Finite Fields and Their Applications 72 (2021) 101815

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

List decoding of convolutional codes over integer residue rings

Julia Lieb [a,*], Diego Napp [b], Raquel Pinto [c]

[a] *Department of Mathematics, University of Zurich, Switzerland*
[b] *Department of Mathematics, University of Alicante, Spain*
[c] *CIDMA - Center for Research and Development in Mathematics and Applications, Department of Mathematics, University of Aveiro, Portugal*

ARTICLE INFO

Article history:
Received 8 September 2020
Received in revised form 19 January 2021
Accepted 22 January 2021
Available online 9 February 2021
Communicated by W. Cary Huffman

MSC:
11T71
94B10
94B35

Keywords:
Convolutional codes
Finite rings
Erasure channel

ABSTRACT

A convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}[D]$ is a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$ where $\mathbb{Z}_{p^r}[D]$ stands for the ring of polynomials with coefficients in $\mathbb{Z}_{p^r}$. In this paper, we study the list decoding problem of these codes when the transmission is performed over an erasure channel, that is, we study how much information one can recover from a codeword $w \in \mathcal{C}$ when some of its coefficients have been erased. We do that using the p-adic expansion of w and particular representations of the parity-check polynomial matrix of the code. From these matrix polynomial representations we recursively select certain equations that w must satisfy and have only coefficients in the field $p^{r-1}\mathbb{Z}_{p^r}$. We exploit the natural block Toeplitz structure of the sliding parity-check matrix to derive a step by step methodology to obtain a list of possible codewords for a given corrupted codeword w, that is, a list with the closest codewords to w.

* Corresponding author.
E-mail addresses: julia.lieb@math.uzh.ch (J. Lieb), diego.napp@ua.es (D. Napp), raquel@ua.pt (R. Pinto).

https://doi.org/10.1016/j.ffa.2021.101815

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 [3]). 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 mathematical theory of convolutional codes over finite fields is much developed and has produced many sophisticated classes of codes. On the other hand, very little is known about concrete optimal constructions of convolutional codes over finite rings. In any case, the decoding of these codes is, in general, not easy. Probably the most prominent decoding algorithm is the Viterbi algorithm but its use is limited as its complexity grows exponentially with the size of the memory of the code. However, in [24] it was shown that the decoding of convolutional codes over finite fields requires only linear algebra when they are used over the erasure channel, *i.e.*, when the positions of the errors are known. Despite the fact that convolutional codes that possess optimal erasure correcting capabilities require large finite fields, the results in [24] allow to implement these codes in many practical situations and therefore attracted the interest of many researchers, see for instance [14] and references therein.

Following this thread of research and aiming to extend these results over finite fields to the context of finite rings, we consider in this paper convolutional codes $\mathcal{C}$ over $\mathbb{Z}_{p^r}[D]$ and study the erasure correcting capabilities of these codes over the erasure channel. The extension of the concept of convolutional codes from finite fields to finite rings was first introduced by Massey and Mittelholzer [16], in 1989, and since then has attracted a lot of attention [4,7,11,10,18,21,22]. This interest is due to the discovery that the most appropriate codes for phase modulation are the linear codes over the residue class ring $\mathbb{Z}_M$, M a positive integer. It was immediately apparent that convolutional codes over $\mathbb{Z}_M$ behave very differently from convolutional codes over finite fields. For instance, in contrast with the field case, convolutional codes over $\mathbb{Z}_M$ are not necessarily free modules. We focus on the ring $\mathbb{Z}_{p^r}$ as, obviously, by the Chinese Remainder Theorem, results on codes over $\mathbb{Z}_{p^r}$ can be extended to codes over $\mathbb{Z}_M$ [1].

In particular, our goal is to retrieve as much information as possible from the received corrupted vector. The decoder proposed in this work is a maximum likelihood algebraic decoder and follows succinctly two main steps. Firstly, it searches for unique decoding, *i.e.*, when there exists a unique most likely word, then, the decoder outputs such a word. When this is not possible the algorithm performs a list decoding algorithm, *i.e.*, it computes a complete list of the most likely codewords for a given corrupted codeword.

For this problem, we shall use the parity-check matrix $H(D)$ of $\mathcal{C}$ in a particular form. Then, the number of independent columns of specific submatrices of $H(D)$ will determine the size of the list of possible codewords in the algorithm. Considering the erasures as unknowns to-be-determined, the decoding problem treated here amounts to solving a system of linear equations over $\mathbb{Z}_{p^r}$. The idea we used in this work is to multiply a selected subset of these equations by a power of p in such a way that we

obtain equations with coefficients in the field $p^{r-1}\mathbb{Z}_{p^r}$, isomorphic to $\mathbb{Z}_p$, and therefore we can easily compute the unknowns. Once we know some of the coefficients we can select another set of equations and apply the same ideas to these equations to recover another set of erased symbols. In this way we develop a systematic recursive procedure to recover all possible erasures that could have occurred. This, in turn, provides with a list with the closest codewords to the received information vector.

The outline of this paper is as follows. In Section 2, we present basic results on convolutional codes over the finite ring $\mathbb{Z}_{p^r}$, in particular about their parity-check matrices, which are important for decoding over the erasure channel. In Section 3, we present our erasure decoding algorithm for convolutional codes over $\mathbb{Z}_{p^r}$ and illustrate it with an example. Finally, we conclude with analyzing the complexity of our algorithm in Section 4.

2. Preliminary results

In this section we present the elementary background required in the paper. Let $\mathbb{Z}_{p^r}[D]$ denote the ring of polynomials with coefficients in $\mathbb{Z}_{p^r}$ and let $\mathcal{A} = \{0, 1, 2, \ldots, p-1\}$ be the set of **digits**. We say that $v(D)$ has **order** s, denoted by $\mathrm{ord}(v(D)) = s$, if $p^{s-1}v(D) \neq 0$ and $p^{s-1}v(D) \in p^{r-1}\mathbb{Z}_{p^r}^{\ell}[D]$. Every element in $v(D) \in \mathbb{Z}_{p^r}^{\ell}[D]$ admits a unique p-adic expansion as $v(D) = a_0(D) + a_1(D)p + \cdots + a_{r-1}(D)p^{r-1}$, with $a_i(D) \in \mathcal{A}[D]$, $\mathrm{ord}(a_i(D)) = r-1$ and $i = 0, 1, \ldots, r-1$. We shall extensively use that $p^{r-1}\mathbb{Z}_{p^r}$ is isomorphic to the field $\mathbb{Z}_p$ in our algorithms.

Definition 1. [6,8,22] A **convolutional code** $\mathcal{C}$ of length n is a $\mathbb{Z}_{p^r}[D]$-submodule of $\mathbb{Z}_{p^r}^n[D]$. A polynomial matrix $G(D) \in \mathbb{Z}_{p^r}^{k\times n}[D]$ such that

$$\mathcal{C} = \left\{ G(D)^T u(D) \in \mathbb{Z}_{p^r}^n[D] : \, u(D) \in \mathbb{Z}_{p^r}^k[D] \right\}$$

is called **generator matrix** of the code.

A polynomial matrix $H(D)$ is a **parity-check matrix** (or syndrome former) of a convolutional code $\mathcal{C}$ if $\mathcal{C} = \mathrm{Ker}_{\mathbb{Z}_{p^r}[D]} H(D)$, *i.e.*, for every $w(D) \in \mathbb{Z}_{p^r}^n[D]$,

$$w(D) \in \mathcal{C} \Leftrightarrow H(D)w(D) = 0. \tag{1}$$

Definition 2. Let R be a ring with identity and $U(D) \in R[D]^{n\times n}$. Then $U(D)$ is called **unimodular** if there exists $V(D) \in R[D]^{n\times n}$ such that $U(D)V(D) = V(D)U(D) = I_n$.

