A Matrix based List Decoding Algorithm for Linear Codes over integer residue rings

Diego Napp[1], Raquel Pinto[3], Elif Saçıkara[2] and Marisa Toste[4]

[1] *Department of Mathematics, University of Alicante, Spain, diego.napp@ua.es,*
[2] *Institute of Mathematics, University of Zurich, Switzerland, elif.sacikara@math.uzh.ch,*
[3] *CIDMA - Center for Research and Development in Mathematics and Applications, Department of Mathematics, University of Aveiro, Aveiro, Portugal raquel@ua.pt,*
[4] *CIDMA-Center of Research and Development in Mathematics and Applications, Aveiro, and Superior School of Technologies and Management of Olveira do Hospital, Polytechnic Institute of Coimbra, Coimbra, Portugal, marisa.toste@estgoh.ipc.pt.*

Abstract

In this paper we address the problem of list decoding of linear codes over an integer residue ring $\mathbb{Z}_q$, where q is a power of a prime p. The proposed procedure exploits a particular matrix representation of the linear code over $\mathbb{Z}_{p^r}$, called the standard form, and the p-adic expansion of the to-be-decoded vector. In particular, we focus on the erasure channel in which the location of the errors is known. This problem then boils down to solving a system of linear equations with coefficients in $\mathbb{Z}_{p^r}$. From the parity-check matrix representations of the code we recursively select certain equations that a codeword must satisfy and have coefficients only in the field $p^{r-1}\mathbb{Z}_{p^r}$. This yields a step by step procedure obtaining a list of the closest codewords to a given received vector with some of its coordinates erased. We show that such an algorithm actually computes all possible erased coordinates, that is, the provided list is minimal.

Keywords:
Finite rings, linear codes over finite rings, erasure channel, decoding algorithms, matrix representations, parity-check matrix.

1. Introduction

This paper is concerned with linear codes over $\mathbb{Z}_{p^r}$, *i.e.*, finitely generated $\mathbb{Z}_{p^r}$-modules in $\mathbb{Z}_{p^r}^n$. The local ring $\mathbb{Z}_{p^r}$ is of particular importance in coding

theory, especially after the seminal paper by Hammons et al. [9] where it was shown that important classes of binary nonlinear codes, such as the Preparata or Goethals codes, can be viewed as linear codes over the ring $\mathbb{Z}_4$ via a Gray mapping. This stimulated research in algebraic coding theory by motivating the study of linear codes over finite rings. Since then, a large body of literature on this topic has been produced, and many successful code constructions and other applications have been derived ([6, 10, 12, 18, 22]).

In this paper, we address the problem of decoding linear block codes over the finite ring $\mathbb{Z}_{p^r}$ over the erasure channel, [2, 5, 14, 15] that is, when the location of the errors in the received corrupted codeword is known. When it is not possible to uniquely determine the codeword that was sent from the received one (unique decoding), the decoder searches for the set of closest codewords, which is called list decoding. For this problem there exist several well-known algorithms that exploit the structure of the code, such as Reed-Solomon codes [8, 11]. In this work, we will not make use of the structure of the particular codes in use, but rather exploit the algebraic structure of codes over the ring $\mathbb{Z}_{p^r}$. To this end, we will utilize the parity-check matrix H in standard form of a linear code. In this setting, the number of independent columns of specific submatrices of H will determine the size of the list of possible codewords in our algorithm in Section 3. The decoding problem treated in Section 3 amounts to solving a system of linear equations over $\mathbb{Z}_{p^r}$. Our approach in this work is to multiply a certain set of these equations by a power of p in such a way that we obtain a subset of equations with coefficients in $p^{r-1}\mathbb{Z}_{p^r}$. Since $p^{r-1}\mathbb{Z}_{p^r}$ is a field isomorphic to $\mathbb{Z}_p$, we can easily solve the new system. Once we compute certain of the coefficients that are involved in the equations, we can apply similar ideas to a different set of equations to recover another set of erased symbols. We develop in this way a systematic procedure to recover all possible errors, obtaining a minimal set with all possible codewords.

Efficient decoding algorithms for codes over rings have been studied for errors (not necessarily erasures) for classes of codes with particular structure, such as Alternant and BCH codes [1, 10, 19]. Typically, the first steps of these decoding algorithms are devoted to determine the location of the errors. In this paper, we consider the erasure channel, i.e., the location of the errors is known. Thus, the matrix approach we propose in this work can be used for the last steps of these more general decoding algorithms. Also, related to this work is the list decoding problem: the decoding radius for unique

decoding (which is $\lfloor \frac{d-1}{2} \rfloor$, where d the distance of the code) is increased to allow the decoder to output a list of codewords rather than a single solution [2, 15]. In this context, minimal decoding lists are sought after for a given decoding radius.

The outline of this paper is as follows. In Section 2 we collect fundamental results on the structure of codes over the finite ring $\mathbb{Z}_{p^r}$. We also present preliminary results that will be essential for our algorithm. Section 3 is devoted to establishing the framework of the problem to be addressed, and to compute the number of possible codewords that our algorithm will yield. We give a basic constructive decoding algorithm in terms of the parity check matrix for building a minimal list of possible codewords. We show that this algorithm computes all possible codewords. In Section 4 we present our conclusions and also address possible future research.

2. Preliminaries

In this section we present the setting and the necessary results to address the problems in the next section. Let $\mathbb{Z}_{p^r}$ the ring of integers modulo p^r. Any element $a \in \mathbb{Z}_{p^r}$ can be written uniquely as a linear combination of $1, p, p^2, \ldots \ldots, p^{r-1}$, with coefficients in $\mathcal{A}_p = \{0, 1, \ldots, p-1\} \subset \mathbb{Z}_{p^r}$, *i.e.*,

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

called the p-adic expansion of the element [4]. Note that all elements in $\mathcal{A}_p \backslash \{0\}$ are units. We use $[a]_p = \alpha_0$ to denote the (modulo) canonical projection of $a \in \mathbb{Z}_{p^r}$ over $\mathbb{Z}_p$. We say that an element, vector o matrix v has order $j \in \{1, 2, \ldots, r\}$ if $p^j v = 0$ and $p^{j-1} v \neq 0$.

