Universidade de Aveiro Departamento de Matemática
Universidade de Minho
2016

Marisa Lapa Toste

Propriedades das Distâncias dos Códigos Convolucionais sobre $\mathbb{Z}_{p^r}$

Distance Properties of Convolutional Codes over $\mathbb{Z}_{p^r}$

Universidade de Aveiro Departamento de Matemática
Universidade de Minho
2016

Marisa Lapa Toste

Propriedades das Distâncias dos Códigos Convolucionais sobre $\mathbb{Z}_{p^r}$

Distance Properties of Convolutional Codes over $\mathbb{Z}_{p^r}$

Tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Matemática, Programa Doutoral em Matemática e Aplicações da Universidade de Aveiro e Universidade do Minho, realizada sob a orientação científica do Doutor Diego Oscar Napp Avelli, Investigador Auxiliar do Departamento de Matemática da Universidade de Aveiro e da Doutora Maria Raquel Rocha Pinto, Professora Auxiliar do Departamento de Matemática da Universidade de Aveiro.

o júri

Presidente — Reitor da Universidade de Aveiro

Doutora Maria Paula Macedo Rocha Malonek
Professora Catedrática, Faculdade de Engenharia, Universidade do Porto

Doutor Miguel Carriegos Vieira
Professor Titular, Escuela de Ingenierías, Universidad de Léon, Espanha

Doutor José Pedro Miranda Mourão Patrício
Professor Auxiliar, Escola de Ciências, Universidade do Minho

Doutor Paulo José Fernandes Almeida
Professor Auxiliar, Universidade de Aveiro

Doutor Diego Oscar Napp Avelli
Investigador Auxiliar, Universidade de Aveiro (Orientador)

agradecimentos

acknowledgements

Este trabalho foi uma longa viagem e não teria sido possível sem a ajuda de algumas pessoas a quem aproveito para agradecer.

- Aos meus orientadores, Professora Doutora Maria Raquel Rocha Pinto e Professor Doutor Diego Oscar Napp Avelli, por me terem aceitado como sua orientanda e terem acreditado em mim. Pela disponibilidade desde o primeiro momento, pelos seus contributos, pelo contínuo apoio e encorajamento e pela inesgotável energia, entusiasmo e dedicação, o meu obrigada. Para além da admiração e estima, poderão sempre contar com a minha amizade.

- Ao grupo de Sistemas e Controlo do CIDMA, em especial ao Professor Doutor Delfim Torres pelo acolhimento e disponibilidade.

- Aos Professores Doutores Paolo Vettori, Paulo Almeida e Rita Simões pela simpatia e amizade.

- Ao CIDMA – UA e à ESTGOH - IPC pelos apoios concedidos.

- Aos meus amigos que, de uma forma ou de outra, contribuíram com a sua força e estímulo para que conseguisse completar este percurso. A destacar:

  - Carla Reis, colega e amiga que está presente há muitos anos;
  - Rita Branco, uma das mais recentes amizades, mas cujo apoio é imprescindível, tendo sempre uma palavra amiga;
  - Catarina, Pedro, David e Duarte por serem mais do que amigos…

- Aos meus pais que sempre me ajudaram e que, nos momentos de desânimo, estiveram sempre comigo incentivando-me a continuar;

- Ao meu filho Artur pelos sorrisos, amor e carinho que me dedica todos os dias;

- Ao meu marido Bruno por ser o meu “mais que tudo”. Sem ele não teria sido possível terminar mais esta jornada…. Obrigada pelo incentivo, amor, presença e apoio incondicional.

A todos os que, direta ou indiretamente, estiveram comigo e me apoiaram, o meu bem-haja.

palavras-chave

Códigos convolucionais, anéis finitos, distância livre, distância de coluna, MDS, MDP, código dual.

resumo

Nesta tese consideramos códigos convolucionais sobre o anel polinomial $\mathbb{Z}_{p^r}[D]$, onde p é primo e r é um inteiro positivo. Em particular, focamo-nos no conjunto das palavras de código com suporte finito e estudamos as suas propriedades no que respeita às distâncias. Investigamos as duas propriedades mais importantes dos códigos convolucionais, nomeadamente, a distância livre e a distância de coluna.

Começamos por analisar e solucionar o problema de, dado um conjunto de parâmetros, determinar a distância livre máxima possível que um código convolucional sobre $\mathbb{Z}_{p^r}[D]$ pode atingir. Com efeito, obtemos um novo limite superior para esta distância generalizando os limites obtidos no contexto dos códigos convolucionais sobre corpos finitos. Além disso, mostramos que esse limite é ótimo, no sentido em que não pode ser melhorado. Para tal, apresentamos construções de códigos convolucionais (não necessariamente livres) que permitem atingir esse limite, para um certo conjunto de parâmetros. De acordo com a literatura chamamos a esses códigos MDS.

Definimos também distâncias de coluna de um código convolucional. Obtemos limites superiores para as distâncias de coluna e chamamos MDP aos códigos cujas distâncias de coluna atingem estes limites superiores. Além disso, mostramos a existência de códigos MDP. Note-se, porém, que os códigos MDP apresentados não são completamente gerais pois os seus parâmetros devem satisfazer determinadas condições.

Finalmente, estudamos o código dual de um código convolucional definido em $\mathbb{Z}_{p^r}((D))$. Os códigos duais de códigos convolucionais sobre corpos finitos foram exaustivamente investigados, como é refletido na literatura sobre o tema. Estes códigos são relevantes pois fornecem informação sobre a distribuição dos pesos do código e é neste sentido a inclusão deste assunto no âmbito desta tese. Outra razão importante para o estudo de códigos duais é a sua utilidade para o desenvolvimento de algoritmos de descodificação quando consideramos um *erasure channel*. Nesta tese são analisadas algumas propriedades fundamentais dos duais. Em particular, mostramos que códigos convolucionais definidos em $\mathbb{Z}_{p^r}((D))$ admitem uma matriz de paridade. Para além disso, apresentamos um método construtivo para determinar um codificador de um código dual.

keywords

Convolutional codes, finite rings, free distance, column distance, MDS, MDP, dual code

abstract

In this thesis we consider convolutional codes over the polynomial ring $\mathbb{Z}_{p^r}[D]$, where p is a prime and r is a positive integer. In particular, we focus in the set of finite support codewords and study their distances properties. We investigate the two most important distance properties of convolutional codes, namely, the free distance and the column distance.

First we address and fully solve the problem of determining the maximum possible free distance a convolutional code over $\mathbb{Z}_{p^r}[D]$ can achieve, for a given set of parameters. Indeed, we derive a new upper bound on this distance generalizing the Singleton-type bounds derived in the context of convolutional codes over finite fields. Moreover, we show that such a bound is optimal in the sense that it cannot be improved. To do so we provide concrete constructions of convolutional codes (not necessarily free) that achieve this bound for any given set of parameters. In accordance with the literature we called such codes Maximum Distance Separable (MDS).

We define the notion of column distance of a convolutional code. We obtain upper-bounds on the column distances and call Maximum Distance Profile (MDP) the codes that attain the maximum possible column distances. Furthermore, we show the existence of MDP codes. We note however that the MDP codes presented here are not completely general as their parameters need to satisfy certain conditions.

Finally, we study the dual code of a convolutional code defined in $\mathbb{Z}_{p^r}((D))$. Dual codes of convolutional codes over finite fields have been thoroughly investigated as it is reflected in the large body of literature on this topic. They are relevant as they provide value information on the weight distribution of the code and therefore fit in the scope of this thesis. Another important reason for the study of dual codes is that they can be very useful for the development of decoding algorithms of convolutional codes over the erasure channel. In this thesis some fundamental properties have been analyzed. In particular, we show that convolutional codes defined in $\mathbb{Z}_{p^r}((D))$ admit a parity-check matrix. Moreover, we provide a constructive method to explicitly compute an encoder of the dual code.

Contents

Notation

$\mathbb{Z}_p$	prime field of order p
$\mathbb{Z}_p[D]$	ring of polynomials with coefficients in $\mathbb{Z}_p$
$\mathbb{Z}_p(D)$	field of rational matrices with coefficients in $\mathbb{Z}_p$
$\mathbb{Z}_{p^r}$	ring of integers modulo p^r
$\mathbb{Z}_{p^r}[D]$	ring of polynomials with coefficients in $\mathbb{Z}_{p^r}$
$\mathbb{Z}_{p^r}(D)$	ring of rational matrices with coefficients in $\mathbb{Z}_{p^r}$
$\mathbb{Z}_{p^r}((D))$	ring of the Laurent series with coefficientsin $\mathbb{Z}_{p^r}$
$\mathcal{A}_p$	$\{0, 1, \cdots, p-1\}$
$\mathcal{A}_p[D]$	set of polynomials with coefficients in $\mathcal{A}_p$
$\mathcal{A}_p(D)$	set of rational matrices with coefficients in $\mathcal{A}_p$
(n, k, δ)	parameter of a code: n the length, k the p-dimension, δ the p-degree
$(\tilde{n}, \tilde{k}, \tilde{\delta})$	parameter of a code: n the length, k the dimension, δ the degree

Chapter 1

Introduction

Communication systems are everywhere and they have become increasingly important with the development of new technologies for data communications and data storage. Errors in digital communication systems may occur due to noisy communication channels, electrical interference, human error, or equipment error. To guarantee reliable transmission or to recover degraded data, techniques from Coding Theory are used. The aim of Coding Theory is to develop methods to detect and correct these errors. Hence, in the last decades it became an active subject of research in different areas of knowledge such as mathematics, computer science, electrical engineering, statistics, among others.

Shannon, Hamming and Golay were the pioneers that started working with the subject of Coding Theory. They developed studies and ideas that are still used nowadays in, for instance, mobile communications, data storage devices, satellite communications, digital image processing, internet, radio, among others.

A representation of a transformation of information (or storage) from a source to a receiver can be represented as in Figure 1.1. When a message is sent from an information source a process, called *source encoder*, divides the message into sequences or blocks. Each of them is transformed into a digital form (a group of symbols often called "alphabet") forming an algebraic structure, usually a field or a ring. The original message becomes a *source message*. Then redundancy is added by the *channel encoder* to each source block to create a longer block called *codeword*. The set of codewords forms the *code*. A codeword is transmitted over a *transmission channel* (or stored in memory) where errors can occur. To recover the original message, a *channel decoder* uses the redundancy of the information to detect and correct the errors, when it is possible, and retrieve the most likely codeword that had been sent. Finally, a *source decoder* determines the source message and delivers the reconstructed message to the destination.

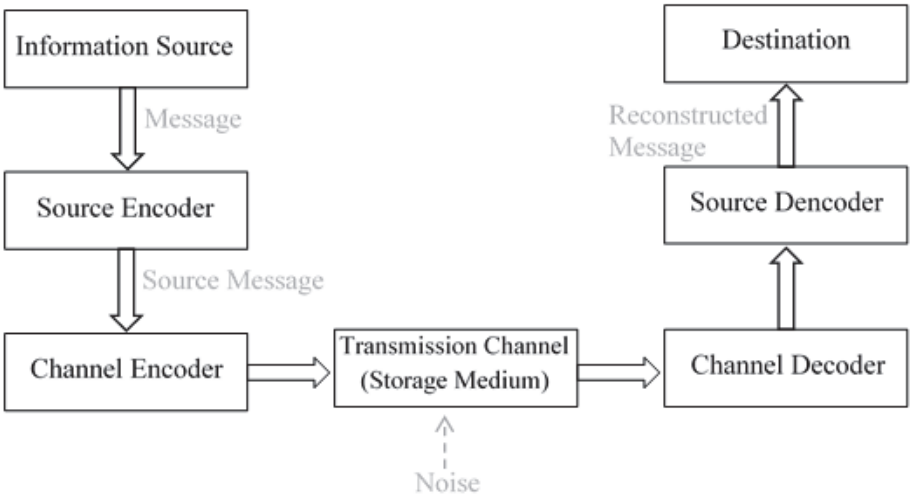
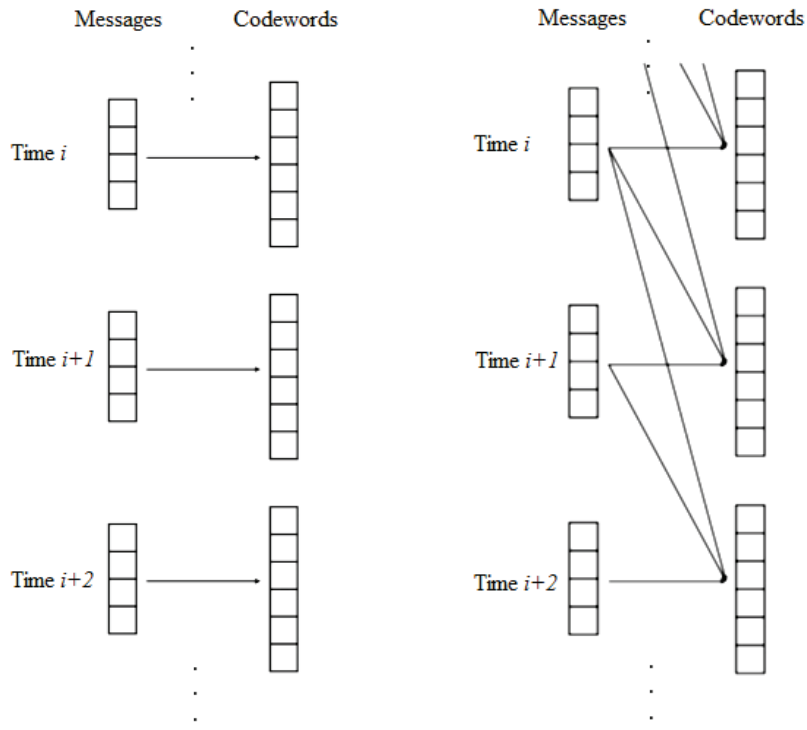


Figure 1.1: Communication (storage) system

In this thesis we focus on the problem of adding redundancy to the source message. In other words we deal with the problem of constructing "good" codes. A "good" code is one that not only detects and corrects the largest number of errors but it is also easy to implement.

The encoding process is described as follows. The information sequence is sliced into blocks of k symbols of information, say $u = (u_0, \ldots, u_{k-1}) \in \mathbb{F}^k$, where $\mathbb{F}$ is a finite field. At time i, the encoder shifts an k-block of the information sequence and generates a block of n encoded symbols, say $v = (v_0, \ldots, v_{n-1}) \in \mathbb{F}^n$, called codeword, via a linear map, *i.e.*, $v = uG$, $G \in \mathbb{F}^{k \times n}$. An (n, k)-linear block code is the set of all possible codewords and it has structure of a k-dimensional subspace of the vector space $\mathbb{F}^n$. In these codes the data is encoded into independent blocks of length n, *i.e.*, the encoded block at time i depends only on the information block at time i (see Figure 1.2a). Hamming's codes [Ham50] were the first block codes, but many other authors developed variations. The first followers of Hamming were Hocquenghem [Hoc59], in 1959, and Bose and Ray-Chaudhari [BRC60], in 1960. They introduced the BCH codes, a generalization of the Hamming codes for multiple-error correction over the binary field. Also in 1960, Reed and Solomon [RS60] built a class of codes for nonbinary channels, named Reed-Solomon codes. Over the years new codes have been discovered and a well-developed algebraic theory of linear block codes has been developed [MS77, LC83, HP98, vL99].

Besides the class of linear *block* codes there are a more general class of linear codes, called convolutional codes. The main difference between these two classes of codes is that the encoded block at time i depends not only on the information block at time



(a) Block Code (b) Convolutional Code

Figure 1.2: Block codes versus convolutional codes

i, but also on a fixed number of previous information blocks, that is, a convolutional encoder requires memory (see Figure 1.2b). In this thesis we shall focus on this class of codes. Convolutional codes were introduced in 1955 by Peter Elias [Eli55]. In 1957, Wozencraft [Woz57] developed the first algorithm capable of decoding such codes, called sequential decoding. Around the same time other decoding algorithms were developed, such as threshold decoding and the Viterbi algorithm. Threshold decoding was first introduced for block codes but Massey [Mas63], in 1963, applied it to convolutional codes. This algorithm is simpler than sequential decoding however less efficient. In 1967, Viterbi [Vit67] presented an optimum decoding method for convolutional codes using the Viterbi algorithm. However, the decoding effort grows exponentially with memory orders. These decoding methods allowed the application of convolutional codes in several types of systems.

Forney [For70], Piret [Pir88] and McEliece [McE98], in 1970, 1988 and 1998, respectively, formalized the theory of convolutional codes and thoroughly studied the algebraic structure of these codes.

In order to determine the performance of convolutional codes, the distance is argu-

ably the most important parameter. The rule is, the larger the distance, the better the code. For convolutional codes the free distance and the column distance are the most important distance properties.

In [RS99], Rosenthal and Smarandache determined an upper bound on the free distance of a convolutional code. This bound was called the generalized Singleton bound since it generalizes in a natural way the Singleton bound for block codes. An MDS convolutional code is one whose free distance achieves the generalized Singleton bound. In 2001, Smarandache, Gluesing-Luerssen and Rosenthal [SGLR01] presented constructions of MDS convolutional codes. The same three authors in [HGLS06] constructed strongly MDS convolutional codes, in 2006. These codes are characterized by attaining the generalized Singleton bound at the earliest possible column distance. These constructions were restricted to some parameters and the general case was treated in 2015 by Napp and Smarandache [NR16]. Other examples related with MDS are [RL89, Hut08, CNPP12, CNPP16].

Convolutional codes whose column distances increase as rapidly as possible for as long as possible are called maximum distance profile (MDP) codes. These codes are specially appealing for sequential decoding algorithms because they have the potential to have a maximum number of errors corrected per time interval, hence they achieve good performance. Regarding MDP convolutional codes we can highlight the work of R. Hutchinson, J. Rosenthal and R. Smarandache [RHS05], in 2005. Later, R. Hutchinson [HST08] and P. Almeida, D. Napp and R. Pinto [ANP13], in 2008 and 2013, respectively, discussed how superregular matrices may be used to construct MDP codes. V. Tomás, J. Rosenthal and R. Smarandache [VTS09, TRS12], in 2009 and 2012, respectively, analysed decoding capabilities of convolutional codes over the erasure channel and showed how MDP convolutional codes perform particularly well over the erasure channel.

The extension of the concept of convolutional codes from finite fields to finite rings was first introduced by Massey and Mittelholzer [MM89], in 1989, and has attracted much attention in recent years. This interest is mainly due to the discovers that the most appropriate codes for phase modulation are the linear codes over the residue class ring $\mathbb{Z}_M$, M a positive integer. It was immediately apparent that convolutional codes over $\mathbb{Z}_M$ behave very differently from convolutional codes over finite fields. For instance, in contrast with the field case, convolutional codes over $\mathbb{Z}_M$ are not necessarily free modules.

Fundamental results of the structural properties of convolutional codes over finite rings have been studied over the years and can be found in [JWW98, Nor99, NS00,

FZ01]. In particular, the properties of being noncatastrophic, right invertible, basic and systematic ring convolutional encoders were thoroughly discussed. The problem of deriving minimal encoders (left prime and row-reduced) was posed in 1997 by Fagnani and Zampieri [FZ97] and in 2007 by Solé and Sison [SS07]. This problem was solved in 2007 by Kuiper, Pinto and Polderman [KPP07] and in 2009 by Kuiper, Pinto [KP09] using the concept of minimal p-encoder, which is an extension of the concept of p-basis introduced in [VSA96] to the polynomial context.

The search for and design of unit-memory convolutional codes over $\mathbb{Z}_4$ that gives rise to binary trellis codes with high free distance was investigated by Ashikhmin and Zyablov [AZ94] and by Kötter, Dettmar and Sorger [KDS95] in 1994 and 1995, respectively, where several concrete constructions were reported. In 1998, Johannesson and Wittenmark [JW98] found, by computer search, two 16-state trellis codes of rate $\frac{2}{4}$ again over $\mathbb{Z}_4$. However, in contrast to the block code case [GG12, NS01] little is known about distance properties and constructions of convolutional codes over large rings, see [SS07].

Recently, in 2013 El Oued and Solé [EOS13] derived a bound for the free distance of convolutional codes over $\mathbb{Z}_{p^r}$, generalizing the bound given in [RS99] for convolutional codes over finite fields. The concrete constructions of MDS convolutional codes over $\mathbb{Z}_{p^r}$ presented in this paper were restricted to *free* codes and cannot be extended to the general case. An explicit general construction of nonfree MDS codes over finite rings was left as an open problem and we address it in this thesis. Another fundamental problem treated in this dissertation is the study of column distance and constructions of MDP convolutional codes over $\mathbb{Z}_{p^r}$. In order to investigate these two problems, we adopt a novel approach, in particular, we derive new upper-bounds on the free distance and the column distances and provide explicit novel constructions of MDS (not necessarily free) and MDP convolutional codes over $\mathbb{Z}_{p^r}$ for a set of given parameters. In the proof of these results, an essential role is played by the theory of p-basis and in particular of a canonical form of the p-encoders. In contrast with the papers [NS01, EOS13] where the Hensel lift of a cyclic code was used, in this thesis a direct lifting is employed to build convolutional codes over $\mathbb{Z}_{p^r}$ from known constructions of convolutional codes over $\mathbb{Z}_p$. Note that even though we will focus on the ring $\mathbb{Z}_{p^r}$, by the Chinese Remainder Theorem, results on codes over $\mathbb{Z}_{p^r}$ can be extended to codes over $\mathbb{Z}_M$, as can be seen in [McD74, CCL94, JWW98].

We also investigate the dual codes of convolutional codes over $\mathbb{Z}_{p^r}$. They are useful for the development of decoding algorithms of convolutional codes by erasure channel. In this thesis we present a preliminary study of these codes.

This thesis is divided into six chapters. A brief outline of the contents of the chapters is given below.

Chapter 2 - The module $\mathbb{Z}_{p^r}^n[D]$

This chapter presents some preliminaries on $\mathbb{Z}_{p^r}^n[D]$ related with p-basis. Most of the definitions and results were presented in [KPP07] and [KP09]. The results that are well known will be presented without proof, together with the reference of the respective author(s).

Chapter 3 - Convolutional codes over $\mathbb{Z}_{p^r}$

We start by considering block codes and propose a novel special form for its generator matrix, called the p-standard form. We give an algorithm to construct such generator matrix which will be very useful throughout the thesis.

We define a convolutional code as a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$. We introduce its free and row distance using the notion of the Hamming weight of a polynomial vector and we establish an upper-bound on the free distance generalizing the main result in [EOS13]. We define maximal distance separable (MDS) convolutional codes as those which their free distance reach this upper-bound. Moreover, we show the existence of MDS convolutional codes by providing a class of convolutional codes whose distance achieve such an upper bound. These results have been published in [NPT16].

Next we address the notion of column distance of a convolutional code over $\mathbb{Z}_{p^r}$. We derive upper-bounds on the column distances and we define maximal distance profile (MDP) convolutional codes as the ones that their column distances achieve the maximum possible values.

Chapter 4 - Constructions of convolutional codes over $\mathbb{Z}_{p^r}$

In this chapter we concentrate on constructions of MDS and MDP convolutional codes over $\mathbb{Z}_{p^r}$.

First we build MDS convolutional codes that are not necessarily free. We *lift* MDS convolutional codes over $\mathbb{Z}_p$ to $\mathbb{Z}_{p^r}$ in such a way that the resulting convolutional code is MDS over $\mathbb{Z}_{p^r}$. These results have been published in [NPT16]. In the second part of this chapter, we present constructions of MDP convolutional codes given a set of parameters. We consider two cases regarding this set of parameters and the idea is the same as that given for the construction of MDS codes: start from well-known constructions of MDP convolutional codes over $\mathbb{Z}_p$ and then *lift* them to $\mathbb{Z}_{p^r}$ in such a way that the resulting convolutional code is MDP over $\mathbb{Z}_{p^r}$.

Chapter 5 - Duality

We also investigate the dual codes of convolutional codes defined in $\mathbb{Z}_{p^r}((D))$, the ring of Laurent series with coefficients in $\mathbb{Z}_{p^r}$ [EONPT]. We show that, as opposed to convolutional codes over $\mathbb{Z}_{p^r}$, convolutional codes defined in $\mathbb{Z}_{p^r}((D))$ always admit a kernel representation, which defines an image representation of the dual, and we give a procedure to determine it. Thus, given a convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$, we are able to determine a kernel representation of the smallest convolutional $\tilde{\mathcal{C}}$ defined in $\mathbb{Z}_{p^r}((D))$ that contains $\mathcal{C}$. This property is fundamental when we consider decoding over an erasure channel.

The work on Chapter 5 have been presented in MAT-TRIAD 2015 and published in [EONPT].

Chapter 6 - Conclusions

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

Chapter 2

The module $\mathbb{Z}_{p^r}^n[D]$

In this chapter we will consider $\mathbb{Z}_{p^r}^n[D]$-submodules of $\mathbb{Z}_{p^r}[D]$, where $\mathbb{Z}_{p^r}[D]$ denotes the ring of polynomials with coefficients in $\mathbb{Z}_{p^r}$, with p prime and r an integer greater than one. We will study these modules using known concepts of p-generator sequence, p-linearly independence and p-basis and we will present novel results on these modules using these notions. Most of these definitions and results come from [KPP07] and [KP09].

2.1 P-basis

Any element $a \in \mathbb{Z}_{p^r}$ can be written uniquely as a linear combination of $1, p, p^2, \ldots$ $\ldots, p^{r-1}$, with coefficients in $\mathcal{A}_p = \{0, 1, \ldots, p-1\} \subset \mathbb{Z}_{p^r}$, *i.e.*,

$$a = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1} p^{r-1}, \;\; \alpha_i \in \mathcal{A}_p, \;\; i = 0, 1, \ldots, r-1,$$

called the p-adic expansion of the element [CS95]. Note that all elements in $\mathcal{A}_p \backslash \{0\}$ are units. In [VSA96], the authors considered this property to define a special type of linear combination of vectors, called *p-linear combination*, which allows to define the notion of *p-generator sequence*, *p-basis* and *p-dimension* for every submodule of $\mathbb{Z}_{p^r}^n[D]$. These notions were extended for vectors in [KPP07] and we recall them in this section.

Definition 2.1. *[KPP07] Let $v_1(D), \ldots, v_k(D)$ be in $\mathbb{Z}_{p^r}^n[D]$. The vector*

$$\sum_{j=1}^{k} a_j(D) v_j(D),$$

with $a_j(D) \in \mathcal{A}_p[D]$, is said to be a **p-linear combination** *of $v_1(D), \ldots, v_k(D)$ and the set of all p-linear combinations of $v_1(D), \ldots, v_k(D)$ is called the* **p-span** *of*

$\{v_1(D), \ldots, v_k(D)\}$, *denoted by p-span* $(v_1(D), \ldots, v_k(D))$.

Notice that p-span$(v_1(D), \ldots, v_k(D))$ may not be a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$ as can be seen in the next example.

Example 2.2. *Consider the module* $\mathbb{Z}_4^2[D]$ *and*

$$M = p\text{-}span((1+D, 0), (0, 1+D)).$$

M is not a $\mathbb{Z}_4[D]$*-submodule of* $\mathbb{Z}_4^2[D]$ *since, for instance,*

$$(2+2D, 0) \notin M.$$

The next definition introduces a property on sequences of vectors $(v_1(D), \ldots, v_k(D))$ in $\mathbb{Z}_{p^r}^n[D]$ that will guarantee that p-span$(v_1(D), \ldots, v_k(D))$ is a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$.

Definition 2.3. *[KPP07] An ordered set of vectors* $(v_1(D), \ldots, v_k(D))$ *in* $\mathbb{Z}_{p^r}^n[D]$ *is said to be a* ***p*-generator sequence** *if* $p\, v_i(D)$ *is a p-linear combination of* $v_{i+1}(D), \ldots, v_k(D)$, $i = 1, \ldots, k-1$, *and* $p\, v_k(D) = 0$.

Lemma 2.4. *[KPP07] Let* $v_1(D), \ldots, v_k(D)$ *be in* $\mathbb{Z}_{p^r}^n[D]$. *If* $(v_1(D), \ldots, v_k(D))$ *is a p-generator sequence, it holds that*

$$p\text{-}span(v_1(D), \ldots, v_k(D)) = span(v_1(D), \ldots, v_k(D)).$$

Consequently p*-span*$(v_1(D), \ldots, v_k(D))$ *is a* $\mathbb{Z}_{p^r}$*-submodule of* $\mathbb{Z}_{p^r}^n[D]$.