For any matrix A with entries in $\mathbb{Z}_{p^r}$ or $\mathbb{Z}_{p^r}[D]$, we denote by $[A]_p$ the (componentwise) projection of A into $\mathbb{Z}_p$.

Lemma 1. *[13] Let $U(D) \in \mathbb{Z}_{p^r}[D]^{n\times n}$. Then $U(D)$ is unimodular (over $\mathbb{Z}_{p^r}[D]$) if and only if $[U(D)]_p$ is unimodular (over $\mathbb{Z}_p[D]$).*

Definition 3. Let $\mathbb{F}$ be a finite field. A polynomial matrix $P(D) \in \mathbb{F}[D]^{k\times n}$ with $k \leq n$ is **left prime** if in all factorizations $P(D) = \Delta(D)\bar{P}(D)$ with $\Delta(D) \in \mathbb{F}[D]^{k\times k}$ and $\bar{P}(D) \in \mathbb{F}[D]^{k\times n}$, the left factor $\Delta(D)$ is unimodular.

Lemma 2. *[12] Let $P(D) \in \mathbb{Z}_p[D]^{k\times n}$ with $k \leq n$. Then, the following conditions are equivalent:*

(i) $P(D)$ is left prime.

(ii) There exists $N(D) \in \mathbb{Z}_p[D]^{(n-k)\times k}$ such that $\begin{pmatrix} P(D) \\ N(D) \end{pmatrix}$ is unimodular.

(iii) $u(D)P(D) \in \mathbb{Z}_{p^r}^n[D] \Rightarrow u(D) \in \mathbb{Z}_{p^r}^k[D]$, for all $u(D) \in \mathbb{Z}_{p^r}^k(D)$, where $\mathbb{Z}_{p^r}(D)$ denotes the ring of rational functions with coefficients in $\mathbb{Z}_{p^r}$.

The next result follows immediately from Lemma 1 and Lemma 2.

Corollary 1. *Let $P(D) \in \mathbb{Z}_{p^r}[D]^{k\times n}$ with $k \leq n$. Then $[P(D)]_p$ is left prime over $\mathbb{Z}_p[D]$ if and only if there exists $N(D) \in \mathbb{Z}_{p^r}[D]^{(n-k)\times k}$ such that $\begin{pmatrix} P(D) \\ N(D) \end{pmatrix}$ is unimodular.*

If $\mathcal{C}$ is a convolutional code that admits a parity-check matrix, then a parity-check matrix of $\mathcal{C}$ can be constructed as follows (for more details see [21]): Let $\hat{G}(D) \in \mathbb{Z}_{p^r}[D]^{\hat{k}\times n}$ be a generator matrix of $\mathcal{C}$ and consider

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

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

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

where the coefficients a_i are in $\mathbb{Z}_{p^r}$ and only finitely coefficients with negative indices may be nonzero. Note that $\mathcal{C} = \hat{\mathcal{C}} \cap \mathbb{Z}_{p^r}[D]^n$. Then, there exists

$$G(D) = \begin{bmatrix} G_0(D) \\ pG_1(D) \\ \vdots \\ p^{r-1}G_{r-1}(D) \end{bmatrix}, \ G_i(D) \in \mathbb{Z}_{p^r}[D]^{k_i\times n} \text{ for } i = 0, \ldots, r-1 \tag{2}$$

with $\mathcal{G} = \begin{bmatrix} G_0(D) \\ G_1(D) \\ \vdots \\ G_{r-1}(D) \end{bmatrix}_p$ full row rank over $\mathbb{Z}_p[D]$ such that

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

where $k = k_0 + k_1 + \cdots + k_{r-1}$. A procedure to obtain $G(D)$ in this particular form is described in [21, Theorem 1]. A parity-check matrix of $\hat{C}$ can be determined as follows Consider the generator matrix $G(D)$ defined in (2) and let $N(D) \in \mathbb{Z}_{p^r}[D]^{(n-k)\times n}$ such that

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

is unimodular. Then, there exists $H_i(D) \in \mathbb{Z}_{p^r}[D]^{l_i \times n}$ where $l_0 = n - k$ and $l_i = k_{r-i}$, $i = 1, 2, \ldots, r-1$, and $L(D) \in \mathbb{Z}_{p^r}[D]^{k_0 \times n}$ such that

$$\begin{pmatrix} L(D) \\ H_{r-1}(D) \\ H_{r-2}(D) \\ \vdots \\ H_1(D) \\ H_0(D) \end{pmatrix} [G_0(D)^\top \ G_1(D)^\top \ \ldots \ G_{r-1}(D)^\top \ N(D)^\top] = P(D) \tag{3}$$

for some

$$P(D) = \begin{bmatrix} \gamma_1(D) & & & \\ & \gamma_2(D) & & \\ & & \ddots & \\ & & & \gamma_n(D) \end{bmatrix},$$

where $\gamma_i(D)$ are nonzero polynomials in $\mathbb{Z}_{p^r}[D]$. Then,

$$H(D) = \begin{bmatrix} H_0(D) \\ pH_1(D) \\ \vdots \\ p^{r-1}H_{r-1}(D) \end{bmatrix}, \ H_i(D) \in \mathbb{Z}_{p^r}[D]^{l_i \times n}, \ l_i = k_{r-i}, \text{ for } i = 1, \ldots, r-1, \ l_0 = n-k$$

with $\mathcal{H} = \begin{bmatrix} H_0(D) \\ H_1(D) \\ \vdots \\ H_{r-1}(D) \end{bmatrix}_p$ full row rank over $\mathbb{Z}_p[D]$, such that

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

More details can be found in [21]. Then,

$$\hat{\mathcal{C}} = \{w(D) \in \mathbb{Z}_{p^r}((D))^n : \ H(D)w(D) = 0\},$$

and consequently,

$$\mathcal{C} = \operatorname{Ker}_{\mathbb{Z}_{p^r}[D]} H(D),$$

which means that $H(D)$ is a parity-check matrix of $\mathcal{C}$.

However, not all convolutional codes admit a parity-check matrix as the following example shows.

Example 1. Let $G(D) = \begin{bmatrix} 1+D & 1+D & 1+D \\ 3 & 3 & 0 \end{bmatrix} \in \mathbb{Z}_9[D]^{2\times 3}$ and $\mathcal{C}$ be the convolutional code with generator matrix $G(D)$. Let us assume that $\mathcal{C}$ admits a parity-check matrix $H(D)$. Then, since $w(D) = [1+D \quad 1+D \quad 1+D]^\top \in \mathcal{C}$, it follows that $H(D)w(D) = 0$. Then, $(1+D)H(D)\begin{pmatrix}1\\1\\1\end{pmatrix} = 0$ and therefore, $H(D)\begin{pmatrix}1\\1\\1\end{pmatrix} = 0$. This means that $\begin{pmatrix}1\\1\\1\end{pmatrix} \in \mathcal{C}$, which is not true.

However, in the case that a convolutional code does not admit a parity-check matrix, the procedure above constructs a matrix $H(D)$ such that $\mathcal{C} \subset \operatorname{Ker}_{\mathbb{Z}_{p^r}[D]} H(D)$ because $\mathcal{C} \subset \hat{\mathcal{C}}$.

If a convolutional code $\mathcal{C}$ admits a parity-check matrix, it is called **observable** or **non-catastrophic**. The characterization of the non-catastrophic convolutional codes over $\mathbb{Z}_{p^r}[D]$ is still an open problem. However, for a certain class of convolutional codes, the following lemma characterizes the non-catastrophic codes.

