrix  $G(D)$  for a given convolutional code  $C$  can also be realized. For example, let

$$G(D) = \begin{pmatrix} 1 & 0 & \frac{1}{1+D} & \frac{D}{1+D} \\ 0 & 1 & \frac{D}{1+D} & \frac{1}{1+D} \end{pmatrix}.$$

There are at least two physical realizations of  $G(D)$  which are shown in Figure 3.1.

We can find that although the circuit may contain feedback loop, there exists a realization which has the fewest degree. Hence for a given convolutional code  $C$ , there are many rational generator matrices, and each one has their own minimal realization. We will use similar way to calculate a McMillan degree of a rational generator matrix.

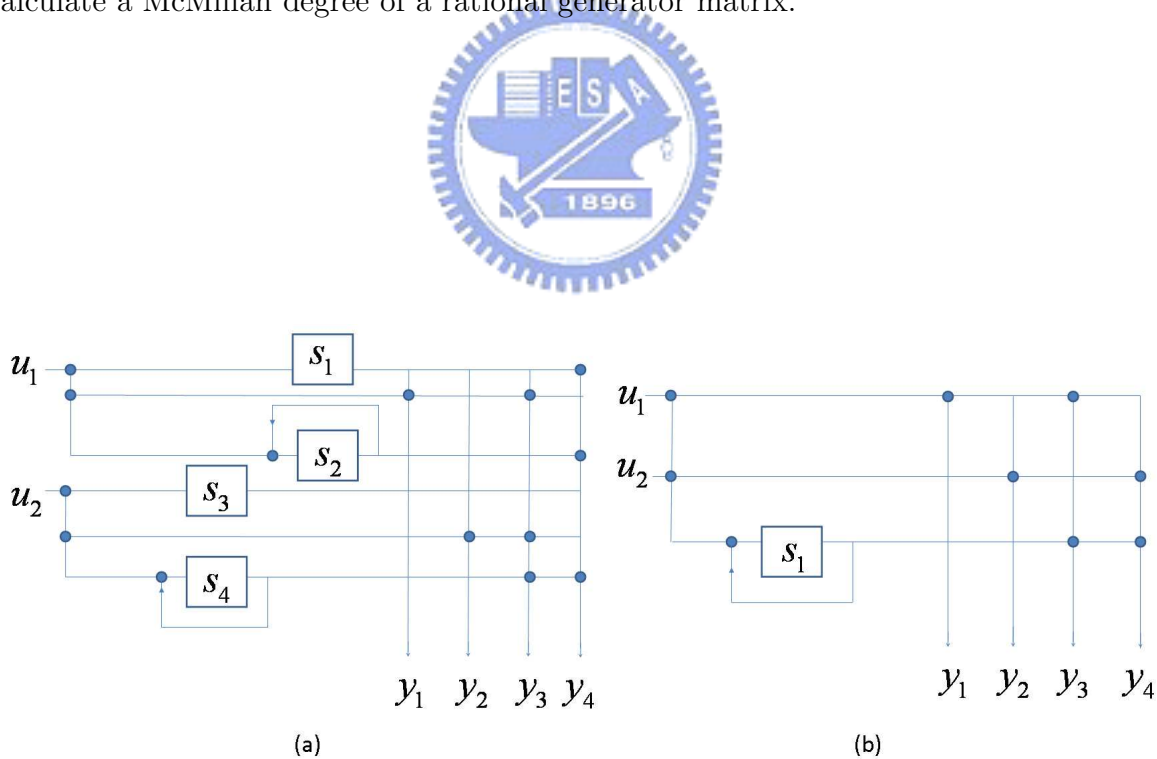


Figure 3.1: (a) A physical realization of rational  $G(D)$ , (b) minimal realization of rational  $G(D)$ .



### 3.2 Smith-McMillan decomposition on rational polynomial generator matrices over $F(D^{-1})$

If  $G(D)$  is a  $k \times n$  rational polynomial generator matrix. Suppose  $L(D)$  is l.c.m of denominator of  $g_{ij}(D)$ , where  $g_{ij}(D)$  is the entries of  $G(D)$ ,  $\forall 1 \leq i \leq k$  and  $\forall 1 \leq j \leq n$ . Then we get that

$$\frac{1}{L(D)}G_p(D) = G(D),$$

where  $G_p(D)$  is a polynomial generator matrix. Let  $G_p(D)$  have a invariant factor decomposition  $G_p(D) = A_{-1}(D^{-1})\widehat{\Gamma}_{-1}(D^{-1})B_{-1}(D^{-1})$  with field  $F[D^{-1}]$ , and suppose the invariant factors are  $\widehat{\gamma}_{-1}(D^{-1})$ ,  $\forall 1 \leq i \leq k$ . Suppose degree of  $L(D)$  is  $d$ , then we divided  $\frac{1}{L(D)}$  by  $D^d$  on both numerator and denominator. Hence we get a rational polynomial  $\frac{D^{-d}}{L'(D^{-1})}$ , whose numerator and denominator are polynomials in  $D^{-1}$ . So it follows that

$$\frac{D^{-d}}{L'(D^{-1})}G_p(D) = \frac{D^{-d}}{L'(D^{-1})}A_{-1}(D^{-1})\widehat{\Gamma}_{-1}(D^{-1})B_{-1}(D^{-1}) = A_{-1}(D^{-1})\Lambda'_{-1}(D^{-1})B_{-1}(D^{-1}),$$

where  $\Lambda'_{-1}(D^{-1})$  is a  $k \times n$  diagonal matrix with diagonal entries  $\lambda'_i(D^{-1}) = \widehat{\gamma}_{-1}(D^{-1})\frac{D^{-d}}{L'(D^{-1})}$ ,  $\forall 1 \leq i \leq k$ . Let  $\lambda'_i(D^{-1}) = \alpha'_i(D^{-1})/\beta'_i(D^{-1})$  with  $(\alpha'_i(D^{-1}), \beta'_i(D^{-1})) = 1$ , where  $\alpha'_i(D^{-1})$  and  $\beta'_i(D^{-1})$  are both polynomial in  $D^{-1}$ , and  $\alpha'_i(D^{-1})|\alpha'_{i+1}(D^{-1})$ ,  $\beta'_{i+1}(D^{-1})|\beta'_i(D^{-1})$ . Hence we get the Smith-McMillan decomposition of  $G(D) = A_{-1}(D^{-1})\Lambda'_{-1}(D^{-1})B_{-1}(D^{-1})$ , and from Theorem 9, we know that  $\text{Mcdeg}(G(D)) = \sum_{i=1}^k \text{deg}(\beta'_i(D^{-1}))$

