On duals and parity-checks of convolutional codes over $\mathbb{Z}_{p^r}$

M. El Oued and Diego Napp and Raquel Pinto and Marisa Toste

M. El Oued FSMMath Department, University of Monastir, Monastir 5050, Tunisia e-mail: Mohamed.Eloued@isimm.rnu.tn
Diego Napp, Raquel Pinto and Marisa Toste: CIDMA - Center for Research and Development in Mathematics and Applications, Department of Mathematics, University of Aveiro, Aveiro, Portugal diego@ua.pt and raquel@ua.pt
Marisa Toste, Superior School of Technologies and Management of Oliveira do Hospital, Polytechnic Institute of Coimbra, Coimbra, Portugal marisa.toste@estgoh.ipc.pt

Abstract

A convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}((D))$ is a $\mathbb{Z}_{p^r}((D))$-submodule of $\mathbb{Z}_{p^r}^n((D))$ that admits a polynomial set of generators, where $\mathbb{Z}_{p^r}((D))$ stands for the ring of (semi-infinity) Laurent series. In this paper we study several structural properties of its dual $\mathcal{C}^\perp$. We use these results to provide a constructive algorithm to build an explicit generator matrix of $\mathcal{C}^\perp$. Moreover, we show that the transpose of such a matrix is a parity-check matrix (also called syndrome former) of $\mathcal{C}$.

Keywords:
Finite rings, Convolutional codes over finite rings, dual codes, matrix representations

1. Introduction

Convolutional codes form a fundamental class of linear codes that are widely used in applications (see also the related notion of sequential cellular automata [2]) . They are typically described by means of a generator matrix, which is a polynomial matrix with coefficients in a finite field or a finite ring, depending on the application. Yet, the state of the art is totally different for these two classes of convolutional codes. The mathematical theory of convolutional codes over finite fields is much developed and has produced many sophisticated classes of codes. On the other hand, the mathematical theory of convolutional codes over finite rings is still in the beginnings. Many results and notions that are well-known for linear convolutional codes over finite fields have not been fully investigated in the context of finite rings. One of these notions is the one of dual code. Dual codes of convolutional codes over a finite field have been extensively studied, see e.g. the work of Forney and McEliece in [7, 13] where they showed that when $\mathcal{C}$ is defined over $\mathbb{F}((D))$, $\mathbb{F}$ a finite field, then, the dual code of $\mathcal{C}$ is again a convolutional code and $\mathcal{C}$ always admits a parity-check representation.

In our quest to extend these results over finite fields, we consider in this paper convolutional codes $\mathcal{C}$ over $\mathbb{Z}_{p^r}((D))$ which are a particular class of linear codes and investigate their dual codes $\mathcal{C}^\perp$. We derive fundamental structural properties of $\mathcal{C}^\perp$ and show that they possess

the structure of a convolutional code. Moreover, we present a constructive methodology to derive a generator matrix for $\mathcal{C}^\perp$ which will lead to an explicit construction of a parity-check matrix for $\mathcal{C}$. Hence, this work completes previous results in [3, 16, 14] and can be considered a generalization and an extension, to the ring case, of the work previously done for convolutional codes over a finite field.
The outline of this paper is as follows. In Section 2 we present fundamental results on the structure of convolutional codes over the finite ring $\mathbb{Z}_{p^r}((D))$. We also present some results on free convolutional codes. In Section 3 we address and solve the main problems of the paper. We divide this section in three parts. The first treats the simpler case of free convolutional codes over $\mathbb{Z}_{p^r}((D))$ and then we address the general case. We conclude this section presenting a constructive algorithm to build a generator matrix of the dual code. Some of the most technical proof are presented in the appendix to ease readability.

2. Preliminaries results

In this section we present the setting and the necessary results to address the problems in the next section. Following most the literature on convolutional codes over a finite ring, we consider an approach in which code sequences are semi-infinite Laurent series, *i.e.*, convolutional codes constituted by left compact sequences in $\mathbb{Z}_{p^r}$, see [4, 8, 9, 10, 12]. Hence, the elements of the code (codewords) 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 $\ell \in \mathbb{Z}$ and 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 polynomials with coefficients in $\mathbb{Z}_{p^r}$ and 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

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

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 $\mathbb{Z}_{p^r}(D)$. The next results follow from Theorem 2 and Proposition 2 in [5].

Lemma 1. *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 $L(D)A(D) = I$ which holds if and only if $\overline{A(D)}$ is invertible in $\mathbb{Z}_p^{\ell\times\ell}(D)$, where $\overline{A(D)}$ represents the projection of $A(D)$ into $\mathbb{Z}_p(D)$.*

Proof. If $\overline{A(D)}$ is invertible in $\mathbb{Z}_p(D)$ and $B(D) \in \mathbb{Z}_p^{\ell \times \ell}(D)$ is such that $B(D)A(D) = I \bmod p$, then,

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

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

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

The converse is immediate. □

Definition 1. *[3, 6, 15] A* **convolutional code** $\mathcal{C}$ *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* $G(D) \in \mathbb{Z}_{p^r}^{k \times n}[D]$ *such that*

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

The matrix $G(D)$ *is called a* **generator matrix** *of* $\mathcal{C}$*. If* $G(D)$ *is full row rank*[1]*, then, it is called an* **encoder** *of* $\mathcal{C}$ *and* $\mathcal{C}$ *is a free module, called* **free convolutional code***.*

Note that as we require the generator matrix to be polynomial, not all $\mathbb{Z}_{p^r}((D))$-submodules of $\mathbb{Z}_{p^r}^n((D))$ are convolutional codes. A polynomial matrix $H(D)$ is a **parity-check matrix** (or syndrome former) of a convolutional code $\mathcal{C}$ if $\mathcal{C} = \operatorname{Ker} H^T(D)$, *i.e.*, for every $w(D) \in \mathbb{Z}_{p^r}^n((D))$,

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

It is easy to show that if $G_1(D), G_2(D) \in \mathbb{Z}_{p^r}^{k \times n}[D]$ are two encoders of a free convolutional code $\mathcal{C}$, then,

$$G_1(D) = R(D)G_2(D),$$

for some invertible matrix $R(D) \in \mathbb{Z}_{p^r}^{k \times n}(D)$.
Next, we present some properties on *free* convolutional codes that will be fundamental for the study of the dual codes. First we consider the following auxiliary lemmas for free modules. From the lineality of $\mathcal{C}$ it readily follows that

$$\mathcal{C} \cap p^i \mathbb{Z}_{p^r}^n((D)) = p^i \mathcal{C}, \tag{1}$$

which immediately implies the next result.