Lemma 3. *Let $\mathcal{C}$ be a convolutional code of length n that admits a generator matrix $G(D)$ of the form*

$$G(D) = \begin{bmatrix} G_0(D) \\ pG_1(D) \\ \vdots \\ p^{r-1}G_{r-1}(D) \end{bmatrix}, \ G_i(D) \in \mathbb{Z}_{p^r}[D]^{k_i \times n} \text{ for } i = 0, \ldots, r-1 \tag{4}$$

such that

$$\mathcal{G} = \begin{bmatrix} G_0(D) \\ G_1(D) \\ \vdots \\ G_{r-1}(D) \end{bmatrix}_p \tag{5}$$

is full row rank over $\mathbb{Z}_p[D]$. Then, $\mathcal{C}$ admits a parity-check matrix if and only if $\mathcal{G}$ is left prime over $\mathbb{Z}_p[D]$.

Proof. Take $k = k_0 + k_1 + \cdots + k_{r-1}$ and let us assume that $G(D)$ is such that $\mathcal{G}$ is left prime over $\mathbb{Z}_p[D]$. Then, by Corollary 1, there exists $N(D) \in \mathbb{Z}_{p^r}[D]^{(n-k)\times n}$ such that

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

is unimodular. Then

$$\begin{pmatrix} L(D) \\ H_{r-1}(D) \\ H_{r-2}(D) \\ \vdots \\ H_1(D) \\ H_0(D) \end{pmatrix} [G_0(D)^\top \; G_1(D)^\top \; \ldots \; G_{r-1}(D)^\top \; N(D)^\top] = I \tag{6}$$

for some $H_i(D) \in \mathbb{Z}_{p^r}[D]^{l_i \times n}$ where $l_0 = n - k$ and $l_i = k_{r-i}$, $i = 1, 2, \ldots, r-1$, and $L(D) \in \mathbb{Z}_{p^r}[D]^{k_0 \times n}$. Let us define

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

By Corollary 1 we have that

$$\mathcal{H} = \begin{bmatrix} H_0(D) \\ H_1(D) \\ \vdots \\ H_{r-1}(D) \end{bmatrix}_p$$

is left prime over $\mathbb{Z}_p[D]$. Expression (6) also implies that

$$H(D)G(D)^\top = 0. \tag{7}$$

Let us prove that $\mathcal{C} = \operatorname{Ker}_{\mathbb{Z}_{p^r}[D]} H(D)$. Expression (7) shows that $\mathcal{C} \subset \operatorname{Ker}_{\mathbb{Z}_{p^r}[D]} H(D)$. To prove the other inclusion, let us consider that $w(D) \in \operatorname{Ker}_{\mathbb{Z}_{p^r}[D]} H(D)$, i.e., $w(D) \in \mathbb{Z}_{p^r}[D]$ is such that

$$\begin{pmatrix} H_0(D) \\ pH_1(D) \\ \vdots \\ p^{r-1}H_{r-1}(D) \end{pmatrix} w(D) = 0.$$

Then

$$H_i(D)w(D) = p^{r-i}v_i(D)$$

for some $v_i(D) \in \mathbb{Z}_{p^r}[D]^{l_i}$, $i = 0, 1, \ldots, r-1$. Since, by (6),

$$w(D) = [G_0(D)^\top \; G_1(D)^\top \; \cdots \; G_{r-1}(D)^\top \; N(D)^\top] \begin{bmatrix} L(D) \\ H_{r-1}(D) \\ H_{r-2}(D) \\ \vdots \\ H_1(D) \\ H_0(D) \end{bmatrix} w(D),$$

it follows that

$$\begin{aligned} w(D) &= [G_0(D)^\top \; G_1(D)^\top \; \cdots \; G_{r-1}(D)^\top \; N(D)^\top] \begin{bmatrix} L(D)w(D) \\ pv_{r-1}(D) \\ p^2v_{r-2}(D) \\ \vdots \\ p^{r-1}v_1(D) \\ 0 \end{bmatrix} \\ &= G(D)^\top \begin{bmatrix} L(D)w(D) \\ v_{r-1}(D) \\ v_{r-2}(D) \\ \vdots \\ v_1(D) \end{bmatrix}, \end{aligned}$$

which means that $w(D) \in \mathcal{C}$. Thus, we conclude that $\mathcal{C} = \operatorname{Ker}_{\mathbb{Z}_{p^r}[D]} H(D)$, *i.e.*, $\mathcal{C}$ admits a parity-check matrix.

To show the converse, let us assume that $\mathcal{C}$ has a parity-check matrix $H(D)$ and let $\bar{w}(D) \in \mathbb{Z}_p^n[D]$ be such that

$$\bar{w}(D) = \mathcal{G}^\top \bar{u}(D),$$

for some $\bar{u}(D) \in \mathbb{Z}_p^k(D)$. Then,

$$p^{r-1}w(D) = \mathcal{G}^\top p^{r-1}u(D),$$

where $w(D) \in \mathbb{Z}_{p^r}^n[D]$ and $u(D) \in \mathbb{Z}_{p^r}^k(D)$ are such that $[w(D)]_p = \bar{w}(D)$ and $[u(D)]_p = \bar{u}(D)$. Therfore,

$$p^{r-1}w(D) = G(D)^\top u_1(D)$$

where

$$p^{r-1}u(D) = \begin{bmatrix} I_{k_0} & & & \\ & pI_{k_1} & & \\ & & \ddots & \\ & & & p^{r-1}I_{k_{r-1}} \end{bmatrix} u_1(D).$$

Consequently,

$$H(D)p^{r-1}w(D) = H(D)G(D)^\top u_1(D) = 0,$$

which means that $p^{r-1}w(D) \in \mathcal{C}$. Therfore $u_1(D) \in \mathbb{Z}_{p^r}^k[D]$ and hence, $\bar{u}(D) \in \mathbb{Z}_{p^r}^k[D]$. Thus, we conclude by Lemma 2 that $\mathcal{G}$ is left prime over $\mathbb{Z}_p[D]$. □

It is well-known that kernel representations are useful to detect errors introduced during transmission. If a word $w(D)$ is received after channel transmission, the existence of errors is checked by simple multiplication by $H(D)$: if $H(D)w(D) = 0$, it is assumed that no errors occurred. As Example 1 and Lemma 3 show, not all convolutional codes defined in $\mathbb{Z}_{p^r}[D]$ admit a parity-check matrix. Nevertheless we showed that there always exists a matrix $H(D)$ such that $\mathcal{C} \subset \ker H(D)$, and then we still can make use of $H(D)$ to decode when the transmission occurs over the erasure channel. For simplicity, we will also call this matrix a parity-check matrix of $\mathcal{C}$. In an erasure channel a codeword can only have erasures (*i.e.*, we know the positions of the part of the codeword that is missing or erased) but no errors occur. In fact, if one considers the erasures as indeterminates, $H(D)w(D) = 0$ give rise to a system of linear equations. Solving this system amounts to decoding the received word $w(D)$, as we explain in detail in the next section.

The associated **truncated sliding parity-check matrix** of $H(D) = \sum_{i=0}^{\nu} H^i D^i$, is

$$H_j^c = \begin{bmatrix} H^0 & & & \\ H^1 & H^0 & & \\ \vdots & & \ddots & \\ H^j & H^{j-1} & \cdots & H^0 \end{bmatrix} \tag{8}$$

with $H^j = 0$ for $j > \nu$. As any codeword $w(D)$ of $\mathcal{C}$ satisfies $H(D)w(D) = 0$, if $w(D) = \sum_{i\in\mathbb{N}_0} w^i D^i$, we have that, for all $j \geq 0$, $\sum_{i=0}^{j} H^i w^{j-i} = 0$, *i.e.*,

$$\begin{bmatrix} H^0 & & & \\ H^1 & H^0 & & \\ \vdots & & \ddots & \\ H^j & H^{j-1} & \cdots & H^0 \end{bmatrix} \begin{bmatrix} w^0 \\ w^1 \\ \vdots \\ w^j \end{bmatrix} = 0. \tag{9}$$

Two of the main notions of minimum distance of convolutional codes are the free distance and the column distance. Given $w(D) = \sum_{i\in\mathbb{N}_0} w^i D^i$, we define its **Hamming weight** as

$$\mathrm{wt}(w(D)) = \sum_{j\in\mathbb{N}} \mathrm{wt}(w^j)$$

where $\mathrm{wt}(w^j)$ is the number of nonzero elements of w^j.

