Franck Rivel Kamwa Djomou · Hervé Talé Kalachi · Emmanuel Fouotsa

Generalization of low rank parity-check (LRPC) codes over the ring of integers modulo a positive integer

Received: 17 August 2020 / Accepted: 28 May 2021 / Published online: 19 June 2021
© The Author(s) 2021

Abstract Following the work of Gaborit et al. (in: The international workshop on coding and cryptography (WCC 13), 2013) defining LRPC codes over finite fields, Renner et al. (in: IEEE international symposium on information theory, ISIT 2020, 2020) defined LRPC codes over the ring of integers modulo a prime power, inspired by the paper of Kamche and Mouaha (IEEE Trans Inf Theory 65(12):7718–7735, 2019) which explored rank metric codes over finite principal ideal rings. In this work, we successfully extend the work of Renner et al. by constructing LRPC codes over the ring $\mathbb{Z}_m$ which is not a chain ring. We give a decoding algorithm and we study the failure probability of the decoder.

Mathematics Subject Classification 11T71 · 94B35

1 Introduction

In 2013, Gaborit et al. [5] introduced a new family of “rank metric”¹ codes called “low rank parity-check codes” (LRPC codes) over finite fields. These codes are considered to be analogous to low density parity-check (LDPC) codes in Hamming metric, because they share some common ideas on how they are constructed. Compared to others known rank metric codes, LRPC codes have a small minimum distance, but their decoding is efficient and they have a weak algebraic structure [1, 5]; this makes them suitable for cryptography.

The notion of rank metric has recently been extended to Finite Principal Ideal Rings (FPIR) by Kamche et al. in [6], where they analyzed and proposed a decoder for Gabidulin codes over FPIR. Their work inspired the authors of [7] who defined LRPC codes over the small class of rings $\mathbb{Z}_{p^r}$, where p is prime, which are particular FPIR. The authors of [7] conclude their work by introducing the problem of generalization of LRPC codes over a finite ring.

K. D. Franck
Department of Mathematics and Computer Science, Faculty of Sciences, University of Dschang, Dschang, Cameroon
E-mail: rivellkamwa@gmail.com

T. K. Hervé
Computer Engineering Department, National Advanced School of Engineering of Yaoundé, University of Yaoundé 1, Yaoundé, Cameroon
E-mail: hervekalachi@gmail.com

F. Emmanuel (✉)
Department of Mathematics, Higher Teacher Training College, The University of Bamenda, Bamenda, Cameroon
E-mail: emmanuel Fouotsa@yahoo.fr

¹Rank metric is a metric commonly defined on matrices with coefficients in a finite field, where the norm of a matrix is its rank

In this paper, we partially answer this question by extending the construction of LRPC codes to residual rings $\mathbb{Z}_m$, with m not necessarily being a power of a prime integer. We derive a decoder depending on that of Renner et al. and analyze its failure probability.

The article is organized as follows: Sect. 2 recalls the basic notions of the Smith Normal Form of a matrix, the rank metric over the FPIRs and Galois extensions of an FPIR; Sect. 3 presents our main result which is a more general definition of LRPC codes over the rings $\mathbb{Z}_m$; Sect. 4 describes the decoding for this generalization over $\mathbb{Z}_m$ and studies the failure probability of this decoder.

Throughout this paper, unless otherwise specified, we assume that R is a finite commutative principal ideal ring, that means R is finite and all its ideals are principal.

2 Preliminaries

In this section, we provide basic notions needed on FPIR. Indeed, as in the case of finite fields, we need a rank metric for the LRPC codes to evaluate the distance between codewords, and this is defined using the Smith Normal Form of a matrix. We also recall the construction of Galois extensions of FPIR.

2.1 Smith normal form and rank metric

An element $a \in R$ is said to be invertible (or called a unit) if there exists $b \in R$, such that $ab = 1$. Let $a, b \in R$, we say that a divides b , and denote $a|b$, if there exists $c \in R$, such that $b = ca$. We denote by $M_{m \times n}(R)$ the set of all $m \times n$ matrices with entries from R . The $n \times n$ identity matrix is denoted by I_n .

An $m \times n$ matrix $\mathbf{D}$ is diagonal if $D_{i,j} = 0$, whenever $i \neq j$. If $\mathbf{D}$ is a diagonal matrix in $M_{m \times n}(R)$, we will write $\mathbf{D} = \text{diag}(d_1, \dots, d_r)$, where $r = \min\{m, n\}$ and $d_i = D_{i,i}$, $i = 1, \dots, r$.

Theorem 2.1 [3] *For all matrix $\mathbf{A} \in M_{m \times n}(R)$, there are two invertible matrices $\mathbf{P}, \mathbf{Q}$ and a diagonal matrix $\mathbf{D} = \text{diag}(d_1, \dots, d_r)$ with $d_1|d_2|\dots|d_r$, such that $\mathbf{A} = \mathbf{PDQ}$. The elements $d_1, \dots, d_r$ are unique up to associates.*

Definition 2.2 The matrix $\mathbf{D}$, such that $\mathbf{A} = \mathbf{PDQ}$ is called the Smith Normal Form (SNF) of $\mathbf{A}$.

