23rd International Symposium on Mathematical Theory of Networks and Systems
Hong Kong University of Science and Technology, Hong Kong, July 16-20, 2018

List decoding of linear codes over $\mathbb{Z}_{p^r}$

D. Napp[1], M. Toste[1,2] and R. Pinto[1]

***Abstract*— In this work we study the problem of list decoding of block codes over finite rings over the erasure channel. We provide explicit formulas for the list decoding size of a linear code over $\mathbb{Z}_{p^r}$ and show that this number is determined by the number of independent columns of a series of matrices obtained from the p-adic decomposition of a parity-check matrix of the code. The result is constructive in the sense that it can lead to an algorithm for list decoding of these codes. This work can be considered as a first step toward the study of list decoding over more difficult channels and codes, e.g., convolutional codes.**

***Index Terms*— linear codes over finite rings, erasure channel, list decoding.**

***AMS subject classifications* — 68P30, 11T71.**

I. INTRODUCTION

After a paper by Hammons et al. [1], where it was shown that certain binary nonlinear codes can be viewed, via a Gray mapping, as linear codes over the ring $\mathbb{Z}_4$, a great interest raised in linear codes over rings. This line of research continue to attract a great deal of attention for their new role in algebraic coding theory and for their successful application in combined coding and modulation, see [2], [3], [4], [5] for some interesting constructions.

In this paper we address the problem of list decoding of linear block codes over the finite ring $\mathbb{Z}_{p^r}$ [6], [7], [8]. In particular, in this preliminary work we focus on decoding over the erasure channel, i.e., we assume to know the location of the errors in the received corrupted codeword. We provide a result that can be straightward made into an algorithm to solve this problem and formulas for the number of possible outputs of the algorithm. The results will be given in terms of the integers of the p-adic expansion of a parity-check matrix H (the expansion performed componentwise) of the code. The number of independent columns of the matrix obtained by stacking the matrices of the p-adic expansion of H will determine the size of the list in our algorithm for list decoding.

II. PRELIMINARIES RESULTS

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

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

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

$$v \in \mathcal{C} \Leftrightarrow Hv = 0,$$

and then

$$\mathcal{C} = \ker_{\mathbb{Z}_{p^r}} H^T.$$

The ring $\mathbb{Z}_{p^r}$ is a local ring [9], i.e., its elements which are zero divisors form an additive Abelian group and using the p-standard form of H, as described in [10] (see also [11] for details), we can write H uniquely as

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

where $H_i \in \mathbb{Z}_{p^r}^{h_i\times n}$, $\sum_{i=0}^{r-1} h_i = n-k$.

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

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

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

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

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

1) $d(\mathcal{C}) = d$;
2) we can correct $d-1$ erasures;
3) Any $d-1$ columns of H are linearly independents and there exists d columns of H that are linearly dependent;
4) Any $d-1$ columns of H_0 are linearly independents and there exists d columns of H_0 that are linearly dependent.

*This work was not 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] The authors are with CIDMA Center for Research and Development in Mathematics and Applications. Department of Mathematics. University of Aveiro. Campus Universitario de Santiago, 3810-193 Aveiro, Portugal diego@ua.pt, raquel@ua.pt

[2] Instituto Politécnico de Coimbra (ESTGOH), Portugal marisa.toste@estgoh.ipc.pt

Suppose that we receive $v \in \mathbb{Z}_{p^r}^n$ with e erasures and $\widetilde{v} \in \mathbb{Z}_{p^r}^e$ is the subvector of v that corresponds to the positions of the erasures. Then, we can rewrite $Hv = 0$ as

$$\widetilde{H}\widetilde{v} = b, \tag{2}$$

where the matrix $\widetilde{H} \in \mathbb{Z}_{p^r}^{(n-k)\times e}$ is built according to $\widetilde{v}$ and the vector b can be computed from the correct coordinates of v. Obviously, if we regard $\widetilde{v}$ as a vector of to-be-determined variables, the problem of decoding v is equivalent to solving the system of linear equation described in (2). The unique solution of this system is given by the number of linearly independent (over $\mathbb{Z}_{p^r}$) equations (see [9]) which, by Theorem 1, is determined by the number of linearly independent columns of $\widetilde{H}_0$.

If exact decoding is not possible, one may want to perform list decoding and next we will show how this is possible for block codes over $\mathbb{Z}_{p^r}$. In contrast with unique decoding, the list decoding will depend not only on H_0 but also on the remaining $\widetilde{H}_i$, as well $i = 1, \ldots, r-1$.

We divide $\widetilde{H}$ according to the decomposition in (1) as

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

where $\widetilde{H}_i \in \mathbb{Z}_{p^r}^{\widetilde{h}_i \times n}$, $\sum_{i=0}^{r-1} \widetilde{h}_i = n - k$. Let us 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 $i = 0, 1, \ldots, r-1$. Next, we present a result that provides an explicit formula for the number of possible values of the erasures and therefore the size of the list obtained after list decoding.

Theorem 2: Let $\mathcal{C}$ be a block code defined as above. Then, the number of solutions $\widetilde{v}$ in (2) is given by

$$s = p^{er - (c_0 r + \sum_{i=1}^{r-1} (c_i - c_{i-1})(r-i))}.$$

Sketch of the proof: We uniquely decompose the vector of unknowns $\widetilde{v}$ in its p-adic extension as

$$\widetilde{v} = \begin{bmatrix} \widetilde{v}_{01} \\ \widetilde{v}_{02} \\ \vdots \\ \widetilde{v}_{0e} \end{bmatrix} + p \begin{bmatrix} \widetilde{v}_{11} \\ \widetilde{v}_{12} \\ \vdots \\ \widetilde{v}_{1e} \end{bmatrix} + \cdots + p^{r-1} \begin{bmatrix} \widetilde{v}_{(r-1)1} \\ \widetilde{v}_{(r-1)2} \\ \vdots \\ \widetilde{v}_{(r-1)e} \end{bmatrix}$$

and therefore we have er unknowns to determine.