Given an (n,k) convolutional code $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^n[D]$, we define its **free distance** as

$$d_{free}(\mathcal{C}) = \min\{\mathrm{wt}(w(D)) \ : \ w(D) \in \mathcal{C} \text{ and } w(D) \neq 0\}.$$

The free distance gives the correction capability of a convolutional code when considering whole codewords. In other words, there is no maximum degree j for a codeword considered by the free distance. In this work we shall focus on the sliding-window erasure correction capabilities of $\mathcal{C}$ within a time interval and this will be determined by the **j-th column distance** of $\mathcal{C}$, for $j \in \mathbb{N}_0$, which is defined as follows.

$$\begin{aligned} d_j^c(\mathcal{C}) &= \min\{\mathrm{wt}((w^0, w^1, \ldots, w^j)) \ : \ \sum_{i\in\mathbb{N}_0} w^i D^i \in \mathcal{C}, w^0 \neq 0\} \\ &\overset{*}{=} \left\{\mathrm{wt}((w^0, w^1, \ldots, w^j)) \ : \ (w^0, w^1, \ldots, w^j) \text{ satisfies (9) and } w^0 \neq 0\right\} \quad (10) \end{aligned}$$

where the equality $*$ holds for convolutional codes that have a parity-check matrix. Next, we present two preliminary results.

Lemma 4. *[17] Let $Ax = b$ with $A \in \mathbb{Z}_{p^r}^{a\times s}$ and $b \in \mathbb{Z}_{p^r}^a$ be a linear system of equations in x. Suppose this system has a solution. Then, the solution is unique if and only if $[A]_p$ is full column rank or equivalently, if the McCoy[1] rank of A is s.*

Note that, opposed to the field case, a set of vectors in $\mathbb{Z}_{p^r}$ can be linearly dependent but none of them is in the $\mathbb{Z}_{p^r}$-span of the others. The following result states the erasure correcting capability of a convolutional code in terms of its column distance.

Lemma 5. *Let $\mathcal{C} = \mathrm{Ker}_{\mathbb{Z}_{p^r}[D]} H(D)$ and $j \in \mathbb{N}$. The following statements are equivalent:*

1. *the column distance $d_j^c(\mathcal{C}) = d$;*
2. *if $(w^0, w^1, \ldots, w^j)$ contains up to $d-1$ erasures then w^0 can be recovered and there exist d erasures that make it impossible to recover w^0.*
3. *all sets of $d-1$ columns of H_j^c that contain at least one of the first n columns of H_j^c are linearly independent and there exists a set of d columns of H_j^c that contains at least one of the first n columns of H_j^c and is linearly dependent;*

[1] The McCoy rank of a matrix is the largest size of a minor that is an invertible element in the ring, $\mathcal{A} \setminus \{0\}$ in our case.

If these equivalent statements hold, then the following holds:

(4) *none of the first n columns of* $[H_j^c]_p$ *is contained in the* $\mathbb{Z}_p$*-span of any other* $d-2$ *columns of* $[H_j^c]_p$.

Proof. The equivalence of 1., 2. and 3. can be shown exactly in the same way as for finite fields (see [9]). The last statement (4) follows from the fact that if we have a linear combination of columns of $[H_j^c]_p$ in $\mathbb{Z}_p$, we readily obtain linear combinations of H_j^c over $\mathbb{Z}_{p^r}$ (just multiply the coefficients of the linear combination from $\mathbb{Z}_p$ by p^{r-1}). □

We notice that statement (4) of Lemma 5 does not imply the others as we show in the following example.

Example 2. Consider $\mathcal{C} = \operatorname{Ker}_{\mathbb{Z}_9[D]} H(D)$ over $\mathbb{Z}_9$ where $H(D) = H^0 + H^1 D$ with

$$H^0 = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 3 \end{pmatrix} \text{ and } H^1 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Then, none of the first 3 columns of $[H_1^c]_3$ is a linear combination of $1 = 3 - 2$ of the remaining columns of $[H_1^c]_3$. Hence, (4) is fulfilled for $d = 3$. However, it is easy to see that $d_1^c(\mathcal{C}) = 2$ (consider the truncated codeword $(w^0, w^1) = (003\ 002)$), i.e., the first statement of Lemma 5 is not fulfilled for $d = 3$.

3. A decoding algorithm for erasures

In this section we state the problem using the notation presented in the previous section and then propose an efficient decoding algorithm to solve it. More concretely, we aim to recover erasures that may occur during the transmission of the information over an erasure channel using convolutional codes $\mathcal{C} \subset \mathbb{Z}_{p^r}^n[D]$. We derive a constructive step by step decoding algorithm to compute a minimal list with the closest codewords to the received vector. This is equivalent to solving a certain system of linear equations in $\mathbb{Z}_{p^r}$.

Suppose that $w(D) = \sum_{i \in \mathbb{N}_0} w^i D^i \in \mathcal{C}$ is sent and assume that we have correctly received all coefficients up to an instant $i-1$ and some of the components of w^i are erased. The decoder tries to recover w^i up to a given instant $i+T$ and if this is not possible it outputs a list with the closest vectors at time instant $i+T$. The parameter T is called the delay constraint and represents the maximum delay the receiver can tolerate to retrieve w^i, see [2,15]. For the sake of simplicity it will be assumed that $T \leq \nu$, where ν is the degree of the parity-check matrix $H(D)$ of $\mathcal{C}$. The system of equations that involve w^i up to time instant $i+T$ is

$$\begin{bmatrix} H^{\nu} & H^{\nu-1} & \cdots & H^0 & & & \\ & H^{\nu} & H^{\nu-1} & \cdots & H^0 & & \\ & & \ddots & \vdots & \vdots & \ddots & \\ & & & H^{\nu} & H^{\nu-1} & \cdots & H^0 \end{bmatrix} \begin{bmatrix} w^{i-\nu} \\ w^{i-\nu+1} \\ \vdots \\ w^{i} \\ \vdots \\ w^{i+T} \end{bmatrix} = 0. \tag{11}$$

We can take the columns of the matrix in (11) that correspond to the coefficients of the erased elements to be the coefficients of a new system. With the remaining columns we can compute the independent terms, denoted by b^i.

We regard the erasures as to-be-determined variables and denote for $i \in \mathbb{N}_0$ by $\widetilde{w}^i$ the subvector of w^i that corresponds to the positions of the erasures. Similarly, denote by $\widetilde{H}_i^j$ the matrix consisting of the columns of H^j with indices corresponding to the erased positions in w^i. Then, we obtain the following system of linear equations

$$\begin{bmatrix} \widetilde{H}_i^0 & & & \\ \widetilde{H}_i^1 & \widetilde{H}_{i+1}^0 & & \\ \vdots & & \ddots & \\ \widetilde{H}_i^T & \widetilde{H}_{i+1}^{T-1} & \cdots & \widetilde{H}_{i+T}^0 \end{bmatrix} \begin{bmatrix} \widetilde{w}^i \\ \widetilde{w}^{i+1} \\ \vdots \\ \widetilde{w}^{i+T} \end{bmatrix} = \begin{bmatrix} b^i \\ b^{i+1} \\ \vdots \\ b^{i+T} \end{bmatrix}. \tag{12}$$

Hence, the problem of decoding is equivalent to solving the system of linear equations described in (12).