Definition 2.3 The rank and the free rank of $\mathbf{A}$ are, respectively, defined by $rk(\mathbf{A}) := |\{i \in \{1, \dots, r\} : d_i \neq 0\}|$ and $frk(\mathbf{A}) := |\{i \in \{1, \dots, r\} : d_i \text{ is a unit}\}|$, where $\mathbf{D} = \text{diag}(d_1, \dots, d_r)$ is the Smith Normal Form of $\mathbf{A}$.

It is well known that the rank defined above is a norm on the set of matrices with entries from an FPIR [3]. However, in the context of coding in rank metric, we need to define that metric on vectors with entries from a ring. The idea is to consider a ring S larger than the initial FPIR R (S is called an extension of R). The objective being to see the vectors, with coefficients in S , as matrices with coefficients from R and exploit the norm defined above.

2.2 Galois extension of finite local rings

Let R and S be two rings. We say that S is an extension of R if $R \subseteq S$. Suppose R and S are finite and local with respective residue fields $\mathcal{K} = R/m$ and $K = S/M$, respectively, where m and M are their respective maximal ideals, and such that $R \subset S$. Then, S is said to be a separable extension of R if $mS = M$. In this case, K is a separable field extension of $\mathcal{K}$.

Theorem 4.3.1 of [2] gives an equivalent definition of separable extensions:

Theorem 2.4 *Suppose R and S are finite and local with respective residue fields $\mathcal{K} = R/m$ and $K = S/M$, where m and M are their respective maximal ideals, and such that $R \subset S$. S is a separable extension of R of degree r if and only if $S \cong R[x]/(f(x))$, where $f(x) \in S[x]$ is a monic polynomial of degree r , irreducible if projected on $\mathcal{K}$ ($f(x)$ is, therefore, called a basic irreducible polynomial).*

Here, the projection is the epimorphism $\mu : S \rightarrow S/M = K$. The projection of a polynomial $f(x)$ is the polynomial which coefficients are the images of its coefficients under the projection μ .

An R -automorphism of S is an automorphism $\phi : S \rightarrow S$, such that its restriction to R is the identity map on R , i.e., $\phi|_R = 1_R$.

Definition 2.5 [2] The ring S is a Galois extension of R , with Galois group G , if S is a separable extension of R and, for all R -automorphism $\phi \in G$, $\forall s \in S$, $\phi(s) = s$ iff $s \in R$.

Theorem 2.6 [2] The Galois extension S of R of degree r is an R -module and is unique up to isomorphism.

Remark 2.7 Combining Theorem 5.1.5 and Corollary 5.1.6 of [2], we have that a local extension S of a finite and local ring R is a Galois extension if and only if there exists a monic basic irreducible polynomial $f(x) \in S[x]$, such that $S \cong R[x]/(f(x))$.

Definition 2.8 Let S be a Galois extension of an FPIR R . Let $\mathbf{B} = \{b_i, i \in I\}$, be a subset of S . Then:

- The support of $\mathbf{B}$ is the R -submodule generated by $\mathbf{B}$.
- Let us consider F , a submodule of S containing $\mathbf{B}$. Then $\mathbf{B}$ is a basis of F if $\mathbf{B}$ is a generating set of F and its elements are linearly independent. The cardinality of $\mathbf{B}$ is then called the dimension of the submodule.

Remark 2.9 Let us consider particularly the ring $R = \mathbb{Z}_{p^r}$. Then its maximal ideal is $p\mathbb{Z}_{p^r}$. To construct its Galois extension of degree s , find a monic polynomial $f(x) \in \mathbb{Z}_{p^r}[x]$ of degree s that is irreducible when projected on $\mathbb{Z}_p$. The Galois extension in this case is $\mathbb{Z}_{p^r}[x]/(f(x))$ and the Galois group is generated by $\sigma : x \mapsto x^p$.

Analogously to the case of finite fields extensions, we have this Definition of the rank metric of a vector over a finite Galois extension of an FPIR.

Definition 2.10 Let S be a finite Galois extension of the FPIR R of degree r . Then, S is an R -module of dimension r . Let $\mathbf{x} = (x_1, \dots, x_n) \in S^n$ be a vector, and $\{\beta_1, \dots, \beta_r\}$ be a basis of S over R . Then, for $i = 1, \dots, n$, there exists $(x_{j,i})_{j=1,\dots,r} \in R^r$, such that

$$x_i = \sum_{j=1}^r x_{j,i} \beta_j.$$

Thus, we can represent $\mathbf{x}$ by the matrix

$$\mathbf{E}(\mathbf{x}) = \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{r,1} & x_{r,2} & \cdots & x_{r,n} \end{bmatrix} \in M_{r \times n}(R).$$

The rank of $\mathbf{x}$ is then defined as the rank of the matrix $\mathbf{E}(\mathbf{x})$ over R as given in Definition 2.3 using the Smith normal form of $\mathbf{E}(\mathbf{x})$.

This definition is important, since we will deal with vectors with entries from a Galois extension of an FPIR.

In the remaining, unless otherwise specified, we assume that all the vectors are free vectors, that is to say, for any vector $\mathbf{x}$, $\text{frk}(\mathbf{x}) = \text{rk}(\mathbf{x})$; and that value will be called the rank of $\mathbf{x}$.