Decomposing b according to the decomposition of H and $\widetilde{H}$, as in (1), we write

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

it follows that

$$p^i \widetilde{H}_i \widetilde{v} = p^i b_i, \tag{3}$$

for $i = 0, 1, \ldots, r-1$. Note that each equation in (3) determines $r - i$ unknowns.

Hence, the number of unknowns determined by equations of (3) are $(c_i - c_{i-1})(r-i)$ with $c_{-1} = 0$, $i = 0, 1, \ldots, r-1$.

Obviously if $c_0 = e$ the systems is uniquely determine and the decoding is finished.

If not, we next impose more equations to $\widetilde{v}$ from

$$p\widetilde{H}_1 \widetilde{v} = pb_1. \tag{4}$$

Hence, the total number of new linearly independent equations that we add is equal to the number of linearly independent columns of $\widetilde{H}_1$ taking out the equations that already appeared in for $\widetilde{H}_0$, i.e., it holds that the total number of new equations of (4) that are not in (3) is $(c_1 - c_0)(r-1)$. If we continue the same reasoning up to $(r-1)$, the result follows. □

Note that the proof of the theorem can be easily made into an algorithm for list decoding.

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 $H_0 = \begin{bmatrix} 1 & 3 & 0 & 2 & 10 \end{bmatrix}$, $H_1 = \begin{bmatrix} 0 & 4 & 1 & 5 & 7 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}$ and $H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 \end{bmatrix}$ 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

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

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

Then, $\widetilde{H}_0 \widetilde{v} = b_0$ means that

$$v_{10} + 3v_{11} + 9v_{12} = 21 + 25v_{30} + 21v_{31} + 9v_{32}, \tag{5}$$

i.e., $c_0 r = 3$ unknowns, v_{10}, v_{11} and v_{12} are functions of v_{30}, v_{31} and v_{32}.

Therefore,

$$\begin{aligned} & 3\widetilde{H}_1\widetilde{v} = 3b_1 \\ \Leftrightarrow \quad & 3\begin{bmatrix} 0 & 1 & 5 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} 21+25v_{30}+21v_{31}+9v_{32} \\ v_{20}+3v_{21}+9v_{22} \\ v_{30}+3v_{31}+9v_{32} \end{bmatrix} = 3\begin{bmatrix} 2 \\ 0 \end{bmatrix} \\ \Leftrightarrow \quad & 3(v_{20}+3v_{21}) = 3(2+4v_{30}+3v_{31}), \end{aligned} \tag{6}$$

i.e., $v_{20}+3v_{21} = 2+4v_{30}+3v_{31}$. That is, $(c_1-c_0)(r-1) = 2$ unknowns, v_{20}, v_{21} are obtained as a function of v_{30} and v_{31}. The variable v_{22} is free.

Finally,

$$\begin{aligned} & 9\widetilde{H}_2\widetilde{v} = 9b_2 \\ \Leftrightarrow \quad & 9\begin{bmatrix} 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 21+25v_{30}+21v_{31}+9v_{32} \\ 2+4v_{30}+3v_{31}+9v_{22} \\ v_{30}+3v_{31}+9v_{32} \end{bmatrix} = 0 \\ \Leftrightarrow \quad & 9 \cdot v_{30} = 0, \end{aligned} \tag{7}$$

i.e., $v_{30} = 0$ and $v_{31}, v_{32} \in \{0,1,2\}$.

The unknowns v_{31}, v_{32} and v_{22} can take any value in $\{0,1,2\}$ and the values of the other $c_0 \cdot r + (c_1 - c_0) \cdot (r-1) + (c_2 - c_1) \cdot (r-2) = 6$ depend on the values of v_{31}, v_{32} and v_{22} by equations (5), (6) and (7). Then the number of solution is

$$3^{3 \cdot 3 - 6} = 27.$$

III. Conclusions and future work

In this work we have presented preliminary results on list decoding of linear codes over the ring $\mathbb{Z}_{p^r}$. 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 determine by the matrices obtained in the p-adic decomposition of a parity-check matrix of the code. The development of these results for block codes will allow us to address the more involved problem of list decoding for convolutional codes over $\mathbb{Z}_{p^r}$. The study of different types of channels is also an interesting line for future work.

ACKNOWLEDGMENT

This work was partially supported by Spanish grant AICO/2017/128 of the Generalitat Valenciana and 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

References

[1] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The z4-linearity of kerdock, preparata, goethals, and related codes," *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 301–319, 1994.

[2] J. C. Interlando, R. Palazzo, and M. Elia, "On the decoding of reed-solomon and bch codes over integer residue rings," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 1013–1021, 1997.

[3] M. E. Oued and P. Sole, "MDS convolutional codes over a finite ring," *IEEE Trans. Inf. Th.*, vol. 59, no. 11, pp. 7305 – 7313, 2013.

[4] M. Kuijper and R. Pinto, "On minimality of convolutional ring encoders," *IEEE Trans. Automat. Contr.*, vol. 55), no. 11, pp. 4890 –4897, 2009.

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

[6] M. A. Armand, "List decoding of generalized reed-solomon codes over commutative rings," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 411–419, 2005.

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

[8] ——, "Reed-Solomon list decoding from a system theoretic perspective," *IEEE Trans. Inf. Th.*, vol. IT-50, pp. 259–271, 2004.

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

[10] G. H. Norton and A. Salagean, "On the hamming distance of linear codes over a finite chain ring," *IEEE Trans. Information Theory*, vol. 46, no. 3, pp. 1060–1067, 2001.

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