A Class of Locally Recoverable Codes Over Finite Chain Rings

Giulia Cavicchioni, Eleonora Guerrini, Alessio Meneghetti

A CLASS OF LOCALLY RECOVERABLE CODES OVER FINITE CHAIN RINGS

GIULIA CAVICCHIONI, ELEONORA GUERRINI, AND ALESSIO MENEGHETTI

Abstract. Locally recoverable codes deal with the task of reconstructing a lost symbol by relying on a portion of the remaining coordinates smaller than an information set. We consider the case of codes over finite chain rings, generalizing known results and bounds for codes over fields. In particular, we propose a new family of locally recoverable codes by extending a construction proposed in 2014 by Tamo and Barg, and we discuss its optimality. The principal issue in generalizing fields to rings is how to handling the polynomial evaluation interpolation constructions. This leads to deal with substructif and well conditioned sets in order to find optimal constructions.

1. Introduction

Introduced in [5], locally recoverable codes have garnered attention due to their relevance in distributed and cloud storage systems. Data centers and other modern distributed storage systems use redundant data storage to protect against node failures. Indeed they enable local repair of a coordinate by accessing a maximum of r other coordinates. This set of r coordinates is commonly referred to as the *recovering set* and, if a recovering set exists for every coordinate the code has locality r. Many research efforts have been focused on establishing bounds for the minimum distance and developing construction techniques for locally recoverable codes [5, 6, 8, 9, 22, 24].
If C is a linear code of length n, dimension k and locality r over the field $\mathbb{F}_q$, then its minimum distance satisfies [5]

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2 \ . \tag{1.1}$$

In [5], using a probabilistic argument, the authors proved that the bound (1.1) is tight if the field is large enough. Observe that (1.1) is independent of the alphabet size q. In [3] a bound for the minimum distance of a locally recoverable code depending on q is presented.

A central problem in Coding Theory is to construct optimal codes. We remark that usually a code C is said to be optimal if any other code with equal length and minimum distance has at most the same number of codewords as C. In this work we follow instead the route established for example in [5], and we say that a length-n code C with M codewords is optimal if no code over the same alphabet and with the

2020 *Mathematics Subject Classification.* 94B05,13M99.

Key words and phrases. Ring-linear code, Locally recoverable codes.

This paper was partially founded by the french Agence Nationale de la Recherche ANR-21-CE39-0006-SANGRIA and ANR-21-CE39-0009-BARRACUDA (2021-2026) .

same parameters has a strictly larger minimum distance. A code meeting the bound (1.1) is thus an optimal locally recoverable code.

Constructions of locally recoverable codes meeting the bound are given in [2, 6, 8, 9, 22, 24].
In all these constructions, the i-th coordinate together with its recovering set form a 1-erasure correcting code. A possible extension is presented in[18], where the authors introduced the (r, ρ)-locality, allowing recovering $\rho - 1$ erasures by looking at other r coordinates. An additional and relevant generalization can be found in [20], where each coordinate has several pairwise disjoint recovering sets.

In this paper, we present a generalization of the theory, allowing the alphabet to be a ring [15, 16, 21, 23], rather than a field as in classical Coding Theory.

This paper is organized as follows. In Section 2 we recall some basics on linear codes over rings and we introduce locally recoverable codes. In Section 3, similarly to [5], we derive a bound for the minimum distance of a locally recoverable code over a finite chain ring. As in the classical case, the bound is a function of the length, rank, and locality of the code. Additionally, we prove that this bound is not tight for certain values of the parameters of the code. In a similar fashion to [22], in Section 4 we construct a family of optimal locally recoverable codes. The core of this construction lies in the so-called *good polynomials*. In Section 5, we build a class of good polynomials over Galois rings. In Section 6, we insert the construction presented in Section 4 into a more general framework. Finally, in Section 7, we explore various generalizations of the main construction aimed at relaxing some constraints on the code parameters. We finally discuss the maximum possible length of a locally recoverable code over a finite chain ring.

2. Codes over rings and Locality

2.1. **Generalities on codes over rings.** Let R be a finite commutative ring. From the structure theorem for finite commutative rings [13, Theorem VI.2], it is well known that R decomposes uniquely (up to the order of summands) as a finite direct product of w local rings, $R = R_1 \times \cdots \times R_w$. In particular, if R is a principal ideal ring, PIR for short, the R_i are finite chain rings. From the decomposition of R we get, for some n, that $R^n = R_1^n \times \cdots \times R_w^n$.

From now on, let R be a PIR. A code C of length n over R is a subset $C \subseteq R^n$ and its elements are called *codewords*.

Definition 2.1. An *R-linear code* of length n is an R-submodule $C \subseteq R^n$. An R-linear code C is said to be *free* if C is a free submodule of R^n.

Unless otherwise specified, from now on we consider any code to be an R-linear code.

Remark 2.2. Given $R = R_1 \times \cdots \times R_w$, we define e_i as the element in R represented by $(0, \dots, 0, 1, 0, \dots, 0)$ in $R_1 \times \cdots \times R_w$, with 1 in the i-th position. Let $\pi_i \colon R_1^n \times \cdots \times R_w^n \to R_i^n$ be the i-th canonical projection. If C is an R-linear code and $c = (c_1, \dots, c_w) \in C$, where $c_i = \pi_i(c) \in R_i^n$, then the element

$$e_i c = (0, \dots, 0, c_i, 0, \dots, 0) \in C \ .$$

Hence, up to isomorphism, C can be uniquely written as

$$C_1 \times \cdots \times C_w \subseteq R^n \text{ with } C_i = \pi_i(C) \text{ for all } 1 \leq i \leq w \ . \tag{2.1}$$

Therefore, whenever convenient, we may restrict our focus on codes over local rings. In the classical framework, R is usually considered to be a finite field, and in this case an important parameter of linear codes is its dimension as a vector subspace of R^n. In our context, if R is a finite chain ring, we can define instead the $\mathbb{Z}_{p^s}$-*dimension* of the code as

$$k = \log_{p^s}|C| \ .$$

Definition 2.3. Given an R-linear code C, the *rank* of C is the minimum K such that there exists a monomorphism $\phi\colon C \to R^K$ as R-modules. In addition, if ϕ is an isomorphism, then C is free and $k = K$.

A *minimal generating set* of a code $C \subseteq R^n$ is a subset of C that generates C as an R-module and it is minimal with respect to inclusion. If R is a finite chain ring, as a consequence of Nakayama's Lemma [13, Theorem V.5], all the minimal generating sets have the same cardinality. The cardinality of a minimal generating set of C coincides with the rank of C and therefore we will denote it with K.
A matrix whose rows form a generating set for the code is a *generator matrix* for the code.

The Hamming metric is a discrete metric counting the number of entries in which two tuples differ, namely, for any $v = (v_1, \ldots, v_n)$ and $u = (u_1, \ldots, u_n)$ in R^n,

$$\mathrm{d}(v, u) = |\{i : v_i \neq u_i,\ 1 \leq i \leq n\}| \ .$$

The so-called *minimum distance* d, i.e.

$$d = \min_{c_1, c_2 \in C,\ c_1 \neq c_2} \mathrm{d}(c_1, c_2) \ ,$$

is a relevant parameter for the code.

Indeed, it is related to the error correction capability, namely, how many coordinates of a codeword c can be corrupted without compromising our ability of reconstructing c without errors. If the code is linear, the minimum distance coincides with the minimum weight of the codewords.

It is well known (see for example [12]) that the Singleton bound holds for any alphabet R of size q.

Theorem 2.4. (Singleton bound) Let C be a code of length n over an alphabet of size q. Then

$$d \leq n - \log_q|C| + 1 \ .$$

If R is a finite chain ring and C is an R-linear code of length n and type k, the previous bound reads

$$d \leq n - k + 1 \ .$$

Only free codes can meet this bound and they are said *maximum distance separable* (MDS) codes. However, in the framework of codes over finite chain rings, the Singleton bound can be improved (see for example [15]).

Theorem 2.5. (Generalized Singleton bound) Let R be a finite chain ring and let C be an R-linear code of length n and rank K. Then

$$d \leq n - K + 1 \ .$$

This bound is generally tighter than the Singleton bound, and they coincide if and only if the code is free. A linear code meeting this bound is said to be *maximum distance with respect to rank* (MDR).

For any linear code $C \subseteq R^n$ and for any subset $S \subset \{1, \dots, n\}$ of the coordinates, we define C_S to be the *punctured code of C in S*, obtained by deleting in each codeword all but the coordinates indexed in S. If $|C| = |C_S|$ then S is an *information set of size* $|S|$ for C. In the following, we will denote with κ the minimal size of an information set. Note that for codes over finite chain rings the minimum size of an information set coincides with the rank and $\kappa = K$.

Corollary 2.6. Let C be a code with minimum distance d and let S be a subset of coordinates which does not form an information set. Then

$$|S| \leq n - d \ .$$

Proof. By contradiction, assume $|S| \geq n - d + 1$. Since S is not an information set $|C_S| < |C|$. Note that C_S is obtained form C by removing at most $d-1$ coordinates: this contradicts the definition of minimum distance. □

2.2. **Locally recoverable codes.** The goal of a local recovery technique is to enable the retrieval of lost encoded data using only a small portion of the available information, rather than requiring access to the complete codeword c.
Let R be a finite commutative ring.

Definition 2.7. Let C be a (possibly non-linear) code in R^n and let $(c_1, \dots, c_n)$ be a codeword. We say that the coordinate $i \in \{1, \dots, n\}$ has *locality* r if there exists a subset $S_i \subseteq \{1, \dots, n\} \setminus \{i\}$ such that:

- *(locality)* $|S_i| \leq r$,
- *(recovery)* $|C_S| = |C_{S \cup \{i\}}|$.