For this algorithm we consider a parity-check matrix $H(D)$ of the form

$$H(D) = \begin{bmatrix} H_0(D) \\ pH_1(D) \\ \vdots \\ p^{r-1}H_{r-1}(D) \end{bmatrix} \text{ with } \begin{bmatrix} H_0(D) \\ H_1(D) \\ \vdots \\ H_{r-1}(D) \end{bmatrix} \text{ full row rank.} \tag{13}$$

Hence, it readily follows that one can rewrite (12), after appropriate row permutations, as

$$\begin{bmatrix} \widetilde{H}^0_{i,0} & & & & \\ p\widetilde{H}^0_{i,1} & & & & \\ \vdots & & & & \\ p^{r-1}\widetilde{H}^0_{i,r-1} & & & & \\ \widetilde{H}^1_{i,0} & \widetilde{H}^0_{i+1,0} & & & \\ p\widetilde{H}^1_{i,1} & p\widetilde{H}^0_{i+1,1} & & & \\ \vdots & \vdots & & & \\ p^{r-1}\widetilde{H}^1_{i,r-1} & p^{r-1}\widetilde{H}^0_{i+1,r-1} & & & \\ \vdots & & \ddots & & \\ \widetilde{H}^T_{i,0} & \widetilde{H}^{T-1}_{i+1,0} & \cdots & \widetilde{H}^0_{i+T,0} & \\ p\widetilde{H}^T_{i,1} & p\widetilde{H}^{T-1}_{i+1,1} & \cdots & p\widetilde{H}^0_{i+T,1} & \\ \vdots & \vdots & & \vdots & \\ p^{r-1}\widetilde{H}^T_{i,r-1} & p^{r-1}\widetilde{H}^{T-1}_{i+1,r-1} & \cdots & p^{r-1}\widetilde{H}^0_{i+T,r-1} & \end{bmatrix} \begin{bmatrix} \widetilde{w}^i \\ \widetilde{w}^{i+1} \\ \vdots \\ \widetilde{w}^{i+T} \end{bmatrix} = \begin{bmatrix} b^i_0 \\ pb^i_1 \\ \vdots \\ p^{r-1}b^i_{r-1} \\ b^{i+1}_0 \\ pb^{i+1}_1 \\ \vdots \\ p^{r-1}b^{i+1}_{r-1} \\ \vdots \\ b^{i+T}_0 \\ pb^{i+T}_1 \\ \vdots \\ p^{r-1}b^{i+T}_{r-1} \end{bmatrix}, \quad (14)$$

with the property that the rows of the matrices $\widetilde{H}^0_{i,t}, [\widetilde{H}^1_{i,t}\ \widetilde{H}^0_{i+1,t}], \ldots, [\widetilde{H}^T_{i,t}\ \widetilde{H}^{T-1}_{i+1,t} \cdots \widetilde{H}^0_{i+T,t}]$ have order r, for $t = 0, 1, \ldots, r-1$. Note that the number of nonzero rows of each block in the decomposition (14) will depend on the erasure pattern.
Denote by e_s the size of $\widetilde{w}^s$, for $s \in \{i, i+1, \ldots, i+T\}$.

List decoding:
We aim to compute all possible solutions of (14). To this end we define the following matrix for all $0 \le t \le r-1$,

$$\widetilde{\mathcal{H}}^c_t = \begin{bmatrix} \widetilde{H}^0_{i,0} & & & \\ \widetilde{H}^0_{i,1} & & & \\ \vdots & & & \\ \widetilde{H}^0_{i,r-t-1} & & & \\ \widetilde{H}^1_{i,0} & \widetilde{H}^0_{i+1,0} & & \\ \widetilde{H}^1_{i,1} & \widetilde{H}^0_{i+1,1} & & \\ \vdots & \vdots & & \\ \widetilde{H}^1_{i,r-t-1} & \widetilde{H}^0_{i+1,r-t-1} & & \\ \vdots & & \ddots & \\ \widetilde{H}^T_{i,0} & \widetilde{H}^{T-1}_{i+1,0} & \cdots & \widetilde{H}^0_{i+T,0} \\ \widetilde{H}^T_{i,1} & \widetilde{H}^{T-1}_{i+1,1} & \cdots & \widetilde{H}^0_{i+T,1} \\ \vdots & \vdots & & \vdots \\ \widetilde{H}^T_{i,r-t-1} & \widetilde{H}^{T-1}_{i+1,r-t-1} & \cdots & \widetilde{H}^0_{i+T,r-t-1} \end{bmatrix}, \quad (15)$$

and write

$$\begin{bmatrix} \widetilde{w}^i \\ \widetilde{w}^{i+1} \\ \vdots \\ \widetilde{w}^{i+T} \end{bmatrix} = \begin{bmatrix} w_0^i \\ w_0^{i+1} \\ \vdots \\ w_0^{i+T} \end{bmatrix} + p \begin{bmatrix} w_1^i \\ w_1^{i+1} \\ \vdots \\ w_1^{i+T} \end{bmatrix} + \cdots + p^{r-1} \begin{bmatrix} w_{r-1}^i \\ w_{r-1}^{i+1} \\ \vdots \\ w_{r-1}^{i+T} \end{bmatrix}, \tag{16}$$

where w_t^j has entries in $\mathcal{A}_p = \{0, 1, \ldots, p-1\}$, for all $j \in \{i, i+1, \ldots, i+T\}$ and $t \in \{0, 1, \ldots, r-1\}$. We aim at computing the maximum number of coefficients w_t^j in (16).

Step 1: Find the solution $(\widehat{w}_0^i, \widehat{w}_0^{i+1}, \ldots, \widehat{w}_0^{i+T})$ of the system

$$\underbrace{\begin{bmatrix} \widetilde{H}_{i,0}^0 & & & \\ \widetilde{H}_{i,1}^0 & & & \\ \vdots & & & \\ \widetilde{H}_{i,r-1}^0 & & & \\ \widetilde{H}_{i,0}^1 & \widetilde{H}_{i+1,0}^0 & & \\ \widetilde{H}_{i,1}^1 & \widetilde{H}_{i+1,1}^0 & & \\ \vdots & \vdots & & \\ \widetilde{H}_{i,r-1}^1 & \widetilde{H}_{i+1,r-1}^0 & & \\ \vdots & & \ddots & \\ \widetilde{H}_{i,0}^T & \widetilde{H}_{i+1,0}^{T-1} & \cdots & \widetilde{H}_{i+T,0}^0 \\ \widetilde{H}_{i,1}^T & \widetilde{H}_{i+1,1}^{T-1} & \cdots & \widetilde{H}_{i+T,1}^0 \\ \vdots & \vdots & & \vdots \\ \widetilde{H}_{i,r-1}^T & \widetilde{H}_{i+1,r-1}^{T-1} & \cdots & \widetilde{H}_{i+T,r-1}^0 \end{bmatrix}_p}_{[\widetilde{\mathcal{H}}_0^\zeta]_p} \begin{bmatrix} \widehat{w}_0^i \\ \widehat{w}_0^{i+1} \\ \vdots \\ \widehat{w}_0^{i+T} \end{bmatrix} = \begin{bmatrix} b_0^i \\ b_1^i \\ \vdots \\ b_{r-1}^i \\ b_0^{i+1} \\ b_1^{i+1} \\ \vdots \\ b_{r-1}^{i+1} \\ \vdots \\ b_0^{i+T} \\ b_1^{i+T} \\ \vdots \\ b_{r-1}^{i+T} \end{bmatrix}_p, \tag{17}$$