Note that if $M = span(v_1(D), \ldots, v_k(D))$ is a submodule of $\mathbb{Z}_{p^r}^n[D]$ then

$$\begin{aligned}(v_1(D), pv_1(D) \ldots, &p^{r-1}v_1(D), v_2(D), pv_2(D), \ldots, \\ &\ldots, p^{r-1}v_2(D), \ldots, v_k(D), pv_k(D) \ldots, p^{r-1}v_k(D)).\end{aligned} \tag{2.1}$$

is a p-generator sequence of M.

Definition 2.5. *Two p-generator sequences* $V(D) = (v_1(D), \ldots, v_k(D))$ *and* $V'(D) = (v'_1(D), \ldots, v'_{k'}(D))$ *in* $\mathbb{Z}_{p^r}^n[D]$ *are said to be* **equivalent** *if they generate the same module M, i.e.,* $M = span(V(D)) = span(V'(D))$.

Note that in $\mathbb{Z}_{p^r}^n[D]$ it may happen that two vectors are linearly dependent without any of them being a linear combination of the other, which is illustrated in the following example.

Example 2.6. *In $\mathbb{Z}_8^2[D]$, the vectors $(4+4D,0)$ and $(0,2+2D)$ are linearly dependent since*

$$2(4+4D,0)+4(0,2+2D)=(0,0)$$

but none of these vectors is a linear combination of the other.

So, we need to introduce a *new* notion of linear independence.

Definition 2.7. *[KPP07] The vectors $v_1(D),\ldots,v_k(D)$ in $\mathbb{Z}_{p^r}^n[D]$ are said to be* ***p*-linearly independent** *if the only p-linear combination of $v_1(D),\ldots,v_k(D)$ that is equal to 0 is the trivial one. If $v_1(D),\ldots,v_k(D)$ are not p-linearly independent, they are called* ***p*-linearly dependent**.

The following result establishes a necessary condition in order to reduce a given p-generator sequence.

Lemma 2.8. *Let $(v_1(D),\ldots,v_i(D),v_{i+1}(D),\ldots,v_k(D))$ be a p-generator sequence of a submodule M of $\mathbb{Z}_{p^r}^n[D]$, with $v_{i+1}(D),\ldots,v_k(D)$ p-linearly independent vectors. If $v_i(D)$ is written as p-linear combination of $v_{i+1}(D),\ldots,v_k(D)$ then*

$$(v_1(D),\ldots,v_{i-1}(D),v_{i+1}(D),\ldots,v_k(D))$$

is a p-generator sequence of M.

Proof Since $v_i(D)$ is a p-linear combination of $v_{i+1}(D),\ldots,v_k(D)$ then

$$v_i(D)=\beta_{i+1}(D)v_{i+1}(D)+\beta_{i+2}(D)v_{i+2}(D)+\cdots+\beta_k v_k(D), \tag{2.2}$$

for some $\beta_t(D)\in\mathcal{A}_p[D]$, $t=i+1,\ldots,k$. To see that

$$(v_1(D),\ldots,v_{i-1}(D),v_{i+1}(D),\ldots,v_k(D))$$

is a p-generator sequence, we need to prove that $pv_j(D)$ is a p-linear combination of the vectors in $\{v_{j+1}(D),\ldots,v_k(D)\}\backslash\{v_i(D)\}$, for $j<i$.

Let $j<i-1$.

As $(v_1(D),\ldots,v_i(D),v_{i+1}(D),\ldots,v_k(D))$ is a p-generator sequence then

$$\begin{aligned}pv_j(D)=&\alpha_{j+1}(D)v_{j+1}(D)+\cdots+\alpha_{i-1}(D)v_{i-1}(D)+\alpha_i(D)v_i(D)+\\&+\alpha_{i+1}(D)v_{i+1}(D)+\cdots+\alpha_k(D)v_k(D),\end{aligned}$$

for some $\alpha_s(D) \in \mathcal{A}_p[D]$, $s = j+1, \ldots, k$. Replacing $v_i(D)$ as in (2.2) we have that

$$\begin{aligned} pv_j(D) &= \alpha_{j+1}(D)v_{j+1}(D) + \cdots + \alpha_{i-1}(D)v_{i-1}(D) + \\ &\quad +(\alpha_i(D)\beta_{i+1}(D) + \alpha_{i+1}(D))v_{i+1}(D) + (\alpha_i(D)\beta_{i+2}(D) + \alpha_{i+2}(D))v_{i+2}(D) + \\ &\quad + \cdots + (\alpha_i(D)\beta_k(D) + \alpha_k(D))v_k(D) \\ &= \alpha_{j+1}(D)v_{j+1}(D) + \cdots + \alpha_{i-1}(D)v_{i-1}(D) + \\ &\quad +\gamma'_{i+1}(D)v_{i+1}(D) + \gamma'_{i+2}(D)v_{i+2}(D) + \cdots + \gamma'_k(D)v_k(D), \end{aligned}$$

with $\gamma'_t(D) = \alpha_i(D)\beta_t(D) + \alpha_t(D) \in \mathbb{Z}_{p^r}[D]$, $t = i+1, \ldots, k$. Since $(v_{i+1}(D), \ldots, v_k(D))$ is a p-generator sequence, by Lemma 2.4, it follows that

$$p\text{-}span(v_{i+1}(D), \ldots, v_k(D)) = span(v_{i+1}(D), \ldots, v_k(D))$$

and, so

$$pv_j(D) = \alpha_{j+1}(D)v_{j+1}(D) + \cdots + \gamma_{i+1}(D)v_{i+1}(D) + \gamma_{i+2}(D)v_{i+2}(D) + \cdots + \gamma_k(D)v_k(D)$$

for some $\gamma_t(D) \in \mathcal{A}_p[D]$, $t = i+1, \ldots, k$.

Note that if $j = i-1$ then

$$\begin{aligned} pv_{i-1}(D) &= \alpha_i(D)v_i(D) + \alpha_{i+1}(D)v_{i+1}(D) + \cdots + \alpha_k(D)v_k(D) \\ &= (\alpha_i(D)\beta_{i+1}(D) + \alpha_{i+1}(D))v_{i+1}(D) + \cdots + (\alpha_i(D)\beta_k(D) + \alpha_k(D)))v_k(D) \end{aligned}$$

and by the same reasoning as before it follows that

$$pv_{i-1}(D) \in p\text{-}span(v_{i+1}(D), \ldots, v_k(D)).$$

Thus, $(v_1(D), \ldots, v_{i-1}(D), v_{i+1}(D), \ldots, v_k(D))$ is a p-generator sequence.

Finally,

$$\begin{aligned} &span(v_1(D), \ldots, v_{i-1}(D), v_i(D), v_{i+1}(D), \ldots, v_k(D)) = \\ &= span(v_1(D), \ldots, v_{i-1}(D), v_{i+1}(D), \ldots, v_k(D)) \end{aligned}$$

because $v_i(D)$ is a linear combination of $v_{i+1}(D), \ldots, v_k(D)$. Thus, by Lemma 2.4,

$$\begin{aligned} M &= p\text{-}span(v_1(D), \ldots, v_{i-1}(D), v_i(D), v_{i+1}(D), \ldots, v_k(D)) \\ &= p\text{-}span(v_1(D), \ldots, v_{i-1}(D), v_{i+1}(D), \ldots, v_k(D)) \end{aligned}$$

and, therefore $\big(v_1(D),\ldots,v_{i-1}(D),v_{i+1}(D),\ldots,v_k(D)\big)$ is a p-generator sequence of M. □

Note that a set of linearly independent polynomial vectors is also a set of p-linearly independent polynomial vectors, but the reciprocal may not occur as it can be seen in the next example.

Example 2.9. *Let us consider* $(3+3D,3D^2),(3+3D,0)\in\mathbb{Z}_9^2[D]$. *These two vectors are p-linearly independent but not linearly independent. In fact,*

$$3(3+3D,3D^2)+3(3+3D,0)=(0,0),$$

but, if $\alpha_1(D),\alpha_2(D)\in\mathcal{A}_p[D]$ *then*

$$\alpha_1(D)(3+3D,3D^2)+\alpha_2(D)(3+3D,0)=(0,0)\Rightarrow\alpha_1(D)=\alpha_2(D)=0.$$

Definition 2.10. *[KPP07] An ordered set of vectors* $(v_1(D),\ldots,v_k(D))$ *which is a p-generator sequence of* M *and p-linearly independent is said to be a* ***p*-basis** *of* M.

It is proved in [KP09] that two p-bases of a $\mathbb{Z}_{p^r}[D]$-submodule M of $\mathbb{Z}_{p^r}^n[D]$ have the same number of elements and, so the number of elements of a p-basis of M is an invariant of M.

Definition 2.11. *[KPP07] The number of elements of a p-basis of a* $\mathbb{Z}_{p^r}[D]$*-submodule* M *of* $\mathbb{Z}_{p^r}^n[D]$ *is called* ***p*-dimension** *of* M, *denoted as p-dim*(M).

Next we provide new elementary operations on a given p-basis of M so that we obtain another p-basis of M.

Lemma 2.12. *Let* $(v_1(D),\ldots,v_k(D))$ *be a p-generator sequence of a submodule* M *of* $\mathbb{Z}_{p^r}^n[D]$. *Then,*

1. *If* $v_i'(D)=a_iv_i(D)+\sum_{t=i+1}^k a_t(D)v_t(D)$, *where* $a_i\in\mathbb{Z}_{p^r}$ *is a unit and* $a_t(D)\in\mathbb{Z}_{p^r}[D]$, $t=i+1,\ldots,k$ *then*

$$(v_1(D),\ldots,v_{i-1}(D),v_i'(D),v_{i+1}(D),\ldots,v_k(D)) \tag{2.3}$$

   is a p-generator sequence of M. *Moreover, if* $(v_1(D),\ldots,v_k(D))$ *is a p-basis of* M *then (2.3) is a p-basis of* M.

2. *If* $pv_i(D)$ *is a p-linear combination of* $v_t(D),v_{t+1}(D),\ldots,v_k(D)$, *for some* $t>i$, *then*

$$(v_1(D),\ldots,v_{i-1}(D),v_{i+1}(D),\ldots,v_{t-1}(D),v_i(D),v_t(D),\ldots,v_k(D)) \tag{2.4}$$

is a p-generator sequence of M. Moreover, if $(v_1(D), \ldots, v_k(D))$ *is a p-basis of M then (2.4) is a p-basis of M.*

Proof

1. Since $(v_1(D), \ldots, v_k(D))$ is a p-generator sequence then

$$pv_i(D) = \alpha_{i+1}(D)v_{i+1}(D) + \alpha_{i+2}(D)v_{i+2}(D) + \cdots + \alpha_k(D)v_k(D), \tag{2.5}$$

for some $\alpha_t(D) \in \mathcal{A}_p[D]$, $t = i+1, \ldots, k$. From $v_i'(D) = a_i v_i(D) + \sum_{t=i+1}^{k} a_t(D)v_t(D)$ we can write

$$pv_i'(D) = pa_i v_i(D) + \sum_{t=i+1}^{k} pa_t(D)v_t(D)$$

and, replacing $pvi(D)$ as defined in (2.5),

$$\begin{aligned} pv_i'(D) =& (a_i\alpha_{i+1}(D) + pa_{i+1}(D))v_{i+1}(D) + (a_i\alpha_{i+2}(D) + pa_{i+2}(D))v_{i+2}(D) + \\ &+ \cdots + (a_i\alpha_k(D) + pa_k(D))v_k(D). \end{aligned}$$

As $(v_{i+1}(D), \ldots, v_k(D))$ is a p-generator sequence, by Lemma 2.4 we have that

$$p\text{-}span(v_{i+1}(D), \ldots, v_k(D)) = span(v_{i+1}(D), \ldots, v_k(D)) \tag{2.6}$$

and, so

$$pv_i'(D) = \beta_{i+1}(D)v_{i+1}(D) + \beta_{i+2}(D)v_{i+2}(D) + \cdots + \beta_k(D)v_k(D),$$

with $\beta_t(D) \in \mathcal{A}_p[D]$, $t = i+1, \ldots, k$. Thus, $(v_i'(D), v_{i+1}(D), \ldots, v_k(D))$ is a p-generator sequence.

Let $j < i-1$ and

$$\begin{aligned} pv_j(D) &= \gamma_{j+1}(D)v_{j+1}(D) + \cdots + \gamma_{i-1}(D)v_{i-1}(D) + \gamma_i(D)v_i(D) + \\ &\quad + \gamma_{i+1}(D)v_{i+1}(D) + \cdots + \gamma_k(D)v_k(D) \end{aligned}$$

for some $\gamma_t(D) \in \mathcal{A}_p[D]$, $t = i+1, \ldots, k$. Replacing $v_i(D)$ by $a_i^{-1}(v_i'(D) - \sum_{t=i+1}^{k} a_t(D)v_t(D))$ it follows that

$$\begin{aligned} pv_j(D) &= \gamma_{j+1}(D)v_{j+1}(D) + \cdots + \gamma_{i-1}(D)v_{i-1}(D) + \gamma_i(D)a_i^{-1}v_i'(D) + \\ &\quad + (\gamma_{i+1}(D) - \gamma_i(D)a_i^{-1}a_{i+1}(D))v_{i+1}(D) + \cdots + (\gamma_k(D) - \\ &\quad - \gamma_i(D)a_i^{-1}a_k(D))v_k(D). \end{aligned}$$

From (2.6) it follows that

$$\begin{aligned} pv_j(D) &= \gamma_{j+1}(D)v_{j+1}(D) + \cdots + \gamma_{i-1}(D)v_{i-1}(D) + \gamma'_i(D)v'_i(D) + \\ &\quad \gamma'_{i+1}(D)v_{i+1}(D) + \cdots + \gamma'_k(D)v_k(D), \end{aligned}$$

for some $\gamma_t(D) \in \mathcal{A}_p[D]$, $t = i, \ldots, k$.

If $j = i - 1$ then

$$pv_{i-1}(D) = \gamma_i(D)v_i(D) + \gamma_{i+1}(D)v_{i+1}(D) + \cdots + \gamma_k(D)v_k(D),$$

for some $\gamma_t(D) \in \mathcal{A}_p[D]$ and therefore applying the same reasoning as before we have that

$$pv_{i-1}(D) = \gamma'_i(D)v'_i(D) + \gamma'_{i+1}(D)v_{i+1}(D) + \cdots + \gamma'_k(D)v_k(D),$$

for some $\gamma'_t(D) \in \mathcal{A}_p[D]$, $t = i + 1, \ldots, k$.

Thus, $(v_1(D), \ldots, v_{i-1}(D), v'_i(D), v_{i+1}(D), \ldots, v_k(D))$ is a p-generator sequence.

We also have that

$$\begin{aligned} &span(v_1(D), \ldots, v_{i-1}(D), v_i(D), v_{i+1}(D), \ldots, v_k(D)) = \\ =&span(v_1(D), \ldots, v_{i-1}(D), v'_i(D), v_{i+1}(D), \ldots, v_k(D)), \end{aligned}$$

because $v'_i(D)$ is a linear combination of $v_i(D), \ldots, v_k(D)$. By Lemma 2.4,

$$\begin{aligned} M &= p\text{-}span(v_1(D), \ldots, v_{i-1}(D), v_i(D), v_{i+1}(D), \ldots, v_k(D)) \\ &= p\text{-}span(v_1(D), \ldots, v_{i-1}(D), v'_i(D), v_{i+1}(D), \ldots, v_k(D)) \end{aligned}$$

and, therefore $(v_1(D), \ldots, v_{i-1}(D), v'_i(D), v_{i+1}(D), \ldots, v_k(D))$ is a p-generator sequence of M.

To conclude the proof, it remains to show that

$$v_1(D), \ldots, v_{i-1}(D), v'_i(D), v_{i+1}(D), \ldots, v_k(D)$$

are p-linearly independent. Let us consider $\delta_t(D) \in \mathcal{A}_p[D]$, $t = 1, \ldots, k$ such that

$$\begin{aligned} &\delta_1(D)v_1(D) + \cdots + \delta_{i-1}(D)v_{i-1}(D) + \\ &\quad + \delta_i(D)v'_i(D) + \delta_{i+1}(D)v_{i+1}(D) + \cdots + \delta_k(D)v_k(D) = 0. \end{aligned} \tag{2.7}$$

Since $v_i'(D) = a_i v_i(D) + \sum_{t=i+1}^{k} a_t(D)v_t(D)$, then

$$\begin{aligned}\delta_1(D)v_1(D) + \cdots + \delta_{i-1}(D)v_{i-1}(D) + \delta_i(D)a_i v_i(D) + \\ + (\delta_i(D)a_{i+1}(D) + \delta_{i+1}(D))v_{i+1}(D) + \\ + \cdots + (\delta_i(D)a_k(D) + \delta_k(D))v_k(D) = 0.\end{aligned} \tag{2.8}$$

By Lemma 2.4 and using the fact that $(v_1(D), \ldots, v_k(D))$ is a p-generator sequence, we can rewrite (2.8) as

$$\begin{aligned}\delta_1(D)v_1(D) + \ldots + \delta_{i-1}(D)v_{i-1}(D) + \delta_i'(D)v_i(D) + \\ + \delta_{i+1}'(D)v_{i+1}(D) + \cdots + \delta_k'(D)v_k(D) = 0,\end{aligned}$$

for some $\delta_t' \in \mathcal{A}_p[D]$, $t = i, \ldots, k$. As $v_1(D), \ldots, v_k(D)$ are p-linearly independent then

$$\delta_1 = \cdots = \delta_i = \delta_{i+1}' = \cdots = \delta_k' = 0.$$

Thus, substituting δ_t by zero, $t = 1, \ldots i$, in (2.7) we obtain

$$\delta_{i+1}(D)v_{i+1}(D) + \cdots + \delta_k(D)v_k(D) = 0.$$

From the p-linearly independence of $v_{i+1}(D), \ldots, v_k(D)$ we have that

$$\delta_{i+1} = \cdots = \delta_k = 0.$$

2. It is obvious.

□

Note that all definitions and all results above can be applied for submodules over $\mathbb{Z}_{p^r}^n$ [VSA96]. In fact, as mentioned before, these notions were first introduced in this paper for such modules and later extended for the module $\mathbb{Z}_{p^r}^n[D]$ in [KPP07].

Next, we will introduce a special type of p-basis of a submodule of $\mathbb{Z}_{p^r}^n[D]$. For that we need first to introduce some notions on vectors and matrices over $\mathbb{Z}_{p^r}[D]$.

Definition 2.13. *[KPP07] A nonzero polynomial vector $v(D)$ in $\mathbb{Z}_{p^r}^n[D]$, written as $v(D) = \sum_{t=0}^{\nu} v_t D^t$, with $v_t \in \mathbb{Z}_{p^r}^n$, and $v_\nu \neq 0$, is said to have* **degree** *ν, denoted by $deg\, v(D) = \nu$, and v_ν is called the* **leading coefficient vector** *of $v(D)$, denoted by v^{lc}. For a given matrix $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ we denote by $G^{lc} \in \mathbb{Z}_{p^r}^{k\times n}$ the matrix whose rows are constituted by the leading coefficient vectors of the rows of $G(D)$.*

Definition 2.14. *[KPP07] A p-basis $(v_1(D), \ldots, v_k(D))$ of a submodule M of $\mathbb{Z}_{p^r}^n[D]$ is called a* **reduced p-basis** *if the vectors $v_1^{lc}, \ldots, v_k^{lc}$ are p-linearly independent in $\mathbb{Z}_{p^r}^n$.*

Every submodule M of $\mathbb{Z}_{p^r}^n[D]$ has a reduced p-basis. Algorithm 3.11 in [KPP07] constructs a reduced p-basis for a submodule M from a generator sequence of M. For completeness, we rewrite this algorithm as Algorithm 2.15 taking as input a p-generator sequence of M.

Algorithm 2.15. *[KPP07]* Input data: *$V \leftarrow (w_1(D), \ldots, w_g(D))$ p-generator sequence, with $w_i(D) \in \mathbb{Z}_{p^r}^n[D]$.*

Step 1: *Re-order V according to non-increasing degrees such that*

$$V \leftarrow (v_1(D), \ldots, v_k(D), 0, \ldots, 0),$$

making sure that vectors of equal degree are not swapped. Denote $d_i := deg\, v_i(D)$ for $1 \leq i \leq k$.

Step 2: *Remove zero vectors, resulting in*

$$V \leftarrow (v_1(D), \ldots, v_k(D)).$$

Step 3: *Determine the smallest ℓ such that*

$$(v_{\ell+1}^{lc}, \ldots, v_k^{lc})$$

is a p-basis in $\mathbb{Z}_{p^r}^n$.

Step 4: *For $i = 1, \ldots, k - \ell$ let $\alpha_i \in \mathbb{Z}_{p^r}$ be such that*

$$v_\ell^{lc} + \alpha_1 v_{\ell+1}^{lc} + \alpha_2 v_{\ell+2}^{lc} + \ldots + \alpha_{k-\ell} v_k^{lc} = 0.$$

Replace $v_\ell(D)$ by

$$v_\ell(D) + \alpha_1 D^{d_\ell - d_{\ell+1}} v_{\ell+1}(D) + \alpha_2 D^{d_\ell - d_{\ell+2}} v_{\ell+2}(D) + \cdots + \alpha_{k-\ell} D^{d_\ell - d_k} v_k(D).$$

Go to Step 1.

The algorithm stops when $\ell = 0$ at Step 3.
Output data: *$(v_1(D), \ldots, v_k(D))$.*

Remark 2.16. *Algorithm 3.11 in [KPP07] starts by constructing a p-generator sequence for M in an initialization step. If the input of the algorithm is already a p-generator sequence this step is redundant.*

Lemma 2.17. *[KPP07] The degrees of the vectors of two reduced p-bases of M are the same (up to permutation). Therefore, the degrees of a reduced p-basis of a submodule of $\mathbb{Z}_{p^r}^n[D]$ are an invariant of the code.*

Definition 2.18. *The degrees of the vectors of a reduced p-basis of a submodule M of $\mathbb{Z}_{p^r}^n[D]$ are called the* ***p*-indices** *of M and the sum of the p-indices is called the* ***p*-degree** *of M.*

Lemma 2.19. *[KPP07] Any reduced p-basis $(v_1(D), \ldots, v_k(D))$ of M exhibits the* ***p*-predictable degree property***:*

$$deg\left(\sum_{i=1}^{k} a_i(D)v_i(D)\right) = \max_{j:a_j(D)\in\mathcal{A}_p[D]\setminus\{0\}}(deg\, a_j(D) + deg\, v_j(D))$$

By Lemma 2.19, it follows that any reduced p-basis of a submodule M of $\mathbb{Z}_{p^r}^n[D]$ can be ordered by non increasing degrees to produce another reduced p-basis of M.

Chapter 3

Convolutional Codes over $\mathbb{Z}_{p^r}$

In this chapter, we will concentrate on convolutional codes over $\mathbb{Z}_{p^r}$. Particular attention will be given to the class of block codes over $\mathbb{Z}_{p^r}$ seen as an instance of the class of convolutional codes over $\mathbb{Z}_{p^r}$. We will present the definition of convolutional code, encoder and p-encoder, p-basis and reduced p-basis of convolutional codes. At the end of this chapter, we define free distance and column distance of a convolutional code over $\mathbb{Z}_{p^r}$, using the notion of the Hamming weight of a polynomial vector, and establish upper bounds for these distances.

3.1 Block Codes

Definition 3.1. *A* **(linear) block code** $\mathcal{C}$ *of length* n *over* $\mathbb{Z}_{p^r}$ *is a* $\mathbb{Z}_{p^r}$*-submodule of* $\mathbb{Z}_{p^r}^n$ *and the elements of* $\mathcal{C}$ *are called codewords. A* **generator matrix** $\widetilde{G} \in \mathbb{Z}_{p^r}^{\tilde{k}\times n}$ *of* $\mathcal{C}$ *is a matrix whose rows form a minimal set of generators of* $\mathcal{C}$ *over* $\mathbb{Z}_{p^r}$*. If* $\widetilde{G}$ *has full row rank, then it is called an* **encoder** *of* $\mathcal{C}$ *and* $\mathcal{C}$ *is a free module. If* $\mathcal{C}$ *has* p*-dimension* k*, a* ***p*-encoder** $G \in \mathbb{Z}_{p^r}^{k\times n}$ *of* $\mathcal{C}$ *is a matrix whose rows form a* p*-basis of* $\mathcal{C}$ *and therefore*

$$\begin{aligned}\mathcal{C} &= Im_{\mathcal{A}_p} G \\ &= \{v = uG \in \mathbb{Z}_{p^r}^n \ : u \in \mathcal{A}_p^k\}.\end{aligned}$$

Next, we introduce the notion of p-standard form that will play an important role in the sequel. First we recall the definition of standard form as introduced in [NS01].

Definition 3.2. *[NS01] Let* $\mathcal{C}$ *be a block code over* $\mathbb{Z}_{p^r}$*. A generator matrix* $\widetilde{G}$ *for* $\mathcal{C}$ *is*

said to be in **standard form** *if*

$$\widetilde{G} = \begin{bmatrix} I_{k_0} & A^0_{1,0} & A^0_{2,0} & A^0_{3,0} & \cdots & A^0_{r-1,0} & A^0_{r,0} \\ 0 & pI_{k_1} & pA^1_{2,1} & pA^1_{3,1} & \cdots & pA^1_{r-1,1} & pA^1_{r,1} \\ 0 & 0 & p^2 I_{k_2} & p^2 A^2_{3,2} & \cdots & p^2 A^2_{r-1,2} & p^2 A^2_{r,2} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{r-1} I_{k_{r-1}} & p^{r-1} A^{r-1}_{r,r-1} \end{bmatrix}, \tag{3.1}$$

where the columns are grouped into blocks of sizes $k_0, \ldots, k_{r-1}, n - \sum_{i=0}^{r-1} k_i$ *and* I_{k_i} *denotes the identity matrix of size* k_i*.*

Lemma 3.3. *[NS01] Any nonzero block code* $\mathcal{C}$ *over* $\mathbb{Z}_{p^r}$ *has a generator matrix in standard form. Moreover, all generator matrices of* $\mathcal{C}$ *in standard form have the same parameters* $k_0, k_1, \ldots, k_{r-1}$*.*

Remark 3.4. *Note that a block code over* $\mathbb{Z}_{p^r}$ *is free if and only if its parameters are* $k_0 = \tilde{k}$*,* $k_i = 0$*,* $i = 1, \ldots, r-1$*.*

We are now in position to introduce the novel notion of p-standard form that will be extensively use throughout the thesis.

Definition 3.5. *Let* $\mathcal{C}$ *be a block code over* $\mathbb{Z}_{p^r}$*. A* p*-encoder* G *of* $\mathcal{C}$ *is said to be in* ***p*-standard form** *if*

$$G = \left[\begin{array}{ccccccc} I_{k_0} & A^0_{1,0} & A^0_{2,0} & A^0_{3,0} & \cdots & A^0_{r-1,0} & A^0_{r,0} \\ \hline pI_{k_0} & 0 & pA^0_{2,1} & pA^0_{3,1} & \cdots & pA^0_{r-1,1} & pA^0_{r,1} \\ 0 & pI_{k_1} & pA^1_{2,1} & pA^1_{3,1} & \cdots & pA^1_{r-1,1} & pA^1_{r,1} \\ \hline p^2 I_{k_0} & 0 & 0 & p^2 A^0_{3,2} & \cdots & p^2 A^0_{r-1,2} & p^2 A^0_{r,2} \\ 0 & p^2 I_{k_1} & 0 & p^2 A^1_{3,2} & \cdots & p^2 A^1_{r-1,2} & p^2 A^1_{r,2} \\ 0 & 0 & p^2 I_{k_2} & p^2 A^2_{3,2} & \cdots & p^2 A^2_{r-1,2} & p^2 A^2_{r,2} \\ \hline \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ \hline p^{r-1} I_{k_0} & 0 & 0 & 0 & \cdots & 0 & p^{r-1} A^0_{r,r-1} \\ 0 & p^{r-1} I_{k_1} & 0 & 0 & \cdots & 0 & p^{r-1} A^1_{r,r-1} \\ 0 & 0 & p^{r-1} I_{k_2} & 0 & \cdots & 0 & p^{r-1} A^2_{r,r-1} \\ 0 & 0 & 0 & p^{r-1} I_{k_3} & \cdots & 0 & p^{r-1} A^3_{r,r-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{r-1} I_{k_{r-1}} & p^{r-1} A^{r-1}_{r,r-1} \end{array}\right] \tag{3.2}$$

where I_{k_i} *denotes the identity matrix of size* k_i*, with* $i = 0, \ldots, r-1$*.*

Remark 3.6. *The p-standard form defined above is a particular case of a p-basis in row echelon form (see [VSA96]).*

Given a generator matrix of $\mathcal{C}$ in standard form we can extend it to obtain *a* p-encoder in p-standard form applying the following algorithm.