**Example 5** Let

$$G(D) = \begin{pmatrix} 1 & 0 & \frac{1}{1+D} & \frac{D}{1+D} \\ 0 & 1 & \frac{D}{1+D} & \frac{1}{1+D} \end{pmatrix}.$$

So we get  $L(D) = 1 + D$ , and it follows that

$$G(D) = \frac{1}{1+D} \begin{pmatrix} 1+D & 0 & 1 & D \\ 0 & 1+D & D & 1 \end{pmatrix}.$$

Hence we decompose the last polynomial matrix in  $F[D^{-1}]$ , we get

$$\begin{pmatrix} 1+D & 0 & 1 & D \\ 0 & 1+D & D & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ D^{-1} & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{D^{-1}} & 0 & 0 & 0 \\ 0 & \frac{1+D^{-1}}{D^{-1}} & 0 & 0 \end{pmatrix} \begin{pmatrix} 1+D^{-1} & 0 & D^{-1} & 1 \\ D^{-1} & 1 & 1+D^{-1} & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Therefore, it follows that

$$\begin{aligned} G(D) &= \frac{D^{-1}}{1+D^{-1}} \begin{pmatrix} 1 & 0 \\ D^{-1} & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{D^{-1}} & 0 & 0 & 0 \\ 0 & \frac{1+D^{-1}}{D^{-1}} & 0 & 0 \end{pmatrix} \begin{pmatrix} 1+D^{-1} & 0 & D^{-1} & 1 \\ D^{-1} & 1 & 1+D^{-1} & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ D^{-1} & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{1+D^{-1}} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1+D^{-1} & 0 & D^{-1} & 1 \\ D^{-1} & 1 & 1+D^{-1} & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \end{aligned}$$

Hence we get an invariant factor decomposition of  $G(D)$  in  $F(D^{-1})$ , and we can calculate  $\text{Mcdeg}(G(D)) = 1$ , and the realization was shown in Figure 3.1(b).

### 3.3 The least degree encoder for UEP with the non-catastrophic property

We will use the result proved in Section 3.1 to illustrate that there exist an optimal generator matrix with the fewest McMillan degree, and we also guarantee that it is noncatastrophic. Let  $G(D)$  be a  $k \times n$  PGM with  $\text{intdeg}(G(D)) = \kappa$ . Suppose  $G'(D) = A(D)G(D)$ , where

$$A(D) = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & D \end{pmatrix} = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & D \end{pmatrix}. \quad (3.12)$$

By theorem 1, since all  $k \times k$  submatrices of  $A(D)G(D)$  are just the  $k \times k$  submatrices of  $G(D)$ , each multiplied by  $A(D)$ . Hence  $\text{intdeg}G'((D)) = \text{intdeg}(A(D)G(D)) = 1 + \kappa$ , and it

is a method to increase internal degree of  $G(D)$ . By Theorem 4, we know that a PGM is noncatastrophic if and only if the g.c.d of  $k \times k$  minors of  $G(D)$  is a power of  $D$ . Hence if  $G(D)$  is noncatastrophic, then g.c.d of  $k \times k$  minors is  $D^i$ , for some  $i$ . Multiplied by  $A(D)$ , we get  $G'(D) = A(D)G(D)$  has g.c.d of  $k \times k$  minors is  $D^{i+1}$ , hence it is noncatastrophic. Also, if  $U(D)$  is an unimodular matrix, then  $U(D)A(D)G(D)$  is noncatastrophic since  $k \times k$  minors of  $U(D)A(D)G(D) = \det(U(D)) \cdot \det(A(D)) \cdot (k \times k)$  minors of  $G(D)$ , we find that  $U(D)A(D)G(D)$  is also a noncatastrophic generator matrix.

We can use Theorem 11 to find an optimal generator matrix with lowest McMillan degree. By Procedure 2, we can obtain an optimal and basic generator matrix  $G(D)$  for any convolutional code  $C$ . By Theorem 1 and Theorem 8, we know that if  $T(D)$  is unimodular and effectively lower-triangular matrix with respect to  $G(D)$ , then  $T(D)G(D)$  is optimal and  $\text{intdeg}(G(D)) = \text{intdeg}(T(D)G(D))$ . Since  $G(D)$  is basic, so it has the lowest internal degree. By Corollary 1, we know that  $\text{Mcdeg}(G(D)) = \sum_{i=1}^k (m_i - m_{i-1})^+$ , where  $m_i$  is maximum degree of all  $i \times i$  minors. It implies that  $\text{Mcdeg}(G(D)) \geq m_1$ , that is,  $\text{Mcdeg}(G(D))$  is not less than the degree of all entries of  $G(D)$ .

Suppose a  $k \times n$  generator matrix  $G(D)$  with  $\text{intdeg}(G(D)) = \kappa$ , and let  $G_T(D) = T(D)G(D)$  where  $T(D)$  is a effectively lower-triangular matrix with respect to  $G(D)$ . If  $m_1$  of  $G_T(D)$  is greater than  $\kappa$ , it implies that  $\text{Mcdeg}(G_T(D))$  is not equal to  $\kappa$ , that is,  $m_k < m_{k-1}$ . Since we work with finite field  $F$ , suppose  $F = GF(q)$ , we know that the numbers of  $G_T(D)$  with  $m_1$  of  $G_T(D) < \kappa$  at most  $q^{\kappa n k}$  because every entry of  $G_T(D)$  is of the form  $q_0 + q_1 D + \dots + q_\kappa D^\kappa$ , where  $q_i \in F$ ,  $\forall 1 \leq i \leq \kappa$ . If two matrices  $T_1(D)$  and  $T_2(D)$  such that  $T_1(D)G(D) = T_2(D)G(D) = G_T(D)$  has  $m_1 < \kappa$ , it implies that  $T_1(D) = T_2(D)$ . Hence there are finite number matrices  $T(D)$  such that  $m_1$  of  $G_T(D)$  is less or equal to  $\kappa$ . Among all these matrices  $T(D)$ , if there is no any  $T(D)$  such that  $G_T(D) = T(D)G(D)$  with  $m_k \geq m_{k-1}$ , where  $m_k$  and  $m_{k-1}$  means maximum degree of  $G_T(D)$  of  $k \times k$  minors and  $(k-1) \times (k-1)$  minors respectively, it means that there is no such PGM with McMillan

