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

Diego Napp Raquel Pinto Marisa Toste

Abstract

Maximum Distance Profile codes over finite non-binary fields have been introduced and thoroughly studied in the last decade. These codes have the property that their column distances are maximal among all codes of the same rate and degree. In this paper we aim at studying this fundamental concept in the context of convolutional codes over a finite ring. We extensively use the concept of p-encoder to establish the theoretical framework and derive several bounds on the column distances. In particular, a method for constructing (not necessarily free) Maximum Distance Profile convolutional codes over $\mathbb{Z}_{p^r}$ is presented.

I. Introduction

Massey and Mittelholzer [19] showed that the most appropriate codes for phase modulation are the linear codes over the residue class ring $\mathbb{Z}_M$ and this class includes the convolutional codes over $\mathbb{Z}_M$, where M is a positive integer. Fundamental results of the structural properties of convolutional codes over finite rings can be found, for instance, in [7] and [12]. Fagnani and Zampieri [7] studied the theory of convolutional codes over the ring $\mathbb{Z}_{p^r}$ in the case when the input sequence space is a free module. The problem of deriving minimal encoders (left prime and row-reduced) was posed by Solé *et al.* in [26] and solved by Kuijper *et al.* in [16] and [17] using the concept of minimal p-encoder, which is an extension of the concept of p-basis introduced in [29] to the polynomial context.

The search for and design of good convolutional codes over $\mathbb{Z}_{p^r}$ have been investigated in several works in literature. Unit-memory convolutional codes over $\mathbb{Z}_4$ that give rise to binary trellis codes with high free distances together with several concrete constructions of these codes were reported in [2] and [15]. In [13] two 16-state trellis codes of rate $2/4$, again over $\mathbb{Z}_4$, were found by computer search. Also worth

This work was supported by Portuguese funds through the CIDMA – Center for Research and Development in Mathematics and Applications, and the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia), within project PEst-UID/MAT/04106/2013.

Diego Napp and Raquel Pinto and Marisa Toste are with CIDMA – Center for Research and Development in Mathematics and Applications. Department of Mathematics. University of Aveiro. Portugal diego@ua.pt and raquel@ua.pt

Marisa Toste is with Superior School of Technologies and Management of Oliveira do Hospital, Polytechnic Institute of Coimbra, Coimbra, Portugal marisa.toste@estgoh.ipc.pt

mentioning is the paper of [26] where convolutional codes achieving the Gilbert-Varshamov bound were presented. However, in contrast to block codes, as in the case of [10] and [23], little is known about distance properties and constructions of convolutional codes over large rings.

Recently, in [24], a bound on the free distance of convolutional codes over $\mathbb{Z}_{p^r}$ was derived, generalizing the bound given in [25] for convolutional codes over finite fields. Codes achieving such a bound were called Maximal Distance Separable (or MDS). The concrete constructions of MDS convolutional codes over $\mathbb{Z}_{p^r}$ presented in [24] were restricted to *free* codes and general constructions were built in [21].

Column distances of convolutional codes over finite fields have been already studied for decades [14]. However, the concept of Maximum Distance Profile (MDP) convolutional codes over (non-binary) finite fields have been defined and fully studied by Rosenthal *et al.* in [9], [11] and [27]. These codes are characterized by the property that their column distances are optimal. Fast growth of the column distances is an important property for codes to be used with sequential decoding since they have the potential to correct a maximal number of errors per time interval. For this reason these codes are very appealing for streaming applications (see [27]). Despite the importance of the notion, column distances of convolutional code over a finite ring are yet unexplored.

In this paper we aim at investigating this concept. In particular, we derive upper-bounds on the column distances and provide explicit novel constructions of (not necessarily free) MDP convolutional codes over $\mathbb{Z}_{p^r}$. We note that the ring size required to build this class of convolutional codes is in general large. 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. As for the construction of MDP, in contrast with the papers [23] and [24] where the Hensel lift of a cyclic code was used, in this paper a direct lifting is employed to build MDP convolutional codes over $\mathbb{Z}_{p^r}$ from known constructions of MDP convolutional codes over $\mathbb{Z}_p$. Note that by the Chinese Remainder Theorem, results on codes over $\mathbb{Z}_{p^r}$ can be extended to codes over $\mathbb{Z}_M$, see also [12] and [20].

The paper is organized as follows: In the next section we introduce some preliminaries on p-basis of $\mathbb{Z}_{p^r}[D]$-submodules of $\mathbb{Z}_{p^r}^n[D]$. After presenting block codes over $\mathbb{Z}_{p^r}$ we introduce the new concepts of p-standard form and r-optimal parameters. We conclude the preliminaries by defining convolutional codes over $\mathbb{Z}_{p^r}$. In section III we define and study column distances of convolutional codes over $\mathbb{Z}_{p^r}$. Finally, in Section IV we propose a method to build MDP convolutional codes over $\mathbb{Z}_{p^r}$. The most technical proofs of our results are in Section V.

II. Preliminaries

This section presents the necessary background to derive the main results of the paper. Some of these are known in the literature and others are new.

A. P-basis and p-dimension

Let p be a prime integer. Any element 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 $\mathcal{A}_p = \{0, 1, \ldots, p-1\}$ (called the p-adic expansion of the element) [3]. Note that all elements of $\mathcal{A}_p \backslash \{0\}$ are units. Let us denote by $\mathbb{Z}_{p^r}[D]$ ($\mathcal{A}_p[D]$) the ring (set) of polynomials over $\mathbb{Z}_{p^r}$ ($\mathcal{A}_p$) in the indeterminate D. In [29], p-basis for $\mathbb{Z}_{p^r}$-submodules of $\mathbb{Z}_{p^r}^n$ were first presented and later were extended for the module $\mathbb{Z}_{p^r}^n[D]$ in [17]. These notions will play an important role throughout the paper since they will allow us to analyse the distance properties of convolutional codes over $\mathbb{Z}_{p^r}$.

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 $(v_1(D), \ldots, v_k(D))$. 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 $v_{i+1}(D), \ldots, v_k(D)$, $\quad i = 1, \ldots, k-1$, and $p\, v_k(D) = 0$.