C is a *locally recoverable code* (LRC) with *locality* r if each coordinate has locality r.

In other words, any symbol c_i of any codeword c can be recovered by accessing at most r other symbols of c. If we are presented with a codeword c that is error-free except for an erasure at position i, we can retrieve the original codeword by only examining the coordinates in S_i. For this reason, S_i is referred to as a *recovering set* for i. Moreover we will say that $S_i \cup \{i\}$ is a *dependent set*.
If R is a finite chain ring and C is an R-linear code of length n, rank K and locality r, we will say that C is an (n, K, r)-code.

Of course, one can choose $R = \mathbb{F}_q$. In this case we recover the classical theory of locally recoverable codes over finite fields.

In this work we say that an (n, K, r)-code over R with minimum distance d is an *optimal locally recoverable code* if no (n, K, r)-code over R has a minimum distance strictly larger than d.

In 2014 Tamo and Barg [22] presented a clever construction for optimal locally recoverable codes based on polynomial interpolation. In the following sections we

will extend this construction in the more general framework of codes over finite chain rings.

3. Lower bound on the minimum distance of a locally recoverable code

Let R be a commutative ring, let C be a code of length n over R and let κ be the minimum size of its information sets. From now on, we will denote by S_i a recovering set for the coordinate i.

For any code C, the set of dependencies involving at most $r+1$ coordinates defines a directed graph. If S_i is a recovering set for i, we define X to be the graph whose vertex set is the set of coordinates $\{1,\dots,n\}$ and in which there exists a directed edge from i to j if and only if $j \in S_i$. For a vertex v we will denote by $N(v)$ the outgoing neighbors of v.

Theorem 3.1. Let C be a code of length n and locality r over R. Then the minimum distance satisfies

$$d \leq n - \kappa - \left\lceil \frac{\kappa}{r} \right\rceil + 2 \ . \tag{3.1}$$

Moreover

$$\frac{\kappa}{n} \leq \frac{r}{r+1} \ . \tag{3.2}$$

Proof. Let X be the directed graph associated to the code C. Note that the outgoing degree of each vertex is at most r. A modification of Turàn Theorem on the size of the maximal independent set in a graph, [22, Theorem A.1], establishes that X contains an induced acyclic subgraph $X^{\mathcal{U}}$ on the vertex set $\mathcal{U}$ with

$$|\mathcal{U}| \geq \frac{n}{r+1} \ .$$

Let i be a coordinate without outgoing edges: i is a function of the coordinates $\{1,\dots,n\} \setminus \mathcal{U}$. The induced subgraph of X on $\mathcal{U} \setminus \{i\}$ is a directed acyclic subgraph. Let i' be a vertex without outgoing edges in $X^{\mathcal{U}\setminus\{i\}}$: i' is a function of the coordinates $\{1,\dots,n\} \setminus \mathcal{U}$. Iterating, we conclude that any coordinate $i \in \mathcal{U}$ is a function of the coordinates $\{1,\dots,n\} \setminus \mathcal{U}$. Therefore, there are at least $|\mathcal{U}| \geq \frac{n}{r+1}$ redundant coordinates. Thus the number of the information coordinates κ is at most $\kappa \leq n - \frac{n}{r+1} = \frac{nr}{r+1}$.

To establish the bound on the minimum distance, we first build a large set $T \subseteq \{1,\dots,n\}$ which does not form an information set. Then, we use Corollary 2.6 to complete the proof. Let $M(T)$ be the number of independent elements in T. Algorithm 1 constructs the desired set T.

Since the cardinality of an information set is at least κ, there exists j as desired in Line 3 of Algorithm 1,. Let h denote the number of steps of the algorithm, let

$$t_i = |T_i| - |T_{i-1}|, \quad |T_h| = \sum_{i=1}^{h} t_i \ ,$$

Algorithm 1: Construction of T

```
1  Let i = 0, T_0 = {}.
2  while M(T_{i-1}) ≤ κ − 2 do
3  |  Pick j ∈ {1,...,n} \ T_{i-1} such that j has at least one outgoing edge in
   |    V_{{1,...,n}\T_{i-1}}.
4  |  if M(T_{i-1} ∪ N(j)) < κ then
5  |  |  Set T_i = T_{i-1} ∪ N(j) ∪ j;
6  |  end
7  |  else
8  |  |  pick N'(j) ⊂ (N(j) ∪ j) so that M(T_{i-1} ∪ N'(j)) = κ − 1 and set
   |  |    T_i = T_{i-1} ∪ N'(j).
9  |  end
10 |  i = i + 1.
11 end
```

and

$$m_i = M(T_i) - M(T_{i-1}), \quad M(T_h) = \sum_{i=1}^{h} m_i = \kappa - 1 \ .$$

There are two possible cases to consider: one where the **else** condition in Line 7 is reached, and the other where it is never executed.

Case 1. Assume $M(T_{i-1} \cup N(j)) \leq \kappa - 1$ for all $1 \leq i \leq h$. In each step we add $t_i \leq r + 1$ coordinates. Moreover, $m_i \leq t_i - 1 \leq r$. Since in the last step we have $\kappa - 1$ independent coordinates, the number of steps is at least $\lceil \frac{\kappa-1}{r} \rceil$. Thus

$$|T| = \sum_{i=1}^{h} t_i \geq \sum_{i=1}^{h} (m_i + 1) \geq \kappa - 1 + h \geq \kappa - 1 + \left\lceil \frac{\kappa - 1}{r} \right\rceil \ .$$

Since $\kappa - 1 + \lceil \frac{\kappa-1}{r} \rceil \geq \kappa + \lceil \frac{\kappa}{r} \rceil - 2$, we get the claim.

Case 2. Since in the last step we have hit the condition $M(T_{h-1} \cup N(j)) = \kappa$ and M increases at most by r per step, then $h \geq \lceil \frac{\kappa}{r} \rceil$. For any $1 \leq i \leq h - 1$ we add at most $r + 1$ coordinates and $m_i \leq t_i - 1$. Since $M(S_{h-1}) \leq \kappa - 2$, $m_h \geq 1$ and $t_h \geq m_h$. Therefore

$$|T| = \sum_{i=1}^{h} T_i \geq \sum_{i=1}^{h-1} (m_i + 1) + m_h \geq \kappa - 1 + h - 1 \geq \kappa + \left\lceil \frac{\kappa}{r} \right\rceil - 2 \ .$$

□

Let R be a finite chain ring, let γ be the generator of the maximal ideal with nilpotency index s. As shown in [16, Proposition 3.2], any R-linear code C is permutation

equivalent to a code having the following generator matrix in standard form:

$$G = \begin{bmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \dots & A_{0,s-1} & A_{0,s} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \dots & \gamma A_{1,s-1} & \gamma A_{1,s} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \dots & \gamma^2 A_{2,s-1} & \gamma^2 A_{2,s} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \gamma^{s-1} I_{k_{s-1}} & \gamma^{s-1} A_{s-1,s} \end{bmatrix},$$

where $A_{i,s} \in M_{k_i \times n-K}(R/\gamma^{s-i}R)$ and $A_{i,j} \in M_{k_i \times k_j}(R/\gamma^{s-i}R)$ for $j < s$. The parameters $k_0, \dots, k_{s-1}$ are the same for all generator matrices in standard form, and C is said to be of *subtype* $(k_0, k_1, \dots, k_{s-1})$.

In the framework of codes over finite chain rings bound (3.1) reads:

Corollary 3.2. (LRC bound for R-linear codes) Let R be a finite chain ring and let C be an R-linear code of length n, rank K and locality r. Then

$$d \leq n - K - \left\lceil \frac{K}{r} \right\rceil + 2 \ . \tag{3.3}$$

For linear codes over rings, the dependence relations among the columns of G can serve as recovering sets. However, opposed to the case of vector spaces, the notion of linear independence for modules over rings is not well defined. Indeed, for a finite chain ring R, the following two definitions are not equivalent.

Definition 3.3. The vectors $v_1, \dots, v_u \in R^n$ are said to be *modularly independent* over R if $\sum_{i=0}^{u} s_i v_i = 0$ with $s_i \in R$ implies s_i is not a unit for all i.

In particular the vectors $v_1, \dots, v_u \in R^n$ are modularly independent if none of them can be written as a linear combination of the others.

Definition 3.4. The non-zero vectors $v_1, \dots, v_u \in R^n$ are said to be *linear independent* over R if $\sum_{i=0}^{u} s_i v_i = 0$, $s_i \in R$ implies $s_i = 0$ for all i.

Therefore the vectors $v_1, \dots, v_u \in R^n$ are linear independent if the only linear combination of the v_i to 0 is given by setting all the scalars to zero.
For further details on this topic refer to [17].

Hence, the modular dependencies relations allows to gain local recoverability.

Note that each symbol in an R-linear code of rank K has locality at most K. Thus r satisfies $1 \leq r \leq K$. In particular:

- If $r = K$, the LRC bound reduces to the generalized Singleton bound and optimal LRC codes are MDR codes;
- If $r = 1$, bound (3.3) reads

$$d \leq n - 2K + 2 = 2\left(\frac{n}{2} - K + 1\right) .$$

Therefore, by replicating each symbol twice in an MDR code of length $\frac{n}{2}$ and rank K, we get an optimal linear code with locality $r = 1$.

Remark 3.5. If C is an R-linear code of subtype $(k_0, k_1, \ldots, k_{s-1})$, following the same steps of [4, Theorem 3.2], we obtain an upper bound on the minimum distance:

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2 \ , \quad \text{where} \quad k = \frac{1}{s} \sum_{i=0}^{s-1} (s-i)k_i \ . \tag{3.4}$$

Note that bound (3.3) is in general tighter then (3.4) and the two inequalities coincide if and only if the code is free.