Definition 1. *A* **(linear) block code** $\mathcal{C}$ *of length* n *over* $\mathbb{Z}_{p^r}$ *is a* $\mathbb{Z}_{p^r}$*-submodule of* $\mathbb{Z}_{p^r}^n$ *and the elements of* $\mathcal{C}$ *are called codewords. A* **generator matrix** $G \in \mathbb{Z}_{p^r}^{k \times n}$ *of* $\mathcal{C}$ *is a matrix whose rows form a minimal set of generators of* $\mathcal{C}$ *over* $\mathbb{Z}_{p^r}$ *and therefore*

$$\mathcal{C} = \operatorname{Im}_{\mathbb{Z}_{p^r}} G = \{\boldsymbol{v} = \boldsymbol{u}G \in \mathbb{Z}_{p^r}^n \ : \boldsymbol{u} \in \mathbb{Z}_{p^r}^k\}.$$

A matrix $H \in \mathbb{Z}_{p^r}^{(n-\kappa) \times n}$ *is a* **parity-check matrix** *of a block code* $\mathcal{C}$ *if*

$$\boldsymbol{v} \in \mathcal{C} \Leftrightarrow H\boldsymbol{v}^T = 0, \text{ for every } \boldsymbol{v} \in \mathbb{Z}_{p^r}^n,$$

or equivalently,

$$\mathcal{C} = \operatorname{Ker}_{\mathbb{Z}_{p^r}} H,$$

where κ is the rank of $[G]_p$, the (componentwise) projection of an encoder G of $\mathcal{C} \subset \mathbb{Z}_{p^r}^n$ over $\mathbb{Z}_p$, see [20].

Definition 2. *The* **free distance** *$d(\mathcal{C})$ of a linear block code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ is given by*

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

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

Let $\mathcal{C}$ be a block code of length n and H be a parity-check matrix of $\mathcal{C}$. Suppose that we receive a corrupted codeword $\boldsymbol{v} \in \mathbb{Z}_{p^r}^n$ where some of its coordinates, say e, have been erased. Let $\boldsymbol{w} \in \mathbb{Z}_{p^r}^e$ be the subvector of $\boldsymbol{v}$ that corresponds to the positions of the erasures. Then, if we consider $\boldsymbol{w}$ as the vector of unknowns, it follows that

$$\widetilde{H}\boldsymbol{w}^T = b, \tag{1}$$

where the matrix $\widetilde{H} \in \mathbb{Z}_{p^r}^{(n-\kappa)\times e}$ consists of the columns of H whose indices are the indices of the erased components of $\boldsymbol{v}$ and $b = -\hat{H}\hat{\boldsymbol{w}}^T$ where $\hat{\boldsymbol{w}}$ is the vector constituted by the components of $\boldsymbol{v}$ that were received correctly, and $\hat{H}$ is the matrix with the columns of H with the same indices of the (correctly) received symbols of $\boldsymbol{v}$. Obviously, if we regard $\boldsymbol{w}$ as a vector of to-be-determined variables, the problem of decoding $\boldsymbol{v}$ is equivalent to solving (uniquely) the system of linear equations described in (1). This system has a unique solution if the columns of $\widetilde{H}$ are linearly independent (over $\mathbb{Z}_{p^r}$), and these columns are determined by linearly independent columns of $[\widetilde{H}]_p$, the projection of $\widetilde{H}$ over $\mathbb{Z}_p$ ([17]).

Lemma 1. *(Lemma II.10 in [17]) Let $H \in \mathbb{Z}_{p^r}^{l\times n}$. Then the columns of H are linearly independent if and only if the columns of the projection of H over $\mathbb{Z}_p$, that is $[H]_p$, are linearly independent.*

Note that H can be written as

$$H = \begin{bmatrix} H_0 \\ pH_1 \\ \vdots \\ p^{r-1}H_{r-1} \end{bmatrix}, \tag{2}$$

with $H_i \in \mathbb{Z}_{p^r}^{k_i \times n}$, $i = 0, 1, \ldots, r-1$ and $\begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_{r-1} \end{bmatrix}$ is full row rank (see [7, 20, 21]). When H is in such a form, we say that H is in standard form. If we consider the system of equations $H\boldsymbol{v}^T = 0$ with H as in (2) and the corresponding system $\widetilde{H}\boldsymbol{w}^T = b$ as in (1), then $\widetilde{H}$ and b can also be written accordingly as

$$\widetilde{H} = \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-1}\widetilde{H}_{r-1} \end{bmatrix}, \tag{3}$$

with $\widetilde{H}_i \in \mathbb{Z}_{p^r}^{k_i \times e}$, and

$$b = \begin{bmatrix} b_0 \\ pb_1 \\ \vdots \\ p^{r-1}b_{r-1} \end{bmatrix}, \tag{4}$$

with column vectors b_i of length k_i, for $i = 0, 1, \ldots, r-1$. Note that $\widetilde{H}$ is not necessarily full row rank anymore.

The following result characterizes the erasure-correction capability of a code $\mathcal{C}$ in terms of its parity-check matrices.

Theorem 1. *Let $\mathcal{C} = \operatorname{Ker}_{\mathbb{Z}_{p^r}} H$, be a block code of length n and free distance $d(\mathcal{C}) = d$ where the parity-check matrix can be written as in (2) Then, the following are equivalent*

1. $d(\mathcal{C}) = d$;
2. *we can correct up to* $d-1$ *erasures;*
3. *Any* $d-1$ *columns of* H *are linearly independent and there exists* d *columns of* H *that are linearly dependent over* $\mathbb{Z}_{p^r}$;
4. *Any* $d-1$ *columns of* $[H]_p$ *are linearly independent and there exists* d *columns of* H_0 *that are linearly dependent over* $\mathbb{Z}_p$.

Proof. The equivalence of parts 1 and 2 is a classical result of coding theory. Moreover, the equivalence of parts 1 and 3 is obvious and it follows a similar reasoning as linear codes over a finite field, [16]. Lemma 1 proves the equivalence of 3 and 4. □

It immediately follows from the previous theorem that when at most $d-1$ erasures occur, we can fully recover all the erasures and the decoder provides a unique most-likely codeword. When the number of erasures is larger than $d-1$, this is not always possible and there exits a set of possible (most likely) codewords. In the next section we treat this case.

3. A decoding algorithm

In this section, we present the main results of the paper, namely an efficient list decoding algorithm to recover erasures of linear codes over the ring $\mathbb{Z}_{p^r}$ via the standard form of its parity-check matrix. We first present the algorithm and then show that it produces a minimal list of possible codewords, that is, if we receive a codeword with some of its coordinates erased, say $\boldsymbol{v}$, then the algorithm produces the set of closest codewords to $\boldsymbol{v}$.