If $(v_1(D), \ldots, v_k(D))$ is a p-generator sequence, p-span$(v_1(D), \ldots, v_k(D))$ = span$(v_1(D), \ldots, v_k(D))$ [17] and consequently the p-span$(v_1(D), \ldots, v_k(D))$ is a $\mathbb{Z}_{p^r}$-submodule of $\mathbb{Z}_{p^r}^n[D]$. Moreover, note that if $M =$ span$(v_1(D), \ldots, v_k(D))$,

$$(v_1(D), pv_1(D) \ldots, p^{r-1}v_1(D), v_2(D), pv_2(D), \ldots, p^{r-1}v_2(D), \ldots, v_k(D), pv_k(D) \ldots, p^{r-1}v_k(D)) \tag{1}$$

is a p-generator sequence of M.

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.

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 [16] 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. This number of elements is called ***p*-dimension** of M.

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 of the rows of $G(D)$. A p-basis $(v_1(D), \ldots, v_k(D))$ is called a **reduced *p*-basis** if the vectors $v_1^{lc}, \ldots, v_k^{lc}$ are p-linearly independent in $\mathbb{Z}_{p^r}$.

Every submodule M of $\mathbb{Z}_{p^r}^n[D]$ has a reduced p-basis. Algorithm 3.11 in [17] constructs a reduced p-basis for a submodule M from a generator sequence of M. The degrees of the vectors of two reduced p-bases of M are the same (up to permutation) and their sum is called the ***p*-degree** of M.

B. Block codes over a finite ring

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

$$\mathcal{C} = \mathrm{Im}_{\mathcal{A}_p} G = \{v = uG \in \mathbb{Z}_{p^r}^n \ : u \in \mathcal{A}_p^k\}.$$

Note that we use $\tilde{k}$ and k for the number of rows of a generator matrix $\widetilde{G}$ and a p-encoder G respectively. Every block code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ admits (see [23, Theorem 3.3.]) a generator matrix $\widetilde{G}$ in **standard form**, i.e., in the form

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

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

Given a p-basis $(v_1, \ldots, v_k)$ of $\mathcal{C}$ there are certain operations that can be applied to $(v_1, \ldots, v_k)$ so that we obtain another p-basis of $\mathcal{C}$. Some of these elementary operations are described in the following lemma which is not difficult to prove, see more details in [28].

Lemma 1. *Let $(v_1, \ldots, v_k)$ be a p-basis of a submodule M of $\mathbb{Z}_{p^r}^n$. Then,*

1) *If $v_i' = v_i + \sum_{j=i+1}^{k} a_j v_j$, with $a_j \in \mathcal{A}_{p^r}$, then $(v_1, \ldots, v_{i-1}, v_i', v_{i+1}, \ldots, v_k)$ is a p-basis of M.*
2) *If pv_i is a p-linear combination of $v_j, v_{j+1}, \ldots, v_k$, for some $j > i$, then $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_{j-1}, v_i, v_j, \ldots, v_k)$ is a p-basis of M.*

Performing the operations described in the previous lemma it is easy to verify that we can transform a

generator matrix $\widetilde{G}$ of $\mathcal{C}$ in standard form into *a* p-encoder G in the following form:

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

One can verify that the scalars k_i, $i = 0, 1, \ldots, r-1$, are equal for all p-encoders of $\mathcal{C}$ in this form, *i.e.*, they are uniquely determined for a given code $\mathcal{C} \subset \mathbb{Z}_{p^r}^n$ and coincide with the parameters appearing in (2) for generator matrices in standard form. We call $k_0, k_1, \ldots, k_{r-1}$ the **parameters** of $\mathcal{C}$. If G is in such a form we say that G is in the ***p*-standard form**. The p-standard form will be a useful tool to prove our results in the same way the standard form was for previous results in the literature, see for instance [3] and [23]. It is easy to see that if $\mathcal{C}$ has p-dimension k then $k = \sum_{i=0}^{r-1} k_i(r-i)$.

The **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 (or of a generator matrix in standard form) in p-standard form is obviously a codeword we can easily recover the Singleton-type upper bound on the free distance of a block code over $\mathbb{Z}_{p^r}$ derived in [23].

Theorem 2. *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 introduce the notion of an optimal set of parameters of k [28].

Definition 3. *Given an integer $r \geq 1$ and a non-negative integer k we call an ordered set $(k_0, k_1, \cdots, k_{r-1})$, $k_i \in \mathbb{N}_0,\ i = 0, \cdots, r-1$ an* **r-optimal set of parameters** *of k if*

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

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 general, 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 [4].

Lemma 4. *[21] Let $(k_0, k_1, \cdots, k_{r-1})$ be an r-optimal set of parameters of k. Then,*

$$k_0 + k_1 + \cdots + k_{r-1} = \left\lceil \frac{k}{r} \right\rceil.$$

Hence, for a given $\mathcal{C} \subset \mathbb{Z}_{p^r}^n$ with p-dimension k, a Singleton bound can be defined.

Corollary 5. *Given a block code $\mathcal{C} \subset \mathbb{Z}_{p^r}^n$ and p-dimension k,*

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

This bound also follows from the fact that, for any block code (not necessarily linear) we have that $|\mathcal{C}| \leq (p^r)^{n - d(\mathcal{C}) + 1}$, see [23], and it can also be found in [24].

C. Convolutional codes over a finite ring

Next we introduce the class of convolutional codes considered in this work together with some properties of p-encoders, namely, catastrophicity, delay-freness and minimality. Minimal p-encoders allow us to define the p-indices and the p-degree of a convolutional code which are natural extensions of the notions of Forney indices and degree in the context of finite fields.

We will consider convolutional codes constituted by left compact sequences in $\mathbb{Z}_{p^r}$, that is, in which the elements 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 functions over $\mathbb{Z}_{p^r}$ in the indeterminate D. More precisely, $\mathbb{Z}_{p^r}(D)$ is the set

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

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

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

Note that $\mathbb{Z}_{p^r}(D)$ is a subring of of the ring of Laurent series $\mathbb{Z}_{p^r}((D))$ 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 $L(D)A(D) = I$. Moreover, $A(D)$ is invertible if and only if $\bar{A}(D)$ is invertible in $\mathbb{Z}_p^{\ell\times\ell}(D)$, where $\bar{A}(D)$ represents the projection of $A(D)$ into $\mathbb{Z}_p(D)$ [7].