Algorithm 3.7. Input data: $\widetilde{G} \leftarrow \begin{bmatrix} B_{1,k_0} \\ pB_{1,k_1} \\ p^2B_{1,k_2} \\ \vdots \\ p^{r-1}B_{1,k_{r-1}} \end{bmatrix}$ *generator matrix in standard form,* i.e.*, as in (3.1), of a block code* $\mathcal{C}$ *over* $\mathbb{Z}_{p^r}$*, where* B_{1,k_0} *is constituted by the first* k_0 *rows of* $\widetilde{G}$ *defined in (3.1) and* p^iB_{1,k_i}*, for* $i = 1, \ldots, r-1$*, is the matrix constituted by the rows* $k_0 + \cdots + k_{i-1} + 1, \ldots, k_0 + \cdots + k_{i-1} + k_i$ *of* $\widetilde{G}$*.*

Step 1: *Extend* $\widetilde{G}$ *multiplying* p^iB_{1,k_i} *by* $p, p^2, \ldots, p^{r-(i+1)}$*, with* $i = 0, \ldots, r-2$*, resulting in*

$$G \leftarrow \left[\begin{array}{c} B'_{1,k_0} \\ B'_{2,k_0} \\ B'_{3,k_0} \\ \vdots \\ B'_{r,k_0} \\ \hline B'_{1,k_1} \\ B'_{2,k_1} \\ \vdots \\ B'_{r-1,k_1} \\ \hline B'_{1,k_2} \\ \vdots \\ B'_{r-2,k_2} \\ \hline \vdots \\ \hline B'_{1,k_{r-1}} \end{array}\right],$$

where $B'_{j,k_i} = p^{i+j-1}B_{1,k_i}$*,* $j = 1, \ldots, r-i$*,* $i = 0, \ldots, r-1$*.*

Step 2: *For* $j = 2, \ldots, r-i$ *and* $i = 0, \ldots, r-2$ *replace*

$$B'_{j,k_i} \to B'_{j,k_i} - \sum_{t=1}^{j-1} A^i_{i+t,i} B'_{j-t,k_{i+t}}.$$

Step 3: *Reorder the rows in order to have* G *written in p-standard form.*

Output data*:* G*.*

Theorem 3.8. *Given a generator matrix $\widetilde{G}$ in standard form as in (3.2) of a block code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$, the Algorithm 3.7 produces a p-encoder G of $\mathcal{C}$ in p-standard form as in 3.2.*

Proof From (2.1) we guarantee that, in Step 1 of Algorithm 3.7, we construct a p-generator sequence of $\mathcal{C}$. The structure of $\widetilde{G}$ defined in (3.1) allows to state immediately that the rows of G are p-linearly independent and, therefore G is a p-encoder of $\mathcal{C}$. By Lemma 2.12, Step 2 and Step 3 of Algorithm 3.7 always produce a p-encoder. □

Remark 3.9. *If one wants to construct a p-basis in p-standard form from an arbitrary p-basis instead of starting with a set of generators, on can use results in [VSA96]. In fact, in [VSA96] was developed an algorithm, called the Gaussian Elimination algorithm, that constructs a p-basis in row echelon form for a submodule M of $\mathbb{Z}_{p^r}^n$ starting with an arbitrary p-basis of M. This algorithm can be easily adjusted in order to construct a p-basis in p-standard form using the operations of Lemma 2.12 adapted for the constant case.*

The next lemma immediately follows from Lemma 3.3 together with Theorem 3.8.

Lemma 3.10. *Any nonzero block code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ has a p-encoder in p-standard form as in 3.2.*
The scalars k_i, $i = 0, 1, \ldots, r-1$, are equal for all p-encoders of $\mathcal{C}$ written in p-standard form, i.e.*, they are uniquely determined for a given $\mathcal{C}$ and, if $\mathcal{C}$ has p-dimension k then $k = \sum_{i=0}^{r-1} k_i(r-i)$.*

Definition 3.11. *Let G be a p-encoder in p-standard form of a block code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ as in 3.2. The scalars $k_0, k_1, \ldots, k_{r-1}$ are called the* **parameters** *of $\mathcal{C}$.*

Definition 3.12. *The* **free distance** *$d(\mathcal{C})$ of a linear block code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ is given by*

$$d(\mathcal{C}) = \min\{\mathrm{wt}(v), v \in \mathcal{C}, v \neq 0\}$$

where $\mathrm{wt}(v)$ *is the Hamming weight of v,* i.e.*, the number of nonzero entries of v.*

Since the last row of a p-encoder in p-standard form is obviously a codeword it is trivial to derive a Singleton-type of upper bound on the free distance of a block code over $\mathbb{Z}_{p^r}$.

Theorem 3.13. *[NS01] Given a linear block code $\mathcal{C} \subset \mathbb{Z}_{p^r}^n$ with parameters $k_0, \ldots, k_{r-1}$, it must hold that*

$$d(\mathcal{C}) \leq n - (k_0 + \cdots + k_{r-1}) + 1.$$

Among block codes of length n and p-dimension k, we are interested in the ones with largest possible distance. For that we need to define an optimal set of parameters of M.

Definition 3.14. *Given an integer $r \geq 1$ and a non-negative integer k we call an ordered set $(k_0, k_1, \cdots, k_{r-1})$, $k_i \in \mathbb{N}$, $i = 0, \cdots, r-1$ an* **r-optimal set of parameters** *of k if*

$$k_0 + k_1 + \cdots + k_{r-1} = \min_{k = rk'_0 + (r-1)k'_1 + \cdots + k'_{r-1}} (k'_0 + k'_1 + \cdots + k'_{r-1}).$$

Note that when r divides k, $(k_0, 0, \ldots, , 0)$, with $k_0 = \frac{k}{r}$, is the unique r-optimal set of parameters of k. However,in the general case, the r-optimal set of parameters of k is not necessarily unique for a given k and r. For instance if $k = 25$ and $r = 6$, $(4, 0, 0, 0, 0, 1)$ and $(0, 5, 0, 0, 0, 0)$ are two possible 6-optimal set of parameters of 25. Note that the computation of the r-optimal set of parameters is the well-known change making problem [CG70].

Lemma 3.15. *Let $(k_0, k_1, \cdots, k_{r-1})$ be an r-optimal set of parameters of k. Then, $k_0 + k_1 + \cdots + k_{r-1} = \left\lceil \frac{k}{r} \right\rceil$.*

Proof Write $k = rb + a$, where $b, a \in \mathbb{N}$ and $a < r$. Note that a can be written as $a = r - i$, for some $1 \leq i \leq r$.
If $r | k$ then $a = 0$ and necessarily $k_0 = \frac{k}{r}$ and $k_j = 0$, for $1 \leq j \leq r-1$.
If $r \nmid k$, we can select $k_0 = b$, $k_{r-a} = 1$ and $k_j = 0$, for $j \in \{1, \ldots r-1\} \backslash \{r-a\}$. Hence $k_0 + k_1 + \cdots + k_{r-1} = b + 1 = \left\lceil \frac{k}{r} \right\rceil$. It is easy to verify that these values minimize $k_0 + k_1 + \cdots + k_{r-1}$ subject to $k = rk_0 + (r-1)k_1 + \cdots + k_{r-1}$. □

Using the previous lemma, the Singleton bound of codes over $\mathbb{Z}_{p^r}$ in terms of the p-dimension reads as follows.

Corollary 3.16. *Given a block code $\mathcal{C} \subset \mathbb{Z}_{p^r}^n$ and p-dimension k,*

$$d(\mathcal{C}) \leq n - \left\lceil \frac{k}{r} \right\rceil + 1.$$

Using a completely different approach this result was also derived in [EOS13, Theorem 3.1] without using the notions of p-standard form nor the r-optimal set of parameters. We note, however, that our approach and in particular these two notions will turn out to be crucial to derive our results in the next section and Chapter 4.

3.2 Convolutional Codes

Definition 3.17. *A* **convolutional code** $\mathcal{C}$ *of length* n *is a* $\mathbb{Z}_{p^r}[D]$*-submodule of* $\mathbb{Z}_{p^r}^n[D]$*. A* **generator matrix** $\widetilde{G}(D) \in \mathbb{Z}_{p^r}^{\tilde{k}\times n}[D]$ *of* $\mathcal{C}$ *is a polynomial matrix whose rows form a minimal set of generators of* $\mathcal{C}$ *over* $\mathbb{Z}_{p^r}[D]$ *and therefore*

$$\begin{aligned}\mathcal{C} &= Im_{\mathbb{Z}_{p^r}[D]}\widetilde{G}(D)\\ &= \left\{u(D)\widetilde{G}(D) : u(D) \in \mathbb{Z}_{p^r}^{\tilde{k}}[D]\right\}.\end{aligned}$$

If $\widetilde{G}(D)$ *has full row rank, then it is called an* **encoder** *of* $\mathcal{C}$ *and* $\mathcal{C}$ *is a free code. If* $\mathcal{C}$ *has* p*-dimension* k*, a* ***p*-encoder** $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ *of* $\mathcal{C}$ *is a polynomial matrix whose rows form a* p*-basis of* $\mathcal{C}$ *and therefore*

$$\begin{aligned}\mathcal{C} &= Im_{\mathcal{A}_p[D]}G(D)\\ &= \left\{u(D)G(D) : u(D) \in \mathcal{A}_p^k[D]\right\}.\end{aligned}$$

If the rows of $G(D)$ *(*$\widetilde{G}(D)$*) form a reduced* p*-basis (basis) then we say that* $G(D)$ *(*$\widetilde{G}(D)$*) is in* **reduced form**[1]*. The row degrees of any* p*-encoder in reduced form are invariants of the code* $\mathcal{C}$*, see Lemma 2.17, and are called* ***p*-Forney indices** *of* $\mathcal{C}$*. The sum of the* p*-Forney indices is the* ***p*-degree** *of* $\mathcal{C}$*, denoted by* δ*.*

Note that if a convolutional code admits a constant generator matrix, it is called a block code.

In the sequel, we will adopt the notation used by McEliece [McE98, p. 1082] and denote by (n, k, δ)-convolutional code a code $\mathcal{C} \subset \mathbb{Z}_{p^r}^n[D]$ with p-dimension k and p-degree δ.

Note that convolutional codes $\mathcal{C} \subset \mathbb{Z}_{p^r}^n[D]$ always admit a p-encoder however they may not admit a full row rank generator matrix, *i.e.*, an encoder. The difference is that the input vector takes values in $\mathcal{A}_p[D]$ for p-encoders whereas for generator matrices takes values in $\mathbb{Z}_{p^r}[D]$. This idea of using a p-adic expansion for the information input vector is already present in, for instance, [CS95] and was further developed in [VSA96].

Example 3.18. *Let* $\mathcal{C} = span\{g_0, g_1\} \subset \mathbb{Z}_{3^3}^3[D]$ *be a convolutional code, with*

$$g_0 = \begin{bmatrix} 1 & 1+D & 0 \end{bmatrix}$$

[1] A basis $(v_1(D), \ldots, v_k(D))$ of a free submodule M of $\mathbb{Z}_{p^r}^n[D]$ is called reduced if $v_1^{lc}, \ldots, v_k^{lc}$ are linearly independent.

and

$$g_1 = \begin{bmatrix} 3 & 0 & 3+3D \end{bmatrix}.$$

The generator matrix

$$\tilde{G}(D) = \begin{bmatrix} 1 & 1+D & 0 \\ 3 & 0 & 3+3D \end{bmatrix}$$

is not full row rank and $\mathcal{C}$ *does not admit an encoder. However,*

$$G(D) = \begin{bmatrix} g_0 \\ 3g_0 \\ 9g_0 \\ g_1 \\ 3g_1 \end{bmatrix} = \begin{bmatrix} 1 & 1+D & 0 \\ 3 & 3+3D & 0 \\ 9 & 9+9D & 0 \\ 3 & 0 & 3+3D \\ 9 & 0 & 9+9D \end{bmatrix}.$$

is a p-encoder of $\mathcal{C}$*.*

3.3 Distances of Convolutional Codes

It is well-known that the distance is the simple most important parameter to determine the performance of a block code. In the context of convolutional codes there are two fundamental distance properties that are typically analysed, namely the free distance and the column distance. In this section we formally introduce these two notions and study convolutional codes that have good distance properties.

3.3.1 Free distance

Definition 3.19. *The* **weight** *of* $v(D) = \sum_{i\geq 0} v_i D^i$*,* $v_i \in \mathbb{Z}_{p^r}$ *is given by*

$$\mathrm{wt}(v(D)) = \sum_{i\geq 0} \mathrm{wt}(v_i).$$

Definition 3.20. *The* **free distance** *of a convolutional code* $\mathcal{C}$ *is defined as*

$$d(\mathcal{C}) = \min\{\mathrm{wt}(v(D)) : v(D) \in \mathcal{C}, v(D) \neq 0\}.$$

El Oued and Solé in [EOS13] presented for the first time an upper bound on the free distance. Moreover, they showed that the bound is optimal by presenting constructions *free* MDS convolutional codes, *i.e.*, convolutional codes achieving this bound. However, the existence of nonfree MDS convolutional codes were left as an open problem and it was not clear whether nonfree convolutional codes could attain such a bound. Using a

different approach we solve this problem and provide, in the next chapter, explicit novel constructions of nonfree convolutional codes over $\mathbb{Z}_{p^r}$, for every set of given parameters, that reach this bound.
The next definition will allow us to obtain an upper bound on the free distance of an (n, k, δ)-convolutional code over $\mathbb{Z}_{p^r}$. It generalizes to convolutional codes over $\mathbb{Z}_{p^r}$ the notion of row distance for a convolutional code over a finite field [JZ99].

Definition 3.21. *The j-th row distance d_j^r of a p-encoder in reduced form $G(D)$ is defined as the minimum of the weights of all codewords resulting from a nonzero information sequence $u(D) \in \mathcal{A}_p^k[D]$ with $deg(u(D)) \leq j$,* i.e.,

$$d_j^r = \min_{\substack{deg(u(D)) \leq j \\ u(D) \neq 0}} \mathrm{wt}(u(D)G(D)).$$

Clearly, if $\mathcal{C} = \mathrm{Im}_{\mathcal{A}_p[D]} G(D)$,

$$d(\mathcal{C}) \leq \cdots \leq d_j^r \leq \cdots \leq d_1^r \leq d_0^r. \tag{3.3}$$

Let $\mathcal{C}$ be an (n, k, δ)-convolutional code defined over $\mathbb{Z}_{p^r}$. Let

$$G(D) = G_0 + G_1 D + \cdots + G_{\nu_1} D^{\nu_1} \tag{3.4}$$

be a p-encoder in reduced form with ordered row degrees $\nu_1 \geq \nu_2 \cdots \geq \nu_k$, and let $\nu = \min\{\nu_1, \nu_2, \ldots, \nu_k\}$ denote the value of the smallest row degree and ℓ the number of rows with row degree equal to ν.

We can bring the last ℓ rows of G_ν into p-standard form (see Remark 3.9). By Lemma 2.12 we still obtain a p-encoder $\widehat{G}(D)$ of $\mathcal{C}$ in reduced form with the last ℓ rows of $\widehat{G}^{lc}$ in p-standard form. Moreover, by the p-predictable degree property (Lemma 2.19), the last ℓ rows of $\widehat{G}(D)$ have degree equal to ν.

Theorem 3.22. *Let $G(D) = G_0 + G_1 D + \cdots + G_{\nu_1} D^{\nu_1}$ be a p-encoder of an (n, k, δ)-convolutional code $\mathcal{C}$ in reduced form and row degrees $\nu_1 \geq \nu_2 \cdots > \nu_{k-(\ell-1)} = \cdots = \nu_k$ and define $\nu = \nu_k$. Assume that the last ℓ rows of G_ν are in p-standard form with parameters $\ell_0, \ell_1, \ldots, \ell_{r-1}$. Then the free distance of $\mathcal{C}$ must satisfy*

$$d(\mathcal{C}) \leq n(\nu + 1) - (\ell_0 + \ell_1 + \cdots + \ell_{r-1}) + 1. \tag{3.5}$$

Proof We show that the upper bound in (3.5) is actually an upper bound of d_0^r and therefore the result readily follows from (3.3).

Denote by G'_i the last ℓ rows of $G_i(D)$, $i = 0, \ldots, \nu_1$. As these rows have degree ν we can write

$$G'(D) = G'_0 + G'_1 D + \cdots + G'_\nu D^\nu$$

where $G'_i \in \mathbb{Z}_{p^r}^{\ell \times n}$, $i = 0, \ldots, \nu$. Using the fact that G'_ν is in the p-standard form, *i.e.*,

$$G'_\nu = \left[\begin{array}{ccccccc}
I_{\ell_0} & A^0_{1,0} & A^0_{2,0} & A^0_{3,0} & \cdots & A^0_{r-1,0} & A^0_{r,0} \\
\hline
pI_{\ell_0} & 0 & pA^0_{2,1} & pA^0_{3,1} & \cdots & pA^0_{r-1,1} & pA^0_{r,1} \\
0 & pI_{\ell_1} & pA^1_{2,1} & pA^1_{3,1} & \cdots & pA^1_{r-1,1} & pA^1_{r,1} \\
\hline
p^2 I_{\ell_0} & 0 & 0 & p^2 A^0_{3,2} & \cdots & p^2 A^0_{r-1,2} & p^2 A^0_{r,2} \\
0 & p^2 I_{\ell_1} & 0 & p^2 A^1_{3,2} & \cdots & p^2 A^1_{r-1,2} & p^2 A^1_{r,2} \\
0 & 0 & p^2 I_{\ell_2} & p^2 A^2_{3,2} & \cdots & p^2 A^2_{r-1,2} & p^2 A^2_{r,2} \\
\hline
\vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\
\hline
p^{r-1} I_{\ell_0} & 0 & 0 & 0 & \cdots & 0 & p^{r-1} A^0_{r,r-1} \\
0 & p^{r-1} I_{\ell_1} & 0 & 0 & \cdots & 0 & p^{r-1} A^1_{r,r-1} \\
0 & 0 & p^{r-1} I_{\ell_2} & 0 & \cdots & 0 & p^{r-1} A^2_{r,r-1} \\
0 & 0 & 0 & p^{r-1} I_{\ell_3} & \cdots & 0 & p^{r-1} A^3_{r,r-1} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & p^{r-1} I_{\ell_{r-1}} & p^{r-1} A^{r-1}_{r,r-1}
\end{array}\right],$$

it is easy to see that the input vector

$$u = (0, 0, \cdots, 0, 1) \in \mathcal{A}_p^k[D]$$

gives a codeword

$$v(D) = uG(D) = u'G'(D)$$

with $u' = (0, \cdots, 0, 1) \in \mathcal{A}_p^\ell[D]$. The polynomial vector $v(D)$ has the last $n - (\ell_0 + \ell_1 + \cdots + \ell_{r-1}) + 1$ entries with weight at most $\nu + 1$ and the first $\ell_0 + \ell_1 + \cdots + \ell_{r-1} - 1$ coordinates with weight at most ν. Therefore,

$$\begin{aligned} d_0^r &\leq [n - (\ell_0 + \ell_1 + \cdots + \ell_{r-1}) + 1](\nu + 1) + (\ell_0 + \ell_1 + \cdots + \ell_{r-1} - 1)\nu \\ &= n(\nu + 1) - (\ell_0 + \ell_1 + \cdots + \ell_{r-1}) + 1, \end{aligned}$$

which concludes the proof. □

Given a convolutional code $\mathcal{C}$ with a p-encoder in reduced form as defined in (3.4), the parameters $(\ell_0, \ldots, \ell_{r-1})$ are invariants of $\mathcal{C}$ as we can see in the next lemma.

Lemma 3.23. *Let*

$$G(D) = G_0 + G_1 D + \cdots + G_{\nu_1} D^{\nu_1} \quad \textit{and} \quad \overline{G}(D) = \overline{G}_0 + \overline{G}_1 D + \cdots + \overline{G}_{\nu_1} D^{\nu_1}$$

be two p-encoders in reduced form of an (n, k, δ)-convolutional code $\mathcal{C}$ with row degrees $\nu_1 \geq \nu_2 \cdots > \nu_{k-\ell-1} = \cdots = \nu_k$ and define $\nu = \nu_k$. Assume that the last ℓ rows of G_ν and $\overline{G}_\nu$ are in p-standard form with parameters $\ell_0, \ell_1, \ldots, \ell_{r-1}$ and $\overline{\ell}_0, \overline{\ell}_1, \ldots, \overline{\ell}_{r-1}$, respectively. Then $\ell_i = \overline{\ell}_i$, $i = 0, \ldots, r-1$.

Proof Let

$$\overline{G}'(D) = \overline{G}'_0 + \overline{G}'_1 D + \cdots + \overline{G}'_\nu D^\nu$$

and

$$G'(D) = G'_0 + G'_1 D + \cdots + G'_\nu D^\nu$$

be the matrices constituted by the last ℓ rows of $\overline{G}(D)$ and $G(D)$, respectively.

Then, since $G(D)$ and $\overline{G}(D)$ are p-encoders in reduced form, the p-predictable degree property (Lemma 2.19) implies that

$$\operatorname{Im}_{\mathcal{A}_p[D]} G'(D) = \operatorname{Im}_{\mathcal{A}_p[D]} \overline{G}'(D)$$

and furthermore

$$\operatorname{Im}_{\mathcal{A}_p} G'_\nu = \operatorname{Im}_{\mathcal{A}_p} \overline{G}'_\nu$$

which shows, by Lemma 3.10, that $\ell_i = \overline{\ell}_i$, $i = 0, \ldots, r-1$. □

Taking the maximum of the bound (3.5) over all (n, k, δ)-convolutional codes we obtain the main result of [EOS13, Theorem 4.10], stated in the next corollary.

Corollary 3.24. *The free distance of an (n, k, δ) convolutional code $\mathcal{C}$ satisfies*

$$d(\mathcal{C}) \leq n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r} \right\rceil + 1. \tag{3.6}$$

Proof Let $G(D)$ be as in Theorem 3.22. The highest value of (3.5) is obtained by considering the maximum value of ν and the minimum value of $(\ell_0 + \ell_1 + \cdots + \ell_{r-1})$. It is easy to see that the maximum value of ν is when

$$\nu = \left\lfloor \frac{\delta}{k} \right\rfloor \quad \text{and} \quad \nu_1 = \nu_2 = \cdots = \nu_{k-\ell} = \left\lfloor \frac{\delta}{k} \right\rfloor + 1.$$

From this it follows that

$$\delta = (k - \ell)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \ell \left\lfloor \frac{\delta}{k} \right\rfloor$$

and, thus

$$\ell = k\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \delta.$$

On the other hand, the values of $(\ell_0, \ell_1, \ldots, \ell_{r-1})$ that minimize $\ell_0 + \ell_1 + \cdots + \ell_{r-1}$ and such that $\ell = \sum_{i=0}^{r}(r-i)\ell_i$ are the r-optimal set of parameters of ℓ. By Lemma 3.15,

$$\ell_0 + \ell_1 + \cdots + \ell_{r-1} = \left\lceil\frac{\ell}{r}\right\rceil.$$

Finally,

$$d(\mathcal{C}) \leq n\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \left\lceil\frac{k(\lfloor\frac{\delta}{k}\rfloor + 1) - \delta}{r}\right\rceil + 1$$

i.e.,

$$d(\mathcal{C}) \leq n\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \left\lceil\frac{k}{r}\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \frac{\delta}{r}\right\rceil + 1.$$

□

Similarly to the field case, we call the bound (3.6) the **generalized Singleton bound**.

Definition 3.25. *An (n, k, δ)-convolutional code over $\mathbb{Z}_{p^r}$ is said to be* **Maximum Distance Separable** *(MDS) if*

$$d(\mathcal{C}) = n\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \left\lceil\frac{k}{r}\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \frac{\delta}{r}\right\rceil + 1.$$

It is important to remark that the Singleton-type upper bound presented in (3.6) is derived as a corollary of the Theorem 3.22 by taking an r-optimal set parameters of $\ell = k\left(\lfloor\frac{\delta}{k}\rfloor + 1\right) - \delta$ and therefore it follows that MDS convolutional codes over $\mathbb{Z}_{p^r}$ must have these optimal set of parameters.

3.3.2 Column distance

Next definition extends the well-known truncated sliding generator matrix of a convolutional code over a finite field [RS85] to convolutional codes over $\mathbb{Z}_{p^r}$.

Definition 3.26. *Given a p-encoder $G(D) = G_0 + G_1D + \cdots + G_\nu D^\nu \in \mathbb{Z}_{p^r}^{k\times n}[D]$, we*

can define, for every $j \in \mathbb{N}_0$, the **truncated sliding generator matrix** G_j^c *as*

$$G_j^c = \begin{bmatrix} G_0 & G_1 & \cdots & G_j \\ & G_0 & \cdots & G_{j-1} \\ & & \ddots & \vdots \\ & & & G_0 \end{bmatrix} \in \mathbb{Z}_{p^r}^{(j+1)k \times (j+1)n}$$

where $G_j = 0$ whenever $j > \nu$.

Lemma 3.27. *If $G(D) \in \mathbb{Z}_{p^r}^{k \times n}[D]$ is a p-encoder of a convolutional code $\mathcal{C}$ then the rows of G_j^c form a p-generator sequence, for any $j \in \mathbb{N}_0$.*

Proof Let us represent $G(D)$ by

$$G(D) = \begin{bmatrix} g_1(D) \\ g_2(D) \\ \vdots \\ g_k(D) \end{bmatrix}$$

where $g_s(D) = \sum_{i \in \mathbb{N}_0} g_s^i D^i$, with $s = 1, \ldots, k$, is the $s - th$ row of $G(D)$. Since $G(D)$ is a p-encoder, its rows form a p-generator sequence and therefore

1. $p\, g_s(D) \in p\text{-}span\{g_{s+1}(D), \ldots, g_k(D)\}$, $s = 1, \ldots, k-1$;

2. $p\, g_k(D) = 0$.

Thus, $p\, g_s(0) \in p\text{-}span\{g_{s+1}(0), \ldots, g_k(0)\}$, $s = 1, \ldots, k-1$, and $p\, g_k(0) = 0$, which means that the rows of G_0^c form a p-generator sequence.

Let us assume now that the rows of G_j^c form a p-generator sequence and let us prove that the rows of G_{j+1}^c also form a p-generator sequence. For that it is enough to prove that

$$p\, row_s(G_{j+1}^c) \in p\text{-}span\{row_{s+1}(G_{j+1}^c), \ldots, row_{k(j+1)}(G_{j+1}^c)\}, \tag{3.7}$$

$s = 1, \ldots, k-1$, where $row_i(G_{j+1}^c)$ denotes the i-th row of G_{j+1}^c.

Let $s \in \{1, \ldots, k-1\}$. By condition 1. there exists

$$a_t(D) = \sum_{i \in \mathbb{N}_0} a_t^i D^i \in \mathcal{A}_p[D],$$

$t = s+1, \ldots, k$, such that

$$\begin{aligned} p\, g_s(D) &= a_{s+1}(D) \cdot g_{s+1}(D) + a_{s+2}(D) \cdot g_{s+2}(D) + \cdots + a_k(D) \cdot g_k(D) \\ &= \left(\sum_{i\in\mathbb{N}_0} a_{s+1}^i D^i\right)\left(\sum_{i\in\mathbb{N}_0} g_{s+1}^i D^i\right) + \left(\sum_{i\in\mathbb{N}_0} a_{s+2}^i D^i\right)\left(\sum_{i\in\mathbb{N}_0} g_{s+2}^i D^i\right) + \\ &\quad + \cdots + \left(\sum_{i\in\mathbb{N}_0} a_k^i D^i\right)\left(\sum_{i\in\mathbb{N}_0} g_k^i D^i\right), \end{aligned}$$

which implies that

$$p\, g_s^l = \sum_{\alpha=s+1}^{k} \sum_{i=0}^{l} a_\alpha^i \cdot g_\alpha^{l-i},$$

for $l = 0, \ldots, j+1$. Thus

$$\begin{aligned} p \begin{bmatrix} g_s^0 & g_s^1 & \cdots & g_s^{j+1} \end{bmatrix} &= a_{s+1}^0 \cdot \begin{bmatrix} g_{s+1}^0 & g_{s+1}^1 & \cdots & g_{s+1}^{j+1} \end{bmatrix} + \cdots + \\ &\quad + a_k^0 \begin{bmatrix} g_k^0 & g_k^1 & \cdots & g_k^{j+1} \end{bmatrix} + \\ &\quad + a_{s+1}^1 \begin{bmatrix} 0 & g_{s+1}^0 & \cdots & g_{s+1}^{j} \end{bmatrix} + \cdots a_k^1 \begin{bmatrix} 0 & g_k^0 & \cdots & g_k^{j} \end{bmatrix} + \\ &\quad + \cdots + \\ &\quad + a_{s+1}^{j+1} \begin{bmatrix} 0 & \cdots & 0 & g_{s+1}^0 \end{bmatrix} + \cdots + a_k^{j+1} \begin{bmatrix} 0 & \cdots & 0 & g_k^0 \end{bmatrix}, \end{aligned}$$

which proves 3.7. □

Notice that the rows of G_j^c may not be p-linearly independent for some j as the following example shows.