If exact decoding is not possible, one may want to obtain all the possible codewords. Next, we will show how to do so when dealing with block codes over $\mathbb{Z}_{p^r}$. In contrast with unique decoding, this procedure will depend not only on $\widetilde{H}_0$ but also on the remaining $\widetilde{H}_i$, for $i = 1, \ldots, r-1$. To this end we need to consider the system of linear equation (1), $\widetilde{H}\boldsymbol{w}^T = b$, with $\widetilde{H}$ and b defined as in (3) and (4), respectively.

Algorithm 2. Input data: *The matrix* $\widetilde{H}$ *and the column vector* b *that are defined as in (3) and (4) respectively.*

Initialization: *Write the p-adic expansion of* $\boldsymbol{w}$ *as* $\boldsymbol{w}^T = \boldsymbol{w}^{(0)} + p\boldsymbol{w}^{(1)} + \cdots + p^{r-1}\boldsymbol{w}^{(r-1)}$, *where* $\boldsymbol{w}^{(i)}$*'s are column vectors of length* e *with entries from the group of units* $\mathcal{A}_p = \{0, 1, \ldots, p-1\}$ *, for all* i.

Step 1: *Find the solutions of*

$$\begin{bmatrix} \widetilde{H}_0 \\ \widetilde{H}_1 \\ \vdots \\ \widetilde{H}_{r-1} \end{bmatrix}_p \hat{\boldsymbol{w}}^{(0)} = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{r-1} \end{bmatrix}_p , \tag{5}$$

over $\mathbb{Z}_p$, *and let* $S_0 = \{\boldsymbol{w}^{(0)} \in \mathcal{A}_p^e \ : \ [\boldsymbol{w}^{(0)}]_p = \hat{\boldsymbol{w}}^{(0)}$ *with* $\hat{\boldsymbol{w}}^{(0)}$ *solution of (5)*$\}$.

Step 2: *Let* $b_l^{(0)} = b_l$, $l = 0, 1, \ldots, r-1$. *For each* $i = 1, 2, \ldots, r-1$, *step by step we do the following.*

Let

$$\begin{bmatrix} \widetilde{b}_0^{(i)} \\ \widetilde{b}_1^{(i)} \\ \vdots \\ \widetilde{b}_{r-i-1}^{(i)} \end{bmatrix} = \begin{bmatrix} p^{i-1} b_0^{(i-1)} \\ p^i b_1^{(i-1)} \\ \vdots \\ p^{r-2} b_{r-i-1}^{(i-1)} \end{bmatrix} - \begin{bmatrix} p^{i-1}\widetilde{H}_0 \\ p^i \widetilde{H}_1 \\ \vdots \\ p^{r-2}\widetilde{H}_{r-i-1} \end{bmatrix} \boldsymbol{w}^{(i-1)}, \tag{6}$$

write

$$\widetilde{b}_l^{(i)} = p^{i+l} b_l^{(i)}, \tag{7}$$

with $b_l^{(i)} \in \mathbb{Z}_{p^r}^{k_i}$, *for* $l = 0, 1, \ldots, r-i-1$ *and with each* $\boldsymbol{w}^{(i-1)} \in S_{i-1}$, *where*

$$S_{i-1} = \{\boldsymbol{w}^{(i-1)} : \ [\boldsymbol{w}^{(i-1)}]_p = \hat{\boldsymbol{w}}^{(i-1)}, \hat{\boldsymbol{w}}^{(i-1)} \text{ is a solution of (8) for some } \begin{bmatrix} b_0^{(i-1)} \\ b_1^{(i-1)} \\ \vdots \\ b_{r-1-(i-1)}^{(i-1)} \end{bmatrix}\},$$

by solving the system of linear equations in the projection

$$\begin{bmatrix} \widetilde{H}_0 \\ \widetilde{H}_1 \\ \vdots \\ \widetilde{H}_{r-i-1} \end{bmatrix}_p \hat{\boldsymbol{w}}^{(i-1)} = \begin{bmatrix} b_0^{(i-1)} \\ b_1^{(i-1)} \\ \vdots \\ b_{r-1-(i-1)}^{(i-1)} \end{bmatrix}_p, \tag{8}$$

over $\mathbb{Z}_p$. *Then only it remains to solve the equation*

$$\begin{bmatrix} \widetilde{H}_0 \\ \widetilde{H}_1 \\ \vdots \\ \widetilde{H}_{r-i-1} \end{bmatrix}_p \hat{\boldsymbol{w}}^{(i)} = \begin{bmatrix} b_0^{(i)} \\ b_1^{(i)} \\ \vdots \\ b_{r-1-i}^{(i)} \end{bmatrix}_p, \tag{9}$$

by consider the following set

$$S_i = \{\boldsymbol{w}^{(i)} \ : \ [\boldsymbol{w}^{(i)}]_p = \hat{\boldsymbol{w}}^{(i)}, \hat{\boldsymbol{w}}^{(i)} \text{ is a solution of (9) for some } \begin{bmatrix} b_0^{(i)} \\ b_1^{(i)} \\ \vdots \\ b_{r-1-i}^{(i)} \end{bmatrix}\}.$$

Output data: $\{\boldsymbol{w}^{(0)} + p\boldsymbol{w}^{(1)} + \cdots + p^{r-1}\boldsymbol{w}^{(r-1)} \ : \ \boldsymbol{w}^{(i)} \in S_i, \ i = 0, 1, \ldots, r-1\}$.

Next we show that the algorithm actually produces all desired solutions. This will be a corollary of the following result.

Theorem 3. *Let* $\widetilde{H}$ *be in the form of*

$$\widetilde{H} = \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-1}\widetilde{H}_{r-1} \end{bmatrix}, \tag{10}$$

where the rows of $\widetilde{H}_i \in \mathbb{Z}_{p^r}^{k_i \times e}$ *having order* $r - i$, $i = 0, 1, \ldots, r-1$, *and let* b

be given accordingly as

$$b = \begin{bmatrix} b_0 \\ pb_1 \\ \vdots \\ p^{r-1}b_{r-1} \end{bmatrix}. \tag{11}$$

Consider the system of equations

$$\widetilde{H}\boldsymbol{w}^T = b, \tag{12}$$

and the p-adic expansion of $\boldsymbol{w}^T$*,*

$$\boldsymbol{w}^T = \boldsymbol{w}^{(0)} + p\boldsymbol{w}^{(1)} + \cdots + p^{r-1}\boldsymbol{w}^{(r-1)}.$$