Following the generalization of Gabidulin codes [4] over FPIR [6], it was recently shown in [7] that LRPC codes [5] can be defined over the small class of rings of integers modulo a prime power. The authors of [7] also provided a decoding algorithm together with an upper bound of its failure probability.

We now proceed in the next section to our result which is the extension of LRPC codes over the ring $\mathbb{Z}_m$ for any positive integer m .

3 Generalization of LRPC codes to the ring of integers modulo a positive integer

Let us consider the ring $\mathbb{Z}_m$, where $m \in \mathbb{N}$. If m is a prime power, then we know how to define LRPC over $\mathbb{Z}_m$ [7]. We focus here on the case, where m is not a prime power. In this case and from the Chinese Remainder Theorem, we have the ring isomorphism:

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

which is the direct-sum decomposition of $\mathbb{Z}_m$, where $m = p_1^{n_1} \cdots p_k^{n_k}$, p_j distinct prime numbers. In view of presenting our contribution to the generalization of LRPC over $\mathbb{Z}_m$, we then need to highlight some concepts on direct sum of modules and rings, especially the construction of Galois extension of a direct sums of rings. Let $\{R_1, \dots, R_k\}$ be a family of modules. We denote by $R = R_1 \oplus \cdots \oplus R_k$ their direct summand; it is the set of elements $(a_1, \dots, a_k)$ or $a_1 + \cdots + a_k$, where $a_i \in R_i$.

Definition 3.1 Let $\mathbf{T} \in R$. Then $\mathbf{T} = T_1 + \cdots + T_k$, with $T_i \in R_i$, $1 \leq i \leq k$.

We will assimilate an element $\mathbf{T} = T_1 + \cdots + T_k$ to a k -tuple $(T_1, \dots, T_k)$ and vice versa. In this way, all the operations shall be carried out component-wise. That's to say we shall adopt the following operations:

Let $\mathbf{U} = (U_1, \dots, U_k)$ and $\mathbf{V} = (V_1, \dots, V_k)$ in R . Then

$$\begin{aligned}\mathbf{U} \cdot \mathbf{V} &= (U_1 V_1, \dots, U_k V_k) \\ \mathbf{U} + \mathbf{V} &= (U_1 + V_1, \dots, U_k + V_k) \\ \mathbf{U}^n &= (U_1^n, \dots, U_k^n) \text{ for some positive integer } n.\end{aligned}$$

Let $\mathbf{H}(X) = H_0 + H_1 X + \cdots + H_n X^n \in R[X]$ be a polynomial of degree n . Then for $\mathbf{U} = (U_1, \dots, U_k) \in R$, the image of $\mathbf{U}$ by $\mathbf{H}$ is defined by :

$$\begin{aligned}\mathbf{H}(\mathbf{U}) &= (H_{0,1}, \dots, H_{0,k}) + (H_{1,1}, \dots, H_{1,k})(U_1, \dots, U_k) + \cdots + (H_{n,1}, \dots, H_{n,k})(U_1^n, \dots, U_k^n) \\ &= ((H_{0,1} + H_{1,1}U_1 + \cdots + H_{n,1}U_1^n), \dots, (H_{0,k} + H_{1,k}U_k + \cdots + H_{n,k}U_k^n)) \\ &= (H_1(U_1), \dots, H_k(U_k)) \text{ with} \\ H_i(X) &= H_{0,i} + H_{1,i}X + \cdots + H_{n,i}X^n \in R_i[X]\end{aligned}$$

Thus, we can also assimilate the polynomial $\mathbf{H}$ to a k -tuple of polynomials $(H_1, \dots, H_k)$ of the same degree, where $H_i \in R_i[X]$ for $i = 1, \dots, k$.

The polynomial $\mathbf{H}$ will be said monic, irreducible or basic irreducible if and only if its components are monic, irreducible or basic irreducible, respectively.

Theorem 3.2 [6] Let $S_1, \dots, S_k$ be k local Galois extensions of the finite local rings $R_1, \dots, R_k$, respectively. Then, $S = S_1 \oplus \cdots \oplus S_k$ is a Galois extension of the ring $R = R_1 \oplus \cdots \oplus R_k$, where S and R are endowed with the component-wise operations given in Definition 3.1.

3.1 Construction of a Galois extension of $\mathbb{Z}_m$

As in the case of finite fields, LRPC codes shall be defined over an extension of the base ring $\mathbb{Z}_m$ to extend somewhat the notion of vector space, since the code in finite fields case is a vector subspace over the base field.

The following proposition is the application of the previous Theorem to the ring $\mathbb{Z}_m$

Proposition 3.3 Let m be a positive integer. Denote $R_{m,i} = \mathbb{Z}_{p_i^{n_i}} = \mathbb{Z}_{q_i}$ and $R_m = \bigoplus_{i=1}^k R_{m,i}$, with $m = p_1^{n_1} \cdots p_k^{n_k}$. Then, $S_{m,s} = \bigoplus_{i=1}^k S_{m,i}$ is a Galois extension of R_m of degree s , where $S_{m,i}$ is the Galois extension of $R_{m,i}$ of degree r , as previously defined. Moreover, $S_{m,s}$ is a Galois extension of $\mathbb{Z}_m$ of degree s .