degree equal to internal degree, i.e., no minimal PGMs with the optimality. Then we multiply  $G(D)$  by  $A(D)$ , which is shown in (3.12), to increase internal degree by 1 such that  $\text{intdeg}(A(D)G(D)) = \kappa + 1$ . Suppose  $G'(D) = A(D)G(D)$ , and let  $G'_{T'}(D) = T'(D)G'(D)$ , where  $T'(D)$  is unimodular and effectively lower-triangular with respect to  $G'(D)$ . Similarly, the numbers of  $G'_{T'}(D)$  with  $m_1$  of  $G'_{T'}(D) < \kappa + 1$  at most  $q^{(\kappa+1)nk}$  because every entry of  $G'_{T'}(D)$  is of the form  $q_0 + q_1D + \dots + q_{\kappa+1}D^{\kappa+1}$ , where  $q_i \in F, \forall 1 \leq i \leq \kappa + 1$ . Hence there are finite matrices  $T'(D)$  such that  $m_1$  of  $G'_{T'}(D)$  is less or equal to  $\kappa + 1$ . Hence the same way among these  $T'(D)$ , if there is a PGM  $T'(D)G'(D)$  with  $m'_k \geq m'_{k-1}$ , where  $m'_k$  and  $m'_{k-1}$  means maximum degree of  $T'(D)G'(D)$  of  $k \times k$  minors and  $(k-1) \times (k-1)$  minors respectively. It means that this PGM  $G'_{T'}(D) = T'(D)G'(D)$  has McMillan degree equal to  $\kappa + 1$  and is optimal, else keep going on that add 1 to internal degree and do the same thing again. Since we can not find any optimal generator matrix with McMillan degree equal to  $\kappa$ , so we know that  $G'_{T'}(D)$  is optimal PGM with lowest McMillan degree. Also, since  $G(D)$  is basic, hence it is noncatastrophic. So it follows that the optimal PGM with lowest McMillan degree we searched has the noncatastrophic property.

**Example 6** Suppose a convolutional code  $C$  generated by

$$G(D) = \begin{pmatrix} 0 & 1 & D & 0 \\ 1 & 0 & 0 & D^2 \\ 0 & 0 & 1 & 1 + D \end{pmatrix}$$

is an optimal and basic generator matrix with separation  $s(G(D)) = (2, 2, 3)$ , and has internal degree 2. For any  $k \times k$  matrix  $T(D)$  which is unimodular and effective-lower triangular with respect to  $G(D)$ , we can not find any  $T(D)G(D)$  such that  $m_3 \geq m_2$ , where  $m_3$  and  $m_2$  is maximum degree of  $T(D)G(D)$  of  $3 \times 3$  minors and  $2 \times 2$  minors respectively. So there are no optimal generator matrices with minimality. We multiply  $G(D)$  by  $A(D)$  such that

$$G'(D) = A(D)G(D) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & D \end{pmatrix} \begin{pmatrix} 0 & 1 & D & 0 \\ 1 & 0 & 0 & D^2 \\ 0 & 0 & 1 & 1 + D \end{pmatrix} = \begin{pmatrix} 0 & 1 & D & 0 \\ 1 & 0 & 0 & D^2 \\ 0 & 0 & D & D + D^2 \end{pmatrix}.$$

Hence  $G'(D)$  has internal degree 3. Since  $I(D)G(D)$  has  $m_3 = 3 \geq m_2 = 3$ , where  $I(D)$  is an identity matrix and hence a unimodular and effectively-lower triangular matrix. So it follows that  $G'(D)$  is an optimal PGM with lowest McMillan degree degree 3, and is noncatastrophic. Figure 3.2 shows the realization of  $G'(D)$ .

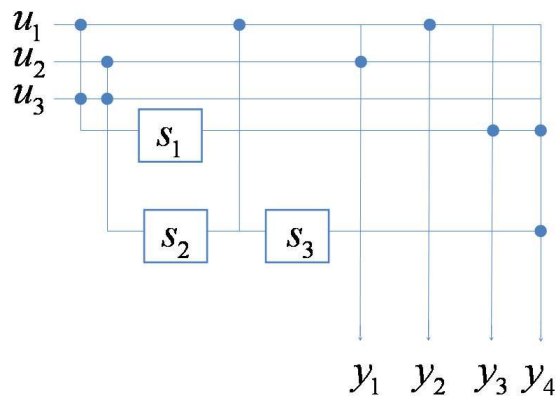


Figure 3.2: A minimal realization of optimal PGM  $G'(D)$  for convolutional code  $C$ .



# Chapter 4

## Optimal PGMs with the lowest McMillan degree

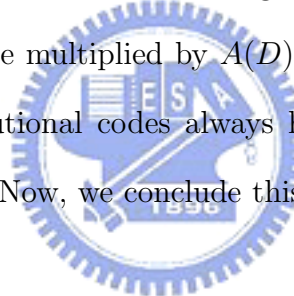
We now give a way to find an polynomial optimal PGM with the fewest McMillan degree which is also noncatastrophic. Suppose  $G_c(D)$  is a canonical generator matrix for a given convolutional code  $C$ . By Procedure 2, we can obtain an optimal and basic generator matrix  $G_o(D)$ , and let  $\text{intdeg}(G_o(D)) = \kappa$ . As we mentioned in Section 3.3, we know that any PGM  $G(D)$  has  $\text{Mcdeg}(G(D)) \geq m_1$ , where  $m_1$  is maximum degree of  $1 \times 1$  minors of  $G(D)$ . Hence if there is a nonsingular matrix  $T(D)$  such that  $m_1$  of  $T(D)G_o(D)$  is greater than  $\kappa$ , then  $\text{Mcdeg}(T(D)G_o(D)) > \kappa$ . Let  $\Pi = \{\forall U(D) : m_1 \text{ of } U(D)G_o(D) \leq \kappa\}$ , where  $U(D)$  an unimodular and effectively lower-triangular matrix respect to  $G_o(D)$ . We have explained that since we work with finite field  $F$ , there are finite matrices in  $\Pi$ . By Corollary 2, we know that for a PGM  $G(D)$ ,  $\text{intdeg}(G(D)) \leq \text{Mcdeg}(G(D))$ , the equality holds when  $m_k$  of  $G(D) \geq m_{k-1}$  of  $G(D)$ .