Example 3.28. *Consider the p-encoder*

$$G(D) = \begin{bmatrix} 1+D & 1+D & 1+D & 1+D \\ 3+3D & 3+3D & 3+3D & 3+3D \\ 0 & 0 & 0 & 3D^2 \end{bmatrix} \in \mathbb{Z}_9^{3\times 4}[D]$$

The rows of

$$G_1^c = \begin{bmatrix} G_0 & G_1 \\ & G_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & 1 & 1 & 1 & 1 \\ & & & & 3 & 3 & 3 & 3 \\ & & & & 0 & 0 & 0 & 0 \end{bmatrix}$$

are not p-linearly independent.

Definition 3.29. *[KP09] A p-encoder $G(D)$ of a convolutional code $\mathcal{C} \subset \mathbb{Z}_{p^r}^n[D]$ is said to be* **delay-free** *if, for any $N \in \mathbb{Z}$ and any $v(D) = u(D)G(D)$, $u(D) \in \mathcal{A}_p^k[D]$, we have*

$$supp\,(v(D)) \subset [N, \infty) \Rightarrow supp\,(u(D)) \subset [N, \infty),$$

where, considering $v(D) = \sum_{i \in \mathbb{N}_0} v_i D^i$, $supp\,(v(D)) = \{i \in \mathbb{N}_0 : v_i \neq 0\}$ ($supp\,(u(D))$ is defined in the same way).

Lemma 3.30. *[KP09] Let $G(D) = G_0 + G_1 D + \cdots + G_\nu D^\nu$, with $G_i \in \mathbb{Z}_{p^r}^{k \times n}$, $i = 0, \ldots, \nu$, be a p-encoder of a convolutional code $\mathcal{C}$ of length n and p-dimension k. Then $G(D)$ is delay-free if and only if the rows of $G(0) = G_0$ are p-linearly independent.*

If $G(D)$ is a delay-free p-encoder, since the rows of $G(0)$ are p-linearly independent, all rows of G_j^c are p-linearly independent, for $j \in \mathbb{N}_0$.
Let us define

$$\mathcal{C}_0 = \{v_0 : v(D) = \sum_{i \geq 0} v_i D^i \in \mathcal{C}\}.$$

It is immediate that

$$\mathcal{C}_0 = \mathrm{Im}\,_{\mathcal{A}_p} G_0,$$

for any p-encoder $G(D)$ of $\mathcal{C}$.

Lemma 3.31. *If a convolutional code $\mathcal{C}$ of length n and p-dimension k admits a delay-free p-encoder, then all the p-encoders of $\mathcal{C}$ are delay-free.*

Proof Let $G(D) \in \mathbb{Z}_{p^r}^{k \times n}[D]$, $G'(D) \in \mathbb{Z}_{p^r}^{k \times n}[D]$ be two different p-encoders of $\mathcal{C}$. If $G(D)$ is delay-free then the rows of $G(0)$ are p-linearly independents and therefore $p\text{-dim}(\mathcal{C}_0) = k$, with $\mathcal{C}_0$ as defined above. So, since $\mathrm{Im}\,_{\mathcal{A}_p} G_0 = \mathrm{Im}\,_{\mathcal{A}_p} G_0'$, the rows of $G'(0)$ must also be p-linearly independent, which means that $G'(D)$ is also delay-free. □

From now on, convolutional codes with delay-free p-encoders will be called **delay-free convolutional codes**.

Definition 3.32. *Given a p-encoder $G(D)$ of a convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ we define the $j-th$* **column distance** *of $G(D)$ as*

$$d_j^c(G) = \min\{\mathrm{wt}(v) : v = u\,G_j^c \in \mathbb{Z}_{p^r}^{n(j+1)},\ u = [u_0 \ldots u_j],\ u_0 \neq 0,\ u \in \mathcal{A}_p^k,\ i = 0, \ldots, j\}.$$

for $j \in \mathbb{N}_0$.

It is obvious that $d_j^c(G) \leq d_{j+1}^c(G)$, for $j \in \mathbb{N}_0$.

Remark 3.33. *If* $\mathcal{C}$ *is a delay-free convolutional code and* $G(D)$ *and* $G'(D)$ *are two* p*-encoders of* $\mathcal{C}$*, then*

$$\begin{aligned} d_j^c(G) &= d_j^c(G') \\ &= \min\{\mathrm{wt}\big(v(D)|_{[0,j]}\big) : v(D) \in \mathcal{C} \ \text{ and } \ v_0 \neq 0\}, \end{aligned}$$

where $v(D)|_{[0,j]} = v_0 + v_1 D + \cdots + v_j D^j$*, for* $v(D) = \sum_{i \in \mathbb{N}} v_i D^i$*. Thus, the* j*-th column distance of* p*-encoders of* $\mathcal{C}$ *is an invariant of the code and we will simply denote it by* d_j^c.

Let $\mathcal{C}$ be a delay-free convolutional code with a p-encoder $G(D)$ written as

$$G(D) = G_0 + G_1 D + \cdots + G_\nu D^\nu,$$

with $G_i \in \mathbb{Z}_{p^r}^{k \times n}$, $i = 0, \ldots, \nu$ and $G_\nu \neq 0$. We can consider G_0 in the p-standard form as

$$G_0 = \left[\begin{array}{ccccccc} I_{k_0} & A_{1,0}^0 & A_{2,0}^0 & A_{3,0}^0 & \cdots & A_{r-1,0}^0 & A_{r,0}^0 \\ \hline pI_{k_0} & 0 & pA_{2,1}^0 & pA_{3,1}^0 & \cdots & pA_{r-1,1}^0 & pA_{r,1}^0 \\ 0 & pI_{k_1} & pA_{2,1}^1 & pA_{3,1}^1 & \cdots & pA_{r-1,1}^1 & pA_{r,1}^1 \\ \hline p^2 I_{k_0} & 0 & 0 & p^2 A_{3,2}^0 & \cdots & p^2 A_{r-1,2}^0 & p^2 A_{r,2}^0 \\ 0 & p^2 I_{k_1} & 0 & p^2 A_{3,2}^1 & \cdots & p^2 A_{r-1,2}^1 & p^2 A_{r,2}^1 \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{3,2}^2 & \cdots & p^2 A_{r-1,2}^2 & p^2 A_{r,2}^2 \\ \hline \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ \hline p^{r-1} I_{k_0} & 0 & 0 & 0 & \cdots & 0 & p^{r-1} A_{r,r-1}^0 \\ 0 & p^{r-1} I_{k_1} & 0 & 0 & \cdots & 0 & p^{r-1} A_{r,r-1}^1 \\ 0 & 0 & p^{r-1} I_{k_2} & 0 & \cdots & 0 & p^{r-1} A_{r,r-1}^2 \\ 0 & 0 & 0 & p^{r-1} I_{k_3} & \cdots & 0 & p^{r-1} A_{r,r-1}^3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{r-1} I_{k_{r-1}} & p^{r-1} A_{r,r-1}^{r-1} \end{array}\right] \tag{3.8}$$

where $k_0, k_1, \ldots, k_{r-1}$ are the parameters of $\mathcal{C}_0$. With these parameters we can rewrite $G(D)$ and G_i, $i = 0, 1, \ldots, \nu$, as

$$G(D) = \begin{bmatrix} \widehat{G}^{(0)}(D) \\ \widehat{G}^{(1)}(D) \\ \vdots \\ \widehat{G}^{(r-2)}(D) \\ \widehat{G}^{(r-1)}(D) \end{bmatrix} \tag{3.9}$$

and

$$G_i = \begin{bmatrix} \widehat{G}_i^{(0)} \\ \widehat{G}_i^{(1)} \\ \vdots \\ \widehat{G}_i^{(r-2)} \\ \widehat{G}_i^{(r-1)} \end{bmatrix}, \tag{3.10}$$

where $\widehat{G}^{(0)}(D)$ and $G_i^{(0)}$, are the submatrices of $G(D)$ and G_i by considering the first k_0 rows, respectively, and $\widehat{G}^{(b)}(D)$ and $\widehat{G}_i^{(b)}$, $b = 1, 2, \ldots r-1$, are constituted by the rows $\bar{k}_0 + \bar{k}_1 + \cdots + \bar{k}_{b-1} + 1, \ldots, \bar{k}_0 + \bar{k}_1 + \cdots + \bar{k}_b$ of $G(D)$ and G_i, respectively, where $\bar{k}_j = k_0 + k_1 + \cdots + k_j$, $j = 0, \ldots, r-1$. Note that $\widehat{G}^{(b)}(D) \in \mathbb{Z}_{p^r}^{\bar{k}_b \times n}[D]$ and $\widehat{G}_i^{(b)} \in \mathbb{Z}_{p^r}^{\bar{k}_b \times n}$.

Lemma 3.34. *Let $\mathcal{C}$ be a delay-free convolutional code with a p-encoder $G(D)$ written as in (3.9) and (3.10). Then, for $b = 1, 2, \ldots, r-1$,*

$$\widehat{G}_i^{(b)} \in p^{\ell} \mathbb{Z}_{p^r}^{\bar{k}_b \times n} \tag{3.11}$$

where $\ell = b - i$, for $b - i \geq 0$ and $\ell = 0$ for $b - i < 0$.

Proof Since $G(D)$ is a p-generator sequence

$$p\, row_l G(D) \in p\text{-span}\{row_{l+1}G(D), \ldots, row_k G(D)\},$$

for $l = 1, \ldots, k-1$, implies that

$$p\, row_j \widehat{G}^{(r-1)}(D) = a_{j+1}(D) row_{j+1}\widehat{G}^{(r-1)}(D) + \cdots + a_{\bar{k}_{r-1}}(D) row_{\bar{k}_{r-1}}\widehat{G}^{(r-1)}(D),$$

where $row_t \widehat{G}^{(r-1)}(D)$ and $row_t \widehat{G}^{(r-1)}$ represent the t-th row of $\widehat{G}^{(r-1)}(D)$ and $\widehat{G}^{(r-1)}$, respectively, and $a_{j+1}(D), \ldots, a_{\bar{k}_{r-1}}(D) \in \mathcal{A}_p[D]$, for $j = 1, \ldots, \bar{k}_{r-1} - 1$.

Note that $\widehat{G}_0^{(r-1)} \in p^{r-1}\mathbb{Z}_{p^r}^{\bar{k}_{r-1} \times n}$. Thus, for $j = 1, \ldots, \bar{k}_{r-1} - 1$,

$$0 = a_{j+1}(0) row_{j+1}\widehat{G}^{(r-1)}(0) + \cdots + a_{\bar{k}_{r-1}}(0) row_{\bar{k}_{r-1}}\widehat{G}^{(r-1)}(0),$$

which implies that

$$a_{j+1}(0) = \cdots = a_{\bar{k}_{r-1}}(0) = 0,$$

since the rows of G_0 are p-linearly independent. Thus, for $i = 1, \ldots, r-1$, it follows that

$$p\,\widehat{G}_i^{(r-1)} \in \operatorname{Im}_{\mathcal{A}_p} \begin{bmatrix} \widehat{G}_{i-1}^{(r-1)} \\ \widehat{G}_{i-2}^{(r-1)} \\ \vdots \\ \widehat{G}_0^{(r-1)} \end{bmatrix}$$

and, therefore

$$\widehat{G}_i^{(r-1)} \in p^{r-1-i}\mathbb{Z}_{p^r}^{\bar{k}_{r-1}\times n}, \quad \text{if} \quad r-1-i \geq 0$$

or

$$\widehat{G}_i^{(r-1)} \in \mathbb{Z}_{p^r}^{\bar{k}_{r-1}\times n}, \quad \text{if} \quad r-i-1 < 0.$$

Following the same reasoning, we prove that

$$p\,\widehat{G}_i^{(b)} \in \operatorname{Im}_{\mathcal{A}_p} \left[\begin{array}{c} \widehat{G}_{i-1}^{(b)} \\ \vdots \\ \widehat{G}_0^{(b)} \\ \hline \widehat{G}_{i-1}^{(b-1)} \\ \vdots \\ \widehat{G}_0^{(b-1)} \\ \hline \vdots \\ \hline \widehat{G}_{i-1}^{(r-1)} \\ \vdots \\ \widehat{G}_0^{(r-1)} \end{array}\right]$$

which implies the result. □

Theorem 3.35. *Given a delay-free convolutional code $\mathcal{C}$ with length n and p-dim$(\mathcal{C}) = k$, with $k_0, k_1, \ldots, k_{r-1}$ being the parameters of $\mathcal{C}_0$, it holds*

$$d_j^c \leq (j+1)\left(n - \sum_{i=0}^{r-j} k_i\right) - \sum_{s=2}^{j} s k_{r-(s-1)} + 1, \quad j \leq r$$

and

$$d_j^c \leq (j+1)n - \sum_{i=0}^{r-1} k_i - k - (j-r)k_0 + 1, \quad j > r.$$

Proof Let $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ be a p-encoder of $\mathcal{C}$ and let us consider the truncated sliding generator matrix G_j^c to obtain

$$d_j^c = d_j^c(G) = \min\{\mathrm{wt}(v) : v = u\,G_j^c, u = [u_0 \dots u_j], u_0 \neq 0, u_i \in \mathcal{A}_p^k, i = 0, \dots, j\}.$$

By Lemma 3.30, the rows of G_0 form a p-basis and then we can assume without loss of generality that G_0 is in p-standard form as in (3.8), with parameters $k_0, k_1, \dots, k_{r-1}$. Let us consider $j = 0$ and take

$$u = u_0 = \left[\begin{array}{cccc} 0 & 0 & \dots & 1 \end{array}\right] \in \mathcal{A}_p^k.$$

Then $v = uG$ is given by

$$v = \left[\begin{array}{ccccc} 0 & \dots & 0 & 1 & p^{r-1}A_{r,r-1}^{r-1,k} \end{array}\right],$$

where $A_{r,r-1}^{r-1,k}$ represents the last row of $A_{r,r-1}^{r-1}$. Since v has at least $(k_0+k_1+\cdots+k_{r-1}-1)$ zero elements, we have that

$$\mathrm{wt}(v) \leq n - (k_0 + k_1 + \cdots + k_{r-1}) + 1,$$

and therefore,

$$d_0^c \leq n - (k_0 + k_1 + \cdots + k_{r-1}) + 1.$$

Let us consider now $j = 1$ and $u = \left[\begin{array}{cc} u_0 & u_1 \end{array}\right]$, with $u_0, u_1 \in \mathcal{A}_p^k$ such that $u_0 \neq 0$, and

$$\begin{aligned} & v = uG_1^c \\ \Leftrightarrow & \left[\begin{array}{cc} v_0 & v_1 \end{array}\right] = u_0 \left[\begin{array}{cc} G_0 & G_1 \end{array}\right] + u_1 \left[\begin{array}{cc} 0 & G_0 \end{array}\right], \end{aligned}$$

with $v_i \in \mathbb{Z}_{p^r}^n$, $i = 0, 1$. Taking again

$$u_0 = \left[\begin{array}{cccc} 0 & 0 & \dots & 1 \end{array}\right]$$

we obtain

$$\left\{\begin{array}{l} v_0 = \left[\begin{array}{ccccc} 0 & \dots & 0 & 1 & p^{r-1}A_{r,r-1}^{r-1,k} \end{array}\right] \\ \\ v_1 = g_1^{'} + u_1 G_0 \end{array}\right.,$$

where $p^{r-1}A_{r,r-1}^{r-1,k}$ represents the last row of $A_{r,r-1}^{r-1}$ and $g_1^{'}$ represents the last row of G_1. Thus,

$$\mathrm{wt}(v_0) \leq n - (k_0 + k_1 + \cdots + k_{r-1}) + 1.$$

Note that, since $G(D)$ is a p-encoder, its last row is in $p^{r-1}\mathbb{Z}_{p^r}^n[D]$ and therefore the last row of G_1 can be written as $p^{r-1}\tilde{g}_1$, for some $\tilde{g}_1 \in \mathbb{Z}_{p^r}^n$. Moreover, $\tilde{g}_1$ can be written uniquely as

$$\tilde{g}_1 = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1}p^{r-1}, \;\; \alpha_i \in \mathcal{A}_p^n, \;\; i = 0, 1, \ldots, r-1.$$

Thus,

$$p^{r-1}\tilde{g}_1 = p^{r-1}\alpha_0.$$

It is now clear that $v_1 = p^{r-1}g_1 + u_1G_0$, with $g_1 \in \mathcal{A}_p^n$.

Write g_1 as

$$g_1 = \left[\begin{array}{cccc} g_{1,k_0} & g_{1,k_1} & \cdots & g_{1,k_{r-1}} \quad g_{1,n-(k_0+\cdots+k_{r-1})} \end{array} \right],$$

with $g_{1,i} \in \mathcal{A}_p^i$, $i = k_0, k_1, \ldots, k_{r-1}$ and $g_{1,n-(k_0+\cdots+k_{r-1})} \in \mathcal{A}_p^{n-(k_0+\cdots+k_{r-1})}$.

Let us construct u_1 such that:

- its first $[(r-1)k_0 + (r-2)k_1 + \cdots + k_{r-2}]$ components are zero;

- the remaining $k_0 + k_1 + \cdots + k_{r-1}$ components are written as

$$\left[\begin{array}{cccc} \alpha_{1,k_0} & \alpha_{1,k_1} & \cdots & \alpha_{1,k_{r-1}} \end{array} \right],$$

where $\alpha_{1,k_i} \in \mathcal{A}_p^i$ are such that $p^{r-1}\left(-g_{1,k_i}\right) = p^{r-1}\alpha_{1,k_i}$, $i = 0, \ldots, r-1$.

So, we obtain v_1 with its first $(k_0 + k_1 + \cdots + k_{r-1})$ elements equal to zero. Thus,

$$\begin{aligned} \mathrm{wt}(v) &= \mathrm{wt}(v_0) + \mathrm{wt}(v_1) \\ &\leq 2n - 2(k_0 + k_1 + \cdots + k_{r-1}) + 1, \end{aligned}$$

and we obtain

$$d_1^c \leq 2n - 2(k_0 + k_1 + \cdots + k_{r-1}) + 1.$$

Let $j = 2$, $u = \left[\begin{array}{ccc} u_0 & u_1 & u_2 \end{array} \right]$, $u_i \in \mathcal{A}_p^k$, $i = 0, 1, 2$, with $u_0 \neq 0$, and let $v =$

$\left[\begin{array}{ccc} v_0 & v_1 & v_2 \end{array}\right]$, with $v_i \in \mathbb{Z}_{p^r}^n$, $i = 0, 1, 2$, such that

$$\begin{aligned} & v = uG_2^c \\ \Leftrightarrow & \left[\begin{array}{ccc} v_0 & v_1 & v_2 \end{array}\right] = u_0 \left[\begin{array}{ccc} G_0 & G_1 & G_2 \end{array}\right] + u_1 \left[\begin{array}{ccc} 0 & G_0 & G_1 \end{array}\right] + u_2 \left[\begin{array}{ccc} 0 & 0 & G_0 \end{array}\right], \end{aligned}$$

Considering

$$u_0 = \left[\begin{array}{cccc} 0 & 0 & \dots & 1 \end{array}\right] \in \mathcal{A}_p^k$$

we have that

$$\begin{cases} v_0 = \left[\begin{array}{cccccc} 0 & \dots & 0 & 1 & p^{r-1}A_{r,r-1}^{r-1,k} \end{array}\right] \\ v_1 = g_1' + u_1 G_0 \\ v_2 = g_2' + u_1 G_1 + u_2 G_0 \end{cases},$$

where $p^{r-1}A_{r,r-1}^{r-1,k}$ represents the last row of $A_{r,r-1}^{r-1}$ in G_0 and g_1' and g_2' represent the last row of G_1 and G_2, respectively, with $g_1', g_2' \in \mathbb{Z}_{p^r}^n$. So,

$$\mathrm{wt}(v_0) \leq n - (k_0 + k_1 + \cdots + k_{r-1}) + 1.$$

Considering u_1 as in the previous case we obtain v_1 with

$$\mathrm{wt}(v_1) \leq n - (k_0 + k_1 + \cdots + k_{r-1}).$$

Let us now consider $v_2 = g_2' + \tilde{g}_1 + u_2 G_0$, with $\tilde{g}_1 = u_1 G_1$. By Lemma 3.34

$$\tilde{g}_1 \in p^{r-2}\,\mathbb{Z}_{p^r}^n$$

and therefore

$$g_2' + \tilde{g}_1 = p^{r-1}\,g_1^1 + p^{r-2}\,g_1^2,$$

for some $g_1^2, g_1^1 \in \mathcal{A}_p^n$.

Write

$$\begin{cases} g_1^2 = \left[\begin{array}{cc} g_{11}^2 & g_{12}^2 \end{array}\right] \\ g_1^1 = \left[\begin{array}{cc} g_{11}^1 & g_{12}^1 \end{array}\right] \end{cases},$$

with $g_{11}^i \in \mathcal{A}_p^{k_0+k_1+\cdots+k_{r-2}}$ and $g_{12}^i \in \mathcal{A}_p^{n-(k_0+k_1+\cdots+k_{r-2})}$, for $i = 1, 2$, and let us construct $\tilde{u}_2 \in \mathbb{Z}_{p^r}^n$ such that:

- its first $[(r-2)k_0 + (r-3)k_1 + \cdots + k_{r-3}]$ components are zero;

- the next $(k_0 + k_1 + \cdots + k_{r-2} + k_0 + k_1 + \cdots + k_{r-2})$ components are written as

$$\left[\begin{array}{cc} -g_{11}^1 & -g_{11}^2 \end{array} \right];$$

- the last k_{r-1} components are zero.

Since the rows of G_0 form a p-generator sequence, consider $u_2 \in \mathcal{A}_p$ such that $\tilde{u}_2 G_0 = u_2 G_0$. Thus, the first $k_0 + k_1 + \cdots + k_{r-2}$ columns of v_2 are zero and consequently

$$\mathrm{wt}(v_2) \leq n - (k_0 + k_1 + \cdots + k_{r-2}).$$

Therefore,

$$\begin{aligned} \mathrm{wt}(v) &= \sum_{i=0}^{2} \mathrm{wt}(v_i) \\ &\leq 3n - 2(k_0 + k_1 + \cdots + k_{r-1}) - (k_0 + k_1 + \cdots + k_{r-2}) + 1, \end{aligned}$$

and therefore

$$d_2^c \leq 3n - 2(k_0 + k_1 + \cdots + k_{r-1}) - (k_0 + k_1 + \cdots + k_{r-2}) + 1.$$

Taking a general j, $u = \left[\begin{array}{cccc} u_0 & u_1 & \cdots & u_j \end{array} \right]$, $u_i \in \mathcal{A}_p^k$, with $u_0 \neq 0$, and let $v = \left[\begin{array}{cccc} v_0 & v_1 & \cdots & v_j \end{array} \right]$, with $v_i \in \mathbb{Z}_{p^r}^n$, $i = 0, 1, \ldots, j$, such that

$$\begin{aligned} & v = uG_j^c \\ \Leftrightarrow & \left[\begin{array}{cccc} v_0 & v_1 & \ldots & v_j \end{array} \right] = u_0 \left[\begin{array}{cccc} G_0 & G_1 & \ldots & G_j \end{array} \right] + u_1 \left[\begin{array}{cccc} 0 & G_0 & \ldots & G_{j-1} \end{array} \right] + \cdots + \\ & \qquad + u_j \left[\begin{array}{cccc} 0 & 0 & \ldots & G_0 \end{array} \right]. \end{aligned}$$

Using the same procedure as before we can construct $u_0, \ldots, u_j \in \mathcal{A}_p^k$, such that

$$\mathrm{wt}(v_0) \leq n - (k_0 + k_1 + \cdots + k_{r-1}) + 1, \tag{3.12}$$

$$\mathrm{wt}(v_i) \leq n - (k_0 + k_1 + \cdots + k_{r-i}), \quad i \leq r \tag{3.13}$$

and

$$\mathrm{wt}(v_i) \leq n - k_0, \quad i > r, \tag{3.14}$$

for all $i = 1, \dots j$. So, since

$$\mathrm{wt}(v) = \sum_{i=0}^{j} \mathrm{wt}(v_i),$$

we conclude that

$$\mathrm{wt}(v) \leq (j+1)n - (k_0 + k_1 + \cdots + k_{r-1}) - \sum_{i=1}^{j}(k_0 + k_1 + \cdots + k_{r-i}) + 1, \text{ if } j \leq r$$

and

$$\mathrm{wt}(v) \leq (j+1)n - (k_0 + k_1 + \cdots + k_{r-1}) - \sum_{i=1}^{r}(k_0 + k_1 + \cdots + k_{r-i}) - \sum_{i=r+1}^{j} k_0 + 1, \text{ if } j > r.$$

Therefore, for $j \leq r$

$$\begin{aligned} d_j^c &\leq (j+1)n - (k_0 + k_1 + \cdots + k_{r-1}) - \sum_{i=1}^{j}(k_0 + k_1 + \cdots + k_{r-i}) + 1 \\ &= (j+1)n - [(j+1)(k_0 + k_1 + \cdots + k_{r-j}) + jk_{r-(j-1)} + \\ &\quad + (j-1)k_{r-(j-2)} + \cdots + 2k_{r-1}] + 1 \\ &= (j+1)\left(n - \sum_{i=0}^{r-j} k_i\right) - \sum_{s=2}^{j} sk_{r-(s-1)} + 1 \end{aligned}$$

and, for $j > r$

$$\begin{aligned} d_j^c &\leq (j+1)n - (k_0 + k_1 + \cdots + k_{r-1}) - \sum_{i=1}^{r}(k_0 + k_1 + \cdots + k_{r-i}) - \sum_{i=r+1}^{j} k_0 + 1 \\ &= (j+1)n - (k_0 + k_1 + \cdots + k_{r-1}) - [rk_0 + (r-1)k_1 + \cdots + k_{r-1}] - (j-r)k_0 + 1 \\ &= (j+1)n - \sum_{i=0}^{r-1} k_i - k - (j-r)k_0 + 1. \end{aligned}$$

□

The column distance measures the distance between two codewords within a time interval. Hence we seek for codes with column distances as large as possible. Column distances are very appealing for sequential decoding: the larger column distance the larger number of error we can correct per time interval. Thus, it follows from Theorem 3.35 that the r-optimal set of parameters of k has to be such that the value of k_0 has

to be the greatest possible. So, the r-optimal set of parameters of k, $(k_0, k_1, \ldots, k_{r-1})$, is given by

$$k_0 = \left\lfloor \frac{k}{r} \right\rfloor, \quad k_{r-R} = 1 \quad \text{and} \quad k_i = 0, \tag{3.15}$$

where $R = k - \left\lfloor \frac{k}{r} \right\rfloor r$ and $i = 1, \ldots, r-1$, $i \neq r - R$.

With this r-optimal set of parameters we can maximize the bound found in Theorem 3.35 as is shown in the next result. Note that if $\mathcal{C}$ is a nondelay-free convolutional code with p-encoder $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ then there exists $u_0 \in \mathcal{A}_p^k \backslash \{0\}$ such that $u_0 G(0) = 0$, which implies that $d_0^c(G) = 0$. Thus, convolutional codes with maximal column distances will always be delay free. From now on, we consider delay-free convolutional codes.

Corollary 3.36. *Given a convolutional code $\mathcal{C}$ with length n and p-dim$(\mathcal{C}) = k$ it holds*

$$d_j^c \leq \left(n - \left\lceil \frac{k}{r} \right\rceil \right)(j+1) + 1, \quad j \leq R$$

and

$$d_j^c \leq \left(n - \left\lfloor \frac{k}{r} \right\rfloor \right)(j+1) - \left(\left\lceil \frac{k}{r} \right\rceil - \left\lfloor \frac{k}{r} \right\rfloor \right)(R+1) + 1, \quad j > R,$$

with $R = k - \left\lfloor \frac{k}{r} \right\rfloor r$.