Most of the literature on convolutional codes over rings considers codewords as elements in the ring of Laurent series [6], [8], [12], [16], [18], [24]. We shall adopt this approach and define a **convolutional code** $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ of length n as 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

$$\mathcal{C} \;=\; \mathrm{Im}_{\mathbb{Z}_{p^r}((D))}\widetilde{G}(D) = \left\{u(D)\widetilde{G}(D) \in \mathbb{Z}_{p^r}^n((D)) :\; u(D) \in \mathbb{Z}_p^{\tilde{k}}((D))\right\}.$$

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

$$\mathcal{C} \;=\; \mathrm{Im}_{\mathcal{A}_p((D))}G(D) = \left\{u(D)G(D) \in \mathbb{Z}_{p^r}^n((D)) :\; u(D) \in \mathcal{A}_p^k((D))\right\},$$

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

Remark 6. *We emphasize that in this paper we do not assume that $\mathcal{C}$ is free. Hence, it is important to underline that there exists convolutional codes that do not admit an encoder. However, they always admit a p-encoder. For this reason the concept of p-encoder is more interesting and natural than the standard concept of the encoder. The difference is that the input vector takes values in $\mathcal{A}_p^k((D))$ for p-encoders whereas for generator matrices it takes values in $\mathbb{Z}_p^{\tilde{k}}((D))$. This idea of using a p-adic expansion for the*

information input vector is already present in, for instance, [3] and was further developed in [29] introducing p-generator sequences of vectors in $\mathbb{Z}_{p^r}$. In [16] and [17] this idea was extended to polynomial vectors.

Next lemma is straightforward and states that a convolutional code can be equivalently defined as the image of a rational matrix.

Lemma 7. *[5] Let $\mathcal{C} = \mathrm{Im}_{\mathbb{Z}_{p^r}((D))} N(D)$, where $N(D) \in \mathbb{Z}_{p^r}^{\widetilde{k}\times n}(D)$. Then $\mathcal{C}$ is a convolutional code, and if $N(D)$ is full row rank, $\mathcal{C}$ is a free code of rank $\widetilde{k}$.*

A generator matrix $\widetilde{G}(D) \in \mathbb{Z}_{p^r}^{\widetilde{k}\times n}[D]$ is said to be **noncatastrophic** ([16]) if for any $u(D) \in \mathbb{Z}_{p^r}^{\widetilde{k}}((D))$,

$$u(D)\widetilde{G}(D) \in \mathbb{Z}_{p^r}^{n}[D] \implies u(D) \in \mathbb{Z}_{p^r}^{\widetilde{k}}[D].$$

Note that this property is a characteristic of a generator matrix and not a property of the code. For example in $\mathbb{Z}_4$, $G_1(D) = [1+D \;\; 1+D]$ and $G_2(D) = [1 \;\; 1]$ are two encoders of the same convolutional code, but $G_2(D)$ is noncatastrophic and $G_1(D)$ is catastrophic. However, there are convolutional codes that do not admit noncatastrophic generator matrices like illustrated in the following example [16].

Example 8. *The convolutional code over $\mathbb{Z}_4$ with encoder $\widetilde{G}(D) = [1+D \;\; 1+3D]$ does not admit a noncatastrophic encoder.*

It is clear that a generator matrix that is not full row rank is catastrophic and therefore convolutional codes that are not free do not admit noncatastrophic encoders.
Analogously, we say that a p-encoder $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ is said to be noncatastrophic [16] if for any $u(D) \in \mathcal{A}_p^k((D))$,

$$u(D)G(D) \in \mathbb{Z}_{p^r}^{n}[D] \implies u(D) \in \mathcal{A}_p^k[D].$$

If a convolutional code $\mathcal{C}$ admits a noncatastrophic encoder $\widetilde{G}(D) \in \mathbb{Z}_{p^r}^{\widetilde{k}\times n}[D]$ then, obviously, it also admits a noncatastrophic p-encoder, namely

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

However, there are convolutional codes that do not admit noncatastrophic encoders but admit noncatastrophic p-encoders like it is shown in the next example [16].

Example 9. *Let us consider again the convolutional code $\mathcal{C}$ over $\mathbb{Z}_4$ of Example 8. The p-encoder*

$$G(D) = \begin{bmatrix} 1+D & 1+3D \\ 2 & 2 \end{bmatrix}$$

of $\mathcal{C}$ is noncatastrophic.

We call a convolutional code that admits a noncatastrophic p-encoder a **noncatastrophic** convolutional code. Thus, the class of noncatastrophic convolutional codes contain the class of convolutional codes that admit a noncatastrophic encoder. In [16] it was conjectured that all the convolutional codes admit a noncatastrophic p-encoder and this is still an open problem.

Another property of p-encoders that is relevant for this work is "*delay-freeness*". We say that a p-encoder $G(D)$ of a convolutional code $\mathcal{C}$ is **delay-free** if for any $u(D) \in \mathcal{A}_p^k((D))$ and any $N \in \mathbb{Z}$

$$\text{supp } (u(D)G(D)) \subset [N, +\infty) \implies \text{supp } (u(D)) \subset [N, +\infty),$$

where supp $(v(D))$ denotes the support of $v(D) = \sum v_i D^i$, *i.e.,* supp $(v(D)) = \{i : v_i \neq 0\}$.

Lemma 10. *[16] Let $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ be a p-encoder. Then $G(D)$ is delay-free if and only if the rows of $G(0)$ are p-linearly independent in $\mathbb{Z}_{p^r}^n$.*

All convolutional codes admit a delay-free p-encoder. Moreover, if $\mathcal{C}$ is a noncatastrophic convolutional code, then it admits a delay-free and noncatastrophic p-encoder which rows form a reduced p-basis [16]. Let $\mathcal{C}$ be a noncatastrophic convolutional code of length n over $\mathbb{Z}_{p^r}$ and let $G(D)$ be a delay-free noncatastrophic p-encoder of $\mathcal{C}$, such that its rows form a reduced p-basis. Then $G(D)$ is called a **minimal p-encoder** of $\mathcal{C}$. The degrees of the rows of $G(D)$ are called the **p-indices** of $\mathcal{C}$ and the **p-degree** of $\mathcal{C}$ is defined as the sum of the p-indices of $\mathcal{C}$. Moreover, if $\mathcal{C}$ has p-dimension k and p-degree δ, $\mathcal{C}$ is called an (n, k, δ)-convolutional code.