Then, $\boldsymbol{w}^T$ *is a solution of the system (12) if and only if, for* $i = 0, 1, \ldots, r-1$*,* $\boldsymbol{w}^{(i)}$ *is a solution of the system of equations*

$$\begin{bmatrix} \widetilde{H}_0 \\ \widetilde{H}_1 \\ \vdots \\ \widetilde{H}_{r-i-1} \end{bmatrix}_p \left[\boldsymbol{w}^{(i)}\right]_p = \begin{bmatrix} b_0^{(i)} \\ b_1^{(i)} \\ \vdots \\ b_{r-i-1}^{(i)} \end{bmatrix}_p, \tag{13}$$

over $\mathbb{Z}_p$*, where* $b_l^{(0)} = b_l$*,* $l = 0, 1, \ldots, r-1$*, and*

$$\begin{bmatrix} b_0 \\ pb_1 \\ \vdots \\ p^{r-i-1}b_{r-i-1} \end{bmatrix} - \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-i-1}\widetilde{H}_{r-i-1} \end{bmatrix} (\boldsymbol{w}^{(0)} + p\boldsymbol{w}^{(1)} + \cdots + p^{i-1}\boldsymbol{w}^{(i-1)}) = \begin{bmatrix} \widetilde{b}_0^{(i)} \\ \widetilde{b}_1^{(i)} \\ \vdots \\ \widetilde{b}_{r-i-1}^{(i)} \end{bmatrix}, \tag{14}$$

where $\widetilde{b}_j^{(i)}$ *is given by*

$$\begin{bmatrix} \widetilde{b}_0^{(i)} \\ \widetilde{b}_1^{(i)} \\ \vdots \\ \widetilde{b}_{r-i-1}^{(i)} \end{bmatrix} = \begin{bmatrix} p^{i-1}b_0^{(i-1)} \\ p^i b_1^{(i-1)} \\ \vdots \\ p^{r-2}b_{r-i-1}^{(i-1)} \end{bmatrix} - \begin{bmatrix} p^{i-1}\widetilde{H}_0 \\ p^i \widetilde{H}_1 \\ \vdots \\ p^{r-2}\widetilde{H}_{r-i-1} \end{bmatrix} \boldsymbol{w}^{(i-1)} \tag{15}$$

and

$$\widetilde{b}_\ell^{(i)} = p^{i+\ell} b_\ell^{(i)},$$

for $\ell = 0, 1, \ldots, r-i-1$.

Proof. Consider the p-adic expansion of $\boldsymbol{w}^T$,

$$\boldsymbol{w}^T = \boldsymbol{w}^{(0)} + p\boldsymbol{w}^{(1)} + \cdots + p^{r-1}\boldsymbol{w}^{(r-1)},$$

with $\boldsymbol{w}^{(i)}$'s are column vectors with e entries from $\mathcal{A}_p$, $i = 0, 1, \ldots, r-1$.

To show the necessary condition, we assume that $\boldsymbol{w}^T$ is a solution of $\widetilde{H}\boldsymbol{w}^T = b$. By induction on i, $i = 0, 1, \ldots, r-1$, we prove that the followings are hold:

(a)

$$\begin{bmatrix} \widetilde{H}_0 \\ \widetilde{H}_1 \\ \vdots \\ \widetilde{H}_{r-i-1} \end{bmatrix}_p \left[\boldsymbol{w}^{(i)}\right]_p = \begin{bmatrix} b_0^{(i)} \\ b_1^{(i)} \\ \vdots \\ b_{r-i-1}^{(i)} \end{bmatrix}_p,$$

over $\mathbb{Z}_p$,

(b)

$$\begin{bmatrix} b_0 \\ pb_1 \\ \vdots \\ p^{r-i-1}b_{r-i-1} \end{bmatrix} - \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-i-1}\widetilde{H}_{r-i-1} \end{bmatrix} (\boldsymbol{w}^{(0)} + p\boldsymbol{w}^{(1)} + \cdots + p^{i-1}\boldsymbol{w}^{(i-1)}) = \begin{bmatrix} \widetilde{b}_0^{(i)} \\ \widetilde{b}_1^{(i)} \\ \vdots \\ \widetilde{b}_{r-i-1}^{(i)} \end{bmatrix},$$

with $\widetilde{b}_j^{(i)}$ obtained in equation (15) such that $\widetilde{b}_l^{(i)} = p^{i+l} b_l^{(i)}$, for some $b_l^{(i)} \in \mathbb{Z}_{p^r}^{k_l}$, and for all $l = 0, 1, \ldots, r-i-1$.

Let $i = 0$.
(a) Since

$$\begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-1}\widetilde{H}_{r-1} \end{bmatrix} [\boldsymbol{w}^{(0)} + p\boldsymbol{w}^{(1)} + \cdots + p^{r-1}\boldsymbol{w}^{(r-1)}] = \begin{bmatrix} b_0 \\ pb_1 \\ \vdots \\ p^{r-1}b_{r-1} \end{bmatrix}, \tag{16}$$

then by multiplying each block $p^i\widetilde{H}_i$ and $p^i b_i$ by p^{r-i-1}, we consider the following equality

$$p^{r-1} \begin{bmatrix} \widetilde{H}_0 \\ \widetilde{H}_1 \\ \vdots \\ \widetilde{H}_{r-1} \end{bmatrix} \boldsymbol{w}^{(0)} = p^{r-1} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{r-1} \end{bmatrix}. \tag{17}$$

Because of the isomorphism $p^{r-1}\mathbb{Z}_{p^r} \cong \mathbb{Z}_p$, $\boldsymbol{w}^{(0)}$ is the solution of (17) if and only if $\boldsymbol{w}^{(0)}$ is the solution of

$$\begin{bmatrix} \widetilde{H}_0 \\ \widetilde{H}_1 \\ \vdots \\ \widetilde{H}_{r-1} \end{bmatrix}_p \left[\boldsymbol{w}^{(0)}\right]_p = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{r-1} \end{bmatrix}_p, \tag{18}$$

over $\mathbb{Z}_p$ (considering the entries of $\boldsymbol{w}^{(0)}$ as an element of $\mathbb{Z}_{p^r}$).

(b) $\begin{bmatrix} \widetilde{b}_0^{(0)} \\ \widetilde{b}_1^{(0)} \\ \vdots \\ \widetilde{b}_{r-1}^{(0)} \end{bmatrix} = \begin{bmatrix} b_0 \\ pb_1 \\ \vdots \\ p^{r-1}b_{r-1} \end{bmatrix}$ by definition (see Step 2 of Algorithm 2).