Codes that attain the LRC bound on finite chain rings can be used as building blocks to construct codes that achieve the LRC bound on finite PIRs.

Lemma 3.6. Let $R = R_1 \times \cdots \times R_w$ be a PIR and let $C = C_1 \times \cdots \times C_w \subseteq R^n$ be an R-linear code. If K and K_i are the ranks of C and C_i respectively, then:

(1) $\mathrm{d}(C) = \min_i \ \mathrm{d}(C_i)$;
(2) $K = \max_i \ K_i$.

Proof. To prove the first statement, let $c = (c_1, \ldots, c_w) \in C$ be a codeword. In accordance with Remark 2.2 $e_i c = (0, \ldots, 0, c_i, 0, \ldots, 0) \in C$ and hence the claim. For the second claim, let $\varphi_i \colon C_i \to R^{K_i}$ be the monomorphism defining the rank of the code. By composing φ_i with the canonical embedding,

$$\psi_i \colon C_i \to R^{K_i} \hookrightarrow R^K \ ,$$

we get another monomorphism. Let

$$(\psi_1, \ldots, \psi_w) \colon C_1 \times \cdots \times C_w \to R_1^K \times \cdots \times R_w^K \ .$$

Since $C = C_1 \times \cdots \times C_w$ and $R^K = R_1^K \times \cdots \times R_w^K$, $(\psi_1, \ldots, \psi_w)$ induces a monomorphism $\psi \colon C \to R^K$. According to the definition of ψ_i, K is the minimum integer ensuring the injectivity of the map ψ and the claim follows.

□

Theorem 3.7. Let $R = R_1 \times \cdots \times R_w$ be a finite PIR and let $C = C_1 \times \cdots \times C_w \subseteq R^n$ be an R-linear code. If C_i is an optimal LRC over R_i for all $1 \leq i \leq w$, then C is optimal LRC over R.

Proof.

$$\begin{aligned} \mathrm{d}(C) = \min_{1 \leq i \leq w} \ \mathrm{d}(C_i) = \min_{1 \leq i \leq w} \ n - K_i - \left\lceil \frac{K_i}{r} \right\rceil + 2 = \\ = n - \max_{1 \leq i \leq w} \left\{ K_i + \left\lceil \frac{K_i}{r} \right\rceil \right\} + 2 = n - K - \left\lceil \frac{K}{r} \right\rceil + 2 \ . \end{aligned}$$

□

Hence, we can focus our studies on LRC codes over finite chain rings.

3.1. **Non-existence of R-linear codes achieving the LRC bound for certain parameters.** The aim of this section is to show that codes achieving the LRC bound do not exist for all possible values of n, K and r. To do this, we will introduce a weaker notion of locality: the information locality.

Let R be a finite chain ring.

Definition 3.8. The code $C \subseteq R^n$ has *information locality* $\bar{r}$ if there exists an information set $I \subset \{1, \ldots, n\}$ such that any information coordinate $i \in I$ has locality as most $\bar{r}$.

Following the same steps of Theorem 3.1 one can prove that the minimum distance of an R-linear code C of length n, rank K and information locality $\bar{r}$ is bounded by

$$d \leq n - K - \frac{K}{\bar{r}} + 2 \ .$$

In the following, we will denote by $\overline{X}_C$ the directed graph defined by the modular dependencies involving at most $\bar{r} + 1$ coordinates of C.

Theorem 3.9. Let C be an R-linear code of length n, rank K and with information locality $\bar{r}$. Suppose $K \mid \bar{r}$ and

$$d = n - K - \frac{K}{\bar{r}} + 2 \ . \tag{3.5}$$

$\overline{X}_C$ has at least $\frac{K}{\bar{r}}$ connected components with exactly $\bar{r} + 1$ vertices.

Proof. Algorithm 1 yields two sequences $\{t_i\}_{1,\ldots,h}$ and $\{m_i\}_{1,\ldots,h}$.

Case 1. If $\bar{r} = 1$, since $m_i \leq 1$, the **else** block (Line 7, Algorithm 1) is never executed. Therefore,

$$|T| = \sum_{i=0}^{h} t_i \geq \sum_{i=0}^{h} m_i + h \geq K - 1 + K - 1 = 2(K-1) = 2(n-d) \ ,$$

where the last equality follows form (3.5). From Corollary 2.6 we get $|T| = n - d = 2(K-1)$. Since $\sum_{i=0}^{h} m_i = K - 1$ then $h = K - 1$, $t_i = 2$, and $m_i = 1$ for all $1 \leq i \leq h$. Therefore there are at least $K - 1$ connected components of size 2.

Case 2. If $\bar{r} \geq 2$ and $\bar{r} \mid K$ then $K \not\equiv 1 \mod \bar{r}$ and $K - 1 + \lceil \frac{K-1}{\bar{r}} \rceil \geq K + \frac{K}{\bar{r}} - 2$. Therefore, in order to find a lower bound on $|T|$, we may assume the **else** condition (Line 7, Algorithm 1) is executed.

$$|T| = \sum_{i=0}^{h} t_i \geq \sum_{i=0}^{h} m_i + h \geq K - 1\frac{K}{\bar{r}} - 1 = n - d \ .$$

From Corollary 2.6 we get $|T| = n - d = K + \frac{K}{\bar{r}} - 2$, and hence we always enter in the **else** block. Since $\sum_{i=0}^{h} m_i = K - 1$, then $h = \frac{K}{\bar{r}}$. Moreover $m_i \leq \bar{r}$ implies $m_j = \bar{r} - 1$ for some $j \in \{1, \ldots, h\}$ and $m_i = \bar{r}$ for all $i \neq j$. In particular $j = h$, otherwise the **else** condition is never executed.
First suppose there exists a connected component with $\bar{r}$ vertices. By adding this component to T in the first step, we would get $m_1 \leq \bar{r} - 1$. Finally, assume there are $\frac{K}{\bar{r}} - 1$ connected components, namely, the recovering set of $j, l \in \{1, \ldots, n\}$ intersects. Let S_j and S_l be the recovering sets of j and l respectively and let $S = S_j \cup S_l$. Note that the number of modularly independent coordinates in S is at most $2\bar{r} - 1$. By including S_j and S_l in the set T at the beginning of the algorithm, we ensure that $m_1 + m_2 \leq 2\bar{r} - 1$. Both cases lead us to a contraction that prevents the **else** condition from being executed.

□

Theorem 3.10. Let C be an R-linear code of length n, rank K. If there exists an information set whose information locality is $\bar{r} \mid K$ and C has minimum distance $d = n - K - \frac{K}{\bar{r}} + 2$ with $d \leq \bar{r} + 2$, then some redundant coordinates have locality $r > \bar{r}$.

Proof. Let I be an information set with information locality $\bar{r}$. We prove that $\overline{X}_C$, the directed graph associated to C, has exactly $\frac{K}{\bar{r}}$ connected components.
From Theorem 3.9 we know that the number of connected components is at least $\frac{K}{\bar{r}}$, we now show they are exactly $\frac{K}{\bar{r}}$.
Let m be the number of connected components. By contradiction assume $m \geq \frac{K}{\bar{r}} + 1$.

$$n \geq m(\bar{r}+1) = K + \frac{K}{\bar{r}} + \bar{r} + 1 > K + \frac{K}{\bar{r}} + d - 2 \ ,$$

which contradicts the choice of n. Therefore $\overline{X}_C$ must contain $n - \frac{K}{\bar{r}}(\bar{r}+1) = d - 2$ isolated vertices which do not participate to any modular relations.
The same argument applies to every choice of an information set and its associated information locality.

□

Corollary 3.11. Let C be an (n, K, r)-code. If $r|K$ and $r + \frac{K}{r} > n - K - 1$, then C does not achieve the LRC bound.

4. Extending the Tamo-Barg construction over finite chain rings

The construction by Tamo and Barg, [22], allows to obtain optimal LRC codes over finite fields using particular types of polynomial, the so-called *good polynomials*. Polynomial interpolation is used in order to recover erased data.

4.1. **Polynomials over rings.**

It is important to have in mind that polynomials over rings lack some desirable properties of polynomials over fields. For example, when considering a ring R, the evaluation map

$$ev_\alpha \colon R[x] \to R \ , \qquad f \mapsto f(\alpha)$$

is an homomorphism if and only if R is commutative. Moreover, in this framework, polynomial interpolation problems also require a greater attention.

If R is a local ring with maximal ideal M and residue field $F = R/M$, we will denote by $\bar{y}$ the image of $y \in R$ under the canonical projection from R to F. In addition, for a set $T \subseteq R$ we define $\overline{T} = \{\bar{t} \mid t \in T\}$.

Let $N(R)$ denote the group of units of R.

Definition 4.1. A subset $T \subseteq N(R)$ is said to be *subtractive* in $N(R)$ if, for all distinct $a, b \in T$, $a - b \in N(R)$.

Here is a simple property of local rings.

Lemma 4.2. Given $r, s \in R$, then $\bar{r} \neq \bar{s}$ if and only if $r - s \in N(R)$.

Therefore T is a subtractive subset of R if and only if $|T| = |\overline{T}|$.

In line with [1], we provide the definition for well-conditioned sets.

Definition 4.3. A set $\{a_1, \ldots, a_n\}$ is *well-conditioned* in R if one of the following conditions is satisfied:

(1) $\{a_1, \ldots, a_n\}$ is subtractive in $N(R)$;
(2) For some i, $\{a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\}$ is subtractive in $N(R)$ and a_i is a zero-divisor or $a_i = 0$.