III. Column distance of convolutional codes over a finite ring

In this section we analyse two fundamental distance properties, namely, free distance and column distance. Once we recall the definition of free distance [21] and [24], we introduce, for the first time, the concept of column distance of convolutional codes over $\mathbb{Z}_{p^r}$. We also derive an upper-bound on these distances which leads to the notion of Maximum Distance Profile convolutional code. The **weight** of $v(D) = \sum_{i\in\mathbb{Z}} v_i D^i \in \mathbb{Z}_{p^r}((D))$ is given by $\text{wt}(v(D)) = \sum_{i\in\mathbb{Z}} \text{wt}(v_i)$ and the **free distance** of a convolutional code $\mathcal{C}$ is defined as

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

Theorem 11. *[24, Theorem 4.10] The free distance of an (n,k,δ) convolutional code $\mathcal{C}$ satisfies*

$$d(\mathcal{C}) \leq n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k}{r}\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \frac{\delta}{r} \right\rceil + 1. \tag{4}$$

Similarly to the field case, the bound (4) is called the **generalized Singleton bound**. As for column distance [14] we define

$$v(D)|_{[i,i+j]} = v_i D^i + v_{i+1} D^{i+1} + \cdots + v_{i+j} D^{i+j}$$

and analogously for $u(D)|_{[i,i+j]}$ for $u(D) = \sum_{\ell \in \mathbb{Z}} u_\ell D^\ell \in \mathcal{A}_p^k((D))$. The j-th **column distance** of a p-encoder $G(D)$ is defined as

$$\begin{aligned} d_j^c(G(D)) &= \min\{\mathrm{wt}(v(D)|_{[i,i+j]}) : v(D) = u(D)G(D),\, u_i \neq 0 \text{ and } u_\ell = 0 \text{ for } \ell < i\} \\ &= \min\{\mathrm{wt}(v(D)|_{[0,j]}) : v(D) = u(D)G(D),\, u_0 \neq 0 \text{ and } u_i = 0 \text{ for } i < 0\}. \end{aligned}$$

This is a property of the p-encoder and different p-encoders can have different column distances. However, the column distances are invariant under the class of delay-free p-encoders of a code and they are equal to

$$d_j^c(G(D)) = \min\{\mathrm{wt}(v(D)|_{[i_{\min}, i_{\min}+j]}) : v(D) \in \mathcal{C}\},$$

where $v(D) = \sum_{\ell \geq i_{\min}} v_\ell D^\ell \in \mathbb{Z}_{p^r}^n((D))$ with $v_{i_{\min}} \neq 0$, for $j \in \mathbb{N}_0$. As every (n,k,δ)-convolutional code $\mathcal{C}$ admits a delay-free p-encoder, we shall define the j-th **column distance** of $\mathcal{C}$, denoted by $d_j^c(\mathcal{C})$, as the column distance of one (and therefore all) of its delay-free p-encoders. If no confusion arises we use d_j^c for $d_j^c(\mathcal{C})$. It is obvious that $d_j^c \leq d_{j+1}^c$ for $j \in \mathbb{N}_0$.

Next definition extends the well-known truncated sliding generator matrix of a convolutional code over a finite field [9] to convolutional codes over finite rings ($\mathbb{Z}_{p^r}$ in our case).

Given a p-encoder $G(D) = G_0 + G_1 D + \cdots + G_\nu D^\nu \in \mathbb{Z}_{p^r}^{k\times n}[D]$, 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 $G_\ell = 0$ whenever $\ell > \nu$. In terms of the truncated sliding generator matrix the column distance reads as follows: Given a delay-free p-encoder $G(D)$ of a convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$, the j-th

column distance of $\mathcal{C}$ is given by

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

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

Next, we present a result that allows to decompose a convolutional code over $\mathbb{Z}_{p^r}$ into simpler components.

Theorem 12. *Every convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ admits a generator matrix of the form*

$$\widetilde{G}(D) = \begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\widetilde{\mathcal{G}}_1(D) \\ \vdots \\ p^{r-1}\widetilde{\mathcal{G}}_{r-1}(D) \end{bmatrix}, \tag{5}$$

and such that

$$\widehat{G}(D) = \begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ \widetilde{\mathcal{G}}_1(D) \\ \vdots \\ \widetilde{\mathcal{G}}_{r-1}(D) \end{bmatrix} \tag{6}$$

is full row rank. Thus, $\mathcal{C}_i := \mathrm{Im}_{\mathbb{Z}_{p^r}((D))}\, \widetilde{\mathcal{G}}_i(D)$ is a free convolutional code, for $i = 0, 1, \dots, r-1$, and

$$\mathcal{C} = \mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \cdots \oplus p^{r-1}\mathcal{C}_{r-1}. \tag{7}$$

Proof: 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

$$F_0(D)\overline{\widetilde{G}}(D) = \begin{bmatrix} \mathcal{G}_0(D) \\ 0 \end{bmatrix} \mod\ p,$$

where $\mathcal{G}_0(D)$ is full row rank with rank ℓ_0. Further, it follows that

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

where $\widetilde{\mathcal{G}}_0(D) \in \mathbb{Z}_{p^r}^{\ell_0\times n}[D]$ is such that $\overline{\widetilde{\mathcal{G}}_0}(D) = \mathcal{G}_0(D)$ and $\widehat{\mathcal{G}}_1(D) \in \mathbb{Z}_{p^r}^{(k-\ell_0)\times n}[D]$. Moreover, since

$F_0(D)$ is invertible, it follows that

$$\text{Im}_{\mathbb{Z}_{p^r}((D))}\widetilde{G}(D) = \text{Im}_{\mathbb{Z}_{p^r}((D))}\begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\widehat{\mathcal{G}}_1(D) \end{bmatrix}$$

and therefore $\begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\widehat{\mathcal{G}}_1(D) \end{bmatrix}$ is also a generator matrix of $\mathcal{C}$. Let us now consider $F_1(D) \in \mathbb{Z}_p^{(k-\ell_0)\times(k-\ell_0)}[D]$ such that