Now we assume that (a) and (b) are satisfied for $j = 0, 1, \ldots, i$. We prove that (a) and (b) are also true for $i+1$. Let us consider first part (b). In this

case, we rewrite

$$\begin{bmatrix} b_0 \\ pb_1 \\ \vdots \\ p^{r-(i+1)-1}b_{r-(i+1)-1} \end{bmatrix} - \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-(i+1)-1}\widetilde{H}_{r-(i+1)-1} \end{bmatrix} (\boldsymbol{w}^{(0)} + p\boldsymbol{w}^{(1)} + \cdots + p^{i-1}\boldsymbol{w}^{(i-1)} + p^i\boldsymbol{w}^{(i)})$$

$$= \begin{bmatrix} b_0 \\ pb_1 \\ \vdots \\ p^{r-(i+1)-1}b_{r-(i+1)-1} \end{bmatrix} - \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-(i+1)-1}\widetilde{H}_{r-(i+1)-1} \end{bmatrix} (\boldsymbol{w}^{(0)} + p\boldsymbol{w}^{(1)} + \cdots + p^{i-1}\boldsymbol{w}^{(i-1)})$$

$$- \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-(i+1)-1}\widetilde{H}_{r-(i+1)-1} \end{bmatrix} p^i\boldsymbol{w}^{(i)}.$$

By induction hypothesis, this is equivalent to

$$\begin{bmatrix} p^i b_0^{(i)} \\ p^{i+1} b_1^{(i)} \\ \vdots \\ p^{r-2} b_{r-(i+1)-1}^{(i)} \end{bmatrix} - \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-(i+1)-1}\widetilde{H}_{r-(i+1)-1} \end{bmatrix} p^i\boldsymbol{w}^{(i)}.$$

By (15), the last statement is presicely $\begin{bmatrix} \widetilde{b}_0^{(i)} \\ \widetilde{b}_1^{(i)} \\ \vdots \\ \widetilde{b}_{r-(i+1)-1}^{(i)} \end{bmatrix}$ where $\widetilde{b}_l^{(i+1)} \in p^{i+1+l}\mathbb{Z}_{p^r}^{k_l}$, $l = 0, 1, \ldots, r-(i+1)-1$. Therefore, $\widetilde{b}_l^{(i+1)} = p^{i+1+l}b_l^{(i+1)}$, for some $b_l^{(i+1)} \in \mathbb{Z}_{p^r}^{k_l}$, $l = 0, 1, \ldots, r-(i+1)-1$.

To prove (a), we rewrite the equality $\widetilde{H}\boldsymbol{w}^T = b$ as

$$\begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-1}\widetilde{H}_{r-1} \end{bmatrix} (\boldsymbol{w}^{(0)} + p\boldsymbol{w}^{(1)} + \cdots + p^{r-1}\boldsymbol{w}^{(r-1)}) = \begin{bmatrix} b_0 \\ pb_1 \\ \vdots \\ p^{r-1}b_{r-1} \end{bmatrix}.$$

By removing the first i-term from the left hand side to the right hand side, we write the following equality

$$\begin{aligned} &\begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-(i+1)-1}\widetilde{H}_{r-(i+1)-1} \\ p^{r-(i+1)}\widetilde{H}_{r-(i+1)} \\ \vdots \\ p^{r-1}\widetilde{H}_{r-1} \end{bmatrix} (p^{i+1}\boldsymbol{w}^{(i+1)} + \cdots + p^{r-1}\boldsymbol{w}^{(r-1)}) \\ &= \begin{bmatrix} b_0 \\ pb_1 \\ \vdots \\ p^{r-1}b_{r-1} \end{bmatrix} - \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-1}\widetilde{H}_{r-1} \end{bmatrix} (\boldsymbol{w}^{(0)}p\boldsymbol{w}^{(1)} + \cdots + p^i\boldsymbol{w}^{(i)}). \end{aligned}$$

From (b), for the first $(i+1)$-th terms of the above equality, we can consider

$$\begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-1-(i+1)}\widetilde{H}_{r-1-(i+1)} \end{bmatrix} (p^{i+1}\boldsymbol{w}^{(i+1)} + \cdots + p^{r-1}\boldsymbol{w}^{(r-1)}) = \begin{bmatrix} p^{i+1}b_0^{(i+1)} \\ p^{i+2}b_1^{(i+1)} \\ \vdots \\ p^{r-2}b_{r-1-(i+1)}^{(i+1)} \end{bmatrix},$$

or equivalently

$$\begin{bmatrix} p^{i+1}\widetilde{H}_0 \\ p^{i+2}\widetilde{H}_1 \\ \vdots \\ p^{r-1}\widetilde{H}_{r-1-(i+1)} \end{bmatrix} (\boldsymbol{w}^{(i+1)} + p\boldsymbol{w}^{(i+2)} + \cdots + p^{r-1-(i+1)}\boldsymbol{w}^{(r-1)}) = \begin{bmatrix} p^{i+1}b_0^{(i+1)} \\ p^{i+2}b_1^{(i+1)} \\ \vdots \\ p^{r-1}b_{r-1-(i+1)}^{(i+1)} \end{bmatrix}.$$

For $t = i+1, \ldots, r-1$, to multiply each corresponding blocks by p^{r-1-t} gives

$$\begin{bmatrix} p^{r-1-(i+1)}p^{i+1}\widetilde{H}_0 \\ p^{r-1-(i+2)}p^{i+2}\widetilde{H}_1 \\ \vdots \\ p^{r-1}\widetilde{H}_{r-1-(i+1)} \end{bmatrix} (\boldsymbol{w}^{(i+1)} + p\boldsymbol{w}^{(i+2)} + \cdots + p^{r-(i+1)-1}\boldsymbol{w}^{(r-1)}) = \begin{bmatrix} p^{r-1-(i+1)}p^{i+1}b_0^{(i+1)} \\ p^{r-1-(i+1)}p^{i+2}b_1^{(i+1)} \\ \vdots \\ p^{r-1}b_{r-1-(i+1)}^{(i+1)} \end{bmatrix},$$

which is equivalent to

$$p^{r-1}\begin{bmatrix} \widetilde{H}_0 \\ \widetilde{H}_1 \\ \vdots \\ \widetilde{H}_{r-(i+1)-1} \end{bmatrix} \boldsymbol{w}^{(i+1)} = p^{r-1}\begin{bmatrix} b_0^{(i+1)} \\ b_1^{(i+1)} \\ \vdots \\ b_{r-(i+1)-1}^{(i+1)} \end{bmatrix}.$$