Proof From the Fundamental Theorem of Arithmetic, m can be decomposed uniquely as products of prime powers, this means it can be written in the form $m = p_1^{n_1} \cdots p_k^{n_k}$, where the p_j are distinct prime numbers, and $n_j \in \mathbb{N}^*$, for $1 \leq j \leq k$.

From the Chinese Remainder Theorem, we get the ring isomorphism

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

which is the local summand decomposition of $\mathbb{Z}_m$.

Let denote $R_{m,i} = \mathbb{Z}_{p_i^{n_i}} = \mathbb{Z}_{q_i}$ and $R_m = \bigoplus_{i=1}^k R_{m,i}$.

We already know how to construct the Galois extensions $S_{m,i}$ of the rings $R_{m,i}$ of degree s (see Remark 2.9).

Set

$$S_{m,s} = \bigoplus_{i=1}^k S_{m,i}$$

then $S_{m,s}$ is a Galois extension of R_m according to Theorem 3.2. Moreover, it is a Galois extension of $\mathbb{Z}_m$ thanks to the isomorphism. $\square$

Remark 3.4 This extension is a direct summand of extensions, and this permits us to see that all operations should be carried out on a direct summand of extensions. Then an element of the extension $S_{m,s}$ is a summand of elements of the extensions $S_{m,i}$.

Definitely, we can only define an extension of $\mathbb{Z}_m$ as a direct summand (or product) of the extensions of the rings $R_{m,i}$. This means that defining an LRPC code over an extension of $\mathbb{Z}_m$ leads to defining an LRPC code over a direct summand of ring extensions.

3.2 Some properties on the Galois extension $S_{m,s}$ of $\mathbb{Z}_m$

We denote by $M_{p \times q}(S_{m,s})$ the set of $p \times q$ matrices with entries from $S_{m,s}$.

Lemma 3.5

$$M_{p \times q}(S_{m,s}) = \bigoplus_{i=1}^k M_{p \times q}(S_{m,i})$$

Proof We already know that each element of $S_{m,s}$ is a unique summand of elements in the $S_{m,i}$.

Let

$$\mathbf{P} = (P_{i,j})_{i=1,\dots,p}^{j=1,\dots,q} \in M_{p \times q}(S_{m,s}).$$

Since $P_{i,j} \in S_{m,s}$, then $P_{i,j} = P_{i,j,1} + \dots + P_{i,j,k}$.

$$\begin{aligned} \mathbf{P} &= \begin{pmatrix} P_{1,1,1} + \dots + P_{1,1,k} & \dots & P_{1,q,1} + \dots + P_{1,q,k} \\ \vdots & \ddots & \vdots \\ P_{p,1,1} + \dots + P_{p,1,k} & \dots & P_{p,q,1} + \dots + P_{p,q,k} \end{pmatrix} \\ &= \begin{pmatrix} P_{1,1,1} & \dots & P_{1,q,1} \\ \vdots & \ddots & \vdots \\ P_{p,1,1} & \dots & P_{p,q,1} \end{pmatrix} + \dots + \begin{pmatrix} P_{1,1,k} & \dots & P_{1,q,k} \\ \vdots & \ddots & \vdots \\ P_{p,1,k} & \dots & P_{p,q,k} \end{pmatrix} \\ \mathbf{P} &= \mathbf{P}_1 + \dots + \mathbf{P}_k, \quad \mathbf{P}_l \in M_{p \times q}(S_{m,l}), \quad l = 1, \dots, k \end{aligned}$$

with $(\mathbf{P}_l)_{i,j} = P_{i,j,l}$.

The decomposition of the entries of $\mathbf{P}$ is unique, so is the one of $\mathbf{P}$ too.

Thus, every matrix $\mathbf{P} \in M_{p \times q}(S_{m,s})$ is a unique summand of matrices with entries from the $S_{m,i}$. The converse is obvious, since if we have any summand of matrices with entries from the $S_{m,i}$, then the matrix which entries are obtained by summation of the entries of those matrices at the same positions is in $M_{p \times q}(S_{m,s})$. $\square$

Lemma 3.6 Let $\mathbf{P} = \mathbf{P}_1 + \dots + \mathbf{P}_k \in M_{p \times q}(S_{m,s})$, such that $rk(\mathbf{P}) = r$. Then $rk(\mathbf{P}_i) = r$, $i = 1, \dots, k$.

Proof Let $I = \{i_1, \dots, i_r\}$, such that the lines $L(\mathbf{P})_e$, $e \in I$, of $\mathbf{P}$ are linearly independent over $S_{m,s}$ (where $L(\mathbf{P})_e$ denote the e -th line of $\mathbf{P}$); r is the maximum, such that this property is verified.

Thus, we have

$$\alpha_1 L(\mathbf{P})_{i_1} + \dots + \alpha_r L(\mathbf{P})_{i_r} = 0 \Rightarrow \alpha_j = 0, \quad j = 1, \dots, r$$

with $\alpha_j = (\alpha_{j,1}, \dots, \alpha_{j,k}) \in S_{m,s}$.