Proof Let $k_0, k_1, \ldots, k_{r-1}$ be the parameters of $\mathcal{C}_0$ and let us recall that

$$d_j^c = d_j^c(G) = \min\{\mathrm{wt}(v) : v = u\, G_j^c, u = [u_0 \ldots u_j], u_0 \neq 0, u_i \in \mathcal{A}_p^k, i = 0, \ldots, j\},$$

where G_j^c the truncated sliding generator matrix of a p-encoder $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ of $\mathcal{C}$.

From (3.12), (3.13) and (3.14) in the proof of Theorem 3.35, and (3.15) we have

$$\mathrm{wt}(v_0) \leq n - \left\lceil \frac{k}{r} \right\rceil + 1,$$

$$\mathrm{wt}(v_i) \leq n - \left\lceil \frac{k}{r} \right\rceil, \; i \leq R$$

and

$$\mathrm{wt}(v_i) \leq n - \left\lfloor \frac{k}{r} \right\rfloor, \; i > R.$$

Therefore, since

$$\mathrm{wt}(v) = \sum_{i=0}^{j} \mathrm{wt}(v_i),$$

we conclude that, for $j \leq R$,

$$d_j^c \leq (n - \left\lceil \frac{k}{r} \right\rceil)(j+1) + 1,$$

and for $j > R$,

$$d_j^c \leq n(j+1) - \left\lceil \frac{k}{r} \right\rceil + 1 - \left\lceil \frac{k}{r} \right\rceil R - \left\lfloor \frac{k}{r} \right\rfloor (j - R)$$

$$= \left(n - \left\lfloor \frac{k}{r} \right\rfloor\right)(j+1) - \left(\left\lceil \frac{k}{r} \right\rceil - \left\lfloor \frac{k}{r} \right\rfloor\right)(R+1) + 1.$$

□

Let us denote the bound obtained in Corollary 3.24 for the column distance by

$$B(j) = \begin{cases} \left(n - \left\lceil \frac{k}{r} \right\rceil\right)(j+1) + 1 & , \ j \leq R \\ \left(n - \left\lfloor \frac{k}{r} \right\rfloor\right)(j+1) - \left(\left\lceil \frac{k}{r} \right\rceil - \left\lfloor \frac{k}{r} \right\rfloor\right)(R+1) + 1 & , \ j > R \end{cases},$$

where $R = k - \left\lfloor \frac{k}{r} \right\rfloor r$, and the singleton bound obtain in Corollary 3.36 for the free distance

$$\begin{aligned} SB &= n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r} \right\rceil + 1 \\ &= \left(n - \frac{k}{r}\right)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \frac{\delta}{r} - \varphi + 1, \end{aligned}$$

with $\varphi = \left\lceil \frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r} \right\rceil - \left(\frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r}\right)$.

Definition 3.37. *An (n, k, δ)-convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ is said to be* **Maximum Distance Profile** *(MDP) if*

$$d_j^c = B(j),$$

for $j \leq L$, where

$$L = max\{j : B(j) \leq SB\}.$$

The next theorem determines explicitly the value of the integer L that appears in the definition of MDP (n, k, δ)-convolutional code over $\mathbb{Z}_{p^r}$.

Theorem 3.38. *Let $\mathcal{C}$ be an MDP (n,k,δ)-convolutional code over $\mathbb{Z}_{p^r}$, $R = k - \left\lfloor \frac{k}{r} \right\rfloor r$,*

$$X = \frac{\left(n - \frac{k}{r}\right)\left\lfloor \frac{\delta}{k} \right\rfloor + \frac{\delta}{r} - \varphi + \left\lceil \frac{k}{r} \right\rceil - \frac{k}{r}}{n - \left\lceil \frac{k}{r} \right\rceil}$$

and

$$X' = \left\lfloor \frac{\delta}{r} \right\rfloor + \frac{-\frac{R}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \frac{\delta}{r} - \varphi + \left(\left\lceil \frac{k}{r} \right\rceil - \frac{k}{r}\right)(r+1)}{n - \left\lfloor \frac{k}{r} \right\rfloor},$$

with $\varphi = \left\lceil \frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r} \right\rceil - \left(\frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r}\right)$.

Then

$$L = \begin{cases} \lfloor X \rfloor, & \text{if } X \leq R \\ R, & \text{if } X > R \ \wedge B(R+1) > SB \\ \lfloor X' \rfloor, & \text{otherwise} \end{cases}.$$

Proof Let us consider the increasing function f defined by

$$\begin{array}{rccc} f: & \mathbb{R}_0^+ & \longrightarrow & \mathbb{R}_0^+ \\ & x & \mapsto & B(x) \end{array},$$

with

$$B(x) = \begin{cases} \left(n - \left\lceil \frac{k}{r} \right\rceil\right)(x+1) + 1 & , \ x \leq R \\ \left(n - \left\lfloor \frac{k}{r} \right\rfloor\right)(x+1) - \left(\left\lceil \frac{k}{r} \right\rceil - \left\lfloor \frac{k}{r} \right\rfloor\right)(R+1) + 1 & , \ x > R \end{cases},$$

where $x \in \mathbb{R}_0^+$ and $R = k - \left\lfloor \frac{k}{r} \right\rfloor r$.

If $X \leq R$ we have that

$$\begin{aligned} f(X) &= \left(n - \left\lceil \frac{k}{r} \right\rceil\right)\left(\frac{\left(n - \frac{k}{r}\right)\left\lfloor \frac{\delta}{k} \right\rfloor + \frac{\delta}{r} - \varphi + \left\lceil \frac{k}{r} \right\rceil - \frac{k}{r}}{n - \left\lceil \frac{k}{r} \right\rceil} + 1\right) + 1 \\ &= SB \end{aligned}$$

and, therefore $L = \lfloor X \rfloor$.

If $X > R$ and $B(R+1) > SB$ it follows immediately that $f(R) = SB$.

Finally if $X > R$ and $B(R+1) \leq SB$ we can write

$$\begin{aligned} f(X') &= \left(n - \left\lfloor \frac{k}{r} \right\rfloor\right)\left(\left\lfloor \frac{\delta}{r} \right\rfloor + \frac{-\frac{R}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \frac{\delta}{r} - \varphi + \left(\left\lceil \frac{k}{r} \right\rceil - \frac{k}{r}\right)(r+1)}{n - \left\lfloor \frac{k}{r} \right\rfloor} + 1\right) - \\ &\quad - \left(\left\lceil \frac{k}{r} \right\rceil - \left\lfloor \frac{k}{r} \right\rfloor\right)(R+1) + 1 \\ &= \left(n - \left\lfloor \frac{k}{r} \right\rfloor\right)\left\lfloor \frac{\delta}{r} \right\rfloor - \frac{R}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \frac{\delta}{r} - \varphi + n - \left\lfloor \frac{k}{r} \right\rfloor + 1 \\ &= SB \end{aligned}$$

and, therefore $L = \lfloor X' \rfloor$.

□

In this thesis we shall consider two particular cases, namely when $k \mid \delta$ and $r \mid k$. For these cases Theorem 3.38 reads as follows.

Corollary 3.39. *Let $\mathcal{C}$ be an MDP (n, k, δ)-convolutional code over $\mathbb{Z}_{p^r}$ with $k \mid \delta$. Let*

$$X = \frac{\delta}{k} + \frac{\left\lceil \frac{k}{r} \right\rceil \frac{\delta}{k}}{n - \left\lceil \frac{k}{r} \right\rceil}$$

and

$$X' = \frac{\delta}{k} + \frac{\left\lfloor \frac{k}{r} \right\rfloor \frac{\delta}{k} + R}{n - \left\lfloor \frac{k}{r} \right\rfloor},$$

with $R = k - \left\lfloor \frac{k}{r} \right\rfloor r$. Then,

$$L = \begin{cases} \lfloor X \rfloor, & \text{if } X \leq R \\ R, & \text{if } X > R \ \wedge \ B(R+1) \leq SB \\ \lfloor X' \rfloor, & \text{otherwise} \end{cases}$$

Corollary 3.40. *Let $\mathcal{C}$ be an MDP (n, k, δ)-convolutional code over $\mathbb{Z}_{p^r}$ with $r \mid k$. Then*

$$L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\left\lfloor \frac{\delta}{r} \right\rfloor}{n - \frac{k}{r}} \right\rfloor.$$

Note that $r \mid k$ means that $R = 0$, and so

$$B(j) = \left(n - \frac{k}{r}\right)(j+1) + 1. \tag{3.16}$$

In this case we can prove the next lemma.

Lemma 3.41. *Let $\mathcal{C}$ be an (n,k,δ)-convolutional code over $\mathbb{Z}_{p^r}$ with $r \mid k$. If $d_j^c = B(j)$ then $d_i^c = B(i)$, for all $i \leq j$.*

Proof It is sufficient to prove that

$$d_j^c = B(j) \Rightarrow d_{j-1}^c = B(j-1), \quad \text{for} \quad j \geq 1.$$

Let us consider G_0 written in p-standard form. Since $r \mid k$, the r-optimal set of parameters $(k_0, k_1, \ldots, k_{r-1})$ of k is such that $k_0 = \frac{k}{r}$ and $k_i = 0$, for all $i = 1, 2, \ldots, r-1$. Let us assume that

$$d_{j-1}^c \leq \left(n - \frac{k}{r}\right) j.$$

Let $v(D) \in \mathcal{C}$ such that $v_0 \neq 0$ and

$$\text{wt}\left(v(D)|_{[0,j-1]}\right) = d_{j-1}^c,$$

where $v(D)|_{[0,j-1]} = v_0 + v_1 D + \cdots + v_{j-1} D^{j-1}$, for $v(D) = \sum_{i \in \mathbb{N}} v_i D^i$.

Then,

$$\begin{aligned} v(D)|_{[0,j-1]} &= \begin{bmatrix} v_0 & v_1 & \ldots & v_{j-1} \end{bmatrix} \\ &= \begin{bmatrix} u_0 & u_1 & \ldots & u_{j-1} \end{bmatrix} \begin{bmatrix} G_0 & G_1 & \ldots & G_{j-1} \\ & \ddots & & \vdots \\ & & & G_0 \end{bmatrix}, \end{aligned}$$

for some $u_i \in \mathcal{A}_p^k$, $i = 0, \ldots, j-1$.

Let $\widetilde{v}(D) \in \mathcal{C}$ be such that

$$\begin{aligned} \widetilde{v}(D)|_{[0,j]} &= \begin{bmatrix} v_0 & v_1 & \ldots & v_{j-1} & v_j \end{bmatrix} \\ &= \begin{bmatrix} u_0 & u_1 & \ldots & u_{j-1} & u_j \end{bmatrix} \begin{bmatrix} G_0 & G_1 & \ldots & G_{j-1} & G_j \\ & & \ddots & \vdots & \vdots \\ & & & G_0 & G_1 \\ & & & & G_0 \end{bmatrix}, \end{aligned}$$

for some $u_j \in \mathcal{A}_p^k$. Then

$$\begin{aligned} v_j &= \begin{bmatrix} u_0 & u_1 & \dots & u_{j-1} & u_j \end{bmatrix} \begin{bmatrix} G_j \\ G_{j-1} \\ \vdots \\ G_1 \\ G_0 \end{bmatrix} \\ &= \sum_{t=0}^{j-1} u_t G_{j-t} + u_j G_0. \end{aligned}$$

Let us consider u_j such that $u_j G_0$ negates the first $k_0 = \frac{k}{r}$ entries of $\sum_{t=0}^{j-1} u_t G_{j-t}$. So,

$$\mathrm{wt}\,(v_j) \leq n - \frac{k}{r},$$

and then, since $\widetilde{v}(D)|_{[0,j-1]} = v(D)|_{[0,j-1]}$ it follows that

$$\mathrm{wt}\left(\widetilde{v}(D)|_{[0,j]}\right) \leq \left(n - \frac{k}{r}\right)(j+1)$$

which contradicts (3.16).

□

Remark 3.42. *Note that, for $r \mid k$ an (n, k, δ)-convolutional code $\mathcal{C}$ is an MDP if and only if*

$$d_L^c = \left(n - \frac{k}{r}\right)(L+1) + 1.$$

Chapter 4

Constructions of convolutional codes over $\mathbb{Z}_{p^r}$

In this chapter we address the problem of providing explicit constructions of convolutional codes over $\mathbb{Z}_{p^r}$ that are optimal with respect to the free distance and column distance, *i.e.*, MDS and MDP convolutional codes. These constructions generalize the existing constructions of convolutional codes over finite fields [SGLR01, ANP13, Gua14, NR16]).

4.1 MDS Convolutional Codes

We start by presenting a general procedure for building (non necessarily free) MDS convolutional codes over $\mathbb{Z}_{p^r}$. The idea is to start from well-known constructions of MDS convolutional codes over $\mathbb{Z}_p$ and then *lift* them to $\mathbb{Z}_{p^r}$ in such a way that the resulting convolutional code is MDS over $\mathbb{Z}_{p^r}$. This method is direct and works for any given set of parameters (n, k, δ).

For the sake of simplicity of exposition, we first assume that $k \mid \delta$. The general case will be treated at the end of the section.

Since $k \mid \delta$ the row degrees ν_i, $i = 1, \ldots, k$ of any p-encoder $G(D)$ of $\mathcal{C}$ in reduced form are

$$\nu = \nu_1 = \cdots = \nu_k = \frac{\delta}{k}$$

The MDS (n, k, δ)-convolutional $\mathcal{C}$ that we aim to construct must satisfy

$$d(\mathcal{C}) = n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r} \right\rceil + 1.$$

Note that

$$n\left(\left\lfloor\frac{\delta}{k}\right\rfloor+1\right)-\left\lceil\frac{k}{r}\left(\left\lfloor\frac{\delta}{k}\right\rfloor+1\right)-\frac{\delta}{r}\right\rceil+1$$

$$=n(\nu+1)-(k_0+k_1+\cdots+k_{r-1})+1$$

where $(k_0,k_1,\ldots,k_{r-1})$ is an r-optimal set of parameters of k (by Theorem 3.22 and Corollary 3.24).

Take

$$\begin{cases}\widetilde{k}=k_0+k_1+\cdots+k_{r-1}\\ \widetilde{\delta}=\nu\widetilde{k}\end{cases},$$

and let us consider an MDS convolutional code $\widetilde{\mathcal{C}}$ with length n, dimension $\widetilde{k}$ and degree $\widetilde{\delta}$ over the field $\mathbb{Z}_p$ (constructions of such codes can be found in [SGLR01, Gua14, NR16]).
The distance of $\widetilde{\mathcal{C}}$ equals (see [RS99])

$$d(\widetilde{\mathcal{C}})=(n-\widetilde{k})\left(\left\lfloor\frac{\widetilde{\delta}}{\widetilde{k}}\right\rfloor+1\right)+\widetilde{\delta}+1.$$

Let

$$\widetilde{G}(D)=\begin{bmatrix}\widetilde{G}_{k_0}(D)\\ ---\\ \widetilde{G}_{k_1}(D)\\ ---\\ \vdots\\ ---\\ \widetilde{G}_{k_{r-1}}(D)\end{bmatrix}, \tag{4.1}$$

with $\widetilde{G}(D)\in\mathbb{Z}_p^{\widetilde{k}\times n}[D]$ be an encoder of $\widetilde{\mathcal{C}}$ in reduced form, where $\widetilde{G}_{k_i}(D)$ is a $k_i\times n$ matrix, $i=0,1,\ldots,r-1$.

By Lemma 3.15,

$$\widetilde{k}=\left\lceil\frac{k}{r}\right\rceil$$

and since

$$\widetilde{\delta}=\nu\widetilde{k}$$

we get

$$d(\widetilde{\mathcal{C}})=n\,(\nu+1)-\left\lceil\frac{k}{r}\right\rceil+1. \tag{4.2}$$

Next, we *lift* $\widetilde{G}(D)$ to construct a $k \times n$ matrix $G(D)$ over $\mathbb{Z}_{p^r}[D]$ as follows,

$$G(D) = \begin{bmatrix} \widetilde{G}_{k_0}(D) \\ p\widetilde{G}_{k_0}(D) \\ \vdots \\ p^{r-1}\widetilde{G}_{k_0}(D) \\ - - - - \\ p\widetilde{G}_{k_1}(D) \\ p^2\widetilde{G}_{k_1}(D) \\ \vdots \\ p^{r-1}\widetilde{G}_{k_1}(D) \\ - - - - \\ \vdots \\ - - - - \\ p^{r-1}\widetilde{G}_{k_{r-1}}(D) \end{bmatrix}. \tag{4.3}$$

G(D) is a p-encoder of an MDS (n, k, δ)-convolutional code as we will prove in the next lemma.

Lemma 4.1. *The matrix $G(D)$ defined in (4.3) is a p-encoder in reduced form with row degrees all equal to ν. Moreover, the convolutional code generated by $G(D)$ has length n, p-dimension k and p-degree δ.*

Proof Since all the rows of $\widetilde{G}(D)$ have row degrees ν, the rows of $G(D)$ have also degree ν. From the construction of $G(D)$, it is straightforward to verify that its rows form a p-generator sequence. It remains to show that $G(D)$ is in reduced form, *i.e.*, that the rows of

$$G^{lc} = \begin{bmatrix} \widetilde{G}^{lc}_{k_0} \\ p\widetilde{G}^{lc}_{k_0} \\ \vdots \\ p^{r-1}\widetilde{G}^{lc}_{k_0} \\ - - - - \\ p\widetilde{G}^{lc}_{k_1} \\ p^2\widetilde{G}^{lc}_{k_1} \\ \vdots \\ p^{r-1}\widetilde{G}^{lc}_{k_1} \\ - - - - \\ \vdots \\ - - - - \\ p^{r-1}\widetilde{G}^{lc}_{k_{r-1}} \end{bmatrix},$$

are p-linearly independent. This amounts to show that for $a_j^i \in \mathcal{A}_p$, with $i = j, \ldots, r-1$ and $j = 0, \ldots, r-1$,

$$\begin{aligned} a_0^0 \widetilde{G}_{k_0}^{lc} + a_0^1 p \widetilde{G}_{k_0}^{lc} + \cdots + a_0^{r-1} p^{r-1} \widetilde{G}_{k_0}^{lc} + a_1^1 p \widetilde{G}_{k_1}^{lc} + a_1^2 p^2 \widetilde{G}_{k_1}^{lc} + \cdots + \\ + \cdots + a_1^{r-1} p^{r-1} \widetilde{G}_{k_1}^{lc} + \cdots + a_{r-1}^{r-1} p^{r-1} \widetilde{G}_{k_{r-1}}^{lc} = 0 \end{aligned} \tag{4.4}$$

implies that

$$a_0^0 = a_0^1 = \cdots = a_0^{r-1} = 0, \;\; a_1^1 = a_1^2 = \cdots = a_1^{r-1} = 0, \;\; \ldots, \;\; a_{r-1}^{r-1} = 0.$$

Note that, multiplying (4.4) by p^{r-1} we obtain

$$a_0^0 p^{r-1} \widetilde{G}_{k_0}^{lc} = 0.$$

As $\widetilde{G}(D)$ is in reduced form, $\widetilde{G}_{k_0}^{lc}$ must be full row rank over $\mathbb{Z}_p$ and therefore $a_0^0 = 0$. Proceeding in the same way, by successively multiplying (4.4) by $p^{r-2}, \ldots, 1$, we show that $a_j^i = 0$, with $i = j, \ldots, r-1$ and $j = 0, \ldots, r-1$.

For the proof of the last statement note that since $\widetilde{k} = k_0 + k_1 + \cdots + k_{r-1}$ and $(k_0, \ldots, k_{r-1})$ is an r-optimal set of parameters of k we obtain that $G(D)$ has k rows, *i.e.*, $\mathcal{C}$ has p-dimension equal to k. Moreover, since $G(D)$ is in reduced form, the degree of $\mathcal{C}$ is

$$\nu k = \frac{\delta}{k} k = \delta.$$

□

The following technical lemma will be used in the next theorem. First, we need to define the order of a codeword.

Definition 4.2. *If $v(D) \in \mathbb{Z}_{p^r}[D] \setminus \{0\}$ we define the* **order** *of $v(D)$, denoted by $ord(v(D))$, as the $j \in \{1, 2, \ldots, r\}$ such that*

$$p^j v(D) = 0 \text{ and } p^{j-1} v(D) \neq 0.$$

Lemma 4.3. *Let $\mathcal{C}$ be the convolutional code generated by the encoder $\widetilde{G}(D)$ and p-encoder $G(D)$ defined in (4.1) and (4.3), respectively. Then, if $v(D) \in \mathcal{C}$ has order j,*

$$p^{j-1} v(D) \in Im_{\mathcal{A}_p[D]} \; p^{r-1} \widetilde{G}(D).$$

Proof Since the matrix $\widetilde{G}(D)$ defined in (4.1) is full row rank over $\mathbb{Z}_p[D]$, it follows that, for any nonzero codeword of $\mathcal{C}$,

$$v(D) = \sum_{i=0}^{r-1} \sum_{l=i}^{r-1} u_i^l(D) p^l \widetilde{G}_{k_i}(D), \text{ with } u_i^l(D) \in \mathcal{A}_p^{k_i}[D],$$

we have that

$$ord(v(D)) = \max_{i,l:u_i^l(D)\neq 0} ord(p^l \widetilde{G}_{k_i}(D)). \tag{4.5}$$

Thus, if $v(D)$ has order j then $p^{j-1}v(D)$ has order one and therefore, by (4.5),

$$p^{j-1}v(D) \in \operatorname{Im}_{\mathcal{A}_p[D]} p^{r-1}\widetilde{G}(D).$$

□

Now we are ready to present the result that shows that our construction is indeed an MDS convolutional code.

Theorem 4.4. *Let $\mathcal{C}$ be the (n, k, δ)-convolutional code with $k \mid \delta$ and p-encoder $G(D)$ as in (4.3). Then, $\mathcal{C}$ is MDS,* i.e.*,*

$$d(\mathcal{C}) = n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r} \right\rceil + 1.$$

Proof Since $k \mid \delta$ the Singleton bound can be written as

$$n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r} \right\rceil + 1 = n\left(\frac{\delta}{k} + 1\right) - \left\lceil \frac{k}{r} \right\rceil + 1.$$

Let $v(D) \in \mathcal{C} \setminus \{0\}$. Obviously,

$$\operatorname{wt}(v(D)) \geq \operatorname{wt}(p^{j-1}v(D)),$$

where j is the order of $v(D)$. By Lemma 4.3,

$$\operatorname{wt}(p^{j-1}v(D)) = \operatorname{wt}(p^{r-1}u(D)\widetilde{G}(D)),$$

for some $u(D) \in \mathcal{A}_p^k[D]$. Note that, since $u(D) \in \mathcal{A}_p^k[D]$,

$$\operatorname{wt}(p^{r-1}u(D)\widetilde{G}(D)) = \operatorname{wt}_p(\bar{u}(D)\widetilde{G}(D)),$$

where $\bar{u}(D) = u(D)$ is the projection of $u(D)$ over $\mathbb{Z}_p[D]$ and wt_p represents the Hamming weight over $\mathbb{Z}_p$. This together with the fact that $\widetilde{\mathcal{C}}$ is an MDS convolutional code over $\mathbb{Z}_p$ shows that

$$\mathrm{wt}(p^{r-1}u(D)\widetilde{G}(D)) \geq (n-\widetilde{k})\left(\left\lfloor \frac{\widetilde{\delta}}{\widetilde{k}} \right\rfloor + 1\right) + \widetilde{\delta} + 1.$$

It is straightforward to check that for

$$\begin{cases} \widetilde{\delta} = \nu\widetilde{k} = \frac{\delta}{k}\widetilde{k} \\ \widetilde{k} = \left\lceil \frac{k}{r} \right\rceil \end{cases}$$

this lower bound coincides with the Singleton bound given in Corollary 3.24. This shows that

$$d(\mathcal{C}) = n\left(\frac{\delta}{k} + 1\right) - \left\lceil \frac{k}{r} \right\rceil + 1.$$

□

Let us now assume that $k \nmid \delta$ and let us construct an MDS (n, k, δ)-convolutional code $\mathcal{C}$. Note that a p-encoder $G(D)$ of $\mathcal{C}$ in reduced form has:

- ℓ rows of degree $\nu = \left\lfloor \frac{\delta}{k} \right\rfloor$
- $k - \ell$ rows of degree $k - \ell$, where

$$\ell = k\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \delta.$$

Select $(\ell_0, \ldots, \ell_{r-1})$ an r-optimal set of parameters of ℓ. Then

$$d(\mathcal{C}) = n(\nu+1) - (\ell_0 + \ell_1 + \cdots + \ell_{r-1}) + 1.$$

Let $a, b \in \mathbb{N}_0$ such that

$$k - \ell = ar + b,$$

with $b < r$. Take

$$\begin{cases} \widetilde{k} = a + 1 + \ell_0 + \ell_1 + \cdots + \ell_{r-1} \\ \nu = \left\lfloor \frac{\delta}{k} \right\rfloor \\ \widetilde{\delta} = (a+1)(\nu+1) + (\ell_0 + \ell_1 + \cdots + \ell_{r-1})\nu \end{cases}$$

and let $\widetilde{\mathcal{C}}$ be an MDS convolutional code of length n, dimension $\widetilde{k}$ and degree $\widetilde{\delta}$ over the field $\mathbb{Z}_p$. Construct

$$\widetilde{G}(D) = \left[\begin{array}{c} \widetilde{G}_a(D) \\ \hline \widetilde{G}_1(D) \\ \hline \widetilde{G}_{\ell_0}(D) \\ \hline \widetilde{G}_{\ell_1}(D) \\ \hline \vdots \\ \hline \widetilde{G}_{\ell_{r-1}}(D) \end{array}\right] \in \mathbb{Z}_p[D]^{\widetilde{k}\times n} \tag{4.6}$$

to be an encoder of $\widetilde{\mathcal{C}}$ in reduced form, where $\widetilde{G}_a(D)$ is a $a \times n$ matrix and $\widetilde{G}_1(D)$ is a $1 \times n$ matrix with row degrees $\nu + 1$ and $\widetilde{G}_{\ell_i}(D)$ is an $\ell_i \times n$ matrix with row degrees ν, $i = 0, 1, \ldots, r-1$.

Since $\widetilde{\mathcal{C}}$ is an MDS $(n, \widetilde{k}, \widetilde{\delta})$-convolutional code over $\mathbb{Z}_p$, its distance equals (see [RS99])

$$d(\widetilde{\mathcal{C}}) = (n - \widetilde{k}) \left(\left\lfloor \frac{\widetilde{\delta}}{\widetilde{k}} \right\rfloor + 1 \right) + \widetilde{\delta} + 1.$$

Note that from

$$\begin{cases} \widetilde{k} = a + 1 + \ell_0 + \ell_1 + \cdots + \ell_{r-1} \\ \\ \widetilde{\delta} = (a+1)(\nu+1) + (\ell_0 + \ell_1 + \cdots + \ell_{r-1})\nu \end{cases}$$

we have that

$$\frac{\widetilde{\delta}}{\widetilde{k}} = \nu + \frac{a+1}{\widetilde{k}}$$

and therefore

$$\nu = \left\lfloor \frac{\widetilde{\delta}}{\widetilde{k}} \right\rfloor,$$

and also that

$$d(\widetilde{\mathcal{C}}) = n(\nu + 1) - (\ell_0 + \ell_1 + \cdots + \ell_{r-1}) + 1.$$

Now, let us consider the following $k \times n$ matrix in $\mathbb{Z}_{p^r}[D]$,

$$G(D) = \left[\begin{array}{c} \widetilde{G}_a(D) \\ p\widetilde{G}_a(D) \\ \vdots \\ p^{r-1}\widetilde{G}_a(D) \\ --\!-- \\ p^{r-b}\widetilde{G}_1(D) \\ \vdots \\ p^{r-1}\widetilde{G}_1(D) \\ --\!-- \\ \widetilde{G}_{\ell_0}(D) \\ p\widetilde{G}_{\ell_0}(D) \\ \vdots \\ p^{r-1}\widetilde{G}_{\ell_0}(D) \\ --\!-- \\ p\widetilde{G}_{\ell_1}(D) \\ p^2\widetilde{G}_{\ell_1}(D) \\ \vdots \\ p^{r-1}\widetilde{G}_{\ell_1}(D) \\ --\!-- \\ \vdots \\ --\!-- \\ p^{r-1}\widetilde{G}_{\ell_{r-1}}(D) \end{array}\right]. \tag{4.7}$$

In order to prove that $G(D)$ defined as in (4.7) is a p-encoder of an MDS convolutional code we first need the next lemmas.