Hence if there is a matrix  $U_{el}(D) \in \Pi$  such that  $U_{el}(D)G_o(D)$  has  $m_k \geq m_{k-1}$ , where  $m_i$  is maximum degree of  $i \times i$  minor of  $U_{el}(D)G_o(D)$  for  $i = k - 1, k$ . It implies that  $\text{Mcdeg}(U_{el}(D)G_o(D)) = \text{intdeg}(U_{el}(D)G_o(D)) = \kappa$ , and hence it is minimal and optimal. If there does not exist a PGM  $U_{el}(D)G(D)$  with  $m_k \geq m_{k-1}$ , it means that there are no PGMs with optimal and minimal property. Then let  $G_o(D)$  be multiplied by  $A(D)$ , where  $A(D)$  is a

$k \times k$  diagonal matrix as follows:

$$A(D) = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & D \end{pmatrix}.$$

Suppose  $G_A(D) = A(D)G_o(D)$ , and we know that  $\text{intdeg}(G_A(D)) = \kappa + 1$ . Then again search all generator matrices  $U_{elA}(D)G_A(D)$  with  $U_{elA}(D) \in \Pi_A$ , where the collection  $\Pi_A = \{U_A(D) : m_1 \text{ of } U_A(D)G_A(D) \leq \kappa + 1\}$  and  $U_A(D)$  is an unimodular and effectively lower-triangular matrix respect to  $G_A(D)$ . Similarly, there are finite number of matrices in  $\Pi_A$ , if there exists a generator matrix  $U_{elA}(D)G_A(D)$  with  $m_k$  of  $U_{elA}(D)G_A(D) \geq m_{k-1}$  of  $U_{elA}(D)G_A(D)$ , then it is an optimal PGM with the lowest McMillan degree  $\kappa + 1$ , and as we mentioned, it is noncatastrophic; else let  $G_A(D)$  be multiplied by  $A(D)$  again and recursive searching again. Since by Procedure 2, all convolutional codes always have an optimal and basic generator matrix, hence the work will stop. Now, we conclude this as below:



### **Procedure 3**

**Step 1** Give an  $(n, k)$  convolutional  $C$ , by Procedure 2 we obtain a generator matrix  $G(D)$  which is basic and optimal. Set  $\text{intdeg}(G(D)) = \kappa$ ,  $i = 0$ .

**Step 2** Let  $A_i(D)$  be a  $k \times k$  diagonal matrix:

$$A_i(D) = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & D^i \end{pmatrix}$$

Set  $\Pi_i = \{U(D) : m_1 \text{ of } U(D)A_i(D)G(D) \leq \kappa + i\}$ , where  $U(D)$  is an unimodular and effectively lower-triangular matrix respect to  $A_i(D)G(D)$ . Check all  $U_{el}(D)A_i(D)G(D)$  with  $U_{el}(D) \in \Pi_i$ , if there exist a PGM  $U_{el}(D)A_i(D)G(D)$  with  $m_k$  of  $U_{el}(D)A_i(D)G(D) \geq m_{k-1}$

of  $U_{el}(D)A_i(D)G(D)$ , then go to Step 4; else go to next step.

**Step 3** Set  $i = i+1$ , and go back to Step 2.

**Step 4** Set  $G^*(D) = U_{el}A_i(D)G(D)$ , and it is a desired optimal PGM which is noncatastrophic and has the lowest McMillan degree  $\kappa + i$ .

Also, we can conclude that for any  $(n, 1)$  and  $(n, 2)$  convolutional codes, there exists an generator matrix with the optimal and minimal property to generate these codes:

**Theorem 12** *For any  $(n, 1)$  and  $(n, 2)$  convolutional codes, there always exist generator matrices which are both optimal and minimal.*

**Proof:** Since  $(n, 1)$  code is a trivial case, we give a simple proof for  $(n, 2)$  code. Suppose  $G(D)$  is a generator matrix of a given  $(n, 2)$  convolutional code. Then by Procedure 3, we first obtain an optimal and basic generator matrix from  $G(D)$ , say  $G_b(D)$ . Since  $G_b(D)$  is a  $2 \times n$  generator matrix, we can find that any  $2 \times 2$  minor has greater degree than any  $1 \times 1$  minor, hence  $m_2 \geq m_1$ . From (1.11), we know that  $G_b(D)$  has  $\text{Mcdeg}(G_b(D)) = \text{intdeg}(G(D))$ . Since  $G_b(D)$  is basic, it has the lowest internal degree, hence  $G_b(D)$  is an optimal and minimal generator matrix. ■

Hence, for  $(n, 1)$  and  $(n, 2)$  convolutional codes, we can obtain an optimal and minimal generator matrix by Procedure 3, and of course is noncatastrophic. Moreover, there are some convolutional codes can be generated by an optimal PGM which is obtained by Procedure 3, and we conclude that it has the lowest McMillan degree among all optimal generator matrices.