Using the decomposition of $\mathbf{P}$ into $\mathbf{P}_1 + \dots + \mathbf{P}_k$ We have

$$\begin{aligned} L(\mathbf{P})_{i_1} &= L(\mathbf{P}_1)_{i_1} + \dots + L(\mathbf{P}_k)_{i_1} \\ &\vdots \\ L(\mathbf{P})_{i_r} &= L(\mathbf{P}_1)_{i_r} + \dots + L(\mathbf{P}_k)_{i_r} \end{aligned}$$

where $L(\mathbf{P}_i)_{i_j}$ is the i_j -th line of the matrix $\mathbf{P}_i$ in the decomposition of $\mathbf{P}$. Therefore

$$\sum_{j=1}^r \alpha_j L(\mathbf{P})_{i_j} = 0$$

implies that

$$\begin{aligned} & (\alpha_{1,1} + \cdots + \alpha_{1,k}) (L(\mathbf{P}_1)_{i_1} + \cdots + L(\mathbf{P}_k)_{i_1}) + \cdots + \\ & (\alpha_{r,1} + \cdots + \alpha_{r,k}) (L(\mathbf{P}_1)_{i_r} + \cdots + L(\mathbf{P}_k)_{i_r}) = 0 \\ & \underbrace{(\alpha_{1,1} L(\mathbf{P}_1)_{i_1} + \cdots + \alpha_{r,1} L(\mathbf{P}_1)_{i_r})}_{\in S_{m,1}} + \cdots + \\ & \underbrace{(\alpha_{1,k} L(\mathbf{P}_k)_{i_1} + \cdots + \alpha_{r,k} L(\mathbf{P}_k)_{i_r})}_{\in S_{m,k}} = 0 \end{aligned}$$

This leads to the system:

$$\begin{cases} \alpha_{1,1} L(\mathbf{P}_1)_{i_1} + \cdots + \alpha_{r,1} L(\mathbf{P}_1)_{i_r} = 0 \\ \vdots \\ \alpha_{1,k} L(\mathbf{P}_k)_{i_1} + \cdots + \alpha_{r,k} L(\mathbf{P}_k)_{i_r} = 0 \end{cases}$$

In addition, the fact that the $L(\mathbf{P})_e$, $e \in I$, are linearly independent implies that we must have $\alpha_j = 0$, $j = 1, \dots, r$.

Therefore, $\alpha_{j,1} + \cdots + \alpha_{j,k} = 0$, thus $\alpha_{j,1} = \cdots = \alpha_{j,k} = 0$, $j = 1, \dots, r$. This comes from the fact that we can assimilate the summand $\alpha_{j,1} + \cdots + \alpha_{j,k}$ to the k -tuple $(\alpha_{j,1}, \dots, \alpha_{j,k})$.

Thus, in this case, the lines of the matrices $\mathbf{P}_i$ at the same positions I are linearly independent, since any linear combination of the $L(\mathbf{P})_e$, $e \in I$, that is zero implies linear combinations of the lines $L(\mathbf{P}_i)_e$, $e \in I$, $i = 1, \dots, k$, that equal zero. Notice here that this hold exactly at the same positions.

If we admit that r is not the maximum, such that the property is verified for the matrices $\mathbf{P}_i$, then we can find $r + 1$ lines of those matrices $\mathbf{P}_i$ that are linearly independent (we suppose here that the lines are exactly at the same positions).

By applying the converse of the preceding, we have that the $r + 1$ lines of $\mathbf{P}$ at the same positions are linearly independent, this contradicts the fact that $\mathbf{P}$ has rank r , hence r is the maximum for the $\mathbf{P}_i$ too, and this permits to conclude that $rk(\mathbf{P}_i) = r$, $i = 1, \dots, k$. $\square$

A direct application of Lemma 3.6 is that, For all $\mathbf{H} \in M_{(n-u) \times n}(S_{m,s})$, such that $rk(\mathbf{H}) = n - u$, then $\mathbf{H} = \mathbf{H}_1 + \cdots + \mathbf{H}_k$, with $\mathbf{H}_i \in M_{(n-u) \times n}(S_{m,i})$ and $rk(\mathbf{H}_i) = n - u$, for some positive integers $u \leq n$.

Lemma 3.7 *Let M be a free R_m -submodule of $S_{m,s}$ of dimension d . Then, $M = M_1 \oplus \cdots \oplus M_k$, where M_i is a free $R_{m,i}$ -submodule of $S_{m,i}$ of dimension d .*

Proof Let $\{\beta_1, \dots, \beta_d\}$ an R_m -basis of M , $\beta_i \in S_{m,s}$ $i = 1, \dots, d$.

Let $\mathbf{X} \in M$, then $\exists (\alpha_i) \in R_m^d$, $i = 1, \dots, d$, such that $\mathbf{X} = \alpha_1 \beta_1 + \cdots + \alpha_d \beta_d$.

$$\begin{aligned} \mathbf{X} &= (\alpha_{1,1} + \cdots + \alpha_{1,k}) (\beta_{1,1} + \cdots + \beta_{1,k}) + \cdots \\ &+ (\alpha_{d,1} + \cdots + \alpha_{d,k}) (\beta_{d,1} + \cdots + \beta_{d,k}) \\ &= (\alpha_{1,1} \beta_{1,1} + \cdots + \alpha_{d,1} \beta_{d,1}) + \cdots + (\alpha_{1,k} \beta_{1,k} + \cdots + \alpha_{d,k} \beta_{d,k}) \\ &= \mathbf{X}_1 + \cdots + \mathbf{X}_k, \quad \mathbf{X}_i = \sum_{j=1}^d \alpha_{j,i} \beta_{j,i}. \end{aligned}$$

The families $\{\beta_{j,i}, j = 1, \dots, d\}$ are generating families of $R_{m,i}$ -submodules of $S_{m,i}$, $i = 1, \dots, k$. We show easily that the families $\{\beta_{j,i}, j = 1, \dots, d\}$ are free for $i = 1, \dots, k$. Hence, they form bases for the corresponding $R_{m,i}$ -submodules.