Polynomial reconstruction remains valid if we restrict to well-conditioned sets.

Proposition 4.4. [19, Corollary 9] Let $f \in R[x]$ be a polynomial of degree at most $n-1$ with at least n roots in a well-conditioned set of R. Then $f = 0$.

Corollary 4.5. [19, Corollary 10] Let $\{a_1, \ldots, a_n\}$ be a well-conditioned set in R and let $\{y_1, \ldots, y_n\}$ be a subset of R. Then there exists a unique polynomial $f \in R[x]$ of degree at most $n-1$ such that $f(a_i) = y_i$ for all $1 \leq i \leq n$.

Proposition 4.4 points out that, unlike polynomials over fields, the number of roots of a polynomial over a ring is not bounded by its degree. Nonetheless, for polynomials over local rings, there exists a bound on the number of roots, which depends on the polynomial's degree. The following Corollary is a consequence of the Hensel lifting [13, Chapter XIII, Section (C)].

Corollary 4.6. Let R be a finite chain ring whose residue field F has size $|F| = p^m$ and $|R| = p^{sm}$. Let $f(x) \in R[x]$ be a polynomial of degree n. The number of roots of f in R is at most $np^{(s-1)m}$.

4.2. **Code construction.** Let R be a finite chain ring with $|R| = q$. Given $f \in R[x]$, if f is constant on the set A, we will denote by $f(A)$ the value of f on A.

From now on, we will refer to a polynomial whose leading coefficient is a unit as a monic polynomial.

Definition 4.7. Let $l \in \mathbb{N}^+$ and $A_1, \ldots, A_l$ pairwise disjoint subsets of R of size $r+1$. A polynomial $g \in R[x]$ such that:

- Its degree is $r+1$;
- It is monic;
- It is constant on A_i, i.e., for any $1 \leq i \leq l$, $g(A_i) = c_i$ with $c_i \in R$;

is said to be (r, l)-*good* on the blocks $A_1, \ldots, A_l$.

Theorem 4.8. Let $r \geq 1$ and let $A_1, \ldots, A_l$ be subsets of R such that $A = \bigcup_{i=1}^{l} A_i$ is well-conditioned. Let $g(x) \in R[x]$ be an (r, l)-good polynomial on the blocks of the partition of A. For $t \leq l$, set $n = (r+1)l$ and $K = rt$. Let

$$a = (a_{i,j},\ 0 \leq i \leq r-1,\ 0 \leq j \leq t-1) \in R^K\ .$$

We define the *encoding polynomial*

$$f_a(x) = \sum_{i=0}^{r-1} \sum_{j=0}^{t-1} a_{i,j} g(x)^j x^i\ ; \tag{4.1}$$

and the code

$$\mathcal{C} = \left\{ (f_a(\alpha),\ \alpha \in A) \mid a \in R^K \right\} .$$

Then $\mathcal{C}$ is a free (n, K, r)-code with minimum distance $d = n - K - \frac{K}{r} + 2$. Hence $\mathcal{C}$ is an optimal locally recoverable code.

Remark 4.9. In the following, we provide an overview of the technique we will use to recover an erased symbol. Let $a \in R^K$ be the message vector and assume $(f_a(\gamma),\ \gamma \in A)$ is sent. Suppose that the symbol corresponding to the location $\alpha \in A_j$ is erased and let c_β for all $\beta \in A_j \setminus \{\alpha\}$ represent the remaining r symbols in the locations of the set A_j. Since g is an (r, l)-good polynomial on the blocks of the partition of A, $f_a(x)$ is a polynomial of degree at most $r - 1$ when restricted to A_j. Hence, in order to find $c_\alpha = f_a(\alpha)$, we find the unique polynomial $\delta(x)$ of degree strictly less than r such that $\delta(\beta) = c_\beta$ for all $\beta \in A_j \setminus \{\alpha\}$ and we set $c_\alpha = \delta(\alpha)$. The polynomial $\delta(x)$ is called the *decoding polynomial* for c_α.

Proof.

- **Type of the code:** Recall that g is monic and of degree $r + 1$. Therefore, for $i = 0, \dots, r - 1$ and $j = 0, \dots t - 1$ the K polynomials $g(x)^j x^i$ are all of distinct degrees. Suppose $f_a(x) = f_b(x)$ for some $a \neq b$. Then

$$f_a(x) - f_b(x) = \sum_{i=0}^{r-1} \sum_{j=0}^{t-1} (a_{i,j} - b_{i,j}) g(x)^j x^i = 0$$

  if and only if $a_{i.j} = b_{i,j}$ for all i and j, and in this case the map $a \mapsto f_a$ is injective. On the other hand, by (4.1), the degree of $f_a(x)$ is bounded by

$$(t - 1)(r + 1) + r - 1 = K + \frac{K}{r} - 2 \leq n - 2 ,$$

  where the last inequality comes from (3.2). Since the set of evaluation point is well-conditioned, f_a and f_b give rise to two distinct codewords and $|\mathcal{C}| = q^K$. Therefore $\mathcal{C}$ is of type K.
- **Minimum distance and rank:** Since the set of evaluation points $A = \bigcup_{i=1}^{l} A_i$ is well-conditioned, the number of zeros of $f_a(x)$ is bounded by its degree. The encoding is linear and hence

$$d \geq n - \max_a \ \deg(f_a) = n - K - \frac{K}{r} + 2.$$

  On the converse, let $\overline{K}$ be the rank of $\mathcal{C}$. By (2.6),

$$d \leq n - \overline{K} - \frac{\overline{K}}{r} + 2 \leq n - K - \frac{K}{r} + 2 .$$

  Therefore $d = n - K - \lceil \frac{K}{r} \rceil + 2$, $K = \overline{K}$ and the code is free.
- **Locality:** Assume that the symbol $c_\alpha = f_a(\alpha)$ corresponding to the location $\alpha \in A_j$ is lost. Let

$$f_i(x) = \sum_{j=0}^{t-1} a_{i,j} g(x)^j .$$

Since g is constant on the sets A_j, f_i is also constant on A_j. If

$$\delta(x) = \sum_{i=0}^{r-1} f_i(\alpha) x^i \ ,$$

then

$$\delta(\beta) = \sum_{i=0}^{r-1} f_i(\alpha) x^i = \sum_{i=0}^{r-1} f_i(\beta) x^i = f_a(\beta) \ ,$$

namely, $f_a(x)$ and $\delta(x)$ coincides on the locations of the set A_j. Since the degree of $\delta(x)$ is at most $r-1$ on a subtractive subset A_j, δ can be interpolated from the r symbols c_β for $\beta \in A_j \setminus \{\alpha\}$. Finally c_α is obtained by computing $\delta(\alpha)$.

□

Remark 4.10. We have that:

(1) If $r = K$ the construction does not require good polynomials and reduces to Reed-Solomon codes.
(2) Analogously to the classical case [22, Section 3A], the construction can be generalized even for the case $r \nmid K$.

Notice that the assumption that a good polynomial must be monic is unnecessary. If we remove it in Definition 4.7, following the same steps of Theorem 4.8, we obtain a non-free code with the same parameters but having a smaller size.

Example 4.11. In the following, we construct an optimal code over $\mathbb{Z}_{11^2}$ with length $n = 10$, rank $K = 8$ and locality $r = 4$. Since $r+1 = 5$, we need to find a polynomial $g(x)$ of degree 5 which is constant on 2 disjoint sets of size 5. If

$$A = A_1 \cup A_2 \ \text{ with } \ A_1 = \{1, 3, 9, 27, 81\} \ \text{ and } \ A_2\{40, 94, 112, 118, 120\} \ ,$$

then the polynomial $g(x) = x^5$ is constant on A_1 and A_2:

$$g(1) = g(3) = g(27) = g(81) = 1 \text{ and } g(40) = g(94) = g(112) = g(118) = g(120) = 120 \ .$$

If

$$a = (a_{0,0},\ a_{0,1},\ a_{1,0},\ a_{1,1},\ a_{2,0},\ a_{2,1},\ a_{3,0},\ a_{3,1})$$

is the message vector, the encoding polynomial associated to a reads

$$f_a(x) = a_{3,1}x^8 + a_{2,1}x^7 + a_{1,1}x^6 + a_{0,1}x^5 + a_{3,0}x^3 + a_{2,0}x^2 + a_{1,0}x + a_{0,0} \ .$$

Since A is subtractive and $\deg f_a(x) \leq 8$ we have $d_C \geq 2$ and, by the LRC bound (3.3), $d_C = 2$. If

$$\bar{a} = (1, 0, 3, 7, 0, 0, 11, 1) \ ,$$

is sent then the encoding polynomial associated to $\bar{a}$ is

$$f_{\bar{a}} = x^8 + 7x^6 + 11x^3 + 3x + 1 \ .$$

The codeword corresponding to $\bar{a}$ is found to be

$$c = (23, 113, 6, 33, 72, 114, 116, 106, 7, 25) \ .$$

Suppose c is sent

$$y = (23, 113, 6, 33, \times, 114, 116, 106, 7, 25)$$

is received. The fifth coordinate has been erased and $f_{\bar{a}}(81)$ is unknown. Theorem 4.8 ensures that it can be recovered just by accessing to the first 4 codeword symbols. After having computed the decoding polynomial $\delta(x) = 12x^3 + 10x + 1$, we can find the missing value $\delta(81) = 72$.

5. Construction of good polynomials over Galois ring

Good polynomials play a fundamental role in the previous construction, therefore it becomes crucial to produce good polynomials together with the partition of the set A. It is known that classes of good polynomials over finite fields exist [11, 14, 22]. In particular, Micheli in [14] introduced a framework that allows the generation of good polynomials over finite fields.The natural question that arises now is whether there exist good polynomials over rings which are not fields.
Indeed, they do exists. Here we construct a class of good polynomials over Galois rings exploiting the structure of its group of units.