**Theorem 13** *For an  $(n, k)$  convolutional code  $C$  with  $k \geq 3$ , suppose  $G(D)$  is an optimal generator matrix where the separations are of the same value. Then there exists an optimal and minimal generator matrix for  $C$ .*

**Proof:** It is a trivial case since the optimal generator matrix  $G(D)$  has the separations are all the same, hence the effectively lower-triangular matrix with respect to  $G(D)$  is a nonsingular



matrix. So all generator matrices for  $C$  is optimal, hence we can obtain a minimal and optimal generator matrix for  $C$ . ■

**Theorem 14** *For an  $(n, k)$  convolutional codes  $C$  with  $k \geq 3$ , suppose  $C$  can be generated by an optimal and basic generator matrix with the lower external degree  $G_b(D)$ , where  $G_b(D)$  has the separations of the form*

$$s(G_b(D)) = (\alpha, \dots, \alpha, \beta)$$

*for some positive integers  $\alpha$  and  $\beta$  with  $\alpha < \beta$ ; the first  $k - 1$  separations of  $G_b(D)$  are the same and the last separation is greater than the first  $k - 1$  separations. And suppose every row of  $G_b(D)$  has only one row degree position. Then among all optimal generator matrices, there exists an optimal PGM with the lowest McMillan degree for  $C$ .*

**Proof:** By Procedure 2, we can always obtain an optimal and basic generator matrix  $G_b(D)$  with the lowest external degree for  $C$ . Suppose  $G_b(D)$  has  $k$  rows, denoted by  $g_{b,i}(D)$ ,  $\forall 1 \leq i \leq k$ , and let  $m_k$  of  $G_b(D)$  be  $\delta$  and  $m_{k-1}$  of  $G_b(D)$  be  $\nu$ . By Corollary 2, if  $\delta \geq \nu$ , then  $G_b(D)$  is a minimal and optimal PGM. Suppose  $\delta < \nu$ . If  $G_b(D)$  is reduced, then  $G_b(D)$  is canonical and hence is minimal. It is a contradiction that  $\delta < \nu$ . Hence  $G_b(D)$  is not reduced and of course is not canonical. Since  $G_b(D)$  has the lowest external degree among all optimal and basic PGMs, the submatrix which consists of the first  $k - 1$  rows of  $G_b(D)$  forms a canonical generator matrix for the supercode spanned by  $g_{b,1}, g_{b,2}, \dots, g_{b,k-1}$ , denoted by  $G_{s_1}(D)$ . And since  $G_b(D)$  is not reduced, if  $g_{b,k}(D)$  has greater degree in some position than the degree of any one of the first  $k - 1$  rows in the same position, it will be reduced until it is not greater than them.

Also, we can find that  $\nu$  is the sum of row degrees of  $g_{b,i}(D)$ ,  $\forall 1 \leq i \leq k - 1$ . Suppose  $\nu$  is determined from one of the  $(k - 1) \times (k - 1)$  minors which are obtained from  $g_{b,k}(D)$  and  $k - 2$  rows of  $G_{s_1}(D)$ , W.L.O.G, let the omitted row be  $g_{b,j}(D)$  for some  $j$  and let this submatrix is denoted by  $G_{s_2}(D)$ . It follows that although  $G_{s_1}(D)$  is reduced,  $G_{s_2}(D)$  has larger internal degree. Hence  $g_{b,k}(D)$  has greater degree in some position than the degree of  $g_{b,j}(D)$  in the

same position. So we can reduce the row degree of  $g_{b,k}(D)$  by  $G_{b,j}(D)$  until they have the same degree in this position, but it is a contradiction that  $g_{b,k}(D)$  has less row degree in some position than the row degree of  $g_{b,j}(D)$  in the same position.

In this way we will find that  $\nu$  can be determined from  $G_{s_1}(D)$ . Since  $G_{s_1}(D)$  is canonical,  $\nu$  is just the sum of its external degree. Hence when we want to realize  $G_b(D)$ , we need at least  $\nu$  delay elements to realize the canonical submatrix. By Procedure 3, we multiply  $G_b(D)$  by  $A(D)$  as

$$A(D) = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & D^{\nu-\delta} \end{pmatrix}$$

such that  $A(D)G_b(D) = G_{Ab}(D)$ . So  $m_k$  of  $G_{Ab}(D) = \delta + (\nu - \delta) = \nu$ . Suppose  $G_{Ab}(D)$  has  $k$  rows  $g_{Ab,i}, \forall 1 \leq i \leq k$ . We can find that  $g_{b,i}(D) = g_{Ab,i}(D), \forall 1 \leq i \leq k-1$ , and the highest degree positions of  $g_{b,k}(D)$  and  $g_{Ab,k}(D)$  are the same. In other words,  $G_b(D)$  and  $G_{Ab}(D)$  have the same indicator matrix, which is defined in Theorem 5. Hence if  $g_{Ab,k}(D)$  has greater degree in some position than the degree of any one of the first  $k-1$  rows of  $G_{Ab}(D)$  in the same position, we can reduce it by these  $k-1$  rows until  $g_{Ab,k}(D)$  has less degrees than the degrees of the first  $k-1$  rows of  $G_{Ab}(D)$  in the same positions. It follows that there exists an unimodular and effectively lower-triangular matrix  $U(D)$  of the form:

$$U(D) = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ \times & \times & \dots & \times & 1 \end{pmatrix}$$

such that  $U(D)G_{Ab}(D)$  has the degree of the last row is not greater than the row degrees of the first  $k-1$  row of  $U(D)G_{Ab}(D)$ , where the entries marked  $\times$  are some possible polynomials. So the  $m_{k-1}$  of  $U(D)G_{Ab}(D)$  is  $\nu$ , and since  $U(D)$  is an unimodular matrix, hence  $\text{intdeg}(G_{Ab}(D)) = \text{intdeg}(U(D)G_{Ab}(D)) = \nu$ . It implies that  $U(D)G_{Ab}(D)$  has  $m_k = m_{k-1}$ . By Corollary 2, we

know that  $\text{intdeg}(U(D)G_{Ab}(D)) = \text{Mcdeg}(U(D)G_{Ab}(D)) = \nu$ . Since we at least need  $\nu$  delay elements to realize the optimal generator matrices for  $C_2$ , we conclude that  $U(D)G_{Ab}(D)$  is the optimal PGM with the lowest McMillan degree among all optimal generator matrices. ■