Set $M_i = \langle \{\beta_{j,i}, j = 1, \dots, d\} \rangle$. Then, $\mathbf{X} = \mathbf{X}_1 + \cdots + \mathbf{X}_k$, $\mathbf{X}_i \in M_i$, so $\dim(M_i) = d$. This is true for all $\mathbf{X}$.

Hence $M = M_1 \oplus \cdots \oplus M_k$ due to the unicity of the decomposition on $S_{m,s}$. $\square$

3.3 Main results: our generalization of low rank parity-check codes over $\mathbb{Z}_m$

We can now give the following more general Definition of LRPC codes over $\mathbb{Z}_m$ considering the previous results of Lemmas 3.5, 3.6 and 3.7.

Definition 3.8 Let $\mathbf{H} \in M_{(n-u) \times n}(S_{m,s})$ with $rk(\mathbf{H}) = n - u$, for some positive integers $u \leq n$, and such that its entries generate a free R_m -submodule $\mathcal{F}$ of dimension d . The LRPC code of dimension u , length n and parameter d is the code with parity-check matrix $\mathbf{H}$.

The entries of the matrix $\mathbf{H}$ generate a free R_m -submodule of $S_{m,s}$.

Theorem 3.9 Let $\mathbf{H}$ be as in Definition 3.8. Then, the LRPC code generated by $\mathbf{H}$ is a direct summand of LRPC codes over the $R_{m,i}$ -modules $S_{m,i}$ with the same length, dimension and parameter.

Proof It is obvious from Lemmas 3.5 and 3.7 that $\mathbf{H} = \mathbf{H}_1 + \cdots + \mathbf{H}_k$, $\mathbf{H}_i \in M_{(n-u) \times n}(S_{m,i})$ and $\mathcal{F} = \mathcal{F}_1 \oplus \cdots \oplus \mathcal{F}_k$, where $\mathcal{F}_i$ is a free $R_{m,i}$ -submodule of $S_{m,i}$ of dimension d . Since $rk(\mathbf{H}) = n - u$, then $rk(\mathbf{H}_i) = n - u$, $i = 1, \dots, k$ according to Lemma 3.6.

Let $\{\beta_1, \dots, \beta_d\}$ an R_m -basis of $\mathcal{F}$. Then $H_{i,j} \in \mathcal{F}$, $i = 1, \dots, n - u$; $j = 1, \dots, n$.

Thus, $\exists(\alpha_{i,j,l})_{l=1,\dots,d} \in S_{m,s}^d$ such that $H_{i,j} = \alpha_{i,j,1}\beta_1 + \cdots + \alpha_{i,j,d}\beta_d$.

$H_{i,j} = H_{i,j,1} + \cdots + H_{i,j,k}$ implies

$$\begin{aligned} H_{i,j} &= (\alpha_{i,j,1,1} + \cdots + \alpha_{i,j,1,k})(\beta_{1,1} + \cdots + \beta_{1,k}) + \cdots + (\alpha_{i,j,d,1} + \cdots + \alpha_{i,j,d,k})(\beta_{d,1} + \cdots + \beta_{d,k}) \\ &= (\alpha_{i,j,1,1}\beta_{1,1} + \cdots + \alpha_{i,j,d,1}\beta_{d,1}) + \cdots + (\alpha_{i,j,1,k}\beta_{1,k} + \cdots + \alpha_{i,j,d,k}\beta_{d,k}) \\ H_{i,j,l} &= \sum_{a=1}^d \alpha_{i,j,a,l}\beta_{a,l}, \quad l = 1, \dots, k \end{aligned}$$

Since the coefficients $H_{i,j,l}$ are the entries of $\mathbf{H}_l$, then the families

$\{\beta_{a,l}, a = 1, \dots, d\}$, $l = 1, \dots, k$ are basis for the free $R_{m,i}$ -submodules generated by the entries of $\mathbf{H}_l$, $l = 1, \dots, k$; hence the matrices $\mathbf{H}_l$ are parity-check matrices for LRPC codes over the $S_{m,l}$, $l = 1, \dots, k$.

Thus, the free R_m -submodule generated by the entries of $\mathbf{H}$ is exactly the direct summand of the free $R_{m,i}$ -submodules generated by the entries of $\mathbf{H}_l$, $l = 1, \dots, k$ of the same dimension d .

Thus, every LRPC code over $S_{m,s}$ is a direct summand of LRPC codes over the $R_{m,i}$ -modules $S_{m,i}$. $\square$

We assume that the parity check matrix of the LRPC code fulfills, over R_m , the conditions of Definition 2 in the work of Renner et al. as recalled in Appendix A. This is to say that, according to the above discussion, the same conditions will be fulfilled by the parity check matrices

of the LRPC codes over the rings $S_{m,l}$, $l = 1, \dots, k$. In the following Sect. 4, we study the decoding, the correction capacity and the failure probability of these codes.