Once we use the projection and use the isomorhism $p^{r-1}\mathbb{Z}_{p^r} \simeq \mathbb{Z}_p$, it follows the desired that $\boldsymbol{w}^{(i+1)}$ is solution of

$$\begin{bmatrix} \widetilde{H}_0 \\ \widetilde{H}_1 \\ \vdots \\ \widetilde{H}_{r-(i+1)-1} \end{bmatrix}_p \left[\boldsymbol{w}^{(i+1)}\right]_p = \begin{bmatrix} b_0^{(i+1)} \\ b_1^{(i+1)} \\ \vdots \\ b_{r-(i+1)-1}^{(i+1)} \end{bmatrix}_p.$$

Conversely, we now consider $\boldsymbol{w}^{(i)} \in \mathcal{A}_p^{k_i}$ satisfying (13) and (14), for $i = 0, 1, \ldots, r-1$. From equation (13), we have that

$$p^{r-1}\begin{bmatrix}\widetilde{H}_0\\ \widetilde{H}_1\\ \vdots\\ \widetilde{H}_{r-i}\end{bmatrix}\boldsymbol{w}^{(i)} = p^{r-1}\begin{bmatrix}b_0^{(i)}\\ b_1^{(i)}\\ \vdots\\ b_{r-i}^{(i)}\end{bmatrix},$$

for $i = 0, \ldots, r-1$. In particular, $p^{r-1}\widetilde{H}_0\boldsymbol{w}^{(r-1)} = p^{r-1}b_0^{(r-1)}$.

Let us assume that

$$\begin{bmatrix}\widetilde{H}_0\\ p\widetilde{H}_1\\ \vdots\\ p^{r-(j+1)}\widetilde{H}_{r-(j+1)}\end{bmatrix}(p^j\boldsymbol{w}^{(j)} + \cdots + p^{(r-1)}\boldsymbol{w}^{(r-1)}) = \begin{bmatrix}p^jb_0^{(j)}\\ p^{j+1}b_1^{(j)}\\ \vdots\\ p^{r-1}b_{r-(j+1)}^{(j)}\end{bmatrix},$$

for all $j = 1, \ldots, r-1$, and let us prove that it is also true for $j+1$, *i.e.*,

$$\begin{bmatrix}\widetilde{H}_0\\ p\widetilde{H}_1\\ \vdots\\ p^{r-j}\widetilde{H}_{r-j}\\ p^{r-(j+1)}\widetilde{H}_{r-(j+1)}\end{bmatrix}(p^{j-1}\boldsymbol{w}^{(j-1)}+p^j\boldsymbol{w}^{(j)}+\cdots+p^{(r-1)}\boldsymbol{w}^{(r-1)}) = \begin{bmatrix}p^{j-1}b_0^{(j-1)}\\ p^jb_1^{(j-1)}\\ \vdots\\ p^{r-2}b_{r-(j+1)}^{(j-1)}\\ p^{r-1}b_{r-j}^{(j-1)}\end{bmatrix}. \tag{19}$$

Note that by induction hypothesis, the left hand side of the equality can be

written as

$$\begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-(j+1)}\widetilde{H}_{r-(j+1)} \end{bmatrix} p^{j-1}\boldsymbol{w}^{(j-1)} + \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-(j+1)}\widetilde{H}_{r-(j+1)} \end{bmatrix} (p^j\boldsymbol{w}^{(j)} + \cdots + p^{(r-1)}\boldsymbol{w}^{(r-1)})$$

$$= \begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-(j+1)}\widetilde{H}_{r-(j+1)} \end{bmatrix} p^{j-1}\boldsymbol{w}^{(j-1)} + \begin{bmatrix} p^j b_0^{(j)} \\ p^{j+1} b_1^{(j)} \\ \vdots \\ p^{r-1} b_{r-(j+1)}^{(j)} \end{bmatrix}.$$

From (15), it follows that

$$\begin{bmatrix} \widetilde{H}_0 \\ p\widetilde{H}_1 \\ \vdots \\ p^{r-(j+1)}\widetilde{H}_{r-(j+1)} \end{bmatrix} p^{j-1}\boldsymbol{w}^{(j-1)} + \begin{bmatrix} p^j b_0^{(j)} \\ p^{j+1} b_1^{(j)} \\ \vdots \\ p^{r-1} b_{r-(j+1)}^{(j)} \end{bmatrix} = \begin{bmatrix} p^{j-1} b_0^{(j-1)} \\ p^j b_1^{(j-1)} \\ \vdots \\ p^{r-2} b_{r-(j+1)}^{(j-1)} \end{bmatrix}.$$

Moreover, by (19), for each corresponding blocks, we can consider

$$p^{r-j}\widetilde{H}_{r-j}p^{j-1}\boldsymbol{w}^{(j-1)} = p^{r-1}\widetilde{H}_{r-j}\boldsymbol{w}^{(j-1)} = p^{r-1}b_{r-j}^{(j-1)},$$

. So, we conclude that (17) is true.

□

Note that the algorithm determines, at each iteration, the solutions of (13) and computes the vectors (15). Therefore, we conclude that the output of Algorithm 2 is the set of solutions of the system (12), as stated in the following corollary.

Corollary 1. *Let $\widetilde{H}$ and b be defined as in (3) and (4), respectively. Then the algorithm produces all possible solutions of the system $\widetilde{H}\boldsymbol{w}^T = b$.*

Remark 1. *Algorithm 2 has complexity order $\mathcal{O}(r(k_0+k_1+\cdots+k_{r-1})^2(e+1))$ operations in the finite field $\mathbb{Z}_p$. In fact, the main computational effort in each step of the algorithm is to solve the systems of linear equations (5) (in Step 1) and (9) in the other $r-1$ steps. These r systems have at most*

$k_0 + k_1 + \cdots + k_{r-1}$ equations and e unknowns and the arithmetic complexity order over $\mathbb{Z}_p$ to solve each of these systems, using the Gaussian elimination procedure, is $\mathcal{O}((k_0 + k_1 + \cdots + k_{r-1})^2(e+1))$. In [3] an algorithm to deal with finite rings was presented assuming that an algorithm exists which can perform $n \times n$ matrix multiplication in $\backsim cn\omega$ ring operations, for some c and some ω. But the memory cost of such algorithm is so high that it is mostly of theoretical interest. Note that a naïve matrix multiplication gives $c = 2$ and $\omega = 3$, Strassen's Algorithm $\omega = log_2^7 \approx 2.807$, and c varying by implementation and an improved version given by the Coppersmith-Winograd algorithm can do it in $\mathcal{O}(n^{2.375477})$ time.