Let R be a finite chain ring, $M \subset R$ be the maximal ideal, and let $g \in R$. In accordance with the notation of Section 4, we denote with $\bar{g} \in R/M =: F$ its canonical projection onto F, and we extend this projection to $R[x]$, i.e. if $f \in R[x]$ then $\bar{f} \in F[x]$.

Definition 5.1. Let p be a prime, and s, m positive integers. The *Galois ring* $\mathrm{GR}(p^s, m)$ of characteristic p^s and with p^{sm} elements is the quotient ring

$$\mathrm{GR}(p^s, m) \cong \mathbb{Z}_{p^s}[x]/(f) \ ,$$

where $f \in \mathbb{Z}_{p^s}[x]$ is a monic irreducible polynomial of degree m such that $\bar{f}$ is irreducible in $\mathbb{Z}_p$, where $\bar{f}$ denotes the image of f under the canonical projection.

A Galois ring $\mathrm{GR}(p^s, m)$ is a local ring with maximal ideal $M = (p)$ and whose residue field $F = \mathrm{GR}(p^s, m)/M$ is isomorphic to the finite field $\mathbb{F}_{p^m}$. Its group of units has order $(p^m - 1)p^{m(s-1)}$. Throughout this section let $R = \mathrm{GR}(p^s, m)$.

Theorem 5.2. ([13, Theorem XVI.9]) Let $R = \mathrm{GR}(p^s, m)$. Then

$$N(R) = G_1 \times G_2 \quad \text{where}$$

- G_1 is a cyclic group of order $p^m - 1$;
- G_2 is a group of order $p^{(s-1)m}$ such that
  - if p is odd or $p = 2$ and $s \leq 2$, G_2 is a direct product of r cyclic groups of order p^{s-1};
  - if $p = 2$ and $s \geq 3$, G_2 is a direct product of a cyclic group of order 2, a cyclic group of order 2^{s-2} and $m - 1$ groups of order 2^{s-1}.

Therefore, there is a unique maximal cyclic subgroup of $N(R)$ having order relatively prime to p (namely $p^m - 1$).

Lemma 5.3. ([13, Lemma XV.1]) Let $f \in R[x]$ be a polynomial which is not a zero divisor. Suppose $\bar{f}$ has a zero $s \in F$. Then f has one and only one zero r such that $\bar{r} = s$.

Proposition 5.4. Let $s \in F$ be an element of order $j \mid p^m - 1$ in F. Then there exists a unique $r \in R$ such that $r^j = 1$ and $\bar{r} = s$.

Proof. Since $\gcd(j,p)=1$, x^j-1 has only simple roots in F. By Lemma 5.3, there exists a unique $r\in R$ such that $r^j=1$ and $\bar{r}=s$. □

Hence, the polynomial x^j-1 splits in R if and only if it splits in F.

Since $x^{p^m-1}-1$ splits in F, the following Proposition is a consequence of Lemma 4.2.

Proposition 5.5. Let $q=p^m-1$ and let $g\in R$ be a primitive qth root of unity. Then g^i-g^j is a unit for all $0\le j<i\le q-1$.

Let G be the cyclic subgroup of $N(R)$ whose elements are the roots of the polynomial $x^{p^m-1}-1\in R[x]$. Proposition 5.5 implies that G is a subtractive subset in $N(R)$. Lemma 4.2 implies that the size of any subtractive subset of $N(R)$ cannot exceed p^m-1. A subtractive subset of $N(R)$ of size p^m-1 is said to be a *maximal subtractive subset*. Thus, G is a maximal subtractive subset of R.

Proposition 5.6. Let H be a subgroup of the cyclic group G. The annihilator polynomial of the subgroup

$$p(x)=\prod_{h\in H}(x-h)=x^{|H|}-1\ ,$$

is constant on the cosets of H.

Proof. Let $a\bar{h}$, $\bar{h}\in H$ be two elements in the coset aH.

$$p(a\bar{h})=\prod_{h\in H}(a\bar{h}-h)=\bar{h}^{|H|}\prod_{h\in H}(a-h\bar{h}^{-1})=\prod_{h\in H}(a-h)=p(a)\ .$$

□

Remark 5.7. We can choose $p(x)=x^{|H|}$ instead of dealing with $p(x)=x^{|H|}-1$.

The annihilators of subgroups form a class of $\big(|H|-1,(p^m-1)/|H|\big)$-good polynomials that can be employed in constructing optimal codes. If $|H|=r+1$, since the size of a subgroup divides the size of the group, $r+1$ divides $|G|$ and $p^m\equiv 1 \mod r+1$. Thus, the length of the code is always a multiple of $r+1$. It is worth highlighting that the sizes of the possible subgroups and maximum size of a subtractive subset impose constraints on the parameters of the code.

Remark 5.8. Analogously to [22, Proposition 4.3], by selecting two distinct subgroups of G with coprime orders, we can construct locally recoverable codes with two disjoint recovery sets.

6. A generalized version of the previous construction

6.1. **Algebra of good polynomials over finite chain rings.** Let R be a finite chain ring, let γ be the generator of the maximal ideal and let s be its nilpotency index. Let A be a well-conditioned set of size n and let $A=\bigcup_{i=1}^{l}A_i$ be a partition of A. Let

$$\mathcal{F}_A=\{f\in R[x]\mid f(A_i)=c_i\forall\ i\in\{1,\dots,l\}\ ,\deg f<|A|\} \tag{6.1}$$

be the set of polynomials over R of degree less than $|A|$ which are constant on blocks of the partition.

Definition 6.1. The *annihilator polynomial* of A is the monic polynomial of smallest degree h such that $h(a) = 0$ for all $a \in A$.

We endowed $\mathcal{F}_A$ with the multiplication modulo h:

$$\mathcal{F}_A \times \mathcal{F}_A \to \mathcal{F}_A \ , \quad (f, g) \mapsto fg \mod h \ .$$

We can observe that:

- $\mathcal{F}_A$ is a commutative ring;
- $\mathcal{F}_A$ is an R-module;
- The ring product is compatible with the module product, namely, the scalar multiplication is bilinear:

$$r \cdot (fg) = (r \cdot f)g = f(r \cdot g) \ .$$

Therefore $\mathcal{F}_A$ with the usual addition and the multiplication modulo h is a commutative algebra over R. We now investigate some properties of $\mathcal{F}_A$.

Proposition 6.2. The following holds for $\mathcal{F}_A$:

(1) If $f \in \mathcal{F}_A$ is a non-constant polynomial then $\max_i |A_i| \leq \deg f < |A|$;
(2) $\mathcal{F}_A$ is a free algebra of dimension l, namely, $\mathcal{F}_A$ is a free R-module with basis $\{f_1, \ldots, f_l\}$ with $f_i(A_j) = \delta_{i,j}$ and $\deg f_i < |A|$ (where $\delta_{i,j}$ is the Kroneker delta). Explicitly,

$$f_i(x) = \sum_{a \in A_i} \prod_{b \in A \setminus \{a\}} \frac{x - b}{a - b} \ ;$$

(3) Let $\{c_1, \ldots, c_l\}$ be a well-conditioned set in R and let g be the polynomial of degree less than $|A|$ satisfying $g(A_i) = c_i$ for all $1 \leq i \leq l$, i.e. ,

$$g(x) = \sum_{i=1}^{l} c_i \sum_{a \in A_i} \prod_{b \in A \setminus \{a\}} \frac{x - a}{b - a} \ .$$

Then the polynomials $\{1, g, \ldots, g^{l-1}\}$ form a basis for $\mathcal{F}_A$.

Proof. (1) Let $c \coloneqq f(A_i)$. The polynomial $f(x) - c$ has at least $|A_i|$ roots in the well-conditioned set A. Therefore $\deg f \geq |A_i|$ for all $1 \leq i \leq l$, and hence the claim.

(2) Since A is a well-conditioned set, the polynomials $f_i(x)$ are well-defined for all i. By definition, the set of polynomials $\{f_1, \ldots, f_l\}$ generate $\mathcal{F}_A$. Moreover the f_is are linearly independent: if $\sum_{i=0}^{l} \lambda_i f_i(x) = 0$ then $\sum_{i=0}^{l} \lambda_i f_i(A_j) = \sum_{i=0}^{l} \lambda_i \delta_{i,j} = \lambda_j = 0$. Therefore, $\{f_1, \ldots, f_l\}$ form a basis for $\mathcal{F}_A$.

(3) If $\sum_{j=1}^{l} b_j g(x)^{j-1} = 0$ implies $b_j = 0$ for all $1 \leq j \leq l$ then $1, g, \ldots, g^{l-1}$ are linearly independent. Notice that the equation $\sum_{j=1}^{l} b_j g(x)^{j-1} = 0$, is equivalent to the system

$$V(b_1, \ldots, b_l)^\top = 0 \ ,$$

where $V = (g^{j-1}(A_i))_{1 \leq i,j \leq l}$ is a Vandermonde matrix. Since $\{c_1, \ldots, c_l\}$ is a well-conditioned set in R, $\det V = \prod_{i \neq j}(c_i - c_j)$ is a unit in R, hence V is of full rank and $V(b_1, \ldots, b_l)^\top = 0$ if and only if $b_j = 0$ for all j. Since $\mathcal{F}_A$ has dimension l, $\{1, g, \ldots, g^{l-1}\}$ generate $\mathcal{F}_A$.

□

In the following, we will focus on the algebra of (r,l)-good polynomials $\mathcal{F}_A$ where A is partitioned into blocks of size $r+1$.