Lemma 2. *Let* $\mathcal{C}$ *be a free convolutional code of length* n*. For any given integers* $j \in \{0, \ldots r-1\}$ *and* $i \leq j$ *we have that*

$$p^i \mathcal{C} \cap p^j \mathbb{Z}_{p^r}^n((D)) = p^j \mathcal{C}.$$

Note that if $\mathcal{C}$ is a free convolutional code over $\mathbb{Z}_{p^r}((D))$, then, its projection into $\mathbb{Z}_p((D))$, $\bar{\mathcal{C}} = \mathcal{C}$ *mod* p, is also a convolutional code over $\mathbb{Z}_p((D))$. More generally, one can easily

[1] $G(D) \in \mathbb{Z}_{p^r}^{k \times n}(D)$ is full rank if its projection into $\mathbb{Z}_p((D))$ is full row rank (see Lemma 1)

prove that for free convolutional codes $\mathcal{C}$, $\mathcal{C}_1$, $\mathcal{C}_2$ of length n such that $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$ it holds that for $j = 0, 1, \dots, r-1$,

$$p^j\mathcal{C} = p^j\mathcal{C}_1 \oplus p^j\mathcal{C}_2. \tag{2}$$

From this the next result is straightforward.

Lemma 3. *Let $\mathcal{C}$, $\mathcal{C}_1$, $\mathcal{C}_2$ be free convolutional codes of length n such that $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$. Then, $\bar{\mathcal{C}} = \bar{\mathcal{C}_1} \oplus \bar{\mathcal{C}_2}$ mod p.*

Lemma 4. *Let $\mathcal{C}_1$, $\mathcal{C}_2$ be free convolutional codes of length n. Then, for $i \in \{0, 1, \dots, r-1\}$, it holds that,*

$$p^i\mathcal{C}_1 \cap [p^i\mathcal{C}_2 + p^{r-1}\mathbb{Z}^n_{p^r}((D))] = p^i(\mathcal{C}_1 \cap \mathcal{C}_2) + p^{r-1}\mathcal{C}_1.$$

Proof. It is easy to see that $p^j(\mathcal{C}_1 \cap \mathcal{C}_2) = p^j\mathcal{C}_1 \cap p^j\mathcal{C}_2$, for all $j \in \{0, 1, \dots, r-1\}$ and therefore using Lemma 2 for $j = r-1$ it follows that

$$\begin{aligned} p^i(\mathcal{C}_1 \cap \mathcal{C}_2) + p^{r-1}\mathcal{C}_1 &= p^i\mathcal{C}_1 \cap p^i\mathcal{C}_2 + (p^i\mathcal{C}_1 \cap p^{r-1}\mathbb{Z}^n_{p^r}((D))) \\ &\subset p^i\mathcal{C}_1 \cap (p^i\mathcal{C}_2 + p^{r-1}\mathbb{Z}^n_{p^r}((D))). \end{aligned}$$

Conversely, let $w(D) \in p^i\mathcal{C}_1 \cap (p^i\mathcal{C}_2 + p^{r-1}\mathbb{Z}^n_{p^r}((D)))$, $w(D) = w_1(D) + w_2(D) \in p^i\mathcal{C}_1$ with $w_1(D) \in p^i\mathcal{C}_2$ and $w_2(D) \in p^{r-1}\mathbb{Z}^n_{p^r}((D))$. Further,

$$pw(D) = pw_1(D) \in p^{i+1}\mathcal{C}_2,$$

and therefore

$$pw(D) \in p^{i+1}\mathcal{C}_1 \cap p^{i+1}\mathcal{C}_2 = p^{i+1}(\mathcal{C}_1 \cap \mathcal{C}_2)$$

and consequently

$$w(D) \in p^i(\mathcal{C}_1 \cap \mathcal{C}_2) + p^{r-1}\mathbb{Z}^n_{p^r}((D)).$$

Finally, let

$$w(D) = p^i\tilde{w}_1(D) + p^{r-1}\tilde{w}_2(D),$$

with $\tilde{w}_1(D) \in \mathcal{C}_1 \cap \mathcal{C}_2$ and $\tilde{w}_2(D) \in \mathbb{Z}^n_{p^r}((D))$. Then, since $w(D)$ and $p^i\tilde{w}_1(D)$ are in $p^i\mathcal{C}_1$ it follows that

$$w(D) - p^i\tilde{w}_1(D) = p^{r-1}\tilde{w}_2(D) \in p^i\mathcal{C}_1 \subset \mathcal{C}_1$$

and thus equality 1 implies that $p^{r-1}\tilde{w}_2 \in \mathcal{C}_1 \cap p^{r-1}\mathbb{Z}^n_{p^r}((D)) = p^{r-1}\mathcal{C}_1$, and therefore $w(D) \in p^i(\mathcal{C}_1 \cap \mathcal{C}_2) + p^{r-1}\mathcal{C}_1$. □

We conclude the section by presenting a result that allows to decompose a convolutional code into simpler components. These simpler components are built over free convolutional codes, and therefore the next result together with the previous results on free convolutional codes will constitute the basic tools in order to address the main problem of the paper. This result can be found in [3] and its proof provides a procedure to obtain a generator matrix of the code of the form $\begin{bmatrix} G_0(D) \\ pG_1(D) \\ \vdots \\ p^{r-1}G_{r-1}(D) \end{bmatrix}$, with $\begin{bmatrix} G_0(D) \\ G_1(D) \\ \vdots \\ G_{r-1}(D) \end{bmatrix}$ full row rank. We include the proof here for the sake of completeness.

Theorem 1. *[3] Let $\mathcal{C}$ be a convolutional code over $\mathbb{Z}_{p^r}$. Then, there exist free convolutional codes over $\mathbb{Z}_{p^r}$, $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{r-1}$, such that*

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

and

$$\mathcal{C}_0 + \mathcal{C}_1 + \cdots + \mathcal{C}_{r-1} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1},$$

i.e., $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{r-1}$ form a partition of $\mathcal{C}_0 + \mathcal{C}_1 + \cdots + \mathcal{C}_{r-1}$.