The following result states the number of possible codewords in terms of the parameters of H in the standard form.
In other words, consider $\widetilde{H}$ as in (10) and define c_i as the number of linearly independent columns of

$$\begin{bmatrix} \widetilde{H}_0 \\ \widetilde{H}_1 \\ \vdots \\ \widetilde{H}_i \end{bmatrix},$$

for $i = 0, 1, \ldots, r-1$.

We uniquely decompose the vector of unknowns $\boldsymbol{w} = (w_1, \ldots, w_e)$ as

$$\boldsymbol{w}^T = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_e \end{bmatrix} = \begin{bmatrix} w_{01} \\ w_{02} \\ \vdots \\ w_{0e} \end{bmatrix} + p \begin{bmatrix} w_{11} \\ w_{12} \\ \vdots \\ w_{1e} \end{bmatrix} + \cdots + p^{r-1} \begin{bmatrix} w_{(r-1)1} \\ w_{(r-1)2} \\ \vdots \\ w_{(r-1)e} \end{bmatrix},$$

with $w_{ij} \in \mathcal{A}_p$, $i = 0, 1, \ldots, r-1$, $j = 1, 2, \ldots, e$. The number of solutions of $H\boldsymbol{w}^T = b$ is equal to $\prod_{i=0}^{r-1} |S_i|$, where $|S_i|$ is the number of solutions of (9), and the next corollary follows immediately.

Corollary 2. *Let $\mathcal{C}$ be a block code defined as above. Then, the number of solutions of $\boldsymbol{v}$ is given by*

$$s = p^{er - \sum_{i=0}^{r-1} c_i}.$$

The next example illustrates the application of Algorithm 2 in the determination of the solutions of a system of the form $H\boldsymbol{w}^T = b$.

Example 1. *Let us consider the block code* $\mathcal{C} = \ker H$*, where*

$$H = \begin{bmatrix} H_0 \\ 3H_1 \\ 9H_2 \end{bmatrix} \in \mathbb{Z}_{27},$$

with $H_0 = \begin{bmatrix} 1 & 3 & 0 & 2 & 10 \end{bmatrix}$, $H_1 = \begin{bmatrix} 0 & 4 & 1 & 5 & 7 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}$, $H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 \end{bmatrix}$ *and* $v = \begin{bmatrix} v_1 & 1 & v_2 & v_3 & 3 \end{bmatrix} \in \mathcal{C}$ *with erasures* v_1, v_2, v_3.

To compute the erasures of v*, let us represent* $v_i = v_{i0} + 3v_{i1} + 9v_{i2}$*, with* $v_{ij} \in \{0, 1, 2\}$*,* $i = 1, 2, 3$*,* $j = 0, 1, 2$*. Then, since* $Hv^T = 0$*, we obtain*

$$\begin{bmatrix} \widetilde{H}_0 \\ 3\widetilde{H}_1 \\ 9\widetilde{H}_2 \end{bmatrix} \boldsymbol{w}^T = \begin{bmatrix} b_0 \\ 3b_1 \\ 9b_2 \end{bmatrix},$$

where $\widetilde{H}_0 = \begin{bmatrix} 1 & 0 & 2 \end{bmatrix}$, $\widetilde{H}_1 = \begin{bmatrix} 0 & 1 & 5 \\ 0 & 0 & 0 \end{bmatrix}$, $\widetilde{H}_2 = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$, $\boldsymbol{w} = \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix}$, $b_0 = 21$, $b_1 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$ *and* $b_2 = 0$.

In Step 1, the Algorithm 2 solves the system

$$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}_p \hat{\boldsymbol{w}}^{(0)} = \begin{bmatrix} 21 \\ 2 \\ 0 \\ 0 \end{bmatrix}_p, \tag{20}$$

over $\mathbb{Z}_3$*. It can be written as*

$$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}_p \hat{\boldsymbol{w}}^{(0)} = \begin{bmatrix} 0 \\ 2 \\ 0 \\ 0 \end{bmatrix}_p,$$

which has unique solution $\begin{bmatrix}0\\2\\0\end{bmatrix}$. *Then* $S_0 = \{\begin{bmatrix}0\\2\\0\end{bmatrix}\} \subset \mathcal{A}_p^3$.

The next step computes

$$\begin{bmatrix}\widetilde{b}_0^{(1)}\\ \widetilde{b}_1^{(1)}\\ \widetilde{b}_2^{(1)}\end{bmatrix} = \begin{bmatrix}b_0\\ 3b_1\\ 9b_2\end{bmatrix} - \begin{bmatrix}c\widetilde{H}_0\\ 3\widetilde{H}_1\\ 9\widetilde{H}_2\end{bmatrix} \boldsymbol{w}_0. \tag{21}$$

Note that the last rows of the matrices in equation (21) is equal to 0, *and when we plug in entries of these matrices we obtain the following*

$$\begin{bmatrix}21\\6\\0\end{bmatrix} - \begin{bmatrix}1&0&2\\0&3&15\\0&0&0\end{bmatrix}\begin{bmatrix}0\\2\\0\end{bmatrix} = \begin{bmatrix}21\\0\\0\end{bmatrix}. \tag{22}$$

Then,

$$\begin{aligned}\widetilde{b}_0^{(1)} = 3b_0^{(1)} \quad &\Longleftrightarrow \quad b_0^{(1)} = 7,\\ \widetilde{b}_1^{(1)} = 9b_1^{(1)} \quad &\Longleftrightarrow \quad b_1^{(1)} = \begin{bmatrix}0\\0\end{bmatrix}.\end{aligned} \tag{23}$$

Next, in order to find $\hat{\boldsymbol{w}}^{(1)}$, *the algorithm solves the following equation*

$$\begin{bmatrix}1&0&2\\0&1&5\\0&0&0\end{bmatrix}_p \hat{\boldsymbol{w}}^{(1)} = \begin{bmatrix}7\\0\\0\end{bmatrix}_p, \tag{24}$$

over $\mathbb{Z}_3$, *which is equivalent to*

$$\begin{bmatrix}1&0&2\\0&1&2\\0&0&0\end{bmatrix}_p \boldsymbol{w}^{(1)} = \begin{bmatrix}1\\0\\0\end{bmatrix}_p. \tag{25}$$

The solutions of the system (25) are $\begin{bmatrix} 1+\widetilde{c} \\ \widetilde{c} \\ \widetilde{c} \end{bmatrix}$, *with a free parameter* $\widetilde{c} \in \mathbb{Z}_3$.