over the field $\mathbb{Z}_p$. Let $e = \sum_{s=i}^{i+T} e_s$. Then, the "integer" part of the set of solutions, *i.e.*, the vector $\begin{bmatrix} w_0^i \\ w_0^{i+1} \\ \vdots \\ w_0^{i+T} \end{bmatrix}$ in (16), is given by:

$$\mathcal{S}_0 = \left\{ \begin{bmatrix} w_0^i \\ w_0^{i+1} \\ \vdots \\ w_0^{i+T} \end{bmatrix} \in \mathcal{A}^e \ : \ \begin{bmatrix} w_0^i \\ w_0^{i+1} \\ \vdots \\ w_0^{i+T} \end{bmatrix}_p = \begin{bmatrix} \widehat{w}_0^i \\ \widehat{w}_0^{i+1} \\ \vdots \\ \widehat{w}_0^{i+T} \end{bmatrix} \text{ with } \begin{bmatrix} \widehat{w}_0^i \\ \widehat{w}_0^{i+1} \\ \vdots \\ \widehat{w}_0^{i+T} \end{bmatrix} \text{ satisfying (17)} \right\}.$$

It is straightforward to see that the size of $\mathcal{S}_0$ is given by

$$|\mathcal{S}_0| = p^{e-\operatorname{rank}[\widetilde{\mathcal{H}}_0^c]_p}.$$

To compute the remaining vectors, if necessary, in the p-adic decomposition of (16) we recursively apply the following algorithm in the next step.

Step 2: Let $b_{s,0}^j = b_s^j$, $j = i, i+1, \ldots, i+T$, $s = 0, 1, \ldots, r-1$.
For $t = 1, \ldots, r-1$ do

1. For $j = i, i+1, \ldots, i+T$, consider the solutions $\begin{bmatrix} w_{t-1}^i \\ w_{t-1}^{i+1} \\ \vdots \\ w_{t-1}^{i+T} \end{bmatrix} \in S_{t-1}$ and define

$$\begin{bmatrix} \widehat{b}_{0,t}^j \\ \widehat{b}_{1,t}^j \\ \vdots \\ \widehat{b}_{r-t-1,t}^j \end{bmatrix} = \begin{bmatrix} p^{t-1} b_{0,t-1}^j \\ p^t b_{1,t-1}^j \\ \vdots \\ p^{r-2} b_{r-t-1,t-1}^j \end{bmatrix} - \begin{bmatrix} p^{t-1}\widetilde{H}_{i,0}^{j-i} & \cdots & p^{t-1}\widetilde{H}_{j,0}^0 \\ p^t \widetilde{H}_{i,1}^{j-i} & \cdots & p^t \widetilde{H}_{j,1}^0 \\ \vdots & \vdots & \vdots \\ p^{r-2}\widetilde{H}_{i,r-t-1}^{j-i} & \cdots & p^{r-2}\widetilde{H}_{j,r-t-1}^0 \end{bmatrix} \begin{bmatrix} w_{t-1}^i \\ w_{t-1}^{i+1} \\ \vdots \\ w_{t-1}^j \end{bmatrix}$$

2. For $j = i, i+1, \ldots, i+T$, and $\ell = 0, 1, \ldots, r-t-1$, compute *one* $b_{\ell,t}^i$ such that

$$\widehat{b}_{\ell,t}^j = p^{t+\ell} b_{\ell,t}^j$$

3. Solve the system of linear equations

$$[\widetilde{\mathcal{H}}_t^c]_p \begin{bmatrix} \widehat{w}_t^i \\ \widehat{w}_t^{i+1} \\ \vdots \\ \widehat{w}_t^{i+T} \end{bmatrix} = \begin{bmatrix} b_{t,0}^i \\ b_{t,1}^i \\ \vdots \\ b_{t,r-t-1}^0 \\ b_{t,0}^{i+1} \\ b_{t,1}^{i+1} \\ \vdots \\ b_{t,r-t-1}^{i+1} \\ \vdots \\ b_{t,0}^{i+T} \\ b_{t,1}^{i+T} \\ \vdots \\ b_{t,r-t-1}^{i+T} \end{bmatrix}_p, \tag{18}$$

over $\mathbb{Z}_p$ and let

$$\mathcal{S}_t = \left\{ \begin{bmatrix} w_t^i \\ w_t^{i+1} \\ \vdots \\ w_t^{i+T} \end{bmatrix} : \begin{bmatrix} w_t^i \\ w_t^{i+1} \\ \vdots \\ w_t^{i+T} \end{bmatrix}_p = \begin{bmatrix} \widehat{w}_t^i \\ \widehat{w}_t^{i+1} \\ \vdots \\ \widehat{w}_t^{i+T} \end{bmatrix} \text{ with } \begin{bmatrix} \widehat{w}_t^i \\ \widehat{w}_t^{i+1} \\ \vdots \\ \widehat{w}_t^{i+T} \end{bmatrix} \text{ satisfying (18)} \right\}.$$

Output data:

$$\left\{ \begin{bmatrix} w_0^i \\ w_0^{i+1} \\ \vdots \\ w_0^{i+T} \end{bmatrix} + p \begin{bmatrix} w_1^i \\ w_1^{i+1} \\ \vdots \\ w_1^{i+T} \end{bmatrix} + \cdots + p^{r-1} \begin{bmatrix} w_{r-1}^i \\ w_{r-1}^{i+1} \\ \vdots \\ w_{r-1}^{i+T} \end{bmatrix} : \begin{bmatrix} w_t^i \\ w_t^{i+1} \\ \vdots \\ w_t^{i+T} \end{bmatrix} \in S_t,\ t = 0, 1, \ldots, r-1 \right\}.$$

The size of the list decoding is

$$\prod_{t=0}^{r-1} |S_t|,$$

where each $|S_t|$ is given by

$$|S_t| = p^{e - \operatorname{rank}[\widetilde{\mathcal{H}}_t^c]_p} \tag{19}$$

Note that Steps 1 and 2 deal with systems of linear equations over fields. The fact that these steps yield the set of all solution follows from [19, Theorem 3].

Example 3. Let $\mathcal{C} \subset \mathbb{Z}_8[D]$ be the convolutional code with parity-check matrix $H(D) = H^0 + H^1 D + H^2 D^2 \in \mathbb{Z}_8[D]$ where

$$H^0 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 0 & 2 \\ 4 & 4 & 0 & 4 & 4 \end{bmatrix},\ H^1 = \begin{bmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 4 \\ 4 & 0 & 4 & 4 & 0 \end{bmatrix},\ H^2 = \begin{bmatrix} 3 & 5 & 7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 4 & 0 \end{bmatrix}.$$

It is easy to check that $w(D) = w^0 + w^1 D + w^2 D^2 + w^3 D^3$ with

$$w^0 = [5, 5, 0, 6, 0], \quad w^1 = [6, 6, 4, 3, 6], \quad w^2 = [2, 1, 1, 2, 0], \quad w^3 = [2, 6, 4, 0, 0]$$

is a codeword of $\mathcal{C}$. Assume that one receives

$$w^0 = [5, w^{0,1}, w^{0,2}, 6, w^{0,3}], \quad w^1 = [6, 6, 4, w^{1,1}, 6],$$
$$w^2 = [2, 1, w^{2,1}, w^{2,2}, w^{2,3}], \quad w^3 = [2, w^{3,1}, 4, 0, 0]$$

where $w^{0,1}, w^{0,2}, w^{0,3}, w^{1,1}, w^{2,1}, w^{2,2}, w^{2,3}, w^{3,1}$ are erasures. Let the delay constraint for the decoding be $T = 2$. To firstly recover w^0 we start our list decoding algorithm. One has

$$\widetilde{\mathcal{H}}_0^c = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 5 & 7 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad [\widetilde{\mathcal{H}}_0^c]_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