Proof. Let $G(D) \in \mathbb{Z}_{p^r}^{k \times n}[D]$ be a generator matrix of $\mathcal{C}$. If $G(D)$ is full row rank then $\mathcal{C}$ is free and $\mathcal{C} = \mathcal{C}_0$.

Let us assume now that $G(D)$ is not full row rank. Then, its projection into $\mathbb{Z}_p((D))$ satisfies $\text{rank}(\overline{G(D)}) = k_0 < k$ and there exists a nonsingular matrix $F_0(D) \in \mathbb{Z}_{p^r}^{k \times k}[D]$ such that $\overline{F_0(D)G(D)} = \begin{bmatrix} \widetilde{G}_0(D) \\ 0 \end{bmatrix}$ modulo p, where $\widetilde{G}_0(D)$ is full row rank with rank k_0. Then $F_0(D)G(D) = \begin{bmatrix} G_0(D) \\ p\widehat{G}_1(D) \end{bmatrix}$, where $G_0(D) \in \mathbb{Z}_{p^r}^{k_0 \times n}[D]$ is such that $\overline{G_0(D)} = \widetilde{G}_0(D)$ and $\widehat{G}_1(D) \in \mathbb{Z}_{p^r}^{(k-k_0) \times n}[D]$. Moreover, since $F_0(D)$ is invertible, $\begin{bmatrix} G_0(D) \\ p\widehat{G}_1(D) \end{bmatrix}$ 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 $F_1(D)\overline{\widehat{G}_1(D)} = \begin{bmatrix} \widetilde{G}_1(D) \\ 0 \end{bmatrix}$ modulo p, where $\widetilde{G}_1(D)$ 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 $G_1'(D) \in \mathbb{Z}_{p^r}^{\tilde{k}_1 \times n}$ is such that $\overline{G_1'(D)} = \widetilde{G}(D)$, and therefore

$$\begin{bmatrix} I_{k_0} & 0 \\ 0 & F_1(D) \end{bmatrix} F_0(D)G(D) = \begin{bmatrix} G_0(D) \\ pG_1'(D) \\ p^2\widehat{G}_2(D) \end{bmatrix}.$$

If $\begin{bmatrix} G_0(D) \\ G_1'(D) \end{bmatrix}$ is not full row rank, then there exists a permutation matrix P and a rational matrix $L(D) \in \mathbb{Z}_{p^r}^{\tilde{k}_1 \times k_0}(D)$ such that

$$P \begin{bmatrix} I_{k_0} & 0 \\ L_1(D) & I_{k_1} \end{bmatrix} \begin{bmatrix} G_0(D) \\ pG_1'(D) \end{bmatrix} = \begin{bmatrix} G_0(D) \\ pG_1''(D) \\ p^2 G_2'(D) \end{bmatrix},$$

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 $\begin{bmatrix} G_0(D) \\ G_1''(D) \end{bmatrix}$ 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

$$\mathrm{Im}_{\mathbb{Z}_{p^r}((D))} \begin{bmatrix} G_0(D) \\ pG_1'(D) \end{bmatrix} = \mathrm{Im}_{\mathbb{Z}_{p^r}((D))} \begin{bmatrix} G_0(D) \\ pG_1''(D) \\ p^2 G_2'(D) \end{bmatrix}.$$

Moreover, there exist $G_1(D) \in \mathbb{Z}_{p^r}^{k_1 \times n}[D]$ and $G_2''(D) \in \mathbb{Z}_{p^r}^{(\tilde{k}_1 - k_1)\times n}[D]$ polynomial matrices such that

$$\mathrm{Im}_{\mathbb{Z}_{p^r}((D))} \begin{bmatrix} G_0(D) \\ pG_1''(D) \\ p^2 G_2'(D) \end{bmatrix} = \mathrm{Im}_{\mathbb{Z}_{p^r}((D))} \begin{bmatrix} G_0(D) \\ pG_1(D) \\ p^2 G_2''(D) \end{bmatrix}.$$

Then

$$\begin{bmatrix} G_0(D) \\ pG_1(D) \\ p^2 G_2'''(D) \end{bmatrix},$$

with $p^2 G_2'''(D) = \begin{bmatrix} p^2 G_2''(D) \\ p^2 \widehat{G}_2(D) \end{bmatrix}$, is still a generator matrix of $\mathcal{C}$ such that $\begin{bmatrix} G_0(D) \\ G_1(D) \end{bmatrix}$ is full row rank.

Proceeding in the same way we obtain a generator matrix of $\mathcal{C}$ of the form

$$\begin{bmatrix} G_0(D) \\ pG_1(D) \\ \vdots \\ p^{r-1} G_{r-1}(D) \end{bmatrix},$$

and such that

$$\begin{bmatrix} G_0(D) \\ G_1(D) \\ \vdots \\ G_{r-1}(D) \end{bmatrix}$$

is full row rank. Thus $\mathcal{C} = \mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \cdots \oplus p^{r-1}\mathcal{C}_{r-1}$ with $\mathcal{C}_i := \mathrm{Im}\, G_i(D)$ a free convolutional code, $i = 0, 1, \ldots, r-1$, and such that the sum $\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1}$ is direct.

□

As $\mathbb{Z}_{p^r}^n((D))$ is a semi-simple module [11] the previous result readily follows for any submodule of $\mathbb{Z}_{p^r}^n((D))$. Note however that convolutional codes are submodules of $\mathbb{Z}_{p^r}^n((D))$ that admit a polynomial basis. It is worth mentioning that the previous theorem is the convolutional version of the linear block code decomposition of Caire and Biglieri in [1].

3. Dual Codes

We begin by recalling the standard definition of the dual of a code.

Definition 2. *Let $\mathcal{C}$ be a convolutional code of length n. The* **dual** *of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined as*

$$\mathcal{C}^\perp = \{y(D) \in \mathbb{Z}_{p^r}^n((D)) : y(D)w^T(D) = 0 \textit{ for all } w(D) \in \mathcal{C}\}.$$

The main result of this section is an algorithm for the explicit construction of a matrix representation (generator matrix) of $\mathcal{C}^\perp$. To this end, we shall decompose $\mathcal{C}$ as a direct summand of submodules given in terms of free modules. We first address the case when $\mathcal{C}$ is itself a free module and then, consider the general case.