Thus $S_1 = \{ \begin{bmatrix} 1+c \\ c \\ c \end{bmatrix} \in \mathcal{A}_p^3 \ : \ c \in \mathcal{A}_p \}$. *The next step computes*

$$\begin{aligned} \widetilde{b}_0^{(2)} &= 3b_0^{(1)} - 3\widetilde{H}_0 \boldsymbol{w}^{(1)} \\ &= 3 \times 7 - 3 \begin{bmatrix} 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 1+c \\ c \\ c \end{bmatrix} \\ &= 21 - 3\left[1 + 3c\right] \\ &= 21 - 3 + 18c \\ &= 18 + 18c, \end{aligned}$$

and therefore

$$\widetilde{b}^{(2)} = 9b_0^{(2)} \iff b_0^{(2)} = 2 + 2c.$$

Finally, the algorithm solves the system

$$[\widetilde{H}_0]_p \, \boldsymbol{w}^{(2)} = [2 + 2c]_p,$$

over $\mathbb{Z}_3$, *where* $[\widetilde{H}_0]_p = \begin{bmatrix} 1 & 0 & 2 \end{bmatrix}$. *The solutions of this system are* $\begin{bmatrix} 2 + 2\widetilde{c} + 2\widetilde{c}_1 \\ \widetilde{b}_1 \\ \widetilde{c}_1 \end{bmatrix}$

with $\widetilde{b}_1, \widetilde{c}_1 \in \mathbb{Z}_3$, *and therefore we obtain*

$$S_2 = \{ \begin{bmatrix} 2 + 2c + 2c_1 \\ b_1 \\ c_1 \end{bmatrix} \ : \ b_1, c_1 \in \mathcal{A}_p \}.$$

Consequently, we obtain all solutions as

$$\boldsymbol{w}^T = \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix} + 3 \begin{bmatrix} 1+c \\ c \\ c \end{bmatrix} + 9 \begin{bmatrix} 2+2c+2c_1 \\ b_1 \\ c_1 \end{bmatrix},$$

with b_1, c_1, *and* $c \in \mathcal{A}_p$.

4. Conclusions and future work

In this work we have shown how one should proceed in order to determine all the possible outputs of a list decoding algorithm. Not surprisingly, the number of these possible codewords is determined by the matrices obtained in the standard form of a parity-check matrix of the code. The provided algorithm is simple but computes all possible coordinates of the corrupted vector. An interesting avenue for future research is to extend these results and consider different types of channels when also error may occur. Further, we note that the algorithm presented here combined with the recent results obtained in [13] could be used to develop new Berlekamp-Massey-type decoding algorithms for codes over $\mathbb{Z}_{p^r}$. This also requires further research.

ACKNOWLEDGMENT

This work of the second and forth authors 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. The first author partially supported by Ministerio de Ciencia e Innovación via the grant with ref. PID2019-108668GB-I00. The third author is supported by the Swiss Confederation through the Swiss Goverment Excellence Scholarship no: 2019.0413 and by the Swiss National Science Foundation grant n. 188430.

Referências

[1] Andrade, A., Interlando, J., Palazzo Jr., R., 2003. Alternant and BCH codes over certain rings. Computational & Applied Mathematics 22, 233 – 247.

[2] Armand, M. A., 2005. List decoding of generalized reed-solomon codes over commutative rings. IEEE Trans. Inform. Theory 51 (1), 411–419.

[3] Bard, G. V., 2007. Algorithms for solving linear and polynomial systems of equations over finite fields, with applications to cryptanalysis. Ph.D. thesis, USA.

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

[5] DeCastro-García, N., V. Carriegos, M., Muñoz Castaneda, A., 2016. A characterization of von neumann rings in terms of linear systems. Linear Algebra and its Applications 494, 236–244.

[6] Dougherty, S. T., Saltürk, E., 2017. Codes over a family of local frobenius rings, gray maps and self-dual codes. Discrete Applied Mathematics 217, 512 – 524.

[7] 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.

[8] Guruswami, V., Sudan, M., 1999. Improved decoding of reed-solomon and algebraic-geometric codes. IEEE Trans. Inform. Theory 45, 1757–1767.

[9] Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., Sole, P., 1994. The z4-linearity of kerdock, preparata, goethals, and related codes. IEEE Trans. Inform. Theory 40 (2), 301–319.

[10] Interlando, J. C., Palazzo, R., Elia, M., 1997. On the decoding of reed-solomon and bch codes over integer residue rings. IEEE Trans. Inform. Theory 43 (3), 1013–1021.

[11] Kotter, R., Vardy, A., 2003. Algebraic soft-decision decoding of reed-solomon codes. IEEE Trans. Inform. Theory 49 (11), 2809–2825.

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

[13] Kuijper, M., Pinto, R., May 2017. An iterative algorithm for parametrization of shortest length linear shift registers over finite chain rings. Designs, Codes and Cryptography 83 (2), 283–305.

[14] Kuijper, M., Polderman, J., 2002. Behavioral models for list decoding. Journal of Mathematical and Computer Modeling of Dynamical Systems (MCMDS) 8, 429–443.

[15] Kuijper, M., Polderman, J., 2004. Reed-Solomon list decoding from a system theoretic perspective. IEEE Trans. Inf. Th. IT-50, 259–271.

[16] MacWilliams, F. J., Sloane, N. J., 1977. The Theory of Error-Correcting Codes. North Holland, Amsterdam.

[17] McDonald, B. R., 1984. Linear algebra over commutative rings / Bernard R. McDonald. M. Dekker New York.

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

[19] Norton, G. H., Sălăgean, A., 1999. On efficient decoding of alternant codes over a commutative ring,. In: Walker, M. (Ed.), Cryptography and Coding. Springer Berlin Heidelberg, pp. 173–178.

[20] Norton, G. H., Sălăgean, A., 2001. On the Hamming distance of linear codes over a finite chain ring. IEEE Trans. Inform. Theory 46 (3), 1060–1067.

[21] Oued, M. E., Napp, D., Pinto, R., Toste, M., 2019. On duals and parity-checks of convolutional codes over $\mathbb{Z}_{p^r}$. Finite Fields and Their Applications 55, 1 – 20.

[22] Oued, M. E., Solé, P., 2013. MDS convolutional codes over a finite ring. IEEE Trans. Inform. Theory 59 (11), 7305 – 7313.