Lemma 4.5. *The matrix $G(D)$ defined in (4.7) is a p-encoder in reduced form where the first $k-l$ rows have degree equal to $\nu+1$ and the last ℓ rows have degree equal to ν. Moreover, the convolutional code generated by $G(D)$ has p-dimension k and p-degree δ.*

Proof Since the rows of $\widetilde{G}_a(D)$ and $\widetilde{G}_1(D)$ have degrees $\nu+1$ and the row degree of $\widetilde{G}_{\ell_i}(D)$, for all $i = 0, \ldots, r-1$, is equal to ν, the first $k-l$ rows of $G(D)$ have degree $\nu+1$ and the last ℓ rows have degree ν.
Once the rows of $\widetilde{G}(D)$ are p-linearly independent and form a p-generator sequence, the rows of $G(D)$ are also p-linearly independent and form a p-generator sequence.

Finally let us prove that $G(D)$ is in reduced form. Considering

$$G^{lc} = \begin{bmatrix} \widetilde{G}_a^{lc} \\ p\widetilde{G}_a^{lc} \\ \vdots \\ p^{r-1}\widetilde{G}_a^{lc} \\ - - - - \\ p^{r-b}\widetilde{G}_1^{lc} \\ \vdots \\ p^{r-1}\widetilde{G}_1^{lc} \\ - - - - \\ \widetilde{G}_{\ell_0}^{lc} \\ p\widetilde{G}_{\ell_0}^{lc} \\ \vdots \\ p^{r-1}\widetilde{G}_{\ell_0}^{lc} \\ - - - - \\ p\widetilde{G}_{\ell_1}^{lc} \\ p^2\widetilde{G}_{\ell_1}^{lc} \\ \vdots \\ p^{r-1}\widetilde{G}_{\ell_1}^{lc} \\ - - - - \\ \vdots \\ - - - - \\ p^{r-1}\widetilde{G}_{\ell_{r-1}}^{lc} \end{bmatrix},$$

let us to prove that

$$\begin{aligned} &b_0^0\widetilde{G}_a^{lc} + b_0^1 p\widetilde{G}_a^{lc} + \cdots + b_0^{r-1}p^{r-1}\widetilde{G}_a^{lc} + b_1^{r-b}p^{r-b}\widetilde{G}_1^{lc} + b_1^{r-(b+1)}p^{r-(b+1)}\widetilde{G}_1^{lc} + \cdots + \\ &+b_1^{r-1}p^{r-1}\widetilde{G}_1^{lc} + b_2^0\widetilde{G}_{l_0}^{lc} + b_2^1 p\widetilde{G}_{l_0}^{lc} + \cdots + b_2^{r-1}p^{r-1}\widetilde{G}_{l_0}^{lc} + b_3^1 p\widetilde{G}_{l_1}^{lc} + b_3^2 p^2\widetilde{G}_{l_1}^{lc} + \cdots + \\ &+b_3^{r-1}p^{r-1}\widetilde{G}_{l_1}^{lc} + \cdots + b_{r+1}^{r-1}p^{r-1}\widetilde{G}_{l_{r-1}}^{lc} = 0 \end{aligned} \tag{4.8}$$

implies that

$$b_0^0 = \cdots = b_0^{r-1} = b_1^{r-b} = \cdots = b_1^{r-1} = b_2^0 = \cdots = b_2^{r-1} = b_3^1 = \ldots, b_3^{r-1} = \ldots, b_{r+1}^{r-1} = 0,$$

with $b_0^0, \ldots, b_0^{r-1} \in \mathcal{A}_p^n$, $b_1^{r-b}, \ldots, b_1^{r-1} \in \mathcal{A}_p$, $b_2^0, \ldots, b_2^{r-1} \in \mathcal{A}_p^{\ell_0}$, $b_3^1, \ldots, b_3^{r-1} \in \mathcal{A}_p^{\ell_1}$, $\ldots$, $b_{r+1}^{r-1} \in \mathcal{A}_p^{\ell_{r-1}}$. Note that, multiplying (4.8) by p^{r-1} we obtain

$$b_0^0 p^{r-1} \widetilde{G}_a^{lc} + b_2^0 p^{r-1} \widetilde{G}_{l_0}^{lc} = 0,$$

that implies

$$b_0^0 = b_2^0 = 0,$$

since $\widetilde{G}(D)$ is in reduced form. By successively multiplying (4.8) by $p^{r-2}, \ldots, 1$, and proceeding in the same way, we obtain that

$$\begin{aligned} &b_0^0 = \cdots = b_0^{r-1} = 0, \;\; b_1^{r-b} = \cdots = b_1^{r-1} = 0, \\ &b_2^0 = \cdots = b_2^{r-1} = 0, \;\; b_3^1 = \ldots, b_3^{r-1} = 0, \;\; \ldots, b_{r+1}^{r-1} = 0. \end{aligned}$$

To prove that $\mathcal{C}$ has p-dimension k, note that $\widetilde{k} = a + b + \ell_0 + \ell_1 + \cdots + \ell_{r-1}$ and that $(\ell_0, \ldots, \ell_{r-1})$ is an r-optimal set of parameters of ℓ. Then, the number of rows of $G(D)$ is

$$ra + b + r\ell_0 + (r-1)\ell_1 + \cdots + \ell_{r-1} = ra + b + \ell = k.$$

The p-degree of $\mathcal{C}$ is

$$\begin{aligned} (ra+b)(\nu+1) + \ell\nu &= (k-\ell)(\nu+1) + \ell\nu \\ &= k(\nu+1) - \ell \\ &= k(\left\lfloor \frac{\delta}{k} \right\rfloor + 1) - \ell \\ &= \delta. \end{aligned}$$

□

Applying the same reasoning as in the proof of Lemma 4.3, the next lemma holds immediately.

Lemma 4.6. *Let $\mathcal{C}$ be the convolutional code generated by encoder $\widetilde{G}(D)$ and p-encoder $G(D)$ defined in (4.6) and (4.7), respectively. Then, if $v(D) \in \mathcal{C}$ has order j,*

$$p^{j-1} v(D) \in Im_{\mathcal{A}_p[D]}\ p^{r-1} \widetilde{G}(D).$$

Finally, we can prove our last theorem.

Theorem 4.7. *Let $\mathcal{C}$ be the (n, k, δ)-convolutional code with p-encoder $G(D)$ as in*

(4.7). Then, $\mathcal{C}$ is MDS, i.e.,

$$d(\mathcal{C}) = n\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \left\lceil\frac{k}{r}\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \frac{\delta}{r}\right\rceil + 1$$

Proof Let $v(D) \in \mathcal{C} \setminus \{0\}$ and let j be the order of $v(D)$. We have that

$$\mathrm{wt}(v(D)) \geq \mathrm{wt}(p^{j-1}v(D)).$$

By Lemma 4.6,

$$\mathrm{wt}(p^{j-1}v(D)) = \mathrm{wt}(p^{r-1}u(D)\widetilde{G}(D)),$$

for some $u(D) \in \mathcal{A}_p^k[D]$.

Note that, since $u(D) \in \mathcal{A}_p^k[D]$,

$$\mathrm{wt}(p^{r-1}u(D)\widetilde{G}(D)) = \mathrm{wt}_p(\bar{u}(D)\widetilde{G}(D)),$$

where $\bar{u}(D) = u(D)$ is the projection of $u(D)$ over $\mathbb{Z}_p[D]$ and wt_p represents the Hamming weight over $\mathbb{Z}_p$. This together with the fact that $\widetilde{\mathcal{C}}$ is an MDS convolutional code over $\mathbb{Z}_p$ shows that

$$\mathrm{wt}(p^{r-1}u(D)\widetilde{G}(D)) \geq (n-\widetilde{k})\left(\left\lfloor\frac{\widetilde{\delta}}{\widetilde{k}}\right\rfloor + 1\right) + \widetilde{\delta} + 1.$$

From $\widetilde{k} = a+1+\ell_0+\ell_1+\cdots+\ell_{r-1}$ and $\widetilde{\delta} = (a+1)(\nu+1)+(\ell_0+\ell_1+\cdots+\ell_{r-1})\nu$, we have that

$$(n-\widetilde{k})\left(\left\lfloor\frac{\widetilde{\delta}}{\widetilde{k}}\right\rfloor + 1\right) + \widetilde{\delta} + 1 = n(\nu+1) - (\ell_0+\cdots+\ell_{r-1}) + 1.$$

Since, by Lemma 3.15,

$$\ell_0+\ell_1+\cdots+\ell_{r-1} = \left\lceil\frac{\ell}{r}\right\rceil$$

and

$$\ell = k\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \delta$$

we obtain

$$(n-\widetilde{k})\left(\left\lfloor\frac{\widetilde{\delta}}{\widetilde{k}}\right\rfloor + 1\right) + \widetilde{\delta} + 1 = n\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \left\lceil\frac{k}{r}\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \frac{\delta}{r}\right\rceil + 1.$$

This lower bound coincides with the Singleton bound given in Corolary 3.24, which

means that

$$d(\mathcal{C}) = n\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \left\lceil\frac{k}{r}\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \frac{\delta}{r}\right\rceil + 1$$

□

4.2 MDP Convolutional Codes

In this section we present constructions of MDP (n, k, δ)-convolutional codes over $\mathbb{Z}_{p^r}$. We are going to consider two cases:

Case 1 Constructions of MDP (n, k, δ)-convolutional codes with $r \mid k$, $r \mid \delta$ and $n > \frac{k}{r}$.

Case 2 Constructions of MDP (n, k, δ)-convolutional codes considering equal p-Forney indices.

4.2.1 Case 1

Given $n, k, \delta \in \mathbb{N}$ such that $r \mid k$, $r \mid \delta$ and $n > \frac{k}{r}$, we aim at building an MDP (n, k, δ)-convolutional code over $\mathbb{Z}_{p^r}[D]$.

Take $\widetilde{k} = \frac{k}{r}$ and $\widetilde{\delta} = \frac{\delta}{r}$, and let us consider an MDP convolutional code $\widetilde{\mathcal{C}}$ with length n, dimension $\widetilde{k}$ and degree $\widetilde{\delta}$ over $\mathbb{Z}_p$ and let $\widetilde{G}(D) \in \mathbb{Z}_p^{\widetilde{k}\times n}[D]$ be an encoder of $\widetilde{\mathcal{C}}$ in reduced form (constructions of such codes can be found in [HGLS06, ANP13, NR16]).

Write

$$\widetilde{G}(D) = \widetilde{G}_0 + \widetilde{G}_1 D + \cdots + \widetilde{G}_\nu D^\nu$$

and consider the corresponding j-th truncated sliding generator matrix

$$\widetilde{G}_j^c = \begin{bmatrix} \widetilde{G}_0 & \widetilde{G}_1 & \dots & \widetilde{G}_j \\ & \widetilde{G}_0 & \dots & \widetilde{G}_{j-1} \\ & & \ddots & \vdots \\ & & & \widetilde{G}_0 \end{bmatrix}$$

Note that since $\widetilde{\mathcal{C}}$ is an MDP, $\widetilde{G}(D)$ must be delay-free and therefore $\widetilde{G}_0$ is full row rank.

Since $\widetilde{\mathcal{C}}$ is an MDP it follows that its column distances satisfy

$$\widetilde{d}_j^c = (j+1)(n-\widetilde{k}) + 1, \quad j \leq L$$

where $L = \left\lfloor \frac{\widetilde{\delta}}{\widetilde{k}} \right\rfloor + \left\lfloor \frac{\widetilde{\delta}}{n-\widetilde{k}} \right\rfloor$ (see [HGLS06]).

Construct

$$G(D) = \begin{bmatrix} \widetilde{G}(D) \\ p\widetilde{G}(D) \\ \vdots \\ p^{r-1}\widetilde{G}(D) \end{bmatrix}. \tag{4.9}$$

From the fact that $\widetilde{G}(D)$ is in reduced form, it immediately follows that $G(D)$ is a p-encoder in reduced form.

Theorem 4.8. *Let $\mathcal{C}$ be an (n, k, δ)-convolutional code over $\mathbb{Z}_{p^r}$, with $r \mid k$, $r \mid \delta$ and with p-encoder $G(D)$ as in (4.9). Then $\mathcal{C}$ is an MDP convolutional code .*

Proof We need to show that

$$d_j^c = (j+1)(n - \frac{k}{r}) + 1,$$

for $j \leq L$, with $L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{nr-k} \right\rfloor$.

Consider the j-th truncated sliding matrix correspondent to $G(D)$ is

$$G_j^c = \begin{bmatrix} \widetilde{G}_0 & \widetilde{G}_1 & \dots & \widetilde{G}_j \\ p\widetilde{G}_0 & p\widetilde{G}_1 & \dots & p\widetilde{G}_j \\ \vdots & \vdots & \dots & \vdots \\ p^{r-1}\widetilde{G}_0 & p^{r-1}\widetilde{G}_1 & \dots & p^{r-1}\widetilde{G}_j \\ & \widetilde{G}_0 & \dots & \widetilde{G}_{j-1} \\ & p\widetilde{G}_0 & \dots & p\widetilde{G}_{j-1} \\ & \vdots & \dots & \vdots \\ & p^{r-1}\widetilde{G}_0 & \dots & p^{r-1}\widetilde{G}_{j-1} \\ & & & \vdots \\ & & & \widetilde{G}_0 \\ & & & p\widetilde{G}_0 \\ & & & p^{r-1}\widetilde{G}_0 \end{bmatrix}.$$

Let

$$u = \begin{bmatrix} u_0 & u_1 & \dots & u_j \end{bmatrix},$$

with $u_i \in \mathcal{A}_p^{r\widetilde{k}}$, $i = 0, \dots, j$ and $u_0 \neq 0$, and let

$$v = \begin{bmatrix} v_0 & v_1 & \dots & v_j \end{bmatrix},$$

with $v_i \in \mathbb{Z}_p^n$, $i = 0, \ldots, j$, such that $v = uG_j^c$.

Take

$$\ell = \max_{0 \leq t \leq j} ord(v_t)$$

and

$$i = \min_{0 \leq s \leq j} \{s : ord(v_s) = \ell\} = \min_{0 \leq s \leq j} \{s : p^{\ell-1} v_s \neq 0\}.$$

There exists $\widehat{v}_s \in \mathcal{A}_p^n$ such that

$$\tilde{v}_s = p^{\ell-1} v_s = p^{r-1} \hat{v}_s,$$

$s = i, \ldots, j$ and then

$$\begin{aligned} p^{\ell-1} v &= \begin{bmatrix} 0 & 0 & \ldots & 0 & \widetilde{v}_i & \ldots & \widetilde{v}_j \end{bmatrix} \\ &= p^{r-1} \begin{bmatrix} 0 & 0 & \ldots & 0 & \widehat{v}_i & \ldots & \widehat{v}_j \end{bmatrix}. \end{aligned} \tag{4.10}$$

Applying the same reasoning as in the proof of Lemma 4.3 we conclude that

$$p^{\ell-1} v = p^{r-1} \begin{bmatrix} \widetilde{u}_0 & \widetilde{u}_1 & \ldots & \widetilde{u}_i & \ldots & \widetilde{u}_j \end{bmatrix} \begin{bmatrix} \widetilde{G}_0 & \widetilde{G}_1 & \ldots & \widetilde{G}_i & \ldots & \widetilde{G}_j \\ & \widetilde{G}_0 & \ldots & \widetilde{G}_{i-1} & \ldots & \widetilde{G}_{j-1} \\ & & \ddots & \vdots & & \vdots \\ & & & \widetilde{G}_0 & \ldots & \widetilde{G}_{j-i} \\ & & & & \ddots & \vdots \\ & & & & & \widetilde{G}_0 \end{bmatrix},$$

for some $\widetilde{u}_0, \widetilde{u}_1, \ldots, \widetilde{u}_i, \ldots, \widetilde{u}_j \in \mathcal{A}_p^{\widetilde{k}}$, with $\widetilde{u}_0 = \cdots = \widetilde{u}_{i-1} = 0$, because $\widetilde{G}_0$ is full row rank and $\widetilde{u}_i \neq 0$. Thus

$$\begin{bmatrix} \widetilde{v}_i & \ldots & \widetilde{v}_j \end{bmatrix} = p^{r-1} \begin{bmatrix} \widetilde{u}_i & \ldots & \widetilde{u}_j \end{bmatrix} \begin{bmatrix} \widetilde{G}_0 & \ldots & \widetilde{G}_{j-i} \\ & \ddots & \vdots \\ & & \widetilde{G}_0 \end{bmatrix}$$

where $\widetilde{u}_i \neq 0$. Then, using the fact that $\widetilde{\mathcal{C}} = \mathrm{Im}_{\mathbb{Z}_p[D]} \widetilde{G}(D)$ is MDP we obtain

$$\begin{aligned} \mathrm{wt}\left(\begin{bmatrix} v_i & \ldots & v_j \end{bmatrix}\right) &\geq \mathrm{wt}\left(\begin{bmatrix} \widetilde{v}_i & \ldots & \widetilde{v}_j \end{bmatrix}\right) \\ &\geq (n - \widetilde{k})(j - i + 1) + 1. \end{aligned}$$

Considering

$$\left[\begin{array}{ccc} v_0 & \dots & v_{i-1} \end{array}\right] = \left[\begin{array}{ccc} u_0 & \dots & u_{i-1} \end{array}\right] G_i^c$$

and reasoning in the same way we conclude that

$$\mathrm{wt}\left(\left[\begin{array}{ccc} v_0 & \cdots & v_{i-1} \end{array}\right]\right) \geq (n-\widetilde{k})i+1$$

and therefore

$$\mathrm{wt}\left(\left[\begin{array}{ccc} v_0 & \cdots & v_{j} \end{array}\right]\right) \geq (n-\widetilde{k})(j+1)+1.$$

Consequently, $d_j^c = (n-\widetilde{k})(j+1)+1$, *i.e.*,

$$d_j^c = (n-\frac{k}{r})(j+1)+1,$$

for $j \leq L$, with $L = \left\lfloor \frac{\widetilde{\delta}}{\widetilde{k}} \right\rfloor + \left\lfloor \frac{\widetilde{\delta}}{\widetilde{n}-\widetilde{k}} \right\rfloor = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{nr-k} \right\rfloor$.

□

4.2.2 Case 2

Let us now construct an MDP (n,k,δ)-convolutional code over $\mathbb{Z}_{p^r}$, $n,k,\delta \in \mathbb{N}$, considering equal p-Forney indices. Note that k must divide δ and all the p-Forney indices are equal to $\frac{\delta}{k}$.

We first introduce two technical lemmas that will be useful for this construction. The next one readily follows from Lemma 3.34.

Lemma 4.9. *If $\mathcal{C}$ is a (n,k,δ)-convolutional code with equal p-Forney indices and a reduced p-encoder $G(D)$ written as in (3.4) and (3.10) then*

$$\widehat{G}_i^{(r-1)} \in p^{r-1}\mathbb{Z}_{p^r}^{\bar{k}_{r-1}\times n}, \tag{4.11}$$

$i = 1, \dots, \left\lfloor \frac{\delta}{k} \right\rfloor$.

Proof Since $G(D)$ is a p-generator sequence

$$p\, row_\ell G(D) \in p\text{-span}\{row_{\ell+1}G(D), \dots, row_k(D)\},$$

where $row_\ell G(D)$ represents the ℓ-th row of $G(D)$, for $\ell = 0, \dots, k-1$. The p-predictable degree property (see Lemma 2.19) and the fact that all rows of $G(D)$ have the same

degree imply that

$$p\, row_j \widehat{G}^{(r-1)}(D) = a_{j+1} row_{j+1} \widehat{G}^{(r-1)}(D) + \cdots + a_{\bar{k}_{r-1}} row_{\bar{k}_{r-1}} \widehat{G}^{(r-1)}(D),$$

with $a_{j+1}, \ldots a_{\bar{k}_{r-1}} \in \mathcal{A}_p$, for $j = 1, \ldots, \bar{k}_{r-1} - 1$.

As $\widehat{G}_0^{(r-1)} \in p^{r-1}\mathbb{Z}_{p^r}^{\bar{k}_{r-1} \times n}$ it follows that

$$0 = a_{j+1} row_{j+1} \widehat{G}_0^{(r-1)} + \cdots + a_{\bar{k}_{r-1}} row_{\bar{k}_{r-1}} \widehat{G}_0^{(r-1)},$$

which implies that

$$a_{j+1} = \cdots = a_{\bar{k}_{r-1}} = 0,$$

for $j = 1, \ldots, \bar{k}_{r-1}$ because the rows of G_0 are p-linearly independent. Consequently,

$$\widehat{G}_i^{(r-1)} \in p^{r-1}\mathbb{Z}_{p^r}^{\bar{k}_{r-1} \times n}.$$

□

The following lemma shows that a delay-free convolutional code with equal p-Forney indices is such that

$$d_j^c \leq \left(n - \left\lceil \frac{k}{r} \right\rceil \right)(j+1) + 1,$$

for all j. The proof follows the proof of Theorem 3.35 for this particular case.

Lemma 4.10. *If $\mathcal{C}$ is a (n, k, δ)-convolutional code with equal p-Forney indices then $\mathcal{C}$ is an MDP if and only if*

$$d_j^c = \left(n - \left\lceil \frac{k}{r} \right\rceil \right)(j+1) + 1,$$

for all $j \leq L$, with

$$L = \left\lfloor \frac{\left(n - \frac{k}{r}\right)\left\lfloor \frac{\delta}{k} \right\rfloor + \frac{\delta}{r} - \varphi + \left\lceil \frac{k}{r} \right\rceil - \frac{k}{r}}{n - \left\lceil \frac{k}{r} \right\rceil} \right\rfloor,$$

where $\varphi = \left\lceil \frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r} \right\rceil - \left(\frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r}\right)$.

Proof Let $G(D) \in \mathbb{Z}_{p^r}^{n \times k}[D]$ be a p-encoder of $\mathcal{C}$ in reduced form. Write

$$G(D) = G_0 + G_1 D + \cdots + G_\nu D^\nu,$$

with $\nu = \frac{\delta}{k}$,and let us consider G_0 written in the p-standard form as

$$G_0 = \left[\begin{array}{ccccccc}
I_{k_0} & A^0_{1,0} & A^0_{2,0} & A^0_{3,0} & \cdots & A^0_{r-1,0} & A^0_{r,0} \\
\hline
pI_{k_0} & 0 & pA^0_{2,1} & pA^0_{3,1} & \cdots & pA^0_{r-1,1} & pA^0_{r,1} \\
0 & pI_{k_1} & pA^1_{2,1} & pA^1_{3,1} & \cdots & pA^1_{r-1,1} & pA^1_{r,1} \\
\hline
p^2I_{k_0} & 0 & 0 & p^2A^0_{3,2} & \cdots & p^2A^0_{r-1,2} & p^2A^0_{r,2} \\
0 & p^2I_{k_1} & 0 & p^2A^1_{3,2} & \cdots & p^2A^1_{r-1,2} & p^2A^1_{r,2} \\
0 & 0 & p^2I_{k_2} & p^2A^2_{3,2} & \cdots & p^2A^2_{r-1,2} & p^2A^2_{r,2} \\
\hline
\vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\
\hline
p^{r-1}I_{k_0} & 0 & 0 & 0 & \cdots & 0 & p^{r-1}A^0_{r,r-1} \\
0 & p^{r-1}I_{k_1} & 0 & 0 & \cdots & 0 & p^{r-1}A^1_{r,r-1} \\
0 & 0 & p^{r-1}I_{k_2} & 0 & \cdots & 0 & p^{r-1}A^2_{r,r-1} \\
0 & 0 & 0 & p^{r-1}I_{k_3} & \cdots & 0 & p^{r-1}A^3_{r,r-1} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & p^{r-1}I_{k_{r-1}} & p^{r-1}A^{r-1}_{r,r-1}
\end{array}\right]$$

and $G(D)$ and G_i, $i = 1, \ldots, \nu$, written as in (3.4) and (3.10), respectively. From Theorem 3.35, it follows that

$$d_0^c \leq n - (k_0 + k_1 + \cdots + k_{r-1}) + 1$$

and that

$$d_1^c \leq 2n - 2(k_0 + k_1 + \cdots + k_{r-1}) + 1.$$

Let $j = 2$ and

$$\begin{aligned} & v = uG_2^c \\ \Leftrightarrow & \left[\begin{array}{ccc} v_0 & v_1 & v_2 \end{array}\right] = u_0 \left[\begin{array}{ccc} G_0 & G_1 & G_2 \end{array}\right] + u_1 \left[\begin{array}{ccc} 0 & G_0 & G_1 \end{array}\right] + u_0 \left[\begin{array}{ccc} 0 & 0 & G_0 \end{array}\right], \end{aligned}$$

with $u_0 \neq 0$, $u_i \in \mathcal{A}_p$, $i = 0, 1, 2$. Then, considering

$$u_0 = \left[\begin{array}{cccc} 0 & 0 & \ldots & 1 \end{array}\right] \in \mathcal{A}_p^k$$

we have that

$$\begin{cases} v_0 = \left[\begin{array}{ccccc} 0 & \ldots & 0 & 1 & p^{r-1}A^{r-1,k}_{r,r-1} \end{array}\right] \\ v_1 = g_1 + u_1G_0 \\ v_2 = g_2 + u_1G_1 + u_2G_0, \end{cases}$$

where $p^{r-1}A^{r-1,k}_{r,r-1}$ represent the last row of $A^{r-1}_{r,r-1}$ and g_1 and g_2 represent the last row of G_1 and G_2, respectively, with $g_1, g_2 \in \mathbb{Z}_{p^r}^n$. So,

$$\mathrm{wt}(v_0) \leq n - (k_0, k_1, \ldots, k_{r-1}) + 1.$$

Considering u_1 as in the previous case we obtain v_1 such that

$$\mathrm{wt}(v_1) \leq n - (k_0 + k_1 + \cdots + k_{r-1}).$$

Let us now consider

$$v_2 = g_2 + \tilde{\tilde{g}}_1 + u_2 G_0,$$

with $\tilde{\tilde{g}}_1 = u_1 G_1$. Note that, by Lemma 4.9, $\tilde{\tilde{g}}_1 \in p^{r-1}\,\mathbb{Z}_{p^r}^n$, therefore can be written as $\tilde{\tilde{g}}_1 = p^{r-1}\bar{g}_1$, with $\bar{g}_1 \in \mathcal{A}_p$.

It is easy to see that

$$g_2 + \tilde{\tilde{g}}_1 = p^{r-1}\bar{b}^n,$$

with $\bar{b}^n \in \mathcal{A}_p^n$. Consider

$$\bar{b}^n = \left[\begin{array}{cccc} b_{k_0} & b_{k_1} & \cdots & b_{k_{r-1}} \quad b_{n-(k_0+\cdots+k_{r-1})} \end{array} \right]$$

with $b_i \in \mathcal{A}_p^i$, $i = k_0, k_1, \ldots, k_{r-1}$ and $b_{n-(k_0+\cdots+k_{r-1})} \in \mathcal{A}_p^{n-k_0+\cdots+k_{r-1}}$.

Let us construct $\bar{u}_2 \in \mathbb{Z}_{p^r}^k$ such that:

- its first $[(r-1)k_0 + (r-2)k_1 + \cdots + k_{r-2}]$ columns are zero;

- the remaining $(k_0 + k_1 + \cdots + k_{r-1})$ columns are written as follows

$$\left[\begin{array}{cccc} -b_{k_0} & -b_{k_1} & \ldots & -b_{k_{r-1}} \end{array} \right],$$

and take $u_2 \in \mathcal{A}_p^k$ such that $u_2 G_0 = \bar{u}_2 G_0$. So, we obtain v_2 with its first $(k_0 + k_1 + \cdots + k_{r-1})$ elements equal to zero. Thus,

$$\mathrm{wt}(v_2) \leq n - (k_0 + k_1 + \cdots + k_{r-1}).$$

Therefore,

$$\mathrm{wt}(v) = \sum_{i=0}^{2} \mathrm{wt}(v_i) \leq 3n - 3(k_0 + k_1 + \cdots + k_{r-1}) + 1,$$

i.e.,

$$d_2^c \leq 3n - 3(k_0 + k_1 + \cdots + k_{r-1}) + 1.$$

Applying the same reasoning we prove that

$$d_j^c \leq (j+1)n - (j+1)(k_0 + k_1 + \cdots + k_{r-1}) + 1, \tag{4.12}$$

for all j.