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

where $\mathcal{G}'_1(D)$ is full row rank with rank $\tilde{\ell}_1$ and

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

with $\mathcal{G}''_1(D) \in \mathbb{Z}_{p^r}^{\widetilde{\ell}_1\times n}[D]$ such that $\overline{\mathcal{G}''_1}(D) = \mathcal{G}'_1(D)$ and $\widehat{\mathcal{G}}_2(D) \in \mathbb{Z}_{p^r}^{(k-\ell_0-\widetilde{\ell}_1)\times n}[D]$. Hence,

$$\begin{bmatrix} I_{\ell_0} & 0 \\ 0 & F_1(D) \end{bmatrix} F_0(D)\widetilde{G}(D) = \begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\mathcal{G}''_1(D) \\ p^2\widehat{\mathcal{G}}_2(D) \end{bmatrix}.$$

If $\begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ \mathcal{G}''_1(D) \end{bmatrix}$ is not full row rank, then there exists a permutation matrix P and a rational matrix $L_1(D) \in \mathbb{Z}_{p^r}^{\widetilde{\ell}_1\times\ell_0}(D)$ such that

$$P\begin{bmatrix} I_{\ell_0} & 0 \\ L_1(D) & I_{\widetilde{\ell}_1} \end{bmatrix}\begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\mathcal{G}''_1(D) \end{bmatrix} = \begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\mathcal{G}'''_1(D) \\ p^2\mathcal{G}'_2(D) \end{bmatrix},$$

where $\mathcal{G}'''_1(D) \in \mathbb{Z}_{p^r}^{\ell_1\times n}(D)$ and $\mathcal{G}'_2(D) \in \mathbb{Z}_{p^r}^{(\widetilde{\ell}_1-\ell_1)\times n}(D)$ are rational matrices and $\begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ \mathcal{G}'''_1(D) \end{bmatrix}$ is a full row rank rational matrix. Since $P\begin{bmatrix} I_{\ell_0} & 0 \\ L_1(D) & I_{\widetilde{\ell}_1} \end{bmatrix}$ is nonsingular we also have that

$$\text{Im}_{\mathbb{Z}_{p^r}((D))}\begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\mathcal{G}''_1(D) \end{bmatrix} = \text{Im}_{\mathbb{Z}_{p^r}((D))}\begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\mathcal{G}'''_1(D) \\ p^2\mathcal{G}'_2(D) \end{bmatrix}.$$

Let $\widetilde{\mathcal{G}}_1(D) \in \mathbb{Z}_{p^r}^{\ell_1 \times n}[D]$ and $\mathcal{G}_2''(D) \in \mathbb{Z}_{p^r}^{(\widetilde{\ell}_1 - \ell_1) \times n}[D]$ be polynomial matrices (see Lemma 7) such that

$$\mathrm{Im}_{\mathbb{Z}_{p^r}((D))} \begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\mathcal{G}_1'''(D) \\ p^2\mathcal{G}_2'(D) \end{bmatrix} = \mathrm{Im}_{\mathbb{Z}_{p^r}((D))} \begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\widetilde{\mathcal{G}}_1(D) \\ p^2\mathcal{G}_2''(D) \end{bmatrix}.$$

Then $\begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\widetilde{\mathcal{G}}_1(D) \\ p^2\mathcal{G}_2''(D) \\ p^2\widehat{\mathcal{G}}_2(D) \end{bmatrix}$ is still a generator matrix of $\mathcal{C}$ such that $\begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ \widetilde{\mathcal{G}}_1(D) \end{bmatrix}$ is full row rank.
Proceeding in the same way we conclude the proof. ■

Remark 13. *The decomposition (7) could have been derived using the fact that $\mathbb{Z}_{p^r}^n((D))$ is a semi-simple module. Note, however, that Theorem 12 is constructive and its proof provides an algorithm to build the free modules $\mathcal{C}_i$. Moreover, it states that these submodules of $\mathbb{Z}_{p^r}^n((D))$ are indeed convolutional codes. Note that submodules of $\mathbb{Z}_{p^r}^n((D))$ do not always admit a polynomial or rational set of generators and therefore they are not necessarily convolutional codes.*

If we denote by ℓ_i the rank of $\mathcal{C}_i$ then $\{\ell_0, \ldots, \ell_{r-1}\}$ are clearly invariants of $\mathcal{C}$. We will call them the **parameters of the convolutional code** $\mathcal{C}$.
From now on, in order to simplify the exposition, we assume that the generator matrix $\widetilde{G}(D)$ is as in (5) and such that $\widehat{G}(D)$ in (6) is such that $\widehat{G}(0)$ is full row rank. Hence, we can directly obtain a delay-free p-encoder by extending $\widehat{G}(D)$ as

$$G(D) = \begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\,\widetilde{\mathcal{G}}_0(D) \\ p\,\widetilde{\mathcal{G}}_1(D) \\ p^2\,\widetilde{\mathcal{G}}_0(D) \\ p^2\,\widetilde{\mathcal{G}}_1(D) \\ p^2\widetilde{\mathcal{G}}_2(D) \\ \vdots \\ p^{r-1}\,\widetilde{\mathcal{G}}_0(D) \\ \vdots \\ p^{r-1}\widetilde{\mathcal{G}}_{r-1}(D) \end{bmatrix} = \sum_{i \in \mathbb{N}_0} G_i D^i.$$

As the rows of $G(0) = G_0$ form a p-basis (over $\mathbb{Z}_{p^r}$) then the parameters of the block code

$\mathcal{C}_0 = \mathrm{Im}_{\mathcal{A}_p} G(0)$ coincide with the parameters of $\mathcal{C}$. Before establishing upper bounds on the column distances of a convolutional code we present a useful result on the truncated sliding matrix G_j^c of $G(D)$.

Proposition 14. *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: See appendix. ■

Theorem 15. *Let $\mathcal{C}$ be a (n, k, δ)-convolutional code with parameters $k_0, k_1, \ldots, k_{r-1}$. Then, it holds that*

$$d_j^c \leq (j+1)\left(n - \sum_{i=0}^{r-1} k_i\right) + 1.$$

Proof: See appendix. ■

Column distances are very appealing for sequential decoding: the larger the column distances the larger number of errors we can correct per time interval. Hence we seek for codes with optimal column distances. Selecting an r-optimal set of parameters of a given p-dimension k, $(k_0, k_1, \ldots, k_{r-1})$, the following corollary readily follows from Lemma 4.