3.1. Duals of free convolutional codes over $\mathbb{Z}_{p^r}((D))$

Let $\mathcal{C} = \operatorname{Im}_{\mathbb{Z}_{p^r}((D))} G(D)$ be a free convolutional code with $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ full row rank. Then, it immediately follows from Section 2 that there exist matrices $N(D) \in \mathbb{Z}_{p^r}^{(n-k)\times n}(D)$, $L(D) \in \mathbb{Z}_{p^r}^{k\times n}(D)$ and $\widetilde{H}(D) \in \mathbb{Z}_{p^r}^{(n-k)\times n}(D)$ such that

$$\begin{bmatrix} G(D) \\ N(D) \end{bmatrix} \begin{bmatrix} L^T(D) & \widetilde{H}^T(D) \end{bmatrix} = I. \qquad (3)$$

Lemma 5. *Let $\mathcal{C} = \operatorname{Im}_{\mathbb{Z}_{p^r}((D))} G(D)$ be a free convolutional code with $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ full row rank and let $\widetilde{H}(D)$ be as in (3). It follows that*

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

Proof. If $w(D) \in \mathcal{C}$ then $w(D) = u(D)G(D)$, for some $u(D) \in \mathbb{Z}_{p^r}^k((D))$, and therefore, by (3),

$$w(D)\widetilde{H}^T(D) = u(D)G(D)\widetilde{H}^T(D) = 0.$$

On the other hand, let $w(D) \in \mathbb{Z}_{p^r}^n((D))$ such that $w(D)\widetilde{H}^T(D) = 0$, and consider $u(D) = w(D)L^T(D) \in \mathbb{Z}_{p^r}^k((D))$. Then, by (3)

$$\begin{aligned} w(D) &= w(D) \begin{bmatrix} L^T(D) & \widetilde{H}^T(D) \end{bmatrix} \begin{bmatrix} G(D) \\ N(D) \end{bmatrix} \\ &= \begin{bmatrix} u(D) & 0 \end{bmatrix} \begin{bmatrix} G(D) \\ N(D) \end{bmatrix} \\ &= u(D)G(D) \end{aligned}$$

and therefore $w(D) \in \mathcal{C}$. □

The next result was proven in [3, Theorem 1].

Lemma 6. *If $\mathcal{C}$ is a free convolutional code with length n and rank k, then, $\mathcal{C}^\perp$ is also a free convolutional code of length n and rank $n-k$. Moreover,*

$$\mathcal{C}^\perp = \operatorname{Im}_{\mathbb{Z}_{p^r}((D))} \widetilde{H}(D),$$

with $\widetilde{H}(D)$ a rational matrix as defined in (3).

Proof. Let $G(D) \in \mathbb{Z}_{p^r}^{k\times n}$ be an encoder of $\mathcal{C}$. Since $G(D)$ is full row rank there exists a polynomial matrix $L(D) \in \mathbb{Z}_{p^r}^{(n-k)\times n}[D]$ such that $\begin{bmatrix} G(D) \\ L(D) \end{bmatrix}$ is nonsingular. Let $[X(D)\ Y(D)]$, with $X(D) \in \mathbb{Z}_{p^r}^{n\times k}(D)$ and $Y(D) \in \mathbb{Z}_{p^r}^{n\times(n-k)}(D)$, be the inverse of $\begin{bmatrix} G(D) \\ L(D) \end{bmatrix}$. Then $\mathcal{C}^\perp = \operatorname{Im}_{\mathbb{Z}_{p^r}((D))} Y(D)^t$. Since $Y(D)$ is full column rank, there exists a full row rank matrix polynomial matrix $G^\perp(D) \in \mathbb{Z}_{p^r}^{(n-k)\times n}[D]$ such that $\mathcal{C}^\perp = \operatorname{Im}_{\mathbb{Z}_{p^r}((D))} G^\perp(D)$. Thus $\mathcal{C}^\perp$ is a free convolutional code of rank $n-k$. □

Then, if $H(D) \in \mathbb{Z}_{p^r}^{(n-k)\times n}[D]$ is an encoder of $\mathcal{C}^\perp$ it follows that

$$w(D) \in \mathcal{C} \Leftrightarrow w(D)H^T(D) = 0. \tag{4}$$

Therefore free convolutional codes admit representations by means of parity-check matrices. Note that the transposes of the encoders of $\mathcal{C}^\perp$ are the parity-check matrices of $\mathcal{C}$. We illustrate the free case by a simple example.

Example 1. *Consider the free convolutional code $\mathcal{C}$ over $\mathbb{Z}_9((D))$ with encoder*

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

The matrix

$$\begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \\ 1 & 0 & 0 \end{bmatrix}$$

has rational inverse

$$\begin{bmatrix} 0 & 0 & 1 \\ \frac{1+D}{1+7D+6D^2} & \frac{6D}{1+7D+6D^2} & \frac{8+7D+8D^2}{1+7D+6D^2} \\ \frac{8+8D}{1+7D+6D^2} & \frac{1}{1+7D+6D^2} & \frac{1+2D+D^2}{1+7D+6D^2} \end{bmatrix}.$$

Then,

$$\begin{aligned} \mathcal{C}^\perp &= \operatorname{Im}_{\mathbb{Z}_9((D))} \begin{bmatrix} 1 & \frac{8+7D+8D^2}{1+7D+6D^2} & \frac{1+2D+D^2}{1+7D+6D^2} \end{bmatrix} \\ &= \operatorname{Im}_{\mathbb{Z}_9((D))} \begin{bmatrix} 1+7D+6D^2 & 8+7D+8D^2 & 1+2D+D^2 \end{bmatrix} \end{aligned}$$

and therefore

$$H(D) = \begin{bmatrix} 1+7D+6D^2 \\ 8+7D+8D^2 \\ 1+2D+D^2 \end{bmatrix}$$

is a parity-check matrix of $\mathcal{C}$.

3.2. The dual of a convolutional code over $\mathbb{Z}_{p^r}((D))$: The general case

In this subsection we investigate the structural properties of the dual and the existence of a parity-check matrix of a non necessarily free convolutional code. We use the free modules $\mathcal{C}_i$ of Theorem 1 and the decomposition of $\mathcal{C}$ in terms of those $\mathcal{C}_i$ to characterize the structure of $\mathcal{C}^\perp$ as direct sum of submodules of $\mathcal{C}^\perp$.