We write $w^{i,j} = w_0^{i,j} + 2w_1^{i,j} + 4w_2^{i,j}$ for $i = 0, \ldots, 3$ and $j \in \{1, 2, 3\}$. Solving the linear system

$$\begin{aligned} [\widetilde{\mathcal{H}}_0^c]_2 \cdot [w_0^{0,1}, w_0^{0,2}, w_0^{0,3}, w_0^{1,1}, w_0^{2,1}, w_0^{2,2}, w_0^{2,3}]^\top &= [5, 0, 1, 5, 0, 1, 4, 0, 1]_2^\top \\ &= [1, 0, 1, 1, 0, 1, 0, 0, 1]^\top \end{aligned}$$

over $\mathbb{Z}_2$ gives the (unique) solution

$$[w_0^{0,1}, w_0^{0,2}, w_0^{0,3}, w_0^{1,1}, w_0^{2,1}, w_0^{2,2}, w_0^{2,3}] = [1, 0, 0, 1, 1, 0, 0],$$

i.e., $S_0 = \{[1, 0, 0, 1, 1, 0, 0]\}$. Note that $|S_0| = p^{e - \operatorname{rank}[\widetilde{\mathcal{H}}_0^c]_p} = p^{7-7} = 1$.
Then, in step 2.1 and step 2.2 of the algorithm, one computes

$$\begin{pmatrix} \widehat{b}_{0,1}^0 \\ \widehat{b}_{1,1}^0 \end{pmatrix} = \begin{pmatrix} 5 \\ 0 \end{pmatrix} - \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \end{pmatrix} \quad \Rightarrow \begin{pmatrix} b_{0,1}^0 \\ b_{1,1}^0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

$$\widehat{b}_{0,1}^1 = 5 - \begin{bmatrix} 2 & 0 & 0 & 1 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \end{pmatrix} \qquad \Rightarrow b_{0,1}^1 = 1$$

$$\begin{pmatrix} \widehat{b}_{0,1}^2 \\ \widehat{b}_{1,1}^2 \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \end{pmatrix} - \begin{bmatrix} 5 & 7 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 & 2 & 0 & 2 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 6 \\ 4 \end{pmatrix} \quad \Rightarrow \begin{pmatrix} b_{0,1}^2 \\ b_{1,1}^2 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

Afterwards, according to step 2.3, one has to solve the system of linear equations

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{pmatrix} w_1^{0,1} \\ w_1^{0,2} \\ w_1^{0,3} \\ w_1^{1,1} \\ w_1^{2,1} \\ w_1^{2,2} \\ w_1^{2,3} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

over $\mathbb{Z}_2$, which yields

$$[w_1^{0,1}, w_1^{0,2}, w_1^{0,3}, w_1^{1,1}, w_1^{2,1}, w_1^{2,2}, w_1^{2,3}] = [0, c_1, c_1, 1, c_1 + c_2, 1, c_2]$$

with free parameters $c_1, c_2 \in \mathbb{Z}_2$, i.e.,

$$S_1 = \{[0, c_1, c_1, 1, c_1 + c_2, 1, c_2],\ c_1, c_2 \in \mathcal{A}_2\}$$

with $|S_1| = p^{7-\operatorname{rank}[\widetilde{\mathcal{H}}_1^c]_p} = p^2 = 4$.
In the last iteration, one computes

$$\widehat{b}_{0,2}^0 = 2 \cdot 2 - 2 \cdot \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \begin{pmatrix} 0 \\ c_1 \\ c_1 \end{pmatrix} = 4 - 4c_1 \quad \Rightarrow\ b_{0,2}^0 = 1 - c_1$$

$$\widehat{b}_{0,2}^1 = 2 \cdot 1 - 2 \cdot \begin{bmatrix} 2 & 0 & 0 & 1 \end{bmatrix} \begin{pmatrix} 0 \\ c_1 \\ c_1 \\ 1 \end{pmatrix} = 0 \qquad \Rightarrow\ b_{0,2}^1 = 0$$

$$\widehat{b}_{0,2}^2 = 2 \cdot 3 - 2 \cdot \begin{bmatrix} 5 & 7 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{pmatrix} 0 \\ c_1 \\ c_1 \\ 1 \\ c_1 + c_2 \\ 1 \\ c_2 \end{pmatrix} = 4 - 4c_2 \quad \Rightarrow\ b_{0,2}^2 = 1 - c_2$$

and afterwards solves the system of linear equations

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{pmatrix} w_2^{0,1} \\ w_2^{0,2} \\ w_2^{0,3} \\ w_2^{1,1} \\ w_2^{2,1} \\ w_2^{2,2} \\ w_2^{2,3} \end{pmatrix} = \begin{pmatrix} 1 - c_1 \\ 0 \\ 1 - c_2 \end{pmatrix}$$

over $\mathbb{Z}_2$, which yields

$$[w_2^{0,1}, w_2^{0,2}, w_2^{0,3}, w_2^{1,1}, w_2^{2,1}, w_2^{2,2}, w_2^{2,3}]$$
$$= [1 + c_2 + c_3 + c_4 + c_5 + c_6, c_3, c_1 + c_2 + c_4 + c_5 + c_6, 0, c_4, c_5, c_6]$$

with free parameters $c_3, c_4, c_5, c_6 \in \mathbb{Z}_2$, i.e.

$$S_2 = \{[1 + c_2 + c_3 + c_4 + c_5 + c_6, c_3, c_1 + c_2 + c_4 + c_5 + c_6, 0, c_4, c_5, c_6],\ c_3, c_4, c_5, c_6 \in \mathcal{A}_2\},$$

with $|S_2| = p^{7-\operatorname{rank}[\widetilde{\mathcal{H}}_2^c]_p} = p^4 = 16$.
In summary, all solutions for the erased positions are given by

$$\begin{pmatrix} w^{0,1} \\ w^{0,2} \\ w^{0,3} \\ w^{1,1} \\ w^{2,1} \\ w^{2,2} \\ w^{2,3} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + 2 \begin{pmatrix} 0 \\ c_1 \\ c_1 \\ 1 \\ c_1 + c_2 \\ 1 \\ c_2 \end{pmatrix} + 4 \begin{pmatrix} 1 + c_2 + c_3 + c_4 + c_5 + c_6 \\ c_3 \\ c_1 + c_2 + c_4 + c_5 + c_6 \\ 0 \\ c_4 \\ c_5 \\ c_6 \end{pmatrix}$$

with $c_1, c_2, c_3, c_4, c_5, c_6 \in \mathcal{A}_2$, i.e.,

$$|S| = p^{0+2+4} = p^6 = 64.$$

Note that for $c_1 = c_2 = c_3 = c_3 = c_4 = c_5 = c_6 = 0$, one gets the solution that leads to the original codeword we started with. Because of the constraint $T = 2$, the vector w^3 is not recovered yet. However, since all other erasures are recovered, the remaining erasure $w^{3,1}$ can now easily be recovered.

Of course the smaller the size of the output the better. Obviously, this holds if $\operatorname{rank}[\widetilde{\mathcal{H}}_t^c]_p$ is maximal.