By Procedure 3, we can get an optimal PGM  $G(D)$  with the lowest McMillan degree, however, we can not guarantee that there is no rational optimal generator matrix whose McMillan degree is less than  $\text{Mcdeg}(G(D))$ . Hence, we will give another way to obtain a optimal generator matrix with the lowest McMillan degree from the different idea. Suppose  $G(D)$  is a minimal generator matrix with  $\text{Mcdeg}(G(D)) = m$  for an  $(n, k)$  convolutional code  $C$ , and its minimal realization has the state space description  $(A, B, C, \bar{D})$  with dimensions  $m \times m$ ,  $k \times m$ ,  $m \times n$ , and  $k \times n$ , respectively. Then if we work with the field  $F = GF(q)$ , there are  $q^{mk} \prod_{i=0}^{k-1} (q^k - q^i)$  minimal generator matrices, whose minimal realizations are different. Also suppose  $(A, B, C, \bar{D})$  and  $(A_1, B_1, C_1, D_1)$  are two minimal realizations of different minimal generator matrices, then there exists an  $m \times k$  matrix  $M$  and a nonsingular  $k \times k$  matrix  $N$  such that  $(A_1, B_1, C_1, D_1) = (A + MB, NB, C + M\bar{D}, N\bar{D})$  [2]. By this result, when we have a minimal realization with degree  $m$ , we can obtain all different minimal realizations with degree  $m$ . Hence we conclude as follows:

**Corollary 4** *For an  $(n, k)$  convolutional code  $C$ , let  $G_c(D)$  is a canonical generator matrix with  $\text{Mcdeg}(G_c(D)) = \mu$ . If the finite field  $F = GF(q)$ , then for  $i \geq 0$ , there are  $q^{(\mu+i)k} \prod_{j=0}^{k-1} (q^k - q^j)$  generator matrices which have different minimal realizations with degrees  $\mu + i$ .*

**Proof:** For  $i \geq 0$ , let

$$A_i(D) = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & D^i \end{pmatrix}$$

Since  $G_c(D)$  is a canonical generator matrix, so it is also a reduced generator matrix. Let  $A_i(D)G_c(D) = G_{A_i}(D)$ , then we have  $G_{A_i}(D)$  is a reduced matrix since the indicator matrices  $\bar{G}_{A_i}(D) = \bar{G}_c(D)$ , which is defined in Theorem 5. So  $\text{intdeg}(G_{A_i}(D)) = \text{Mcdeg}(G_{A_i}(D)) = \text{extdeg}(G_{A_i}(D)) = \mu + i$ . Suppose  $G_{A_i}(D)$  has a minimal realization with state space description  $(A_i, B_i, C_i, \bar{D}_i)$ , where matrix  $A_i$  has dimension  $\mu + i$ . Let  $G_{A_i}(D)$  has state space equation

$$\begin{aligned}\mathbf{s}(t+1) &= \mathbf{s}(t)A_i + \mathbf{u}(t)B_i \\ \mathbf{y}(t) &= \mathbf{s}(t)C_i + \mathbf{u}(t)\bar{D}_i\end{aligned}$$

where  $\mathbf{s}(t)$ ,  $\mathbf{x}(t)$ , and  $\mathbf{y}(t)$  are the state vector, input vector, and output vector at time  $t$ . By applying linear state variable feedback, we obtain a new state space description  $(A_i + M_i B_i, N_i B_i, C_i + M_i \bar{D}_i, N_i \bar{D}_i)$  from  $(A_i, B_i, C_i, \bar{D}_i)$  with a  $(\mu + i) \times k$  matrix  $M_i$  and a nonsingular  $k \times k$  matrix  $N_i$ , where the input is chosen as  $\mathbf{u}^*(t) = (\mathbf{u}(t) + \mathbf{s}(t)M)N^{-1}$  for some new input  $\mathbf{u}^*(t) \in F(D)^k$ . In other words, let  $G^*(D) = N_i \bar{D}_i + N_i B_i (D^{-1}I - A_i)^{-1} (C_i + M_i \bar{D}_i)$ , we have

$$y(D) = u(D)G_{A_i}(D) = u^*(D)G^*(D).$$

So  $G^*(D)$  is another generator matrix with McMillan degree  $\mu + i$ . By choosing different  $(\mu + i) \times k$  matrices  $M_i$ 's and nonsingular  $k \times k$  matrices  $N_i$ 's, we have all different state space descriptions  $(A_i + M_i B_i, N_i B_i, C_i + M_i \bar{D}_i, N_i \bar{D}_i)$ . Let the collection  $\Pi_i = \{G(D) | N_i \bar{D}_i + N_i B_i (D^{-1}I - A_i)^{-1} (C_i + M_i \bar{D}_i)\}$ , we obtain all generator matrices with McMillan degree  $\mu + i$ . Therefore, there are  $q^{(\mu+i)k} \prod_{j=0}^{k-1} (q^k - q^j)$  generator matrices with McMillan degrees  $m + i$ . ■

By Corollary 4, we obtain all generator matrices from a canonical generator matrix. And then we check all of them to obtain an optimal and noncatastrophic generator matrix with the lowest McMillan degree, as shown in Figure 4.1. Since by Procedure 2, all convolutional codes always have an optimal and basic generator matrix, hence we will obtain an optimal and noncatastrophic generator matrix with the lowest McMillan degree  $\mu + i$ . We conclude it as Procedure 4:

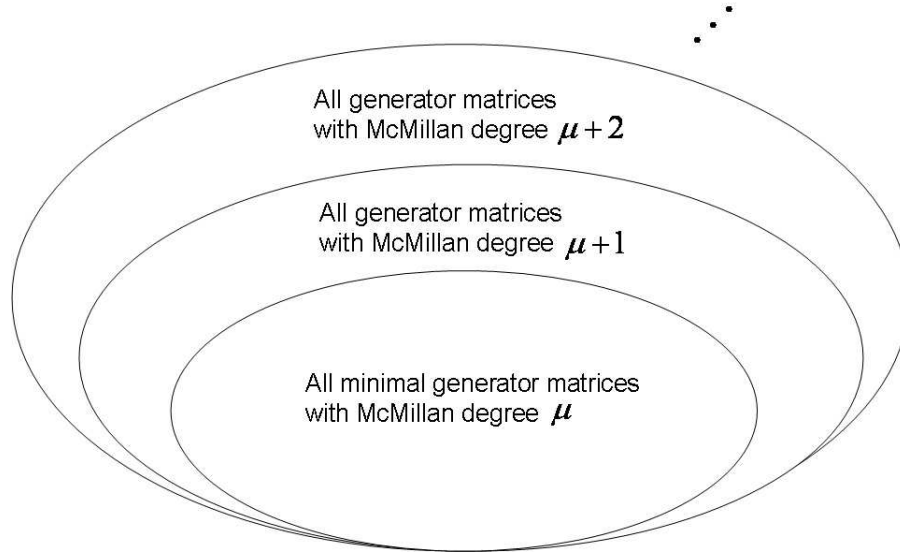


Figure 4.1: Sets of all generator matrices with equal McMillan degree.