Lemma 7. *Let $\mathcal{C}$ be a convolutional code defined in $\mathbb{Z}_{p^r}((D))$. Then, for all integers $i \in \{0, \dots r-1\}$ it follows that*

$$(p^j\mathcal{C})^\perp = \mathcal{C}^\perp + p^{r-j}\mathbb{Z}^n_{p^r}((D)). \tag{5}$$

If $\mathcal{C}_i$ are as in Theorem 1, then, for all $k \in \{0, 1, \dots, r-1\}$ it holds that

$$(\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \cdots \oplus p^k\mathcal{C}_k)^\perp = \sum_{i=0}^{k}[(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{k-i})^\perp \cap p^i\mathbb{Z}^n_{p^r}((D))].$$

Proof. Clearly $\mathcal{C}^\perp + p^{r-i}\mathbb{Z}^n_{p^r}((D)) \subset (p^i\mathcal{C})^\perp$. For the other inclusion, let $y \in (p^i\mathcal{C})^\perp$, then for all $x \in \mathcal{C}$ we have $y \cdot p^i x^T = p^i y \cdot x^T = 0$, thus $p^i y \in \mathcal{C}^\perp$. It is easy to see that there exists $x \in \mathcal{C}^\perp$ such that $p^i y = p^i x$. This implies that $\overline{y} = \overline{x}$. Thus there exists $y_1 \in \mathcal{C}^\perp$, $y_2 \in \mathbb{Z}_{p^r}((D))$ satisfying $y = y_1 + py_2$. We have $p^i y = p^i y_1 + p^{i+1}y_2$, then $p^i y - p^i y_1 = p^{i+1}y_2 \in \mathcal{C}^\perp$. Then $y_2 = y_3 + py_4$ where $y_3 \in \mathcal{C}^\perp$ and $y_4 \in \mathbb{Z}^n_{p^r}((D))$. Then $y = \underbrace{y_1 + py_3}_{\in \mathcal{C}^\perp} + p^2 y_4$. By repeating this procedure $r-i$ times, we obtain $y = x_1 + p^{r-i}x_2$ with $x_1 \in \mathcal{C}^\perp$.

For the second statement we proceed by induction on k. For $k = 1$ we use (5) to obtain that

$$(\mathcal{C}_0 + p\mathcal{C}_1)^\perp \;=\; \mathcal{C}_0^\perp \cap (p\mathcal{C}_1)^\perp = (\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp + (\mathcal{C}_0 \cap p^{r-1}\mathbb{Z}^n_{p^r}((D))).$$

Assume now that the statement holds for k, we shall prove that it also holds for $k+1$. Using (5) and the assumption,

$$\begin{aligned}(\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \cdots \oplus p^{k+1}\mathcal{C}_{k+1})^\perp &= (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \cdots \oplus p^k\mathcal{C}_k)^\perp \cap (p^{k+1}\mathcal{C}_{k+1})^\perp = \\ &= \sum_{i=0}^{k}[(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{k-i})^\perp \cap p^i\mathbb{Z}^n_{p^r}((D)) \cap (\mathcal{C}_{k+1}^\perp + p^{r-k-1}\mathbb{Z}^n_{p^r}((D))) \\ &= \sum_{i=0}^{k+1}[(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{k+1-i})^\perp \cap p^i\mathbb{Z}^n_{p^r}((D)).\end{aligned}$$

□

Lemma 8. *Let $\mathcal{C}$ be a convolutional code of length n and let $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{r-1}$ be free convolutional codes such that $\mathcal{C} = \mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1}$ with*

$$\mathcal{C}_0 + \mathcal{C}_1 + \ldots + \mathcal{C}_{r-1} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \ldots \oplus \mathcal{C}_{r-1}.$$

Then,

$$\mathcal{C}^\perp = (\mathcal{C}_0 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + p(\mathcal{C}_0 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp + \cdots + p^{r-2}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp + p^{r-1}\mathcal{C}_0^\perp. \qquad (6)$$

Proof. ($\supset$) We shall show that each term of the form $p^{r-i}(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^\perp$ on the right-hand side of (6) is contained in $\mathcal{C}^\perp$, for $i = 1, 2, \ldots, r$. First note that

$$p^{r-i}(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^\perp \subset (p^i\mathcal{C}_i)^\perp \cap \cdots \cap (p^{r-1}\mathcal{C}_{r-1})^\perp$$

and since, obviously,

$$p^{r-i}(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^\perp \subset (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^\perp \subset (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \cdots \oplus p^{i-1}\mathcal{C}_{i-1})^\perp$$

the result follows.
($\subset$) On the other hand, let $w(D) \in \mathcal{C}^\perp = (\mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \ldots \oplus p^{r-1}\mathcal{C}_{r-1})^\perp$. Then, using Lemma 7 we get

$$\begin{aligned} w(D) \in (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + [(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp \cap p\mathbb{Z}_{p^r}^n((D))] + \\ + [(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-3})^\perp \cap p^2\mathbb{Z}_{p^r}^n((D))] + \cdots + [\mathcal{C}_0^\perp \cap p^{r-1}\mathbb{Z}_{p^r}^n((D))]. \end{aligned}$$

Finally, by equation 1,

$$w(D) \in (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + p(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp + p^2(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-3})^\perp + \cdots + p^{r-1}\mathcal{C}_0^\perp.$$

□

Next we present our main result that fully characterizes the structure of $\mathcal{C}^\perp$ as direct summand of some submodules which are given in terms of the free $\mathcal{C}_i$ derived in Theorem 1.