Corollary 16. *Given a convolutional code $\mathcal{C}$ with length n and p-dim$(\mathcal{C}) = k$ it holds*

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

Let us denote the bound obtained in Corollary 16 for the column distance by

$$B(j) = \left(n - \left\lceil \frac{k}{r} \right\rceil\right)(j+1) + 1$$

and the Singleton bound obtained in Theorem 11 for the free distance by

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

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

Now we are in position to introduce maximum distance profile convolutional codes over a finite ring. These codes generalize the notion introduced in [9] for maximum distance profile convolutional codes over finite fields to the ring case.

Definition 17. *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* $L = max\{j : B(j) \leq SB\}$.

A simple counting argument leads to the following result which determines the value of such an L.

Theorem 18. *Let* $\mathcal{C}$ *be an MDP* (n, k, δ)*-convolutional code over* $\mathbb{Z}_{p^r}$ *and*

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

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* $L = \lfloor X \rfloor$.

IV. Constructions of MDP Convolutional Codes over $\mathbb{Z}_{p^r}$

In this section we will show the existence of MDP convolutional codes over $\mathbb{Z}_{p^r}$ for any given set of parameters (n, k, δ) such that $k \mid \delta$. Moreover, we will do that by building concrete constructions of such codes. In contrast with other existing constructions of convolutional codes over $\mathbb{Z}_{p^r}$ with designed distance [23], [24] where Hensel lifts of a cyclic code were used, we propose a method based on a direct *lifting* of an MDP convolutional code from $\mathbb{Z}_p$ to $\mathbb{Z}_{p^r}$. We note that similar lifting techniques can be applied for different set of parameters (n, k, δ), see for more details [28].

Given the finite ring $\mathbb{Z}_{p^r}$ and the set of parameters (n, k, δ) with $k \mid \delta$, we aim to construct an MDP (n, k, δ)-convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$. To this end, denote $k_0 = \left\lfloor \frac{k}{r} \right\rfloor$ and $\nu = \frac{\delta}{k}$. Take $\widetilde{k} = k_0 + 1$ and $\widetilde{\delta} = \widetilde{k}\nu$, and let us consider an MDP convolutional code $\widetilde{\mathcal{C}}$ with length n, dimension $\widetilde{k}$ and degree $\widetilde{\delta}$ over $\mathbb{Z}_p$. Let $\widetilde{G}(D) \in \mathbb{Z}_p^{\widetilde{k} \times n}[D]$ be a minimal basic encoder of $\widetilde{\mathcal{C}}$, *i.e.*, with $\widetilde{G}^{lc}$ full row rank over $\mathbb{Z}_p$ and left prime (constructions of such codes can be found in [1], [9], [22]). Therefore,

$$\begin{aligned} \widetilde{d}_j^c &= \min\{\mathrm{wt}(v(D)|_{[0,j]}) : v(D) = u(D)\widetilde{G}(D),\ u(D) = \sum_{i \in \mathbb{N}_0} u_i D^i \in \mathbb{Z}_p((D)),\ u_0 \neq 0\} \\ &= (j+1)(n - \widetilde{k}) + 1, \quad j \leq \widetilde{L} \end{aligned}$$

where $\widetilde{L} = \left\lfloor \frac{\widetilde{\delta}}{\widetilde{k}} \right\rfloor + \left\lfloor \frac{\widetilde{\delta}}{n - \widetilde{k}} \right\rfloor$, see [14], [9].

Let $R = k - k_0 r$ and decompose $\widetilde{G}(D)$ as

$$\widetilde{G}(D) = \begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ \widetilde{\mathcal{G}}_{r-R}(D) \end{bmatrix} = \sum_{0 \leq i \leq \nu} \widetilde{G}_i D^i$$

where $\widetilde{\mathcal{G}}_{k_0}(D)$ has k_0 rows and $\widetilde{\mathcal{G}}_{k_{r-R}}(D)$ has 1 row. In the case $r|k$ then $\widetilde{G}(D) = \widetilde{\mathcal{G}}_0(D)$. Next, we straightforward expand $\widetilde{G}(D)$ as

$$G(D) = \begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\,\widetilde{\mathcal{G}}_0(D) \\ \vdots \\ p^r\,\widetilde{\mathcal{G}}_0(D) \\ p^{r-R}\,\widetilde{\mathcal{G}}_{r-R}(D) \\ p^{r-R+1}\,\widetilde{\mathcal{G}}_{r-R}(D) \\ \vdots \\ p^{r-1}\,\widetilde{\mathcal{G}}_{r-R}(D) \end{bmatrix} = \sum_{0\leq i\leq \nu} G_i D^i. \tag{8}$$

Since $\widetilde{G}^{lc}$ is full row rank over $\mathbb{Z}_p$, it immediately follows that $G(D)$ is a p-encoder in reduced form.

Theorem 19. *Let $\mathcal{C}$ be a convolutional code over $\mathbb{Z}_{p^r}$ with p-encoder $G(D)$ as in (8). Then, $\mathcal{C}$ is an MDP (n,k,δ)-convolutional code over $\mathbb{Z}_{p^r}$.*

Proof It is straightforward to verify that $\mathcal{C}$ is an (n,k,δ)-convolutional code. It is left to show that it is an MDP code, *i.e.*, we need to show that

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

for $j \leq L$ as in Theorem 18. It is a matter of straightforward computations to verify that since $k \mid \delta$, $L = \widetilde{L} = \left\lfloor \frac{\widetilde{\delta}}{\widetilde{k}} \right\rfloor + \left\lfloor \frac{\widetilde{\delta}}{n-\widetilde{k}} \right\rfloor$.