**Procedure 4**

**Step 1** Give an  $(n, k)$  convolutional code  $C$ , first we construct a canonical generator matrix  $G_c(D)$  for  $C$ , and by Procedure 1, we also construct an optimal PGM  $G_o(D)$  for  $C$ . Set  $\text{Mcdeg}(G_c(D)) = \mu$ ,  $i = 0$ , and  $\hat{G}(D) = G_c(D)$ .

**Step 2** Set the minimal realization of  $\hat{G}(D)$  has state space description  $(A_i, B_i, C_i, \bar{D}_i)$ , and  $\Omega = \{G(D) | G(D) = N\bar{D}_i + NB_i(D^{-1}I - (A_i + MB_i))^{-1}(C_i + M\bar{D}_i)\}$ , where  $M$  is a  $(\mu + i) \times k$  arbitrary matrix and  $N$  is a  $k \times k$  nonsingular matrix. Check whether there exists a non-catastrophic  $G^*(D) \in \Omega$  such that  $T(D)G_o(D) = G^*(D)$ , where  $T(D)$  is an effectively lower-triangular matrix with respect to  $G_o(D)$ . If exists, then go to Step 4; else go to next step.

**Step 3** Set  $i = i + 1$ , let

$$A_i(D) = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & D^i \end{pmatrix}$$

Construct a new generator matrix  $\hat{G}(D) = A_i(D)G_c(D)$ , and go to Step 2.

**Step 4**  $G^*(D)$  is the desired generator matrix, which is optimal and noncatastrophic with

$\text{Mcdeg}(G^*(D)) = \mu + i$  is the lowest.

**Example 7** Suppose a convolutional code  $C$  can be generate by a canonical generator matrix

$G(D)$  as

$$G(D) = \begin{pmatrix} 1 & 0 & 1 \\ D & 1+D & 1+D \end{pmatrix}.$$

We find that  $\text{Mcdeg}(G(D))= 1$ . By Procedure 1, we obtain an optimal generator matrix

$G_o(D)$  as

$$G_o(D) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1+D & 0 \end{pmatrix},$$

with  $s(G_o(D)) = (2, 3)$ . By Procedure 3, we can obtain all minimal generator matrices of the

form  $G_m(D) = T(D)H(D)$ , where  $T(D)$  is one of six  $2 \times 2$  nonsingular scalar matrices over

$GF(2)$ , and  $H(D)$  is one of the following four generator matrices:

$$\left\{ \begin{array}{l} H_1(D) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1+D & 0 \end{pmatrix}, \\ H_2(D) = \begin{pmatrix} 1 & 0 & 1 \\ 1+D & 1+D & D \end{pmatrix}, \\ H_3(D) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & \frac{D}{1+D} \end{pmatrix}, \\ H_4(D) = \begin{pmatrix} 1 & 0 & 1 \\ \frac{1}{1+D} & 1 & 0 \end{pmatrix}. \end{array} \right.$$

Hence check all of them, we find that there are only 8 generator matrices which have the

optimal, minimal, and noncatastrophic properties as follows:

$$\begin{aligned} G_1(D) &= \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1+D & 0 \end{pmatrix}, G_2(D) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1+D & 1 \end{pmatrix} \\ G_3(D) &= \begin{pmatrix} 1 & 0 & 1 \\ 1+D & 1+D & D \end{pmatrix}, G_4(D) = \begin{pmatrix} 1 & 0 & 1 \\ D & 1+D & 1+D \end{pmatrix} \\ G_5(D) &= \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & \frac{D}{1+D} \end{pmatrix}, G_6(D) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & \frac{1}{1+D} \end{pmatrix} \\ G_7(D) &= \begin{pmatrix} 1 & 0 & 1 \\ \frac{1}{1+D} & 1 & 0 \end{pmatrix}, G_8(D) = \begin{pmatrix} 1 & 0 & 1 \\ \frac{D}{1+D} & 1 & 1 \end{pmatrix}. \end{aligned}$$

This is another way for obtaining an optimal and noncatastrophic generator matrix with lowest McMillan degree. Procedure 3 starts from a basic and optimal generator matrix, and Procedure 4 starts from a minimal generator generator matrix. Somehow Procedure 3 is also like the brute force, but this two procedures use different ideas. Procedure 4 is an easier way since when we use Procedure 4, we need to construct a minimal realization before every searching step because we want to get its state space description  $(A, B, C, \bar{D})$ . Although authors in [18] proposed that for a given convolutional code  $C$  they can from Procedure 2 to produce an optimal and basic generator matrix with lowest external degree, they can not guarantee that it has the lowest McMillan degree. For example, suppose a canonical generator matrix

$$G(D) = \begin{pmatrix} 1 & 1+D & 0 & 1 \\ 0 & 1 & 1+D^2 & 0 \\ 0 & 0 & 1 & 1+D \end{pmatrix}$$

with  $\text{intdeg}(G(D)) = \text{extdeg}(G(D)) = 4$  and  $s(G(D)) = (2,2,2)$ . By Procedure 2, we may get an optimal generator matrix with lowest external degree as

$$G^*(D) = \begin{pmatrix} 1 & 0 & 0 & D^4 \\ 0 & 1 & 1+D^2 & 0 \\ 0 & 0 & 1 & 1+D \end{pmatrix}$$

with  $\text{extdeg}(G^*(D)) = 7$ ,  $\text{Mcdeg}(G^*(D)) = 6$ , and  $s(G^*(D)) = (2,3,3)$ . But by Procedure 3, first, we construct a basic and optimal generator matrix  $G_b(D)$  as follows:

$$G_b(D) = \begin{pmatrix} 1 & 0 & 0 & D^4 \\ 1 & 1 & D^3 & 1+D+D^2 \\ 1 & 1 & 1+D^3 & D^2 \end{pmatrix},$$

with  $s(G_b(D)) = (2,3,3)$  and  $\text{intdeg}(G_b(D)) = 4$ . Second, check all matrices  $U(D)$  which are unimodular and effectively lower-triangular matrix with respect to  $G_b(D)$  and  $m_1$  of  $U(D)G_b(D) \leq 4$ . We find that there is a matrix  $U_{el}(D)$  such that

$$U_{el}(D)G_b(D) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1+D^3 & D^3 \\ 0 & 1 & 1 \end{pmatrix} G_b(D) = \begin{pmatrix} 1 & 0 & 0 & D^4 \\ 0 & 1 & 0 & 1+D+D^2+D^3 \\ 0 & 0 & 1 & 1+D \end{pmatrix},$$

where  $U_{el}(D)$  is unimodular and effectively lower-triangular matrix with respect to  $G_b(D)$  and  $m_1$  of  $U_{el}(D)G_b(D) \leq 4$ . Hence we conclude that  $U_{el}(D)G_b(D) = G'(D)$  is an optimal PGM with the McMillan degree 4. Although  $G'(D)$  has more external degree than  $G^*(D)$ , it has the lowest McMillan degree 4, and hence is minimal.





# Chapter 5

## Concluding remarks

Authors in [18] proved that for any convolutional code, there exists at least one optimal generator matrix. Furthermore, they use Procedure 1 as mentioned in Chapter 2 to obtain an optimal generator matrix for a given convolutional code. In order to reduce the complexity, and guarantee the noncatastrophic property, they also proposed the Procedure 2 to obtain an optimal and basic generator matrix with the lowest external degree. However, not all convolutional codes have the optimal and the minimal property at the same time. In this thesis, we first obtain a result in order that we are able to calculate the McMillan degree of a polynomial generator matrix without decomposing by the Smith-McMillan decomposition. From this result, we then explain why internal degree of  $G(D)$  is not greater than McMillan degree of  $G(D)$ , where  $G(D)$  is a PGM. Although Procedure 2 can produce an optimal and basic PGM with lowest external degree, it may not have the lowest McMillan degree. From this result we provide a procedure to obtain an optimal polynomial generator matrix with lowest McMillan degree. Unfortunately, although we can get an optimal PGM  $G(D)$  with the lowest  $\text{Mcdeg}(G(D))$ , we can not guarantee that there is no any rational generator matrix  $G'(D)$  which has  $\text{Mcdeg}(G'(D))$  less than  $\text{Mcdeg}(G(D))$ . In the future, we can also focus on how to find a minimal generator matrix with the greatest separation.

# Bibliography

- [1] I. M. Boyarinov and G. L. Katsman, "Liner unequal error protection codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 168-175, Mar. 1981.
- [2] B. W. Dickinson, "A new characterization of canonical convolutional encoders", *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 352-354, May 1976.
- [3] L. A. Dunning and W. E. Robbins, "Optimum encoding of linear block codes for unequal error protection," *Inform. Contr.*, vol. 37, pp.150-177, 1978.
- [4] E. K. Englund, "Nonlinear unequal error-protection codes are sometimes better than linear ones," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1418-1420, Sept. 1991.
- [5] G. D. Forney, Jr., "Convolutional Codes I: algebraic structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720-738, Nov. 1970.
- [6] G. D. Forney, Jr., "Structure analysis of convolutional codes via dual codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 512-518, July 1993.
- [7] W. J. van Gils, "Two topics on linear unequal error protection codes: Bounds on their length and cyclic code classes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 866-876, 1983.
- [8] G. L. Heide, and S. Gert, "State space realizations and monomial equivalence for convolutional codes," *Linear Algebra and its Application*, vol. 425, pp. 518-533, 2005.

- [9] R. Johannesson and Z. X. Wan, "A linear algebra approach to minimal convolutional encoders," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1219-1233 1993.
- [10] R. E. Kalman, "Irreducible realizations and the degree of a rational matrix," *SIAM J. Appl. Math.*, vol. 13, no.2, pp. 520-544, June 1965.
- [11] S Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, 2<sup>nd</sup> Ed., Prentice Hall, Englewood Cliffs, 1983.
- [12] B. Masnick and J. K. Worf, "On liner unequal error protection codes," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 600-607, July 1967.
- [13] R. H. Morelos-Zaragoza and H. Imai, "Binary multilevel convolutional codes with unequal error protection capabilities," *IEEE Trans. Commun.*, vol. 46, pp. 850-853, July 1998.
- [14] D. G. Mills and D.J. Costello, Jr., "Using a modified transfer function to calculate unequal error protection capabilities of convolutional codes, " in *Proc. 1993 IEEE Int. Symp. Inform. Theory*, San Antonio, TX, Jan. 1993, p. 144.
- [15] R. J. McEliece, "The algebraic theory of convolutional codes," in *Handbook of Coding Theory*, V. S Pless and W. C. Huffman eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 1065-1138.
- [16] J. L. Massey and M. K. Sain, "Inverses of linear sequential circuits," *IEEE Trans. Comput.*, vol. 17, pp. 330-337, April 1968.
- [17] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*, Englewood Cliffs, NJ: Prentice-Hall, 1993.
- [18] C. H. Wang, M. C. Chiu, and C. C. Chao, "On unequal error protection of convolutional codes from an algebraic perspective," submitted to *IEEE Trans. Inform. Theory*.

- [19] W. A. Wolovich, "The use of state feedback for exact model matching," *SIAM J. Contr.*, vol. 10, No. 3, pp. 512-523, Aug. 1972.
- [20] K. Yamaguchi and H. Imai, "Construction of unequal error protecting convolutional codes from low rate convolutional codes," in *Proc. 1994 IEEE Int. Symp. Inform. Theory*, Trondheim, Norway, June 1994, p. 275.
- [21] V. A. Zinov'ev and V. V. Zyablov, "Codes with unequal protection of information symbols," *Probl. Peredach. Inform.*, vol. 15, no. 3, pp. 50-60, 1979.