Theorem 2. *Let $\mathcal{C}$ be a convolutional code of length n and let $\mathcal{C}_0, \mathcal{C}_1, \cdots, \mathcal{C}_{r-1}$ be free convolutional codes such that $\mathcal{C} = \mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \cdots \oplus p^{r-1}\mathcal{C}_{r-1}$ with*

$$\mathcal{C}_0 + \mathcal{C}_1 + \cdots + \mathcal{C}_{r-1} = \mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1},$$

and let B_{r-i} be a free convolutional code such that

$$(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^\perp = (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1} \oplus \mathcal{C}_i)^\perp \oplus B_{r-i}, \qquad (7)$$

$i = 1, \ldots, r-1$, *and* $B_0 = (\mathcal{C}_0 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp$. *Then,*

$$\mathcal{C}^\perp = B_0 \oplus pB_1 \oplus \cdots \oplus p^{r-1}B_{r-1}.$$

Proof. First note that the existence of such free B_i's follows from previous results in Section 3 as the dual of a free code is free. Since all the modules in (7) are free we can apply equation 2 to obtain that

$$p^j(\mathcal{C}_0 \oplus \cdots \oplus \mathcal{C}_{i-1})^\perp = p^j(\mathcal{C}_0 \oplus \cdots \oplus \mathcal{C}_i)^\perp \oplus p^j B_{r-i} \tag{8}$$

for all $j \in \{0, 1, \ldots, r-1\}$.
By Lemma 8 we have that

$$\begin{aligned} \mathcal{C}^\perp &= (\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-1})^\perp + p(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{r-2})^\perp + \\ &\quad + \cdots + p^{r-3}(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \mathcal{C}_2)^\perp + p^{r-2}(\mathcal{C}_0 \oplus \mathcal{C}_1)^\perp + p^{r-1}\mathcal{C}_0^\perp \end{aligned} \tag{9}$$

Using (8) for each term of (9) we get that

$$\mathcal{C}^\perp = B_0 + pB_1 + p^2B_2 + \cdots + p^{r-1}B_{r-1}.$$

It remains to show that

$$B_0 + pB_1 + p^2B_2 + \cdots + p^{r-1}B_{r-1} = B_0 \oplus pB_1 \oplus p^2B_2 \oplus \cdots \oplus p^{r-1}B_{r-1}. \tag{10}$$

Using recursively equation (7) it is easy to verify that

$$\mathcal{C}_0^\perp = B_0 \oplus B_1 \oplus B_2 \oplus \cdots \oplus B_{r-1}.$$

Thus,

$$B_j \cap \sum_{\substack{i=1 \\ i \neq j}}^{r-1} B_i = \{0\},$$

$j = \{0, 1, \ldots, r-1\}$. Since $p^jB_j \subset B_j$ we have that

$$p^jB_j \cap \sum_{\substack{i=1 \\ i \neq j}}^{r-1} p^iB_i = \{0\}$$

which proves (10). □

Next theorem shows that all convolutional codes admit parity-check matrices.

Theorem 3. *Let $\mathcal{C}$ be a convolutional code of length n and $H(D)$ be a generator matrix of $\mathcal{C}^{\perp}$. Then, for $w(D) \in \mathbb{Z}_{p^r}^n((D))$,*

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

Proof. See Appendix. □

Corollary 1. *Let $\mathcal{C}$ be a convolutional code. Then, $\mathcal{C} = (\mathcal{C}^{\perp})^{\perp}$.*

3.3. An algorithm for building a generator matrix of $\mathcal{C}^{\perp}$

We are now in position to present a constructive algorithm that produce a generator matrix of the dual of a given convolutional code $\mathcal{C} = \operatorname{Im}_{\mathbb{Z}_{p^r}((D))} G(D)$. First we treat the case where $\overline{G(D)}$ is not the zero matrix. At the end of the section we indicate how to proceed in the other case.

Step 1: Find $G_i(D)$, $i = 0, \dots, r-1$ such that

$$G(D) = \begin{bmatrix} G_0(D) \\ pG_1(D) \\ \vdots \\ p^{r-1}G_{r-1}(D) \end{bmatrix}, \text{ with } \widehat{G}(D) = \begin{bmatrix} G_0(D) \\ G_1(D) \\ \vdots \\ G_{r-1}(D) \end{bmatrix} \text{ full row rank.} \qquad (11)$$

This is possible due to Theorem 1, where $\mathcal{C} = \mathcal{C}_0 \oplus p\mathcal{C}_1 \oplus \dots \oplus p^{r-1}\mathcal{C}_{r-1}$, $\mathcal{C}_i = \operatorname{Im} G_i(D)$, with $G_i(D) \in \mathbb{Z}_{p^r}^{k_i \times n}[D]$ and $\sum_{i=0}^{r-1} k_i = k$, $i = 0, \dots, r-1$. Details on how one can effectively compute $G(D)$ and $\widehat{G}(D)$ as in (11) can be found in [16, 3].

Step 2: Compute $H_i(D)$ such that the following holds:

$$\begin{bmatrix} G_0(D) \\ G_1(D) \\ \vdots \\ G_{r-(i+1)}(D) \end{bmatrix} \begin{bmatrix} H_i^T(D) & H_{i-1}^T(D) & \dots & H_0^T(D) \end{bmatrix} = 0.$$

To compute them we use that

$$\begin{bmatrix} G_0(D) \\ G_1(D) \\ \vdots \\ G_{r-1}(D) \end{bmatrix}$$

is full row rank and then, we can construct an $n \times n$ invertible matrix

$$\begin{bmatrix} G_0(D) \\ G_1(D) \\ \vdots \\ G_{r-1}(D) \\ N(D) \end{bmatrix},$$

with $N(D) \in \mathbb{Z}_{p^r}^{(n-k)\times n}[D]$, such that

$$\begin{bmatrix} G_0(D) \\ G_1(D) \\ \vdots \\ G_{r-1}(D) \\ N(D) \end{bmatrix} \begin{bmatrix} L^T(D) & H_{r-1}^T(D) & H_{r-2}^T(D) & \dots & H_0^T(D) \end{bmatrix} = P(D),$$

with $H_0(D) \in \mathbb{Z}_{p^r}^{(n-\sum_{i=0}^{r-1} k_i)\times n}[D]$, $H_i(D) \in \mathbb{Z}_{p^r}^{k_{r-i}\times n}[D]$, $i = 1, \dots, r-1$, $L(D) \in \mathbb{Z}_{p^r}^{k_0\times n}[D]$, $i = 0, \dots, r-1$, and

$$P(D) = \begin{bmatrix} p_1(D) & & & \\ & p_2(D) & & \\ & & \ddots & \\ & & & p_n(D) \end{bmatrix},$$

where $p_i(D)$ are nonzero polynomials with coefficients in $\mathbb{Z}_{p^r}$.

Step 3: The output gives

$$H(D) = \begin{bmatrix} H_0(D) \\ pH_1(D) \\ \vdots \\ p^{r-1}H_{r-1}(D) \end{bmatrix}$$

which is a generator matrix of $\mathcal{C}^\perp$.