Remark 6.3. If $g \in \mathcal{F}_A$ is monic polynomial of degree $r+1$, then g always takes different values on the blocks of the partition of A. Otherwise, for some constant $c \in R$ the non-zero polynomial $g(x)-c$ would have $2(r+1)$ roots in a well-conditioned set. Moreover if g takes values $c_1,\dots,c_l$ on $A_1,\dots,A_l$ respectively, then $\{c_1,\dots,c_l\}$ is a subtractive subset of R. By contradiction, assume $g(A_i)=c_i$ and $g(A_j)=c_i+\lambda\gamma$ for some $\lambda \in R$. Then the polynomial $h(x)=\gamma^{s-1}\big(g(x)-c_i\big)$ is a non-zero polynomial of degree $r+1$ having at least $2(r+1)$ roots in a well-conditioned set, which leads to a contradiction. From Proposition 6.2(3) follows that the algebra $\mathcal{F}_A$ is generated by the powers of g. Hence, if g is the good polynomial introduced in Theorem 4.8 then its powers span the algebra of (r,l)-good polynomials.

6.2. **A family of Locally Recoverable Codes.** Let A be a well-conditioned set of size n and let $A=\bigcup_{i=1}^{l} A_i$ be a partition of A into l subssets of size $r+1$. Let

$$\mathcal{F}_A^r = \bigoplus_{i=0}^{r-1} \mathcal{F}_A x^i \ .$$

Note that $\mathcal{F}_A^r$, being the direct sum of algebras of dimension l, has dimension lr. The idea behind the next construction is to associate in a injective way the messages $a \in R^K$ to polynomials $f_a(x) \in \mathcal{F}_A^r$, and then evaluate f_a in the points of A.

Theorem 6.4. Let $A_1,\dots,A_l$ be subsets of R such that $A=\bigcup_{i=1}^{l} A_i$ is well-conditioned. Let $r \geq 1$ and assume there exists a polynomial $g \in \mathcal{F}_A$ of degree $r+1$ whose powers span $\mathcal{F}_A$. Let $K=rt$ and let

$$\Phi\colon R^K \to \mathcal{F}_A^r, \quad a \mapsto f_a(x) \ ,$$

be an injective map. If we define the code as

$$\mathcal{C} = \left\{ (f_a(\alpha),\ \alpha \in A) \mid a \in R^K \right\} \ ,$$

then $\mathcal{C}$ is a free (n,K,r)-code with minimum distance

$$d \geq n - \max_{a,b \in R^K} \deg(f_a - f_b) \geq n - \max_{a \in R^K} \deg f_a \ .$$

Proof. In order to determine the parameters of the code, we essentially repeat the proof of Theorem 4.8. We explicitly determine the bound on the minimum distance. For a given message vector $a \in R^K$ the encoding polynomial reads

$$f_a(x) = \sum_{i=0}^{r-1} f_i(x) x^i \ ,$$

with $f_i(x) \in \mathcal{F}_A$. Since $\{1, g, \dots g^{l-1}\}$ is a basis for $\mathcal{F}_A$,

$$\begin{aligned} \deg f_a &\leq (r+1)(l-1) + (r-1) \leq rl + l - r - 1 + r - 1 = \\ &= \frac{nr}{r+1} + \frac{n}{r+1} - 2 = n - 2 < n \ . \end{aligned}$$

Let $c_a = (f_a(\alpha), \alpha \in A)$ and $c_b = (f_b(\alpha), \alpha \in A)$ be two codewords corresponding to the distinct message vectors a and b. Since Φ is injective and $\deg(f_a - f_b) < n$, c_a and c_b are distinct and the claim follows. □

Notice that the recovering procedure follows the same steps of Construction 4.8.

7. Removing the constraints on code length

7.1. **Codes over well-conditioned sets with arbitrary length.** If n is the code length and r is the locality, Theorem 4.8 and Theorem 7.9 require the assumption that $r+1$ divides n.We provide a different construction that relaxes this condition.

Let R be a finite chain ring, A be a well-conditioned set, $|A| = n$ with $n \mod (r+1) = m \neq 0, 1$, and let $h_A(x) = \prod_{a \in A}(x-a)$ be the annihilator polynomial of the set A. Let r, K be positive integers and assume $r \mid K+1$ (this constraint can be lift, see Remark 4.10.2.).

Let $g \in \mathcal{F}_A$ be a polynomial of degree $r+1$ whose powers span $\mathcal{F}_A$. Without loss of generality we may assume that g vanishes on A_l, otherwise one can consider the powers of the polynomial $g(x) - g(A_l)$.

Theorem 7.1. Let $A = \bigcup_{i=1}^{l} A_i$ be a well-conditioned set with $|A_i| = r+1$ for all $1 \leq i \leq l-1$ and $|A_l| = m < r+1$. Let $g(x)$ be a polynomial of degree $r+1$ whose powers span $\mathcal{F}_A$. Let $a = (a_0, \ldots, a_{r-1}) \in R^K$ be the message vector with $a_i \in R^{\frac{K+1}{r}}$ for $i \neq m-1$ and $a_{m-1} \in R^{\frac{K+1}{r}-1}$. We define the encoding polynomial as

$$f_a(x) = \sum_{i=0}^{m-2} \sum_{j=0}^{\frac{K+1}{r}-1} a_{i,j} g(x)^j x^i + \sum_{j=1}^{\frac{K+1}{r}-1} a_{m-1,j} g(x)^j x^{m-1} + \sum_{i=m}^{r-1} \sum_{j=0}^{\frac{K+1}{r}-1} a_{i,j} g(x)^j h_{A_l}(x) \, .$$

Let

$$\mathcal{C} = \left\{ (f_a(\alpha), \ \alpha \in A) \mid a \in R^K \right\} .$$

Then $\mathcal{C}$ is a free (n, K, r)-LRC code with minimum distance

$$d \geq n - K - \left\lceil \frac{K}{r} \right\rceil + 1$$

Proof. The degree of the encoding polynomial $f_a(x)$ is at most

$$\left(\frac{K+1}{r} - 1 \right)(r+1) + r - 1 = K + 1 + \frac{K+1}{r} - 1 + r - 1 \leq K + \left\lceil \frac{K}{r} \right\rceil + 1 \, .$$

Since the encoding is linear, the bound on the minimum distance follows.
For any position $\alpha \in \bigcup_{i=1}^{l-1} A_i$, the recovery procedure follows the same steps of 6.4. Indeed $f_a(x) \in \bigoplus_{i=0}^{r-1} \mathcal{F}_A x^i$, and hence, any symbol can be recovered by accessing r symbols. The only specific situation worth examining is when the symbol α to be recovered belongs to A_l. It is essential to note that the polynomial $f_a(x)$ restricted to A_l has degree at most $m-2$. Therefore, in order to recover the value of $f_a(\alpha)$, $\alpha \in A_m$, we find the decoding polynomial $\delta(x) = \sum_{i=0}^{m-2} f_i(\alpha) x^i$. $\delta(x)$ is obtained from the set of $m-1$ values $f_a(\beta) = \delta(\beta)$, $\beta \in A_m \setminus \{\alpha\}$. Finally we compute $f_a(\alpha) = \delta(\alpha)$. □

Note that the minimum of the code $\mathcal{C}$ in Theorem 7.1 distance is at most one less than the maximum possible value.

7.2. **LRC codes from arbitrary MDS codes.** We present an alternative construction that relaxes the condition $r+1 \mid n$. In the following, we will construct a code such that its symbols can be partitioned into t MDS codes C_i of length n_i and rank K_i.

Definition 7.2. Let C be a code whose coordinates are partitioned into l sets A_i of size n_i. Let C_i be the code restricted to the coordinates in A_i. The code C has (r,ρ)-*locality* if for all $1 \le i \le l$ we have

- $n_i \le r+\rho-1$;
- $d_{C_i} \ge \rho$.

From the Singleton bound it follows that the rank of C_i is at most r.

On the same line of [10, Theorem 2.1], it is possible to improve bound 3.3.

Theorem 7.3. Let R be a finite chain ring and let C be a linear code of length n, rank K and with (r,ρ)-locality. Then

$$d \le n - K + 1 - \left(\left\lceil \frac{K}{r} \right\rceil - 1 \right)(\rho - 1) \ . \tag{7.1}$$

Theorem 7.4. Let $r \ge 1$ and let $A = \bigcup_{i=1}^{l} A_i$ be a partition of the well-conditioned set A into l subsets with $|A_i| = r+\rho-1$ for all $1 \le i \le l$. Let $g(x) \in R[x]$ be an $(r+\rho-1, l)$-good polynomial on the blocks of the partition of A. For $r \mid K$ (this constraint can be lifted, see Remark 4.10), let $a = (a_0, \ldots, a_{r-1}) \in R^K$ be the message vector with $a_i \in R^{\frac{K}{r}}$ for all $1 \le i \le l$. We define

$$f_a(x) = \sum_{i=0}^{r-1} \sum_{j=0}^{\frac{K}{r}-1} a_{i,j} g(x)^j x^i \ ; \tag{7.2}$$

and

$$\mathcal{C} = \left\{ (f_a(\alpha),\ \alpha \in A) \mid a \in R^K \right\} .$$

Then $\mathcal{C}$ is a free code with (r,ρ)-locality and rank K. Moreover C is an optimal (r,ρ)-LRC code.

Proof. Suppose there is an erased symbol $f_a(\alpha)$ for some $\alpha \in A_i$. The restriction of f_a to A_i is a polynomial of degree at most $r-1$. On the other hand $|A_i \setminus \{\alpha\}| = r+\rho-2$ and hence $f_a(\alpha)$ can be reconstructed from any r values in the locations of the set A_i. Since $\mathcal{C}$ is linear and $\deg f_a \le \left(\frac{K}{r}-1\right)(\rho+r-1)+r-1 = K-r+r-1+(\frac{K}{r}-1)(\rho-1)$, then $\mathcal{C}$ is (r,ρ)-optimal. □

The previous construction is a particular case of a more general one based on the Chinese Remainder Theorem for rings [13, Section V].