The highest value of (4.12) is obtained by considering the minimum value of $(k_0 + k_1 + \cdots + k_{r-1})$. By Lemma 3.15 this minimum is given by $\left\lceil \frac{k}{r} \right\rceil$, and, from the definition of MDP convolutional code, we have that

$$d_j^c = \left(n - \left\lceil \frac{k}{r} \right\rceil \right) (j+1) + 1.$$

The value of L follows immediately from Theorem 3.38. □

Let $\widetilde{\mathcal{C}}$ be an MDP $(n, \widetilde{k}, \frac{\delta}{k}\widetilde{k})$-convolutional code over $\mathbb{Z}_p$ with Forney indices all equal to $\frac{\delta}{k}$ and $\widetilde{k} = \left\lceil \frac{k}{r} \right\rceil$. Consider $\widetilde{G}(D)$ an encoder of $\widetilde{\mathcal{C}}$ in reduced form and write

$$\widetilde{G}(D) = \begin{bmatrix} \widetilde{G}^{(1)}(D) \\ \widetilde{G}^{(2)}(D) \end{bmatrix},$$

with $\widetilde{G}^{(1)}(D) \in \mathbb{Z}_p^{\left\lfloor \frac{k}{r} \right\rfloor \times n}[D]$ and $\widetilde{G}^{(1)}(D) \in \mathbb{Z}_p^{1\times n}[D]$. Construct

$$G(D) = \begin{bmatrix} \widetilde{G}^{(1)}(D) \\ p\widetilde{G}^{(1)}(D) \\ \vdots \\ p^{r-1}\widetilde{G}^{(1)}(D) \\ p^{r-b}\widetilde{G}^{(2)}(D) \\ p^{r-(b-1)}\widetilde{G}^{(2)}(D) \\ \vdots \\ p^{r-1}\widetilde{G}^{(2)}(D) \end{bmatrix} \in \mathbb{Z}_{p^r}^{k\times n}[D], \tag{4.13}$$

where b is such that $k = r\left\lfloor \frac{k}{r} \right\rfloor + b$.

Theorem 4.11. *Let $\mathcal{C}$ be an (n, k, δ)-convolutional code with p-encoder $G(D)$ as in (4.13). Then $\mathcal{C}$ is an MDP convolutional code over $\mathbb{Z}_{p^r}$.*

The proof of the above theorem follows the same reasoning as the proof of Theorem 4.8.

Remark 4.12. *If $r \mid k$, we consider $\widetilde{G}(D) \in \mathbb{Z}_p^{\widetilde{k}\times n}[D]$ an encoder of an MDP $(n, \widetilde{k}, \frac{\delta}{k}\widetilde{k})$-*

convolutional code over $\mathbb{Z}_p$ *with Forney indices all equal to* $\frac{\delta}{k}$ *and* $\widetilde{k} = \left\lceil \frac{k}{r} \right\rceil$. *Then,*

$$G(D) = \begin{bmatrix} \widetilde{G}(D) \\ p\widetilde{G}(D) \\ \vdots \\ p^{r-1}\widetilde{G}(D) \end{bmatrix} \in \mathbb{Z}_{p^r}^{k \times n}[D],$$

is a p-encoder of an MDS (n, k, δ)*-convolutional code over* $\mathbb{Z}_{p^r}$.

Chapter 5

Duality

Encoders of a convolutional codes define an image representation of these codes. However there are some convolutional codes that admit another type of representation of such codes, called kernel representation. For this type of representation another type of matrices is used: parity-check matrices or syndrome formers. A polynomial matrix $H(D)$ is a **parity-check matrix** of a convolutional code $\mathcal{C}$ if, for every word $w(D)$,

$$w(D) \in \mathcal{C} \Leftrightarrow w(D)H(D) = 0.$$

However, convolutional codes defined in $\mathbb{Z}_{p^r}[D]$ do not always admit a parity-check matrix as it shown in the next example.

Example 5.1. *Consider the convolutional code $\mathcal{C}$ with encoder*

$$G(D) = \begin{bmatrix} 1+D & 0 & 1+D \\ 0 & 1 & 1 \end{bmatrix} \in \mathbb{Z}_9^{2\times 3}[D].$$

This code does not admit a kernel representation as we shall show by contradiction. Suppose that $H(D)$ is a parity-check matrix of $\mathcal{C}$ and let us consider the word

$$\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} \notin \mathcal{C}.$$

Since

$$\begin{bmatrix} 1+D & 0 & 1+D \end{bmatrix} \in \mathcal{C}$$

then

$$\begin{bmatrix} 1+D & 0 & 1+D \end{bmatrix} H(D) = 0$$

which is equivalent to

$$(1+D)\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} H(D) = 0$$

and consequently

$$\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} H(D) = 0.$$

It is well-known that kernel representations are useful to detect errors introduced during transmission. If a word $w(D)$ is received after channel transmission, the existence of errors is checked by simple multiplication by $H(D)$: if $w(D)H(D) = 0$, it is assumed that no errors occurred. As we have seen in Example 5.1 not all convolutional codes defined in $\mathbb{Z}_{p^r}[D]$ admit a parity-check matrix. However, if there exists a matrix $H(D)$ such that $\mathcal{C} \subset \ker H(D)$, we still make use of $H(D)$ to decode when the transmission occurs over the erasure channel. In this channel the word can have only erasures (*i.e.*, part of the word can be missing) but no errors occur. In fact, if one considers the erasures as indeterminate, $w(D)H(D) = 0$ give rises to a system of linear equations. Solving this system amounts to decoding the received word $w(D)$ (for more details see [VTS09]).

Given a convolutional code $\mathcal{C}$ defined in $\mathbb{Z}_{p^r}[D]$ with encoder $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$, let us consider the set

$$\tilde{\mathcal{C}} = \{u(D)G(D) : u(D) \in \mathbb{Z}_{p^r}^k((D))\},$$

where $\mathbb{Z}_{p^r}((D))$ denotes the **ring of Laurent series** over $\mathbb{Z}_{p^r}$, i.e., $\mathbb{Z}_{p^r}((D))$ the set of elements of the form

$$a(D) = \sum_{i=-\infty}^{+\infty} a_i D^i$$

where the coefficients a_i are in $\mathbb{Z}_{p^r}$ and only finitely coefficients with negative indices may be nonzero.

Note that $\mathcal{C} \subset \tilde{\mathcal{C}}$. In the next section, we will see that $\tilde{\mathcal{C}}$ is also a convolutional code (defined in $\mathbb{Z}_{p^r}((D))$) that always admit a parity-check matrix $H(D)$, and consequently, $\mathcal{C} \subset \ker H(D)$.

5.1 Convolutional codes defined in $\mathbb{Z}_{p^r}((D))$

In this section we will consider convolutional codes constituted by left compact sequences in $\mathbb{Z}_{p^r}$, i.e., the codewords of the code will be of the form

$$\begin{array}{rccc} w: & \mathbb{Z} & \to & \mathbb{Z}_{p^r}^n \\ & t & \mapsto & w_t \end{array}$$

where $w_t = 0$ for $t < \ell$ for some $\ell \in \mathbb{Z}$. These sequences can be represented by Laurent series,

$$w(D) = \sum_{t=\ell}^{\infty} w_t D^t \in \mathbb{Z}_{p^r}((D)).$$

Let us denote by $\mathbb{Z}_{p^r}(D)$ the ring of rational matrices defined in $\mathbb{Z}_{p^r}$. More precisely, $\mathbb{Z}_{p^r}(D)$ is the set

$$\{\frac{p(D)}{q(D)} : p(D), q(D) \in \mathbb{Z}_{p^r}[D] \text{ and the coefficient of the smallest power of } D \text{ in } q(D) \text{ is a unit}\}.$$

This condition allows us to treat a rational function as an equivalence class in the relation

$$\frac{p(D)}{q(D)} \sim \frac{p_1(D)}{q_1(D)} \text{ if and only if } p(D)q_1(D) = f_1(D)q(D).$$

Note that $\mathbb{Z}_{p^r}(D)$ is a subring of $\mathbb{Z}_{p^r}((D))$ and, obviously $\mathbb{Z}_{p^r}[D]$ is a subring of $\mathbb{Z}_{p^r}(D)$.

A rational matrix $A(D) \in \mathbb{Z}_{p^r}^{\ell\times\ell}(D)$ is invertible if there exists a rational matrix $L(D) \in \mathbb{Z}_{p^r}^{\ell\times\ell}(D)$ such that $L(D)A(D) = I$.

Lemma 5.2. *Let $A(D) \in \mathbb{Z}_{p^r}^{\ell\times\ell}(D)$. The following are equivalent:*

i) $A(D)$ is invertible,

ii) $\det \bar{A}(D) \neq 0$,

iii) $\bar{A}(D)$ is invertible in $\mathbb{Z}_p^{\ell\times\ell}(D)$,

where $\bar{A}(D)$ represents the projection of $A(D)$ into $\mathbb{Z}_p(D)$.

In fact, if $\bar{A}(D)$ is invertible in $\mathbb{Z}_p^{\ell\times\ell}(D)$ and $B(D) \in \mathbb{Z}_p^{\ell\times\ell}(D)$ is such that $B(D)A(D) = I \bmod p$, then

$$B(D)A(D) = I - pC(D)$$

over $\mathbb{Z}_{p^r}((D))$, for some $C(D) \in \mathbb{Z}_{p^r}^{\ell\times\ell}(D)$. Then the inverse of $A(D)$ is

$$L(D) = (I + pC(D) + p^2C(D)^2 + \cdots + p^{r-1}C(D)^{r-1})B(D) \in \mathbb{Z}_{p^r}^{\ell\times\ell}(D).$$

Definition 5.3. *[For70, EOS13] A* **convolutional code** $\mathcal{C}$ *defined in $\mathbb{Z}_{p^r}^n((D))$ of length n is a $\mathbb{Z}_{p^r}((D))$-submodule of $\mathbb{Z}_{p^r}^n((D))$ for which there exists a polynomial matrix $\widetilde{G}(D) \in \mathbb{Z}_{p^r}^{\tilde{k}\times n}[D]$ such that*

$$\begin{aligned} \mathcal{C} &= Im_{\mathbb{Z}_{p^r}((D))}\widetilde{G}(D) \\ &= \left\{u(D)\widetilde{G}(D) \in \mathbb{Z}_{p^r}^n((D)) : u(D) \in \mathbb{Z}_p^{\tilde{k}}((D))\right\}. \end{aligned}$$

The matrix $\widetilde{G}(D)$ is called a **generator matrix** *of $\mathcal{C}$. If $\widetilde{G}(D)$ is full row rank then it is called an* **encoder** *of $\mathcal{C}$.*

Moreover, if

$$\begin{aligned}\mathcal{C} &= Im_{\mathcal{A}_p((D))}G(D)\\ &= \left\{u(D)G(D) \in \mathbb{Z}_{p^r}^n((D)) : u(D) \in \mathcal{A}_p^k((D))\right\},\end{aligned}$$

where $\mathcal{A}_p((D)) = \{\sum_{i=s}^{+\infty} a_i D^i : a_i \in \mathcal{A}_p$ and $s \in \mathbb{Z}\}$, and $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ is a polynomial matrix whose rows form a p-basis, then $G(D)$ is a **p-encoder** *of $\mathcal{C}$ and we say that $\mathcal{C}$ has* **p-dimension** *k.*

Note that if $\widetilde{G}(D) \in \mathbb{Z}_{p^r}^{\tilde{k}\times n}[D]$ is a generator matrix of a convolutional code $\mathcal{C}$ and $X(D) \in \mathbb{Z}_{p^r}^{\tilde{k}\times\tilde{k}}(D)$ is an invertible rational matrix such that $X(D)\widetilde{G}(D)$ is polynomial, then

$$\mathrm{Im}_{\mathbb{Z}_{p^r}((D))}\widetilde{G}(D) = \mathrm{Im}_{\mathbb{Z}_{p^r}((D))}X(D)\widetilde{G}(D),$$

which means that $X(D)\widetilde{G}D)$ is also a generator matrix of $\mathcal{C}$. Thus, the next result is straightforward.

Lemma 5.4. *Let $\mathcal{C}$ be a $\mathbb{Z}_{p^r}((D))$-submodule of $\mathbb{Z}_{p^r}^n((D))$ given by $\mathcal{C} = Im_{\mathbb{Z}_{p^r}((D))}N(D)$, where $N(D) \in \mathbb{Z}_{p^r}^{\tilde{k}\times n}(D)$. Then $\mathcal{C}$ is a convolutional code, and if $N(D)$ is full row rank, $\mathcal{C}$ is a free code of rank $\widetilde{k}$.*

Next we will consider a decomposition of a convolutional code into simpler components. For that we need the following lemma.

Lemma 5.5. *Let M be a submodule of $\mathbb{Z}_{p^r}^n((D))$. Then, there exists a unique family $M_0, \ldots, M_{r-1}$ of free submodules of $\mathbb{Z}_{p^r}^n((D))$ such that*

$$M = M_0 \oplus pM_1 \oplus \ldots \oplus p^{r-1}M_{r-1}. \tag{5.1}$$

Proof Let $\overline{M}$ be the projection of M defined $\mathbb{Z}_p((D))$ and denote its dimension by k_0. Let M_0 be the free code defined $\mathbb{Z}_{p^r}((D))$ of rank k_0 satisfying $\overline{M} = \overline{M_0}$ and $M_0 \subset M$. As $\mathbb{Z}_{p^r}^n((D))$ is a semisimple module, M_0 admits a complement code M_0' in M. Necessarily, there exists a code M_1' such that $M_0' = pM_1'$ and we have $M = M_0 \oplus pM_1'$. Applying successively the same reasoning we obtain (5.1). □

Remark 5.6. *It is not always possible to obtain the sum decomposition (5.1) when we consider submodules of $\mathbb{Z}_{p^r}^n[D]$. For example, if we consider the submodule $M = span([1+D \;\; 1+D+9D^2], [3 \;\; 3]) \subset \mathbb{Z}_{27}^2[D]$ there are no free submodules of $\mathbb{Z}_{27}^2[D]$, M_0, M_1, M_2 such that $M = M_0 \oplus 3M_1 \oplus 9M_2$.*

Remark 5.7. *Note that if $\mathcal{C}$ is a block code, this decomposition is directly derived from a generator matrix in standard form. In fact, if G in the form (3.1), is a generator matrix of $\mathcal{C}$ then*

$$p^i\mathcal{C}_i = Im_{\mathbb{Z}_{p^r}((D))}p^iG_i,$$

where $G_i = [0 \cdots 0\ I_{k_i}\ A^i_{2,i} \cdots A^i_{r,i}]$, $i = 0, \ldots, r-1$.

Note that Lemma 5.5 is not constructive and it does not give a clue on how to build the free modules M_i, $i = 0, \ldots, r-1$. Moreover, it is not known whether these modules are indeed convolutional codes. Next, we address these issues and provide a constructive version of the Lemma 5.5 in terms of the associated matrices.

Let $\widetilde{G}(D)$ be a generator matrix of $\mathcal{C}$. If $\widetilde{G}(D)$ is full row rank then $\mathcal{C}$ is free and $\mathcal{C} = \mathcal{C}_0$.
Let us assume now that $\widetilde{G}(D)$ is not full row rank. Then the projection of $\widetilde{G}(D)$ into $\mathbb{Z}_p[D]$,

$$\overline{\widetilde{G}}(D) \in \mathbb{Z}_p^{k\times n}[D],$$

is also not full row rank and there exists a nonsingular matrix $F_0(D) \in \mathbb{Z}_p^{k\times k}[D]$ such that

$$F_0(D)\overline{\widetilde{G}}(D) = \begin{bmatrix} G_0(D) \\ 0 \end{bmatrix} \mod\ p,$$

where $G_0(D)$ is full row rank with rank k_0. Regarding $F_0(D)$ in $\mathbb{Z}_{p^r}^{k\times k}[D]$, it follows that

$$F_0(D)\widetilde{G}(D) = \begin{bmatrix} \widetilde{G}_0(D) \\ p\widehat{G}_1(D) \end{bmatrix},$$

where $\widetilde{G}_0(D) \in \mathbb{Z}_{p^r}^{k_0\times n}[D]$ is such that $\overline{\widetilde{G}_0}(D) = G_0(D)$. Moreover, since $F_0(D)$ is invertible, $\begin{bmatrix} \widetilde{G}_0(D) \\ p\widehat{G}_1(D) \end{bmatrix}$ is also a generator matrix of $\mathcal{C}$.

Let us now consider $F_1(D) \in \mathbb{Z}_p^{(k-k_0)\times(k-k_0)}[D]$ such that

$$F_1(D)\overline{\widehat{G}_1}(D) = \begin{bmatrix} {G'}_1(D) \\ 0 \end{bmatrix} \mod\ p,$$

where ${G'}_1(D)$ is full row rank with rank k_1. Then, considering $F_1(D)$ in $\mathbb{Z}_{p^r}^{(k-k_0)\times(k-k_0)}[D]$, it follows that

$$F_1(D)\widehat{G}_1(D) = \begin{bmatrix} G''_1(D) \\ p\widehat{G}_2(D) \end{bmatrix},$$

where $G_1''(D) \in \mathbb{Z}_{p^r}^{\tilde{k}_1 \times n}[D]$ is such that $\overline{G_1''}(D) = G_1'(D)$, and therefore

$$\begin{bmatrix} I_{k_0} & 0 \\ 0 & F_1(D) \end{bmatrix} F_0(D)\widetilde{G}(D) = \begin{bmatrix} \widetilde{G}_0(D) \\ pG_1''(D) \\ p^2\widehat{G}_2(D) \end{bmatrix}.$$

If $\begin{bmatrix} \widetilde{G}_0(D) \\ G_1''(D) \end{bmatrix}$ is not full row rank, then there exists a permutation matrix P and a rational matrix $L_1(D) \in \mathbb{Z}_{p^r}^{\tilde{k}_1 \times k_0}(D)$ such that

$$P \begin{bmatrix} I_{k_0} & 0 \\ L_1(D) & I_{k_1} \end{bmatrix} \begin{bmatrix} \widetilde{G}_0(D) \\ pG_1''(D) \end{bmatrix} = \begin{bmatrix} \widetilde{G}_0(D) \\ pG_1'''(D) \\ p^2G_2'(D) \end{bmatrix},$$

where $G_1'''(D) \in \mathbb{Z}_{p^r}^{k_1 \times n}(D)$ and $G_2'(D) \in \mathbb{Z}_{p^r}^{(\tilde{k}_1 - k_1) \times n}(D)$ are rational matrices and $\begin{bmatrix} \widetilde{G}_0(D) \\ G_1'''(D) \end{bmatrix}$ is a full row rank rational matrix. Note that since

$$P \begin{bmatrix} I_{k_0} & 0 \\ L_1(D) & I_{k_1} \end{bmatrix}$$

is nonsingular it follows that

$$\operatorname{Im}_{\mathbb{Z}_{p^r}((D))} \begin{bmatrix} \widetilde{G}_0(D) \\ pG_1''(D) \end{bmatrix} = \operatorname{Im}_{\mathbb{Z}_{p^r}((D))} \begin{bmatrix} \widetilde{G}_0(D) \\ pG_1'''(D) \\ p^2G_2'(D) \end{bmatrix}.$$

Let $\widetilde{G}_1(D)\mathbb{Z}_{p^r}^{k_1 \times n}[D]$ and $G_2''(D) \in \mathbb{Z}_{p^r}^{(\tilde{k}_1 - k_1) \times n}[D]$ be polynomial matrices (see Lemma 5.4) such that

$$\operatorname{Im}_{\mathbb{Z}_{p^r}((D))} \begin{bmatrix} \widetilde{G}_0(D) \\ pG_1'''(D) \\ p^2G_2'(D) \end{bmatrix} = \operatorname{Im}_{\mathbb{Z}_{p^r}((D))} \begin{bmatrix} \widetilde{G}_0(D) \\ p\widetilde{G}_1(D) \\ p^2G_2''(D) \end{bmatrix}.$$

Then $\begin{bmatrix} \widetilde{G}_0(D) \\ p\widetilde{G}_1(D) \\ p^2G_2''(D) \\ p^2\widehat{G}_2(D) \end{bmatrix}$ is still a generator matrix of $\mathcal{C}$ such that $\begin{bmatrix} \widetilde{G}_0(D) \\ \widetilde{G}_1(D) \end{bmatrix}$ is full row rank.

Proceeding in the same way we obtain a generator matrix of $\mathcal{C}$ of the form

$$\begin{bmatrix} \widetilde{G}_0(D) \\ p\widetilde{G}_1(D) \\ \vdots \\ p^{r-1}\widetilde{G}_{r-1}(D) \end{bmatrix},$$

and such that

$$\begin{bmatrix} \widetilde{G}_0(D) \\ \widetilde{G}_1(D) \\ \vdots \\ \widetilde{G}_{r-1}(D) \end{bmatrix}$$

is full row rank. Thus

$$\mathcal{C}_i := \mathrm{Im}_{\mathbb{Z}_{p^r}((D))} G_i(D)$$

is a free convolutional code, $i = 0, 1, \ldots, r-1$, and

$$\mathcal{C} = \mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \cdots \oplus p^{r-1}\mathcal{C}_{r-1}.$$

If we denote by k_i the rank of $\mathcal{C}_i$ then the family $\{k_0, \ldots, k_{r-1}\}$ is an invariant of the code. Moreover, it is clear that $\mathcal{C}$ is free if and only if $k_i = 0$ for $i = 1 \ldots r-1$.

The following lemmas will be very useful for deriving the results of the remaining sections.

Lemma 5.8. *Let $\mathcal{C}$ be a free convolutional code of length n defined in $\mathbb{Z}_{p^r}((D))$ with rank k. Then, p-dim $(p^i\mathcal{C}) = (r-i)k$, $i = \{0, \ldots, r-1\}$.*

Proof Let $\widetilde{G}(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ be an encoder of $\mathcal{C}$. The result follows from the fact that

$$\begin{bmatrix} p^i\widetilde{G}(D) \\ p^{i+1}\widetilde{G}(D) \\ \vdots \\ p^{r-1}\widetilde{G}(D) \end{bmatrix}$$

is an p-encoder of $p^i\mathcal{C}$, since $\widetilde{G}D)$ is full row rank. □

Lemma 5.9. *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two convolutional codes defined in $\mathbb{Z}_{p^r}((D))$. Then*

$$p\text{-dim}\,(\mathcal{C}_1 + \mathcal{C}_2) = p\text{-dim}\,\mathcal{C}_1 + p\text{-dim}\,\mathcal{C}_2 - p\text{-dim}\,(\mathcal{C}_1 \cap \mathcal{C}_2).$$

If the sum is direct then

$$p\text{-}dim\,(\mathcal{C}_1 \oplus \mathcal{C}_2) = p\text{-}dim\,\mathcal{C}_1 + p\text{-}dim\,\mathcal{C}_2.$$

Proof Suppose that $\mathcal{C}_1$ and $\mathcal{C}_2$ are in direct sum, i.e,

$$\mathcal{C}_1 \cap \mathcal{C}_2 = \{0\}.$$

If B_1 is a p-basis of $\mathcal{C}_1$ and B_2 is a p-basis of $\mathcal{C}_2$, then (B_1, B_2) is a p-basis of $\mathcal{C}_1 \oplus \mathcal{C}_2$ which gives the result.
For the general case, let denote by $\mathfrak{A}$ a complement of $\mathcal{C}_1 \cap \mathcal{C}_2$ in $\mathcal{C}_1$, i.e.,

$$\mathcal{C}_1 = \mathfrak{A} \oplus (\mathcal{C}_1 \cap \mathcal{C}_2),$$

and let $\mathfrak{B}$ such that

$$\mathcal{C}_2 = \mathfrak{B} \oplus (\mathcal{C}_1 \cap \mathcal{C}_2).$$

Then we have

$$\mathcal{C}_1 + \mathcal{C}_2 = \mathfrak{A} \oplus (\mathcal{C}_1 \cap \mathcal{C}_2) \oplus \mathfrak{B}$$

and the result is immediate. □

Next corollary follows immediately from lemmas 5.8 and 5.9.

Corollary 5.10. *Let $\mathcal{C}$ be a convolutional code defined in $\mathbb{Z}_{p^r}((D))$of length n such that*

$$\mathcal{C} = \mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \cdots \oplus p^{r-1}\mathcal{C}_{r-1}$$

with $\mathcal{C}_i$ a free convolutional code with rank k_i, $i = 0, 1, \ldots, r-1$. Then

$$p\text{-}dim\,(\mathcal{C}) = \sum_{i=0}^{r-1}(r-i)k_i.$$

5.2 Dual Code

Definition 5.11. *Let $\mathcal{C}$ be a convolutional code defined in $\mathbb{Z}_{p^r}((D))$ of length n. The* **dual** *of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined as*

$$\mathcal{C}^\perp = \{y(D) \in \mathbb{Z}_{p^r}^n((D)) : y(D)x^T(D) = 0 \text{ for all } x(D) \in \mathcal{C}\}.$$

In this section we will show that the dual of a convolutional code is still a convolutional code. The next theorem proves this statement for free convolutional codes.

Theorem 5.12. *Let $\mathcal{C}$ be a free convolutional code defined in $\mathbb{Z}_{p^r}((D))$ with length n and rank $\tilde{k}$. Then $\mathcal{C}^\perp$ is also a free convolutional code of length n and rank $n-\tilde{k}$.*

Proof Let $G(D) \in \mathbb{Z}_{p^r}^{\tilde{k}\times n}[D]$ be an encoder of $\mathcal{C}$. Since $G(D)$ is full row rank there exists a polynomial matrix $L(D) \in \mathbb{Z}_{p^r}^{(n-\tilde{k})\times n}[D]$ such that $\begin{bmatrix} G(D) \\ L(D) \end{bmatrix}$ is invertible. Let $[X(D)\ Y(D)]$, with $X(D) \in \mathbb{Z}_{p^r}^{n\times\tilde{k}}(D)$ and $Y(D) \in \mathbb{Z}_{p^r}^{n\times(n-\tilde{k})}(D)$, be the inverse of $\begin{bmatrix} G(D) \\ L(D) \end{bmatrix}$. Then

$$\mathcal{C}^\perp = \mathrm{Im}_{\mathbb{Z}_{p^r}((D))} Y^T(D),$$

which means by Lemma 5.4 that $\mathcal{C}^\perp$ is a convolutional code. Moreover, since $Y(D)$ is full column rank, there exists a full row rank matrix polynomial matrix $G^\perp(D) \in \mathbb{Z}_{p^r}^{(n-\tilde{k})\times n}[D]$ such that

$$\mathcal{C}^\perp = \mathrm{Im}_{\mathbb{Z}_{p^r}((D))} G^\perp(D).$$

Thus $\mathcal{C}^\perp$ is a free convolutional code or rank $n-\tilde{k}$. □

Next corollary is straightforward and generalizes the well-known result for vector spaces.

Corollary 5.13. *Let $\mathcal{C}$ be a free convolutional code defined in $\mathbb{Z}_{p^r}((D))$ of length n. Then*

$$p\text{-}dim\,(\mathcal{C}) + p\text{-}dim\,(\mathcal{C}^\perp) = nr.$$

In the sequel we propose to establish this result for any code defined $\mathbb{Z}_{p^r}((D))$. The following auxiliary lemmas will be fundamental in the proof of next theorem.

Lemma 5.14. *Let $\mathcal{C}$ be a free convolutional code defined in $\mathbb{Z}_{p^r}((D))$. Then*

$$\mathcal{C} \cap p^i \mathbb{Z}_{p^r}^n((D)) = p^i \mathcal{C},$$

for $i \in \{0, \dots r-1\}$.