Note that $[H_i(D) \cdots H_0(D)]$ is a generator matrix of $(\mathcal{C}_0 \oplus \mathcal{C}_{r-1-i})^\perp$, $i = 0, \dots r-1$. Then, by Theorem 2, it follows that $B_i = \operatorname{Im} H_i(D)$, for $i = 0, \dots, r-1$ are such that

$$\mathcal{C}^\perp = B_0 \oplus pB_1 \oplus \dots \oplus p^{r-1}B_{r-1},$$

and therefore by Theorem 3 we conclude that $H^T(D)$ is a parity-check matrix of $\mathcal{C}$.

Consider now the case in which the generator matrix $G(D)$ of $\mathcal{C}$ is such that $\overline{G(D)}$ is the zero matrix. Applying Lemma 7 it follows that we can write $G(D) = p^i\widehat{G}(D)$ with $\widehat{G}(D)$ satisfying the conditions of the first case, *i.e.*, $\overline{G(D)} \neq 0$. Thus, applying the algorithm for $\widehat{G}(D)$ we obtain the parity-check matrix $\widehat{H}(D)$ of $\operatorname{Im}_{\mathbb{Z}_{p^r}((D))}\widehat{G}(D)$ and therefore a generator matrix for $\mathcal{C}^\perp$ is given by

$$H(D) = \begin{bmatrix} \widehat{H}(D) \\ p^{r-i}I_n(D) \end{bmatrix}.$$

We present two examples to illustrate the procedure described above for the two cases considered.

Example 2. *Consider the convolutional code $\mathcal{C}$ defined in $\mathbb{Z}_9((D))$ with generator matrix*

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

Thus,

$$\mathcal{C} = \mathcal{C}_0 \oplus 3\mathcal{C}_1$$

where $\mathcal{C}_0 = \operatorname{Im}_{\mathbb{Z}_9((D))}G_0(D)$ and $\mathcal{C}_1 = \operatorname{Im}_{\mathbb{Z}_9((D))}G_1(D)$, with $G_0(D) = \begin{bmatrix} 1+D & 1 & 3D \end{bmatrix}$ and $G_1(D) = \begin{bmatrix} 0 & 1+D & 1+D \end{bmatrix}$.
Since

$$\begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1+7D+6D^2 \\ 1+D & 6D & 8+7D+8D^2 \\ 8+8D & 1 & 1+2D+D^2 \end{bmatrix} = P(D),$$

with

$$P(D) = \begin{bmatrix} 1+7D+6D^2 & 0 & 0 \\ 0 & 1+7D+6D^2 & 0 \\ 0 & 0 & 1+7D+6D^2 \end{bmatrix},$$

$H_0(D) = \begin{bmatrix} 1+7D+6D^2 & 8+7D+8D^2 & 1+2D+D^2 \end{bmatrix}$ and $H_1(D) = \begin{bmatrix} 0 & 6D & 1 \end{bmatrix}$, are such that

$$H(D) = \begin{bmatrix} H_0(D) \\ 3H_1(D) \end{bmatrix} = \begin{bmatrix} 1+7D+6D^2 & 8+7D+8D^2 & 1+2D+D^2 \\ 0 & 0 & 3 \end{bmatrix}$$

is a generator matrix of $\mathcal{C}^\perp$ and

$$w(D) \in \mathcal{C} \Leftrightarrow w(D) \begin{bmatrix} 1+7D+6D^2 & 0 \\ 8+7D+8D^2 & 0 \\ 1+2D+D^2 & 3 \end{bmatrix} = 0.$$

The following example is very similar to Example 2 but it was modified to illustrate better how to proceed for the second case.

Example 3. *Consider the convolutional code $\mathcal{C}$ defined in $\mathbb{Z}_{27}((D))$ with generator matrix*

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

Write $G(D) = 3\widehat{G}(D)$ and

$$\mathcal{C} = 3\mathcal{C}_0 \oplus 9\mathcal{C}_1$$

where $\mathcal{C}_0 = \mathrm{Im}_{\mathbb{Z}_{27}((D))}\hat{G}_0(D)$ and $\mathcal{C}_1 = \mathrm{Im}_{\mathbb{Z}_{27}((D))}\hat{G}_1(D)$, with $\hat{G}_0(D) = \begin{bmatrix} 1+D & 1 & 3D \end{bmatrix}$ and $\hat{G}_1(D) = \begin{bmatrix} 0 & 1+D & 1+D \end{bmatrix}$.
Since

$$\begin{bmatrix} 1+D & 1 & 3D \\ 0 & 1+D & 1+D \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1+25D+24D^2 \\ 1+D & 24D & 26+25D+26D^2 \\ 26+26D & 1 & 1+2D+D^2 \end{bmatrix} = P(D),$$

with

$$P(D) = \begin{bmatrix} 1+25D+24D^2 & 0 & 0 \\ 0 & 1+25D+24D^2 & 0 \\ 0 & 0 & 1+25D+24D^2 \end{bmatrix},$$

$H_0(D) = \begin{bmatrix} 1+25D+24D^2 & 26+25D+26D^2 & 1+2D+D^2 \end{bmatrix}$ and $H_1(D) = \begin{bmatrix} 0 & 24D & 1 \end{bmatrix}$, are such that

$$H(D) = \begin{bmatrix} H_0(D) \\ 3H_1(D) \\ 9I_3 \end{bmatrix}.$$

4. Appendix

Here we need to introduce an auxiliary lemma.

Lemma 9. *For $j \in \{0, 1, \ldots, r-1\}$ it holds that*

$$[w(D) \in \cap_{i=0}^{j}(B_i^\perp + p^{r-i}\mathbb{Z}_{p^r}^n((D)))] \Longrightarrow [w(D) \in (\bigoplus_{i=0}^{j} B_i)^\perp + \sum_{k=0}^{j-1} p^{r-k-1}(\bigoplus_{s=0}^{k} B_s)^\perp]. \quad (12)$$

Proof of the Auxiliary Lemma 9: We shall prove it using induction. Consider $j = 1$ and $w(D) \in B_0^\perp \cap [B_1^\perp + p^{r-1}\mathbb{Z}_{p^r}^n((D))]$. By Lemma 4 it follows that

$$w(D) \in (B_0^\perp \cap B_1^\perp) + p^{r-1}B_0^\perp = (B_0 \oplus B_1)^\perp + p^{r-1}B_0^\perp.$$