Definition 7.5. Let R be a ring. Two ideals I and J are called *coprime* if $I+J=R$.

Theorem 7.6. (Chinese Remainder Theorem) Let R be a commutative ring and let $I_1, \ldots, I_n$ be pairwise coprime ideals of R. Let $I = I_1 \cap \cdots \cap I_n$. The ring morphism

$$\Phi\colon R/I \to R/I_1 \times \ldots R/I_n, \quad r + I \mapsto (r + I_1, \ldots, r + I_n) \ ,$$

is an isomorphism.

Corollary 7.7. Let $h_1(x), \ldots, h_n(x) \in R[x]$ be pairwise coprime polynomials. Then, for any $a_1(x), \ldots, a_n(x) \in R[x]$, there exists a unique polynomial $f \in R[x]$ of degree at most $\sum_i \deg h_i$ such that

$$f(x) \equiv a_i(x) \bmod h_i(x) \ \text{ for all } 1 \leq i \leq n \ .$$

Let R be a finite chain ring, let A be a subtractive subset of $N(R)$, and let $A = \bigcup_{i=1}^{l} A_i$ be a partition of A. Using the Hensel Lemma [13], one can prove that the annihilator polynomials of the A_is, namely, $h_i(x) = \prod_{a \in A_i}(x - a)$, generate pairwise coprime ideals.

Theorem 7.8. Let R be a finite chain ring and let A be a subtractive subset of $N(R)$. Let $A = \bigcup_{i=1}^{l} A_i$ be a partition of A such that $|A_i| = n_i$ for all $1 \leq i \leq l$. Let

$$\psi\colon R^K \to \mathcal{F}_{K_1} \times \cdots \times \mathcal{F}_{K_l}, \quad a \mapsto (a_1(x), \ldots, a_l(x)) \ ,$$

be an injective mapping, where $\mathcal{F}_{K_i}$ is the space of polynomials of degree less than K_i. Let $h_i(x)$ be the annihilator polynomial of A_i. For any message vector $a \in R^K$ we define the encoding polynomial $f_a(x)$ as the unique polynomial of degree less than n such that

$$f_a(x) = a_i(x) \bmod h_i(x) \ .$$

Let

$$\mathcal{C} = \left\{ (f_a(\alpha), \ \alpha \in A) \mid a \in R^K \right\} \ .$$

Then, $\mathcal{C}$ is a free LRC code of rank K. Moreover $\mathcal{C}$ can be partitioned into l disjoint local codes $\mathcal{C}_i$, where $\mathcal{C}_i$ is an (n_i, K_i)-MDS code.

Proof. Let $f_a(x)$ be the encoding polynomial of the message vector a. By construction, for all $1 \leq i \leq l$, there exists a polynomial $g(x)$ such that

$$f_a(x) = g(x)h_i(x) + a_i(x) \ .$$

Thus, for all $\alpha \in A_i$, $f_a(\alpha) = a_i(x)$. Hence, the restriction of $f_a(x)$ to A_i is a polynomial of degree less than K_i. Since $|A_i| = n_i$, $f_a(x)\big|_{A_i}$ is a polynomial of degree less than K_i evaluated on $n_i > K_i$ points. Therefore the set of codewords

$$(f_a(\alpha), \alpha \in A_i)$$

form an (n_i, K_i)-MDS code for all $1 \leq i \leq l$. □

We observe that the minimum distance of the code constructed in this way is at least the minimum between the distances of the local codes $\mathcal{C}_i$.

7.3. **LRC codes with non-well-conditioned sets.** The most significant limitation in the previous approaches is the restriction on the code length. The maximum code length coincides with the maximum size of a well-conditioned set. To address this problem, we now try to extend Theorem 4.8 to non-well-conditioned sets.

For simplicity, let $R = \mathrm{GR}(p^s, m)$ be a Galois ring and let $N(R)$ denote its group of units having size $p^{m(s-1)}(p^m - 1)$.
Let G be the maximal cyclic subgroup of $N(R)$ of order coprime with p and let H be a subgroup of G. The cosets $A_1, \ldots, A_l$ of H in $N(R)$ induce a partition of $N(R) = \bigcup_{i=1}^{l} A_i$. While H is subtractive in $N(R)$ (see Proposition 5.5), the same does not hold true for $N(R)$. However $N(R)$ contains a (maximal) subtractive subset. Up to reordering, we can assume $\mathcal{A} = \bigcup_{i=1}^{m} A_i$, $m < l$, to be a maximal subtractive subset in $N(R)$.

The difference between Theorem 4.8 and the next construction lies in the choice of the set of evaluation points: in the former a maximal subtractive subset is used, while in the latter the entire $N(R)$ is employed.

Theorem 7.9. Let $r \geq 1$ and let $N(R) = \bigcup_{i=1}^{l} A_i$ be a partition of $N(R)$ into l subtractive subsets A_i of size $r+1$ for all $1 \leq i \leq l$. Let $\mathcal{A} = \bigcup_{i=1}^{m} A_i$, $m < l$, be a maximal subtractive subset of $N(R)$. Let $g(x) \in R[x]$ be an (r, l)-good polynomial on the blocks of the partition of $N(R)$. For $t \leq l$, set $n = (r+1)l$ and $K = rt$. Let

$$a = (a_{i,j},\ 0 \leq i \leq r-1,\ 0 \leq j \leq t-1) \in R^K \ .$$

We define

$$f_a(x) = \sum_{i=0}^{r-1} \sum_{j=0}^{t-1} a_{i,j} g(x)^j x^i \ ; \tag{7.3}$$

and

$$\mathcal{C} = \left\{ (f_a(\alpha),\ \alpha \in N(R)) \mid a \in R^K \right\} .$$

Then $\mathcal{C}$ is a free (n, K, r)-code where $n = |N(R)| = p^{m(s-1)}(p^m - 1)$ and minimum distance

$$d = n - p^{m(s-1)} \left(K + \frac{K}{r} - 2 \right) = p^{m(s-1)} d_{\mathcal{C}'} \ ,$$

where $\mathcal{C}' = \mathcal{C}\big|_{\mathcal{A}}$ is the restriction of $\mathcal{C}$ to the maximal subtractive subset $\mathcal{A} = \bigcup_{i=0}^{m} A_i$.

Proof. The proof follows the same line of 4.8. We explicitly compute the minimum distance of the code.
Let $f_a(x)$ be the encoding polynomial of the message vector a. The maximum number of zeros of $f_a(x)$ establishes a bound on the minimum distance of $\mathcal{C}$. Notice that $\deg f_a(x) = K + \frac{K}{r} - 2$, and hence, by Corollary 4.6,

$$d \geq n - \left(K + \frac{K}{r} - 2 \right) p^{(s-1)m} \ .$$

We show that equality holds. Let $\mathcal{C}'$ be the code obtained from $\mathcal{C}$ by puncturing the last $n - p^m + 1$ positions, i.e., we left with an $(p^m - 1, K, r)$-LRC code over the subtractive subset $\mathcal{A} = \bigcup_{i=0}^{m} A_i$. Note that $f_a(x)$ has at most $K + \frac{K}{r} - 2$

roots in $\mathcal{A}$. Moreover, the LRC bound (3.3) ensures that there exists a message vector $b \in R^K$ such that its encoding polynomial $f_b(x)$ has exactly $K + \frac{K}{r} - 2$ roots in $\mathcal{A}$. Let $\{\bar{x}_1, \ldots, \bar{x}_{K+\frac{K}{r}-2}\}$ be the set of zeros of f_b in $\mathcal{A}$. Since the encoding is linear, $f'(x) = p^{s-1} f_b(x)$ is the encoding polynomial associated to the message vector $p^{s-1}b \in R^K$. If $\{\bar{x}_1, \ldots, \bar{x}_{K+\frac{K}{r}-2}\}$ are the zeros of f_b in $\mathcal{A}$, then $\{\bar{x}_1 + M, \ldots, \bar{x}_{K+\frac{K}{r}-2} + M\}$ are the zeros of f' in $N(R)$. Since $|M| = p^{m(s-1)}$, f' has $p^{m(s-1)}\big(K + \frac{K}{r} - 2\big)$ roots in $N(R)$ and the claim follows. □

Remark 7.10. We have that:

- The central problem of all the previous constructions is to identify families of good polynomials. Construction 7.9 does not lead to a wider class of good polynomials. Let $N(R) = \bigcup_{i=1}^{l} A_i$ be a partition of $N(R)$ and let $\mathcal{A} = \bigcup_{i=1}^{m} A_i$, $m < l$, be a maximal subtractive subset in $N(R)$. Let $h(x) = \prod_{a \in \mathcal{A}}(x - a)$ be the annihilator polynomial of $\mathcal{A}$. If $g'(x)$ is an (r, l)-good polynomial for the partition of $N(R)$, then $g'(x) = g(x) \mod h$ where $g(x)$ is an (r, m)-good polynomial for the partition $\mathcal{A}$. Therefore the class of (r, l)-good polynomials coincides modulo h to the class of (r, m)-good polynomials.
- We have removed the constraint on the maximum code length. Nevertheless, the code does not meet the LRC bound (3.3) and thus it is not known whether it is optimal of not. Let $\overline{C}$ be the projection of C over the residue field of R. $\overline{C}$ is a repetition code. Indeed, a locally recoverable code of length $p^m - 1$, dimension K, and minimum distance $d = n - K - \frac{K}{r} + 2$ is iterated $p^{m(s-1)}$ times. Therefore, $\overline{C}$ is an LRC code with multiple disjoint recovering sets, consisting of $p^{m(s-1)} - 1$ recovering sets of size 1 and $p^{m(s-1)}$ of size r.