Remark 1. The presented decoding algorithm also works in the more general setting of codes over finite chain rings. Since all computations in the several steps of the algorithm are broken down to computations with coefficient matrices, it is not necessary to consider polynomial matrices over finite chain rings but only specially structured block codes over finite chain rings. There already exist some papers on block codes over finite chain rings, e.g. [5], [20].
If $\mathcal{R}$ is a finite chain ring and $\mathfrak{m}$ its unique maximal ideal, then $\mathfrak{m} = \langle\gamma\rangle$ for some $\gamma \in \mathcal{R}$ and $\mathcal{R}/\mathfrak{m}$ is isomorphic to a finite field $\mathbb{F}_q$. Moreover, if e is the nihilpotency index of γ and V a set of representatives for the equivalence classes of $\mathcal{R}$ modulo γ, then each $a \in \mathcal{R}$ can be uniquely written as $a = a_0 + a_1\gamma + \cdots + a_{e-1}\gamma^{e-1}$ with $a_i \in V$ for $i = 0, \ldots, e-1$. If $\mathcal{R} = \mathbb{Z}_{p^r}$, then one can choose $\gamma = p$, i.e. $e = r$. Moreover, $V = \mathcal{A}_p$ and the mentioned unique decomposition of a is just the p-adic expansion.
This has the following impact on our decoding algorithm: One has to solve systems of linear equations in a general finite field $\mathbb{F}_q$ instead of a prime field $\mathbb{F}_p$, which is no major

problem. To obtain a general version of the algorithm for codes over finite chain rings, we just replace r by e and where p indicates the generator of the maximal ideal, we have to replace it by γ, where it indicates the cardinality of $\mathbb{F}_p$ or $\mathcal{A}_p$ we replace it by q.

4. Complexity analysis

In this section, we briefly want to analyze the complexity of the presented decoding algorithm. As we work with the projections of elements from the finite ring $\mathbb{Z}_{p^r}$ in the finite field $\mathbb{Z}_p$, we can state the computational effort in terms of the number of necessary field operations in $\mathbb{Z}_p$.

Theorem 1. *Denote by e the maximal number of erasures that occur in a window of size $(T+1)n$. The number of necessary field operations in $\mathbb{Z}_p$ for our list decoding algorithm is*

$$O(re^2((n-k)(T+1))^{0.8}) \text{ if } e \leq (n-k)(T+1)$$
$$O(re^{0.8}((n-k)(T+1))^2) \text{ if } e > (n-k)(T+1).$$

Proof. The step of the algorithm that is relevant for the complexity of the whole algorithm is to solve the system of linear equations in (18). This linear system has at most $(n-k)(T+1)$ equations and at most e unknowns. It follows from [23] that the number of field operations that is needed to do that is

$$O(e^2((n-k)(T+1))^{0.8}) \text{ if } e \leq (n-k)(T+1)$$
$$O(e^{0.8}((n-k)(T+1))^2) \text{ if } e > (n-k)(T+1).$$

The theorem follows from the fact that we have to solve (18) for $t = 0, \ldots, r-1$, what gives us the factor r. □

Acknowledgments

Julia Lieb acknowledges the support of the German Research Foundation grant LI 3101/1-1 and of the Swiss National Science Foundation grant n. 188430. Diego Napp is partially supported by Ministerio de Ciencia e Innovación via the grant with ref. PID2019-108668GB-I00. Raquel Pinto is supported by The Center for Research and Development in Mathematics and Applications (CIDMA) through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), references UIDB/04106/2020 and UIDP/04106/2020.

References

[1] M. Artin, Algebra, Birkhäuser, 1998.

[2] A. Badr, A. Khisti, Wai-Tian Tan, J. Apostolopoulos, Layered constructions for low-delay streaming codes, IEEE Trans. Inf. Theory 63 (1) (2017) 111–141.
[3] Sara D. Cardell, Amparo Fuster-Sabater, Discrete linear models for the generalized self-shrunken sequences, Finite Fields Appl. 47 (Supplement C) (2017) 222–241.
[4] C-J. Chen, T-Y. Chen, H-A. Loeliger, Construction of linear ring codes for 6 PSK, IEEE Trans. Inf. Theory 40 (2) (1994) 563–566.
[5] Steven T. Dougherty, Hongwei Liu, Young Ho Park, Lifted codes over finite chain rings, Math. J. Okayama Univ. 53 (2011) 39–53.
[6] M. El Oued, D. Napp, R. Pinto, M. Toste, The dual of convolutional codes over $\mathbb{Z}_{p^r}$, in: N. Bebiano (Ed.), Applied and Computational Matrix Analysis, MAT-TRIAD 2015, in: Springer Proceedings in Mathematics & Statistics, vol. 192, 2017, pp. 79–91.
[7] F. Fagnani, S. Zampieri, System-theoretic properties of convolutional codes over rings, IEEE Trans. Inf. Theory 47 (6) (2001) 2256–2274.
[8] G.D. Forney, Convolutional codes I: algebraic structure, IEEE Trans. Inf. Theory 16 (1970) 720–738, Correction, IEEE Trans. Inf. Theory 17 (1971) 360.
[9] H. Gluesing-Luerssen, J. Rosenthal, R. Smarandache, Strongly MDS convolutional codes, IEEE Trans. Inf. Theory 52 (2) (2006) 584–598.
[10] J.C. Interlando, R. Palazzo, M. Elia, On the decoding of Reed-Solomon and bch codes over integer residue rings, IEEE Trans. Inf. Theory 43 (3) (1997) 1013–1021.
[11] R. Johannesson, Z.X. Wan, E. Wittenmark, Some structural properties of convolutional codes over rings, IEEE Trans. Inf. Theory 44 (2) (1998) 839–845.
[12] Kailath Tom, Linear Systems, Prentice Hall Information and System Sciences Series, Prentice-Hall, Englewood Cliffs, 1980.
[13] M. Kuijper, R. Pinto, J.W. Polderman, The predictable degree property and row reducedness for systems over a finite ring, Linear Algebra Appl. 425 (2–3) (2007) 776–796.
[14] R. Mahmood, A. Badr, A. Khisti, Streaming-codes for multicast over burst erasure channels, IEEE Trans. Inf. Theory 61 (8) (2015) 4181–4208.
[15] E. Martinian, C.E.W. Sundberg, Burst erasure correction codes with low decoding delay, IEEE Trans. Inf. Theory 50 (10) (2004) 2494–2502.
[16] J.L. Massey, T. Mittelholzer, Convolutional codes over rings, in: Proc. 4th Joint Swedish-Soviet Int. Workshop Information Theory, 1989, pp. 14–18.
[17] Bernard R. McDonald, Linear Algebra over Commutative Rings, M. Dekker, New York, 1984.
[18] D. Napp, R. Pinto, M. Toste, Column distances of convolutional codes over $\mathbb{Z}_{p^r}$, IEEE Trans. Inf. Theory 65 (2) (2017) 1063–1071.
[19] Diego Napp, Raquel Pinto, Elif Sacikara, Marisa Toste, A matrix based list decoding algorithm for linear codes over integer residue rings, Linear Algebra Appl. 614 (2021) 376–393.
[20] Graham H. Norton, Ana Salagean, On the Hamming distance of linear codes over a finite chain ring, IEEE Trans. Inf. Theory 46 (2000) 1060–1067.
[21] M. El Oued, Diego Napp, Raquel Pinto, Marisa Toste, On duals and parity-checks of convolutional codes over $\mathbb{Z}_{p^r}$, Finite Fields Appl. 55 (2019) 1–20.
[22] M. El Oued, P. Solé, MDS convolutional codes over a finite ring, IEEE Trans. Inf. Theory 59 (11) (2013) 7305–7313.
[23] V. Strassen, Gaussian elimination is not optimal, Numer. Math. 13 (1969) 354–356.
[24] V. Tomas, J. Rosenthal, R. Smarandache, Decoding of convolutional codes over the erasure channel, IEEE Trans. Inf. Theory 58 (1) (January 2012) 90–108.