Let $u = [u_0\ u_1\ \ldots\ u_j]$, with $u_i \in \mathcal{A}_p^k$, $i = 0,\ldots,j$ and $u_0 \neq 0$, and let $v = [v_0\ v_1\ \ldots\ v_j]$, with $v_i \in \mathbb{Z}_p^n$, $i = 0,\ldots,j$, such that $v = uG_j^c$, where G_j^c is the j-th truncated sliding matrix correspondent to $G(D)$. The idea of the proof is to multiply v by a power of p such that the resulting nonzero truncated codeword $\widetilde{v}$ is in $p^{r-1}\mathbb{Z}_{p^r}^n$. Since $p^{r-1}\mathbb{Z}_{p^r}$ is isomorphic to $\mathbb{Z}_p$ then there exists a truncated nonzero codeword $\widehat{v} \in \widetilde{\mathcal{C}} = \mathrm{Im}_{\mathbb{Z}_p((D))}\widetilde{G}(D)$ such that $\mathrm{wt}(\widehat{v}) = \mathrm{wt}(\widetilde{v})$, and then we can use the fact that $\widetilde{\mathcal{C}}$ is MDP. We define the **order** of v, denoted by $ord(v)$, as the $j \in \{1,2,\ldots,r\}$ such that $p^j v = 0$ and $p^{j-1}v \neq 0$. 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

$$p^{\ell-1}v = \begin{bmatrix} 0 & 0 & \ldots & 0 & \widetilde{v}_i & \ldots & \widetilde{v}_j \end{bmatrix} = p^{r-1}\begin{bmatrix} 0 & 0 & \ldots & 0 & \widehat{v}_i & \ldots & \widehat{v}_j \end{bmatrix}. \tag{9}$$

Now it can be easily checked that

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

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

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

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

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

Considering $[v_0 \ \dots v_{i-1}] = [u_0 \ \dots \ u_{i-1}]\, G_i^c$ and reasoning in the same way we conclude that

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

and therefore

$$\mathrm{wt}\left([v_0 \ \cdots \ v_j]\right) \geq (n-\widetilde{k})(j+1)+1.$$

Consequently, $d_j^c = (n-\widetilde{k})(j+1)+1$, *i.e.*, $d_j^c = (n-\lceil \frac{k}{r} \rceil)(j+1)+1$, for $j \leq L$. □

V. Appendix

***Proof of Proposition 14*:** 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 $s = 1, \dots, k$, is the s-th row of $G(D)$. Since $G(D)$ is a p-encoder, its

rows form a p-generator sequence.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

$$p\,row_s(G_{j+1}^c) \in p\text{-}span(row_{s+1}(G_{j+1}^c), \ldots, row_{k(j+1)}(G_{j+1}^c)), \tag{10}$$

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

Let $s \in \{1, \ldots, k-1\}$. Since $G(D)$ is a p-encoder, 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

$$p\,g_s(D) = a_{s+1}(D) \cdot g_{s+1}(D) + a_{s+2}(D) \cdot g_{s+2}(D) + \cdots + a_k(D) \cdot g_k(D)$$

which implies that

$$\begin{aligned} p\left[g_s^0 \; g_s^1 \; \cdots \; g_s^{j+1}\right] = \; & a_{s+1}^0 \cdot \left[g_{s+1}^0 \; g_{s+1}^1 \; \cdots \; g_{s+1}^{j+1}\right] + \cdots + a_k^0 \left[g_k^0 \; g_k^1 \; \cdots \; g_k^{j+1}\right] + a_{s+1}^1 \left[0 \; g_{s+1}^0 \; \cdots \; g_{s+1}^j\right] \\ & \cdots + a_k^1 \left[0 \; g_k^0 \; \cdots \; g_k^j\right] + \cdots + a_{s+1}^{j+1} \left[0 \; \cdots \; 0 \; g_{s+1}^0\right] + \cdots + a_k^{j+1} \left[0 \; \cdots \; 0 \; g_k^0\right], \end{aligned}$$

which proves (10). Finally, let us consider now $s = k$. Since the rows of $G(D)$ form a p-generator sequence, $p\,g_k(D) = 0$ and therefore $p\,row_k(G_{j+1}^c) = 0$. □

Proof of Theorem 15: Let $\widetilde{G}(D) \in \mathbb{Z}_{p^r}^{k \times n}[D]$ be a generator matrix of $\mathcal{C}$ as in (5) with $\widehat{G}(D)$ in (6) full row rank and such that $\widehat{G}(0)$ is also full row rank. Let us consider the p-encoder

$$G(D) = \begin{bmatrix} \widetilde{\mathcal{G}}_0(D) \\ p\,\widetilde{\mathcal{G}}_0(D) \\ p\,\widetilde{\mathcal{G}}_1(D) \\ \vdots \\ p^{r-1}\,\widetilde{\mathcal{G}}_0(D) \\ \vdots \\ p^{r-1}\widetilde{\mathcal{G}}_{r-1}(D) \end{bmatrix} = \sum_{i \in \mathbb{N}_0} G_i D^i.$$

Since $\widehat{G}(0)$ is full row rank, $G(D)$ is delay-free. Moreover, the last $k_0 + k_1 + \cdots + k_{r-1}$ rows of $G(D)$ belong to $p^{r-1}\mathbb{Z}_{p^r}^n[D]$ which implies that the last $k_0 + k_1 + \cdots + k_{r-1}$ rows of G_i belong to $p^{r-1}\mathbb{Z}_{p^r}^n$,

for all i. Let us consider the truncated sliding generator matrix G_j^c to obtain

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

We can assume without loss of generality that G_0 is in p-standard form as in (3), with parameters $k_0, k_1, \dots, k_{r-1}$. Consider $u = [u_0\ u_1\ \cdots\ u_j]$, $u_i \in \mathcal{A}_p^k$, $i = 0, \dots, j$ with $u_0 = [0\ 0\ \dots\ 0\ 1]$ and $v = uG_j^c = [v_0\ v_1\ \cdots\ v_j]$ with $v_i \in \mathbb{Z}_{p^r}^n$, $i = 0, \dots, j$. Then,

$$v_0 = u_0 G_0 = \left[0\ \dots\ 0\ 1\ p^{r-1}A_{r,r-1}^{r-1,k}\right],$$

where $A_{r,r-1}^{r-1,k}$ represents the last row of $A_{r,r-1}^{r-1}$ as in (3). Then,