Proof The inclusion $p^i\mathcal{C} \subset \mathcal{C} \cap p^i\mathbb{Z}_{p^r}^n((D))$ is trivial. For the other direction, let $y(D) \in p^i\mathbb{Z}_{p^r}^n((D)) \cap \mathcal{C}$. Let $\{x_1(D), \dots, x_k(D)\}$ be a basis of $\mathcal{C}$ and its projection $\{\overline{x_1}(D), \dots, \overline{x_k}(D)\}$ over $\mathbb{Z}_p[D]$ be a basis of $\overline{\mathcal{C}}$. Then, there exist $a_1(D), \dots, a_k(D) \in \mathbb{Z}_{p^r}((D))$ such that

$$y(D) = \sum_{j=1}^{k} a_j(D) x_j(D).$$

As $y(D) \in p^i \mathbb{Z}_{p^r}^n((D))$, it follows that

$$\overline{y}(D) = \sum_{j=1}^{k} \overline{a_j}(D)\overline{x_j}(D) = 0 \mod p,$$

where $\overline{a_j}(D) = 0, \ \forall j = 1, \ldots, k$. Then, for all $j = 1, \ldots, k$, $a_j(D)$ can be written as $pb_j(D)$ where $b_j(D) \in \mathbb{Z}_{p^r}((D))$. By repeating this procedure i times, we obtain $a_j(D) = p^i \alpha_j(D), \ j = 1, \ldots, k$, which gives

$$y(D) = p^i \sum_{j=1}^{k} \alpha_j(D) x_j(D) \in p^i \mathcal{C}.$$

□

Lemma 5.15. *Suppose that $\mathcal{C}$ is a free convolutional code defined in $\mathbb{Z}_{p^r}((D))$. Let $y(D) \in \mathbb{Z}_{p^r}^n((D))$ and let $i \in \{0, \ldots, r-1\}$, such that $p^i y(D) \in \mathcal{C}$. Then $y(D) \in \mathcal{C} + p^{r-i}\mathbb{Z}_{p^r}^n((D))$.*

Proof By Lemma 5.14, there exists $x(D) \in \mathcal{C}$ such that $p^i y(D) = p^i x(D)$. This implies that $\overline{y}(D) = \overline{x}(D)$. Thus there exists $y_1(D) \in \mathcal{C}$, $y_2(D) \in \mathbb{Z}_{p^r}((D))$ satisfying

$$y(D) = y_1(D) + py_2(D).$$

Then $p^i y(D) = p^i y_1(D) + p^{i+1} y_2$ which implies that $p^i y(D) - p^i y_1(D) = p^{i+1} y_2(D) \in \mathcal{C}$. Thus

$$y_2(D) = y_3(D) + py_4(D)$$

where $y_3(D) \in \mathcal{C}$ and $y_4(D) \in \mathbb{Z}_{p^r}^n((D))$. Thus

$$y(D) = \underbrace{y_1(D) + py_3(D)}_{\in \mathcal{C}} + p^2 y_4(D).$$

By repeating this procedure $r - i$ times, we obtain

$$y(D) = x_1(D) + p^{r-i} x_2(D)$$

with $x_1(D) \in \mathcal{C}$. □

Lemma 5.16. *Let $\mathcal{C}$ be a free convolutional code defined in $\mathbb{Z}_{p^r}((D))$. Then, for all integer $i \in \{0, \dots r-1\}$ it follows that*

$$(p^i\mathcal{C})^\perp = \mathcal{C}^\perp + p^{r-i}\mathbb{Z}_{p^r}^n((D)).$$

Proof It is clear that

$$\mathcal{C}^\perp + p^{r-i}\mathbb{Z}_{p^r}^n((D)) \subset (p^i\mathcal{C})^\perp.$$

For the other direction, let $y(D) \in (p^i\mathcal{C})^\perp$ and then, for all $x(D) \in \mathcal{C}$, we have

$$y(D)(p^i x(D))^T = (p^i y(D))x^T(D) = 0,$$

and thus $p^i y(D) \in \mathcal{C}^\perp$.
As $\mathcal{C}^\perp$ is a free convolutional code we conclude, by Lemma 5.15, that

$$y(D) \in \mathcal{C}^\perp + p^{r-i}\mathbb{Z}_{p^r}^n((D)).$$

□

Remark 5.17. *Lemmas 5.14, 5.15 and 5.16 are also valid for block codes over $\mathbb{Z}_{p^r}$ and they were first proved in [EO15].*

Given a convolutional code $\mathcal{C} \subset \mathbb{Z}_{p^r}^n((D))$, an explicit construction of the dual code is, in general, difficult. The following result provides a procedure to build $\mathcal{C}^\perp$. The method is constructive as it deals only with free modules.

Theorem 5.18. *Let $\mathcal{C} = \mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1}$ be a convolutional code defined in $\mathbb{Z}_{p^r}((D))$ of length n, such that $\mathcal{C}_i$ is free, $i = 0, 1, \dots, r-1$, with*

$$\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \ldots \oplus \mathcal{C}_{r-1} = \mathcal{C}_0 + \mathcal{C}_1 + \ldots + \mathcal{C}_{r-1}$$

and let B_{r-i} be a free convolutional code defined in $\mathbb{Z}_{p^r}^n((D))$ such that

$$(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^\perp = (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1} \oplus \mathcal{C}_i)^\perp \oplus B_{r-i},$$

$i = 1, \dots, r-1$, and $B_0 = (\mathcal{C}_0 \oplus \ldots \oplus \mathcal{C}_{r-1})^\perp$. Then

$$\mathcal{C}^\perp = B_0 \oplus pB_1 \oplus \ldots \oplus p^{r-1}B_{r-1}.$$

Proof Let us show that

$$(\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp = (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + p(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp + \\ + \cdots + p^{r-3}(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \mathcal{C}_2)^\perp + p^{r-2}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp + p^{r-1}\mathcal{C}_0^\perp.$$

Since

$$\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1} \subset \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1}$$

it follows that

$$(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp \subset (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp.$$

Moreover,

$$p^{r-1}\mathcal{C}_0^\perp \subset \mathcal{C}_0^\perp \text{ and } p^{r-1}\mathcal{C}_0^\perp \subset p^{r-1}\mathbb{Z}_{p^r}^n((D)) \subset (p\mathcal{C}_1)^\perp \cap (p^2\mathcal{C}_2)^\perp \cap \cdots \cap (p^{r-1}\mathcal{C}_{r-1})^\perp$$

and therefore

$$p^{r-1}\mathcal{C}_0^\perp \subset \mathcal{C}_0^\perp \cap (p\mathcal{C}_1)^\perp \cap (p^2\mathcal{C}_2)^\perp \cap \cdots \cap (p^{r-1}\mathcal{C}_{r-1})^\perp = (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp.$$

We have also that

$$p^{r-2}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp \subset (\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp \subset (\mathcal{C}_0 \oplus p\mathcal{C}_1)^\perp$$

and

$$p^{r-2}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp \subset p^{r-2}\mathbb{Z}_{p^r}^n((D)) \subset (p^2\mathcal{C}_2)^\perp \cap \cdots \cap (p^{r-1}\mathcal{C}_{r-1})^\perp$$

and consequently

$$p^{r-2}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp \subset (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp.$$

Applying the same reasoning, we conclude that

$$p^{r-i}(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^\perp \subset (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp,$$

$i = 3, \ldots, r-1$, and therefore

$$(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + p(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp + \cdots + p^{r-3}(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \mathcal{C}_2)^\perp + \\ + p^{r-2}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp + p^{r-1}\mathcal{C}_0^\perp \subset (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp.$$

On the other hand, let $x(D) \in (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp$. So,

$$\begin{aligned} x(D) \in (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp \cap p\mathbb{Z}_{p^r}^n((D)) + \\ + (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-3})^\perp \cap p^2\mathbb{Z}_{p^r}^n((D)) + \cdots + \mathcal{C}_0^\perp \cap p^{r-1}\mathbb{Z}_{p^r}^n((D)). \end{aligned}$$

Then, by Lemma 5.14,

$$x(D) \in (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + p(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp + p^2(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-3})^\perp + \cdots + p^{r-1}\mathcal{C}_0^\perp.$$

Thus

$$\begin{aligned} (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp = (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + p(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp + \\ + \cdots + p^{r-3}(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \mathcal{C}_2)^\perp + p^{r-2}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp + p^{r-1}\mathcal{C}_0^\perp. \end{aligned}$$

Moreover, since B_{r-1}, $\mathcal{C}_0$ and $\mathcal{C}_0 \oplus \mathcal{C}_1$ are free convolutional codes such that

$$\mathcal{C}_0^\perp = (\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp \oplus B_{r-1},$$

it follows that

$$p^{r-1}\mathcal{C}_0^\perp = p^{r-1}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp \oplus p^{r-1}B_{r-1}$$

and therefore

$$\begin{aligned} (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp &= (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + p(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp + \\ &\quad + \cdots + p^{r-3}(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \mathcal{C}_2)^\perp + p^{r-2}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp + \\ &\quad + p^{r-1}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp + p^{r-1}B_{r-1} \\ &= (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + p(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp + \\ &\quad + \cdots + p^{r-3}(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \mathcal{C}_2)^\perp + p^{r-2}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp + p^{r-1}B_{r-1}. \end{aligned}$$

Applying the same reasoning we conclude that

$$(\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp = (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + pB_1 + p^2B_2 + \cdots + p^{r-1}B_{r-1}.$$

Finally, let us see that

$$(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp \cap p^{r-i}B_{r-i} = \{0\},$$

$i = 1, \ldots, r-1$, and that

$$p^{r-j}B_{r-j} \cap p^{r-i}B_{r-i} = \{0\},$$

for $1 \leq j < i \leq r-1$.

Let $i \in \{1, \ldots, r-1\}$. Since $(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_i)^\perp \cap B_{r-i} = \{0\}$, $p^{r-i}B_{r-i} \subset B_{r-i}$ and $(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp \subset (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_i)^\perp$ it follows that

$$(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp \cap p^{r-i}B_{r-i} = \{0\}.$$

Moreover, let $j \in \{1, \ldots, r-1\}$, with $j < i$. Note that $B_{r-i} \subset (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^\perp \subset (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_j)^\perp$ and that $B_{r-j} \cap (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_j)^\perp = \{0\}$. Thus,

$$B_{r-i} \cap B_{r-j} = \{0\}$$

and consequently also

$$p^{r-j}B_{r-j} \cap p^{r-i}B_{r-i} = \{0\}.$$

□

So, we conclude that the dual of a convolutional code defined in $\mathbb{Z}_{p^r}((D))$ is also a convolutional code.

The following result generalizes Corollary 5.13 for general (non necessarily free) convolutional codes.

Corollary 5.19. *Let $\mathcal{C}$ be a convolutional code of length n defined $\mathbb{Z}_{p^r}^n$. Then*

$$p\text{-}dim\,(\mathcal{C}) + p\text{-}dim\,(\mathcal{C}^\perp) = p\text{-}dim\,(\mathbb{Z}_{p^r}^n((D)) = nr.$$

Proof Let $\mathcal{C} = \mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1}$ where $\mathcal{C}_i$ is a free convolutional code with rank k_i, $i = 0, 1, \ldots, r-1$ and $\mathcal{C}_0 + \mathcal{C}_1 + \ldots + \mathcal{C}_{r-1} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \ldots \oplus \mathcal{C}_{r-1}$. Consider also the free convolutional codes of length n, $B_i, i = 0, \ldots, r-1$, as defined in Theorem 5.18. Then

$$\begin{aligned} \text{rank } B_0 &= \text{rank } (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp \\ &= n - \text{rank } (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1}) \\ &= n - (k_0 + k_1 + \cdots + k_{r-1}). \end{aligned}$$

Moreover, since B_{r-i} is such that $(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^{\perp} = (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1} \oplus \mathcal{C}_i)^{\perp} \oplus B_{r-i}$ it follows from Theorem 5.12 that

$$\begin{aligned} \text{rank } B_{r-i} &= \text{rank } (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^{\perp} - (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1} \oplus \mathcal{C}_i)^{\perp} \\ &= n - (k_0 + k_1 + \cdots + k_{i-1}) - (n - (k_0 + k_1 + \cdots + k_{i-1} + k_i)) \\ &= k_i = \text{rank } \mathcal{C}_i. \end{aligned}$$

Then, from Lemma 5.8 it follows that

$$p\text{-dim}\,(p^i B_i) = (r-i)k_{r-i}$$

and

$$p\text{-dim}\,(B_0) = nr - r(k_0 + k_1, \cdots + k_{r-1}).$$

Thus,

$$\begin{aligned} p\text{-dim}\,(\mathcal{C}^{\perp}) &= p\text{-dim}\,(B_0) + p\text{-dim}\,(pB_1) + \cdots + p\text{-dim}\,(p^{r-1}B_{r-1}) \\ &= nr - r(k_0 + k_1 + \cdots + k_{r-1}) + (r-1)k_{r-1} + (r-2)k_{r-2} + \cdots + k_1 \\ &= nr - (k_0 r + k_1(r-1) + \cdots + k_{r-1}) \\ &= nr - p\text{-dim}\,(\mathcal{C}). \end{aligned}$$

□

The next example illustrates the procedure described in Theorem 5.18 to determine the dual of a convolutional code defined in $\mathbb{Z}_{p^r}(D))$.

Example 5.20. *Consider the convolutional code $\mathcal{C}$ defined in $\mathbb{Z}_9((D))$ with generator matrix*

$$G(D) = \begin{bmatrix} 1+D & 1 & 3D \\ 0 & 3+3D & 3 \end{bmatrix}.$$

Thus

$$\mathcal{C} = \mathcal{C}_0 \oplus 3\mathcal{C}_1$$

where $\mathcal{C}_0 = Im_{\mathbb{Z}_9((D))} \begin{bmatrix} 1+D & 1 & 3D \end{bmatrix}$ *and* $\mathcal{C}_1 = Im_{\mathbb{Z}_9((D))} \begin{bmatrix} 0 & 1+D & 1 \end{bmatrix}$.

Since

$$\mathcal{C}_0 \oplus \mathcal{C}_1 = Im_{\mathbb{Z}_9((D))} \begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1 \end{bmatrix}$$

we have that

$$(\mathcal{C}_0 \oplus \mathcal{C}_1)^{\perp} = Im_{\mathbb{Z}_9((D))} \left[\begin{array}{ccc} 1 & 8+5D+4D^2+6D^3 & 1+5D+D^2+3D^4 \end{array} \right].$$

Moreover,

$$\mathcal{C}_0^{\perp} = Im_{\mathbb{Z}_9((D))} \left[\begin{array}{ccc} 1 & 8+5D+4D^2+6D^3 & 1+5D+D^2+3D^4 \\ 8 & 1+D & 0 \end{array} \right]$$

and therefore $B_1 = Im_{\mathbb{Z}_9((D))} \left[\begin{array}{ccc} 8 & 1+D & 0 \end{array} \right]$ *is such that*

$$(\mathcal{C}_0 \oplus \mathcal{C}_1)^{\perp} \oplus B_1 = \mathcal{C}_0^{\perp}.$$

Consequently,

$$\mathcal{C}^{\perp} = (\mathcal{C}_0 \oplus \mathcal{C}_1)^{\perp} \oplus 3B_1$$

has generator matrix

$$\bar{G}(D) = \left[\begin{array}{ccc} 1 & 8+5D+4D^2+6D^3 & 1+5D+D^2+3D^4 \\ 6 & 3+3D & 0 \end{array} \right].$$

Chapter 6

Conclusions

In this thesis a number of problems regarding convolutional codes over the finite ring $\mathbb{Z}_{p^r}$ are studied. In particular the thesis focuses on three main problems. The first two deal with distance properties of a code (Chapters 3 and 4). The last problem investigated (in Chapter 5) involves the notion of dual codes.

Convolutional codes over finite fields have been thoroughly investigated since the fiftieths and are widely used in many communication systems. In [MM89] Massey and Mittelholzer observed for the first time that convolutional codes over the ring $\mathbb{Z}_M$, are the most appropriate class of codes for phase modulation. The algebraic structure of these codes was investigated and it was immediately apparent that these codes were much more involved than the classical convolutional codes over finite fields. Indeed many important properties that hold in the field case, fail to be true in the ring case.

Despite the fact that the distance of a code is the most important single parameter of a code, very little is known about the distance properties of these codes. In this dissertation we have focused on the two distances that are considered the most relevant in the context of convolutional codes, namely, the free distance and the column distance.

As for the free distance we extended the recent work of [EOS13] by introducing a new set of parameters of the code and we derived a novel Singleton type of bound for the free distance. In the particular case of free codes these parameters have special values and then our bound coincides with the bound given in [EOS13]. In order to show that the given upper bound is optimal we presented a constructive method for building general (non necessarily free) MDS convolutional codes over $\mathbb{Z}_{p^r}$ for any given set of parameters. Instead of considering the commonly used Hensel lift of a cyclic code, we proposed a novel type of lifting to build convolutional codes over $\mathbb{Z}_{p^r}$ from convolutional codes over a finite field. According to the coding theory literature we called this class of codes Maximum Distance Separable (MDS). In other words, this thesis has defined and proved the existence of MDS convolutional codes over $\mathbb{Z}_{p^r}$ of

length n, p-dimension k and p-degree δ, for a given n, k and δ.

In the context of convolutional codes the notion of column distance plays a central role as measures the error-correcting capabilities of the code within a given time interval. This feature is fundamental, for instance, for sequential decoding. The column distance of convolutional codes over finite fields have been pretty well investigated and there is already a large body of literature on this topic. However, column distances of convolutional codes over $\mathbb{Z}_{p^r}$ were unexplored to date. In this thesis we have addressed for the first time the notion of column distance of convolutional codes over the finite ring $\mathbb{Z}_{p^r}$. We showed that when the convolutional code is delay-free the concept of column distance is an invariant of the code and does not depend on the choice of the generator matrices representing the code. This property does not hold true for general codes. Upper bounds for the columns distances were presented. These bounds give rise to the notion of Maximum Distance Profile (MDP) codes which are codes that are optimal with respect to the column distance. The presented constructions are restricted to some sets of parameters and a general construction of *all* sets of given parameters is still unknown.

A complete study of the fundamental notions of free and column distance of convolutional codes over the finite ring $\mathbb{Z}_{p^r}$ was presented in this dissertation.

The last part of the dissertation deals with dual codes of convolutional codes defined in $\mathbb{Z}_{p^r}((D))$. In this last chapter we have considered the ring of Laurent series $\mathbb{Z}_{p^r}((D))$ instead of $\mathbb{Z}_p[D]$ due to technical reasons. For example, we showed that not all codes $\mathcal{C} \subset \mathbb{Z}_{p^r}^n[D]$ can be represented via a parity-check matrix of $\mathcal{C}$, i.e., the dual code of $\mathcal{C}$ does not exist. However, there always exists the dual code of a convolutional code defined in $\mathbb{Z}_{p^r}((D))$. Still, several technical problems due to the presence of zero divisors appear when trying to explicitly describe this dual code. We presented an explicit method to derive a representation of the dual code and moreover the method is constructive since it is based on certain associated *free* $\mathbb{Z}_{p^r}(D)$-modules.

The thesis raises several follow-up questions. For instance, the characterization of the dual of a convolutional code defined in $\mathbb{Z}_{p^r}[D]$ remains widely open. Also the proposed constructions of MDP requires large ring sizes due to the fact that they are based on a lifting of an MDP convolutional codes over $\mathbb{Z}_p[D]$ that itself requires very large finite fields. It would be interesting to come up with constructions of MDP over not too large finite rings, maybe using different type of lifting. This seems to be a highly non-trivial problem.

Another challenging direction of future research is to analyze the distance properties of the proposed codes in terms of different metrics. Two decades ago it was found out how important binary non-linear block codes (such as the binary Golay code) can be

constructed using linear codes over the ring $\mathbb{Z}_4$ by means of the Gray mapping and the Lee metric. This was a breakthrough in the area of coding theory and the study of analogous ideas in the context of this thesis is an interesting line of future research. Can we build in a similar way *good* nonlinear (binary) trellis codes (over $\mathbb{Z}_p$) from good linear convolutional codes over $\mathbb{Z}_{p^r}$?

Finally, another important avenue for future research is to develop the decoding algorithms for the classes of codes studied in this thesis. Particularly promising is the performance of these codes over the erasure channel. We expect that making use of the parity check matrix, efficient decoding algorithms can be developed. This is left as an open problem.

Index

Bibliography

[ANP13] P. Almeida, D. Napp, and R. Pinto. A new class of superregular matrices and MDP convolutional codes. *Linear Algebra and its Applications*, 439(7):2145–2157, 2013.

[AZ94] A. Ashikhmin and V. Zyablov. Samples of unit-memory codes over $\mathbb{Z}_4$. *Proc. 1994 IEEE Int. Workshop Inf. Theory, Moscow, Russia,*, pages 119–121, 1994.

[BRC60] R.C. Bose and D.K. Ray-Chaudhuri. On a Class of Error Correcting Binary Group Codes. *Information and Control*, 3:68–79, 1960.

[CCL94] C-J. Chen, T-Y. Chen, and H-A. Loeliger. Construction of linear ring codes for 6 PSK. *IEEE Trans. Inf. Th.*, 40(2):563–566, 1994.

[CG70] S. K. Chang and A. Gill. Algorithmic solution of the change-making problem. *Assoc. Comput. Mach.*, 17(1):113–122, 1970.

[CNPP12] J. Climent, D. Napp, C. Perea, and R. Pinto. A construction of MDS 2D convolutional codes of rate 1/n based on superregular matrices. *Linear Algebra and Its Applications*, 437(3):766–780, 2012.

[CNPP16] J. Climent, D. Napp, C. Perea, and R. Pinto. Maximum distance separable 2d convolutional codes. *IEEE Transactions on Information Theory*, 62(2):669–680, 2016.

[CS95] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography*, 6(1):21–35, 1995.

[Eli55] P. Elias. Coding for Noisy Channels. *IRE Conv. Record*, part 4:37–47, 1955.

[EO15] M. El Oued. On MDR codes over a finite ring. *IJICoT*, 3(2):107–119, 2015.

[EONPT] M. El Oued, D. Napp, R. Pinto, and M. Toste. The dual of convolutional codes over $\mathbb{Z}_{p^r}$. To appear as a chapter in book in Applied and Computational Matrix Analysis, Springer Verlag.

[EOS13] M. El Oued and P. Solé. MDS convolutional codes over a finite ring. *IEEE Trans. Inf. Th.*, 59(11):7305 – 7313, 2013.

[For70] G.D. Forney. Convolutional Codes I: Algebraic Structure. *IEEE Trans. Inform. Theory*, 16:720–738, 1970. Correction, Ibid., IT-17,pp. 360, 1971.

[FZ97] F. Fagnani and S. Zampieri. Canonical kernel representations for behaviors over finite abelian groups. *Systems and control letters*, 32(5):271–282, 1997.

[FZ01] F. Fagnani and S. Zampieri. System-theoretic properties of convolutional codes over rings. *IEEE Trans. Information Theory*, 47(6):2256–2274, 2001.

[GG12] K. Guendaa and T. A. Gulliver. MDS and self-dual codes over rings. *Finite Fields and Their Applications*, 18(6):1061–1075, 2012.

[Gua14] G. G. La Guardia. On classical and quantum MDS-convolutional bch codes. *IEEE Trans. Information Theory*, 60(1):304–312, 2014.

[Ham50] R.W. Hamming. Error Detecting and Error Correcting Codes. *Bell System Technical Journal*, 29:147–160, 1950.

[HGLS06] J. Rosenthal H. Gluesing-Luerssen and R. Smarandache. Strongly MDS convolutional codes. *IEEE Trans. Inform. Theory*, 52:584–598, 2006.

[Hoc59] A. Hocquenghem. Codes Correcteurs d'Errors. *Chiffres (Paris)*, 2:147–156, 1959.

[HP98] C. Huffman and V. Pless. *Handbook of Coding Theory, volumes 1,2*. Elsevier Sciences, North-Holland, 1998.

[HST08] R. Hutchinson, R. Smarandache, and J. Trumpf. On superregular matrices and MDP convolutional codes. *Linear Algebra and its Applications*, 428(11–12):2585–2596, 2008.

[Hut08] R. Hutchinson. The existence of strongly MDS convolutional codes. *SIAM Journal on Control and Optimization*, 47(6):2812–2826, 2008.

[JW98] R. Johannesson and E. Wittenmark. Two 16-state, rate r=2/4 trellis codes whose free distances meet the heller bound. *IEEE Trans. Information Theory*, 44(4):1602–1604, 1998.

[JWW98] R. Johannesson, Z.X. Wan, and E. Wittenmark. Some structural properties of convolutional codes over rings. *IEEE Trans. Inform. Theory*, 44(2):839–845, 1998.

[JZ99] R. Johannesson and K. Sh. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press, New York, 1999.

[KDS95] R. Kötter, U. Dettmar, and U. K. Sorger. On the construction of trellis codes based on (P)UM codes over $\mathbb{Z}_4$. *Problems Inform. Transmission*, 31(2):154–161, 1995.

[KP09] M. Kuijper and R. Pinto. On minimality of convolutional ring encoders. *IEEE Trans. Automat. Contr.*, 55)(11):4890 –4897, 2009.

[KPP07] M. Kuijper, R. Pinto, and J. W. Polderman. The predictable degree property and row reducedness for systems over a finite ring. *Linear Algebra and its Applications*, 425(2–3):776–796, 2007.

[LC83] S. Lin and D.J. Costello. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, Inc, Englewood Cliffs, New Jersey, 1983.

[Mas63] J.L. Massey. *Threshold Decoding*. MIT Press, Cambridge, Mass., 1963.

[McD74] B.R. McDonald. *Finite rings with identity*. Marcel Dekker, New York, 1974.

[McE98] R. J. McEliece. The algebraic theory of convolutional codes. In V. Pless and W.C. Huffman, editors, *Handbook of Coding Theory*, volume 1, pages 1065–1138. Elsevier Science Publishers, Amsterdam, The Netherlands, 1998.

[MM89] J. L. Massey and T. Mittelholzer. Convolutional codes over rings. *In Proc. 4th Joint Swedish-Soviet Int. Workshop Information Theory*, pages 14–18, 1989.

[MS77] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier Science, North-Holland, 1977.

[Nor99] G. Norton. On minimal realization over a finite chain ring. *Designs, Codes and Cryptography*, 16(2):161–178, 1999.

[NPT16] D. Napp, R. Pinto, and M. Toste. On mds convolutional codes over $\mathbb{Z}_{p^r}$. *Designs, Codes and Cryptography*, pages 1–14, 2016.

[NR16] D. Napp and R.Smarandache. Constructing strongly-mds convolutional codes with maximum distance profile. *Adv. in Math. of Comm.*, 10(2):275–290, 2016.

[NS00] G. Norton and A. Salagean. On the key equation over a commutative ring. *Designs, Codes and Cryptography*, 20(2):125–141, 2000.

[NS01] G. Norton and A. Salagean. On the hamming distance of linear codes over a finite chain ring. *IEEE Trans. Information Theory*, 46(3):1060–1067, 2001.

[Pir88] P. Piret. *Convolutional Codes: an Algebraic Approach*. Cambridge, Mass.: MIT Press, 1988.

[RHS05] J. Rosenthal R. Hutchinson and R. Smarandache. Convolutional codes with maximum distance profile. *Systems & Control Letters*, 54(1):53–63, 2005.

[RL89] R. M. Roth and A. Lempel. On MDS codes via cauchy matrices. *IEEE Trans. Inf. Th.*, 35(6):1314–1319, 1989.

[RS60] I.S. Reed and G. Solomon. Polynomial Codes over Certain Finite Fields. *J. SIAM*, 8:300–304, 1960.

[RS85] R. M. Roth and G. Seroussi. On generator matrices of MDS codes. *IEEE Trans. Inf. Th.*, 31(6):826–830, 1985.

[RS99] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput.*, 10(1):15–32, 1999.

[SGLR01] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions for MDS-convolutional codes. *IEEE Trans. Automat. Control*, 47(5):2045–2049, 2001.

[SS07] P. Solé and V. Sison. Quaternary convolutional codes from linear block codes over galois rings. *IEEE Trans. Information Theory*, 53:2267–2270, 2007.

[TRS12] V. Tomás, J. Rosenthal, and R. Smarandache. Decoding of convolutional codes over the erasure channel. *IEEE Transactions on Information Theory*, 58(1):90–108, 2012.

[Vit67] A.J. Viterbi. Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm. *IEEE Trans. Inform. Theory*, 13:260–269, 1967.

[vL99] J.H. van Lint. *Introduction to Coding Theory*. Springer-Verlag, Berlin, 1999.

[VSA96] V.V. Vazirani, H. Saran, and B.S. Rajan. A. An efficient algorithm for constructing minimal trellises for codes over finite abelian groups. *IEEE Trans. Inf. Th*, 42:1839–1854, 1996.

[VTS09] J. Rosenthal V. Tomás and R. Smarandache. Decoding of MDP convolutional codes over the erasure channel. In *Proceedings of the 2009 IEEE International Symposium on Information Theory (ISIT 2009)*, pages 556–560, Seoul, Korea, June 2009.

[Woz57] J.M. Wozencraft. Sequential Decoding for Reliable Communication. *IRE Nat. Conv. Rec.*, 5, pt. 2:11–25, 1957.