Now assume the statement holds for $j-1$. We shall prove it holds for j. Consider

$$w(D) \in \cap_{i=0}^{j}(B_i^\perp + p^{r-i}\mathbb{Z}_{p^r}^n((D))) = [\cap_{i=0}^{j-1}(B_i^\perp + p^{r-i}\mathbb{Z}_{p^r}^n((D)))] \cap [B_j^\perp + p^{r-j}\mathbb{Z}_{p^r}^n((D))].$$

Using the assumption and then multiplying $w(D)$ by p^{j-1} the last term of (12) vanishes and we get that

$$p^{j-1}w(D) \in p^{j-1}(\bigoplus_{i=0}^{j-1} B_i)^\perp \cap [p^{j-1}B_j^\perp + p^{r-1}\mathbb{Z}_{p^r}^n((D))].$$

Again we use Lemma 4 to conclude that

$$p^{j-1}w(D) \in p^{j-1}(\bigoplus_{i=0}^{j-1} B_i^\perp \cap B_j^\perp) + p^{r-1}(\bigoplus_{i=0}^{j-1} B_i)^\perp = p^{j-1}(\bigoplus_{i=0}^{j} B_i)^\perp + p^{r-1}(\bigoplus_{i=0}^{j-1} B_i)^\perp,$$

which implies that

$$w(D) \in (\bigoplus_{i=0}^{j} B_i)^\perp + p^{r-j}(\bigoplus_{i=0}^{j-1} B_i)^\perp + \sum_{k=0}^{j-2} p^{r-k-1}(\bigoplus_{s=0}^{k} B_s)^\perp = (\bigoplus_{i=0}^{j} B_i)^\perp + \sum_{k=0}^{j-1} p^{r-k-1}(\bigoplus_{s=0}^{k} B_s)^\perp.$$

This completes the proof.
Proof of Theorem 3: We have to show that $\mathcal{C} = \operatorname{Ker} H^T(D)$. The proof of $(\subset)$ is obvious as $H(D)$ is the generator matrix of $\mathcal{C}^\perp$.
$(\supset)$: Let $\mathcal{C}^\perp = B_0 \oplus pB_1 \oplus \ldots \oplus p^{r-1}B_{r-1}$ as in Theorem 2 and write

$$H(D) = \begin{bmatrix} H_0(D) \\ pH_1(D) \\ \vdots \\ p^{r-1}H_{r-1}(D) \end{bmatrix} \tag{13}$$

where $H_i(D)$ is an encoder of B_i, $i = 0, \ldots, r-1$. Let $w(D) \in \mathbb{Z}_{p^r}^n((D))$ be such that $w(D)H^T(D) = 0$, *i.e.*, $p^i w(D)H_i^T(D) = 0$, for $i = 0, \ldots, r-1$, which amounts to saying that

$$w(D) \in \cap_{i=0}^{r-1}(B_i^\perp + p^{r-i}\mathbb{Z}_{p^r}^n((D))). \tag{14}$$

Applying Lemma 9 in (14) for $j = r-1$ we immediately obtain that

$$w(D) \in (\bigoplus_{i=0}^{r-1} B_i)^\perp + \sum_{k=0}^{r-2} p^{r-k-1}(\bigoplus_{s=0}^{k} B_s)^\perp. \tag{15}$$

On the other hand, in the light of the relation (7) we can readily obtain the following relation

$$(\mathcal{C}_0 \oplus \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_{i-1})^\perp = B_0 \oplus B_1 \oplus \cdots \oplus B_{r-i}.$$

Finally, applying these equalities in (15) we get that

$$w(D) \quad \in \quad \mathcal{C}_0 + \sum_{k=0}^{r-2} p^{r-k-1}(\bigoplus_{s=0}^{r-k-1} \mathcal{C}_s) = \mathcal{C}_0 + \sum_{k=0}^{r-2} p^{r-k-1}\mathcal{C}_{r-k-1}) = \bigoplus_{i=0}^{r-1} p^i\mathcal{C}_i = \mathcal{C},$$

which concludes the proof.

Finally, let $\tilde{H}(D)$ be any generator matrix of $\mathcal{C}^{\perp}$ (not necessarily in the form of (13)). Then, since

$$\tilde{H}(D) = X(D)H(D) \text{ and } H(D) = Y(D)\tilde{H}(D),$$

for some matrices $X(D)$ and $Y(D)$ in $\mathbb{Z}_{p^r}((D))$, it follows that

$$w(D) \in \mathcal{C} \Leftrightarrow w(D)\tilde{H}^T(D) = 0,$$

i.e., the transposes of the generator matrices of $\mathcal{C}^{\perp}$ are parity-check matrices of $\mathcal{C}$.

ACKNOWLEDGMENT

We would like to thank the Reviewer for the useful comments and suggestions. This work was supported by the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UID/MAT/04106/2013.

[1] Caire, G., Biglieri, E., Sep 1995. Linear block codes over cyclic groups. IEEE Transactions on Information Theory 41 (5), 1246–1256.

[2] Cardell, S. D., Fuster-Sabater, A., 2017. Discrete linear models for the generalized self-shrunken sequences. Finite Fields and Their Applications 47 (Supplement C), 222 – 241.

[3] El Oued, M., Napp, D., Pinto, R., Toste, M., 2017. 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.

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

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

[6] Forney, G., 1970. Convolutional Codes I: Algebraic Structure. IEEE Trans. Inform. Theory 16, 720–738, correction, Ibid., IT-17,pp. 360, 1971.

[7] Forney, G., 1973. Structural Analysis of Convolutional Codes via Dual Codes. IEEE Trans. Inform. Theory 19, 512–518.

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

[9] Johannesson, R., Wan, Z., Wittenmark, E., 1998. Some structural properties of convolutional codes over rings. IEEE Trans. Inform. Theory 44 (2), 839–845.

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

[11] Lang, S., 2002. Algebra. Graduate Texts in Mathematics, Series Volume 211. Springer-Verlag, New York.

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

[13] McEliece, R., 1977. The Theory of Information and Coding. Encyclopedia of Mathematics and Its Applications volume 3.

[14] Napp, D., Pinto, R., Toste, M., 2017. Column distances of convolutional codes over $\mathbb{Z}_{p^r}$. submitted (http://arxiv.org/abs/1708.00336).

[15] Oued, M. E., Sole, P., 2013. MDS convolutional codes over a finite ring. IEEE Trans. Inf. Th. 59 (11), 7305 – 7313.

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