4 Decoding of LRPC codes over $\mathbb{Z}_m$, correction capacity and failure probability

4.1 Encoding and decoding of LRPC codes over $\mathbb{Z}_m$

The LRPC code is defined by a special parity-check matrix $\mathbf{H}$. We suppose that the codeword $\mathbf{c}$ was transmitted and the word $\mathbf{y} = \mathbf{c} + \mathbf{e}$ is received, where $\mathbf{e}$ is the rank t error vector due to the channel. Since the error vector $\mathbf{e}$ is of rank t , its support is a free module of rank t . The error vector is taken among the free vectors ($frk(e) = rk(e)$) of $S_{m,s}^n$ of rank t . The decoding algorithm, that generalizes the one in [7], is given in Algorithm 1.

We can observe that this decoding algorithm depends on the application of that in [7] on every $S_{m,i}$, $1, \dots, k$. Thus it may be slower in comparison, since in our case, we need to apply the decoding of [7] k times.

Algorithm 1 DECODING ALGORITHM FOR LRPC CODES C OVER $\mathbb{Z}_m$ **INPUT :**

- LRPC parity-check matrix $\mathbf{H}$
- $\mathbf{y} = (y_1, \dots, y_n) = \mathbf{c} + \mathbf{e} \in S_{m,s}^n$, such that
 - $\mathbf{c}$ is in the LRPC code C given by $\mathbf{H}$
 - the support of $\mathbf{e}$ is a free module of dimension t .

OUTPUT : a code word $\mathbf{c}$ or 'decoding failure'.

1:

$$\begin{aligned}
 \mathbf{y} &= (y_{1,1} + \dots + y_{1,k}, \dots, y_{n,1} + \dots + y_{n,k}) \\
 &= ((c_{1,1} + e_{1,1}) + \dots + (c_{1,k} + e_{1,k})) + \dots + ((c_{n,1} + e_{n,1}) + \dots + (c_{n,k} + e_{n,k})) \\
 &= (c_{1,1} + e_{1,1}, \dots, c_{n,1} + e_{n,1}) + \dots + (c_{1,k} + e_{1,k}, \dots, c_{n,k} + e_{n,k}) \\
 &= \mathbf{Z}_1 + \dots + \mathbf{Z}_k \\
 \mathbf{Z}_i &= (c_{1,i} + e_{1,i}, \dots, c_{n,i} + e_{n,i}) \in S_{m,i}^n, \quad i = 1, \dots, k \\
 \mathbf{Z}_i &= (y_{1,i}, \dots, y_{n,i})
 \end{aligned}$$

2: Apply the decoding algorithm presented in [7] to each $\mathbf{Z}_i$ on $S_{m,i}$ and obtain the vectors $(c_{1,i}, \dots, c_{n,i}) \in S_{m,i}$.3: $\mathbf{c} = (c_{1,1} + \dots + c_{1,k}, \dots, c_{n,1} + \dots + c_{n,k})$ 4: return $\mathbf{c}$ **4.2 Correction capacity and failure probability**

For $i \in \{1, \dots, k\}$, let us denote by C_i the LRPC code defined on $S_{m,i}$, so that C is the direct summand of the codes C_i . Each C_i has error correction capacity $t_i \leq s \cdot \frac{n-u}{n}$.

From the precedings, a rank t vector with entries in $S_{m,s}$ is a summand of rank t vectors with entries from the $R_{m,i}$ -modules $S_{m,i}$. Thus a rank t error from $S_{m,s}^n$ is a summand of rank t errors from $S_{m,i}^n$. Indeed, a rank t error in $S_{m,s}^n$ is a summand of rank t errors in $S_{m,i}^n$ due to Lemma 3.6. Of course, $e = e_1 + \dots + e_k \in M_{1 \times n}(S_{m,s}) := S_{m,s}^n$, with $e_i \in M_{1 \times n}(S_{m,i})$ and $rk(e_i) = t$, $i = 1, \dots, k$.

When a rank t error occurs, we suppose these occur at the same positions in the summand of errors according to the preceding. Hence, the error correction capacity of the code is still $t \leq s \cdot \frac{n-u}{n}$, and is the same for all the LRPC codes C_i .

We are given a vector $\mathbf{y} \in S_{m,s}^n$ to be decoded according to the LRPC code C . Since the decoding algorithm relies on the application of the one in [7] on every summand $\mathbf{y}_i \in S_{m,i}^n$ of $\mathbf{y}$ (according to the LRPC code C_i), a failure occurs if it occurs at least once when applying the decoding algorithm of [7].