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

Write g_1 as

$$g_1 = \left[g_{1,k_0}\ g_{1,k_1}\ \cdots\ g_{1,k_{r-1}}\ g_{1,n-(k_0+\cdots+k_{r-1})}\right],$$

with $g_{1,i} \in \mathbb{Z}_{p^r}^i$, $i = k_0, k_1, \dots, k_{r-1}$ and $g_{1,n-(k_0+\cdots+k_{r-1})} \in \mathbb{Z}_{p^r}^{n-(k_0+\cdots+k_{r-1})}$. Let us consider u_1 with its first $[(r-1)k_0 + (r-2)k_1 + \cdots + k_{r-2}]$ components equal to zero and the remaining $k_0 + k_1 + \cdots + k_{r-1}$ components equal to $\left[\alpha_{1,k_0}\ \alpha_{1,k_1}\ \cdots\ \alpha_{1,k_{r-1}}\right]$, where $\alpha_{1,k_i} \in \mathcal{A}_p^i$ are such that

$$-p^{r-1}\,g_{1,k_i} = p^{r-1}\alpha_{1,k_i},\ \ i = 0, \dots, r-1.$$

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

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

In the same way, $v_2 = p^{r-1}\,g_2 + u_1G_1 + u_2G_0$ where $p^{r-1}\,g_2$ represent the last row of G_2 and $u_1G_1 \in p^{r-1}\mathbb{Z}_{p^r}^n$. Take u_2 such that its first $[(r-1)k_0 + (r-2)k_1 + \cdots + k_{r-2}]$ components are zero and the remaining $(k_0 + k_1 + \cdots + k_{r-1})$ components are equal to $\left[\alpha_{2,k_0}\ \alpha_{2,k_1}\ \cdots\ \alpha_{2,k_{r-1}}\right]$, where $\alpha_{2,k_i} \in \mathcal{A}_p^i$ are such that

$$-p^{r-1}\,\tilde{g}_{2,k_i} = p^{r-1}\alpha_{2,k_i},\ i = 0, \dots, r-1,$$

where $\left[p^{r-1}g_{2,k_0}\ \ p^{r-1}g_{2,k_0}\ \cdots\ p^{r-1}g_{2,k_{r-1}}\right]$ represent the first $k_0 + k_1 + \cdots + k_{r-1}$ components of $p^{r-2}g_2 + u_1G_1$. As before, the first $k_0 + k_1 + \cdots + k_{r-1}$ elements of v_2 are zero and therefore

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

Applying the same reasoning we construct $u_i \in \mathcal{A}_p^k$ such that $\mathrm{wt}(v_i) \leq n - (k_0 + k_1 + \cdots + k_{r-1})$,

$i = 3, \ldots, j$ and therefore

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

□

REFERENCES

[1] 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.

[2] 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.

[3] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography*, 6(1):21–35, 1995.

[4] S. K. Chang and A. Gill. Algorithmic solution of the change-making problem. *Assoc. Comput. Mach.*, 17(1):113–122, 1970.

[5] M. El Oued, D. Napp, R. Pinto, and M. Toste. The dual of convolutional codes over $\mathbb{Z}_{p^r}$. *In: Bebiano N. (eds) Applied and Computational Matrix Analysis. MAT-TRIAD 2015. Springer Proceedings in Mathematics & Statistics*, 192:79–91, 2017.

[6] F. Fagnani and S. Zampieri. Dynamical systems and convolutional codes over finite abelian groups. *IEEE Trans. Inform. Theory*, 42(6, part 1):1892–1912, 1996.

[7] F. Fagnani and S. Zampieri. System-theoretic properties of convolutional codes over rings. *IEEE Trans. Information Theory*, 47(6):2256–2274, 2001.

[8] G.D. Forney and M.D. Trott. The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders. *IEEE Trans. Inf. Th*, 39:1491–1513, 1993.

[9] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. Strongly MDS convolutional codes. *IEEE Trans. Inform. Theory*, 52(2):584–598, 2006.

[10] K. Guendaa and T. A. Gulliver. MDS and self-dual codes over rings. *Finite Fields and Their Applications*, 18(6):1061–1075, 2012.

[11] R. Hutchinson, J. Rosenthal, and R. Smarandache. Convolutional codes with maximum distance profile. *Systems & Control Letters*.

[12] 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.

[13] 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.

[14] R. Johannesson and K. Sh. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press, New York, 1999.

[15] 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.

[16] M. Kuijper and R. Pinto. On minimality of convolutional ring encoders. *IEEE Trans. Automat. Contr.*, 55)(11):4890 –4897, 2009.

[17] 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.

[18] H-A Loeliger and T. Mittelholzer. Convolutional codes over groups. *IEEE Trans. Inf. Th.*, IT-42:1660–1686, 1996.

[19] J. L. Massey and T. Mittelholzer. Convolutional codes over rings. *In Proc. 4th Joint Swedish-Soviet Int. Workshop Information Theory*, pages 14–18, 1989.

[20] B.R. McDonald. *Finite rings with identity*. Marcel Dekker, New York, 1974.

[21] D. Napp, R. Pinto, and M. Toste. On MDS convolutional codes over $\mathbb{Z}_{p^r}$. *Designs, Codes and Cryptography*, 83:101–114, 2017.

[22] D. Napp and R. Smarandache. Constructing strongly MDS convolutional codes with maximum distance profile. *Advances in Mathematics of Communications*, 10(2):275–290, 2016.

[23] Graham H. Norton and Ana Salagean. On the hamming distance of linear codes over a finite chain ring. *IEEE Trans. Information Theory*, 46(3):1060–1067, 2001.

[24] M. El Oued and P. Solé. MDS convolutional codes over a finite ring. *IEEE Trans. Inf. Th.*, 59(11):7305 – 7313, 2013.

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

[26] P. Solé and V. Sison. Quaternary convolutional codes from linear block codes over galois rings. *IEEE Trans. Information Theory*, 53:2267–2270, 2007.

[27] V. Tomas, J. Rosenthal, and R. Smarandache. Decoding of convolutional codes over the erasure channel. *IEEE Trans. Inform. Theory*, 58(1):90–108, January 2012.

[28] M. Toste. *Distance properties of convolutional codes over* $\mathbb{Z}_{p^r}$. University of Aveiro, September 2016. PhD Thesis.

[29] 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.