A natural question arises: is there any constraint on the maximum length of a code meeting the LRC bound, as a function of the alphabet size?

7.4. **Bounds on the maximum length of an optimal LRC over finite chain rings.** In the following, we will see that the problem of determining the maximum possible length of an optimal LRC code over a finite chain ring is closely related to the same problem over fields.

Let R be a finite chain ring, let γ be the generator of the maximal ideal and let s be its nilpotency index. Let F be the residue field of R, i.e. $F = R/(\gamma)$. For any $C \subseteq R^n$ we define the code $(C : t) = \{e \in R^n \mid te \in C\}$. In accordance with the notation of Section 4.1, let $\overline{(C : t)}$ be the projection of $(C : t)$ over F.

Definition 7.11. To any code $C \subseteq R^n$ we associate the tower of codes over R

$$C = (C : \gamma^0) \subseteq \cdots \subseteq (C : \gamma^i) \subseteq \cdots \subseteq (C : \gamma^{s-1}) \ ;$$

and its projection over F

$$\overline{C} = \overline{(C : \gamma^0)} \subseteq \cdots \subseteq \overline{(C : \gamma^i)} \subseteq \cdots \subseteq \overline{(C : \gamma^{s-1})} \ .$$

Proposition 7.12. If C is an R-linear code of length n, rank K, minimum distance d then $\overline{(C : \gamma^{s-1})}$ is a linear code over F of length n, dimension K and minimum distance d.

For a proof see [15, Theorem 4.2 and Theorem 4.5].

Proposition 7.13. If $v_1 \dots, v_u \in R^n$ are modularly dependent vectors in R^n then $\overline{v_1}, \dots, \overline{v_u} \in F^n$ are linearly dependent over F.

Proof. If $v_1, \dots, v_u$ are modularly dependent in R^n, i.e. , there exist $b_1, \dots, b_u \in R$, not all zero divisors, such that $\sum_{i=1}^{u} b_i v_i = 0$. Hence $\gamma \mid \sum_{i=1}^{u} b_i v_i$ and $\sum_{i=1}^{u} \overline{b_i}\,\overline{v_i} = 0$ with $\overline{b_i}$ not all zero. Therefore $\overline{v_1}, \dots, \overline{v_u}$ are linearly dependent over F. □

Proposition 7.14. If C is a locally recoverable code with locality r over R then $\overline{(C : \gamma^{s-1})}$ is a locally recoverable code with locality $\tilde{r} \leq r$ such that $\lceil \frac{K}{\tilde{r}} \rceil = \lceil \frac{K}{r} \rceil$.

Proof. Proposition 7.13 implies that the locality of C cannot increase. The claim follows from the fact that minimum distance of C and $\overline{(C : \gamma^{s-1})}$ coincides. □

Consequently, determining the maximum possible length of the optimal LRC code C over R reduces to the problem of determining the maximum possible length of the optimal code $\overline{(C : \gamma^{s-1})}$ over F. While for small code distances ($d = 3, 4$) optimal LRC codes with unbounded length over any fixed alphabet of size $q \geq r + 1$ are known, for $d \geq 5$ there is an upper bound on the length of the optimal LRC as a function of its alphabet size. Guruswami et al. in [7] proved that for $d = 5$ the length of an optimal LRC over an alphabet of size q is at most $\mathcal{O}(q^2)$. Moreover, if $d > 5$ the length is at most $\mathcal{O}(q^3)$.

8. Conclusions

In analogy to codes over finite fields, the minimum distance of a locally recoverable code over a finite chain ring is bounded as a function of the length n, the rank K and the locality r of the code. This bound is tight, as we have constructed a family of evaluation codes that achieves this bound for any value of the locality parameter r and with length bounded by the size of the residue field of the ring. The construction relies on the use of good polynomials as its fundamental components. Moreover, this construction can be extended in various directions: for instance codes over non-well-conditioned sets or codes with multiple recovering sets are presented. An interesting extension of this work would be to try to build longer locally recoverable codes. A second promising line of research would be to build a wider class of good polynomials over finite chain rings.

Acknowledgement

This publication was created with the co-financing of the European Union FSE-REACT-EU, PON Research and Innovation 2014-2020 DM1062/2021, and the French National Agency of Research via the project ANR-21-CE39-0009-BARRACUDA. The authors acknowledge support from Ripple's University Blockchain Research Initiative. The first and third author are members of the INdAM Research Group GNSAGA. A preliminary version of this work was partially presented on talks given at Young researcher Algebra Conference 2023 in L'Aquila, Italy and Convegno annuale del gruppo UMI Crittografia e Codici in Perugia, Italy by the first author.

References

[1] Marc André Armand. List decoding of generalized Reed-Solomon codes over commutative rings. *IEEE transactions on information theory*, 51(1):411–419, 2005.

[2] Alexander Barg, Kathryn Haymaker, Everett W Howe, Gretchen L Matthews, and Anthony Várilly-Alvarado. Locally recoverable codes from algebraic curves and surfaces. In *Algebraic Geometry for Coding Theory and Cryptography: IPAM, Los Angeles, CA, February 2016*, pages 95–127. Springer, 2017.

[3] Viveck R. Cadambe and Arya Mazumdar. Bounds on the size of locally recoverable codes. *IEEE Transactions on Information Theory*, 61(11):5787–5794, 2015.

[4] Michael Forbes and Sergey Yekhanin. On the locality of codeword symbols in non-linear codes. *Discrete Mathematics*, 324:78–84, 2014.

[5] Parikshit Gopalan, Cheng Huang, Huseyin Simitci, and Sergey Yekhanin. On the locality of codeword symbols. *IEEE Transactions on Information theory*, 58(11):6925–6934, 2012.

[6] Sreechakra Goparaju and Robert Calderbank. Binary cyclic codes that are locally repairable. In *2014 IEEE International Symposium on Information Theory*, pages 676–680. IEEE, 2014.

[7] Venkatesan Guruswami, Chaoping Xing, and Chen Yuan. How long can optimal locally repairable codes be? *IEEE Transactions on Information Theory*, 65(6):3662–3670, 2019.

[8] Lingfei Jin. Explicit construction of optimal locally recoverable codes of distance 5 and 6 via binary constant weight codes. *IEEE Transactions on Information Theory*, 65(8):4658–4663, 2019.

[9] Lingfei Jin, Liming Ma, and Chaoping Xing. Construction of optimal locally repairable codes via automorphism groups of rational function fields. *IEEE Transactions on Information Theory*, 66(1):210–221, 2019.

[10] Govinda M Kamath, N Prakash, V Lalitha, and P Vijay Kumar. Codes with local regeneration and erasure correction. *IEEE Transactions on information theory*, 60(8):4637–4660, 2014.

[11] Jian Liu, Sihem Mesnager, and Lusheng Chen. New constructions of optimal locally recoverable codes via good polynomials. *IEEE Transactions on Information Theory*, 64(2):889–899, 2017.

[12] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977.

[13] Bernard R McDonald. *Finite rings with identity*, volume 28. Marcel Dekker Incorporated, 1974.

[14] Giacomo Micheli. Constructions of locally recoverable codes which are optimal. *IEEE transactions on information theory*, 66(1):167–175, 2019.

[15] G.H. Norton and A. Salagean. On the hamming distance of linear codes over a finite chain ring. *IEEE Transactions on Information Theory*, 46(3):1060–1067, 2000.

[16] Graham H Norton and Ana Sălăgean. On the structure of linear and cyclic codes over a finite chain ring. *Applicable algebra in engineering, communication and computing*, 10:489–506, 2000.

[17] Young Ho Park. Modular independence and generator matrices for codes over $\mathbb{Z}_m$. *Designs, codes and Cryptography*, 50(2):147–162, 2009.

[18] N Prakash, Govinda M Kamath, V Lalitha, and P Vijay Kumar. Optimal linear codes with a local-error-correction property. In *2012 IEEE International symposium on information theory proceedings*, pages 2776–2780. IEEE, 2012.

[19] Guillaume Quintin, Morgan Barbier, and Christophe Chabot. On generalized Reed–Solomon codes over commutative and noncommutative rings. *IEEE transactions on information theory*, 59(9):5882–5897, 2013.

[20] Ankit Singh Rawat, Dimitris S. Papailiopoulos, Alexandros G. Dimakis, and Sriram Vishwanath. Locality and availability in distributed storage. *IEEE Transactions on Information Theory*, 62(8):4481–4493, 2016.

[21] Keisuke Shiromoto. Singleton bounds for codes over finite rings. *Journal of Algebraic Combinatorics*, 12:95–99, 2000.

[22] Itzhak Tamo and Alexander Barg. A family of optimal locally recoverable codes. *IEEE Transactions on Information Theory*, 60(8):4661–4676, 2014.

[23] Jay A Wood. Foundations of linear codes defined over finite modules: the extension theorem and the macwilliams identities. In *Codes over rings*, pages 124–190. World Scientific, 2009.

[24] Chaoping Xing and Chen Yuan. Construction of optimal locally recoverable codes and connection with hypergraph. *arXiv preprint arXiv:1811.09142*, 2018.

Department of Mathematics, University of Trento, Italy
Email address: giulia.cavicchioni@unitn.it

LIRMM, Université de Montpellier, France
Email address: eleonora.guerrini@lirmm.fr

Department of Mathematics, University of Trento, Italy
Email address: alessio.meneghetti@unitn.it