The failure probability thus depends on the probability for each C_i to fulfill the three conditions of [7, Theorem 5]. Denote success_i the event "success of the decoding according to C_i ", $i = 1, \dots, k$ (the decoding according to C_i considers the algorithm of [7] applied to a vector $\mathbf{y}_i$ from $S_{m,i}^n$). For $i = 1, \dots, k$, set

$$\begin{aligned}
 r_i &= t \sum_{j=0}^{n_i-1} \left[\left(q_i / p_i^j \right)^d - \left(q_i / p_i^{j+1} \right)^d \right] \left(q_i / p_i^j \right)^{d \cdot t - s} \\
 &\quad + \prod_{j=0}^{d \cdot t - 1} \left(1 - p_i^{j - (n-u)} \right) \\
 &\quad + t \sum_{j=0}^{n_i-1} \left[\left(q_i / p_i^j \right)^d - \left(q_i / p_i^{j+1} \right)^d \right] \left(q_i / p_i^j \right)^{\frac{d \cdot t(d+1)}{2} - s}
 \end{aligned}$$

We have in [7]

$$\Pr(\text{success}_i) \geq 1 - r_i$$

Indeed, Theorems 9, 11 and 14 in [7] give upper bounds of the failure probabilities of the different conditions of Theorem 5 in [7]. So their summation gives an upper bound of the overall failure probability.

Denote success the event "success of the overall decoding according to C ". Notice that success is true if and only if all the events success_i are true, and since we have a direct summand, the events success_i are

independent. Thus

$$\begin{aligned}\Pr(\text{success}) &= \prod_{i=1}^k \Pr(\text{success}_i) \\ &\geq \prod_{i=1}^k (1 - r_i)\end{aligned}$$

Set $r = \max\{r_i, i = 1, \dots, k\}$. Then

$$\Pr(\text{success}) \geq (1 - r)^k.$$

5 Conclusion

We have extended the notion of LRPC codes over the rings of integers modulo a prime number, recently defined in [7], to LRPC codes over residual rings $\mathbb{Z}_m$ for a positive integer m . We have first constructed a Galois extension of the ring $\mathbb{Z}_m$ that is needed for our definition, and we have stated component-wise operations that was used for manipulating elements of the defined LRPC codes. We have deduced a decoding algorithm of those LRPC codes over $\mathbb{Z}_m$ using the one of Renner et al. [7]. It is noticed that this decoder is slower than the one of [7], since it results in the application of this at least twice. We have also derived a bound for the success probability of the decoder.

Acknowledgements Authors are supported by the Simons Foundation through the project PREMA. The third author acknowledges the support of TWAS UNESCO under the Grant 20-063 RG/MATHS/AF/AC-I.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Appendix

Let d , $\mathcal{F}$ and $\mathbf{H}$ be defined as in definition 3.8. Let $f_1, \dots, f_d \in S_{m,s}$ be a free basis of $\mathcal{F}$. For $i = 1, \dots, n - u$, $j = 1, \dots, n$, and $l = 1, \dots, d$, let $h_{i,j,l} \in R_m$ be the unique elements such that $H_{i,j} = \sum_{l=1}^d h_{i,j,l} f_l$. Define

$$\mathbf{H}_{\text{ext}} = \begin{pmatrix} h_{1,1,1} & h_{1,2,1} & \cdots & h_{1,n,1} \\ h_{1,1,2} & h_{1,2,2} & \cdots & h_{1,n,2} \\ \vdots & \vdots & \ddots & \vdots \\ h_{2,1,1} & h_{2,2,1} & \cdots & h_{2,n,1} \\ h_{2,1,2} & h_{2,2,2} & \cdots & h_{2,n,2} \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix} \in M_{(n-u)d \times n}(R_m).$$

Then, $\mathbf{H}$ has the

1. *unique-decoding property* if $d \geq \frac{n}{n-u}$ and $\text{frk}(\mathbf{H}_{\text{ext}}) = \text{rk}(\mathbf{H}_{\text{ext}}) = n$,
2. *maximal-row-span property* if every row of the parity check matrix $\mathbf{H}$ spans the entire space $\mathcal{F}$,
3. *unity property* if every entry $H_{i,j}$ of $\mathbf{H}$ is chosen from the set $H_{i,j} \in \tilde{\mathcal{F}} = \{\sum_{i=1}^d \alpha_i f_i : \alpha_i \in R_m^* \cup \{0\}\} \subseteq \mathcal{F}$.

References

1. Aragon, N.; Gaborit, P.; Hauteville, A.; Ruatta, O.; Zémor, G.: Low rank parity check codes: new decoding algorithms and applications to cryptography. *IEEE Trans. Inf. Theory* **65**(12), 7697–7717 (2019)
2. Bini, G.; Flamini, F.: *Finite Commutative Rings and Their Applications*. The Springer International Series in Engineering and Computer Science, vol. 680. Springer, New York (2002)
3. Brown, W.C.: *Matrices Over Commutative Rings*. Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, New York (1993)
4. Gabidulin, E.: Theory of codes with maximum rank distance (translation). *Prob. Inf. Transmiss.* **21**, 1–12 (1985)
5. Gaborit, P.; Murat, G.; Ruatta, O.; Zemor, G.: Low rank parity check codes and their application to cryptography. In: *The International Workshop on Coding and Cryptography (WCC 13)*, Apr 2013.
6. Kamche, H.T.; Mouaha, C.: Rank-metric codes over finite principal ideal rings and applications. *IEEE Trans. Inf. Theory* **65**(12), 7718–7735 (2019)
7. Renner, J.; Puchinger, S.; Wachter-Zeh, A.; Hollanti, C.; Freij-Hollanti, R.: Low-rank parity-check codes over the ring of integers modulo a prime power. In: *IEEE International Symposium on Information Theory, ISIT 2020, Los Angeles, CA, USA, June 21–26, 2020*. IEEE, pp. 19–24 (2020)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.