Information Set Decoding for Ring-Linear Codes

Giulia Cavicchioni[1], Alessio Meneghetti[1], Giovanni Tognolini[1]

[1]Department of Mathematics, University of Trento, Trento, Italy.

Contributing authors: giulia.cavicchioni@unitn.it;
alessio.meneghetti@unitn.it; giovanni.tognolini@unitn.it;

Abstract

Information set decoding (ISD) algorithms currently offer the most powerful tool to solve the two archetypal problems of coding theory, namely the Codeword Finding Problem and the Syndrome Decoding Problem. Traditionally, ISD have primarily been studied for linear codes over finite fields, equipped with the Hamming metric. However, recently, other possibilities have also been explored. These algorithms have been adapted to different ambient spaces and metrics, such as the rank metric or the Lee metric over $\mathbb{Z}_m$. In this paper, we show that it is possible to leverage the ring structure to construct more efficient decoding algorithms than those obtained by simply adapting ISD. In particular, we describe a framework that can be applied to any additive metric including Hamming and Lee, and that can be adapted to the case of the rank metric, providing algorithms to solve the two aforementioned problems, along with their average computational costs.

Keywords: Ring-linear code, Hamming metric, Locally recoverable codes, Erasure recovery

1 Introduction

The theory of linear codes is an excellent source of hard problems, with the two most notable examples being the decoding of an arbitrary linear code and the determination of whether a given code possesses a codeword of a specified (typically low) weight. These problems, referred to as the Syndrome Decoding Problem (SDP) and the Codeword Finding Problem (CFP), are ubiquitous in the context of linear codes; for instance, in code-based cryptography, both the SDP and CFP have been fundamental security assumptions for decades [1, 2].

Traditionally, linear codes are algebraic varieties living in a finite-dimensional vector space over a finite field equipped with Hamming metric. In this context,

information set decoding (ISD) algorithms currently represent the best-known method for solving both the SDP and CFP, establishing themselves as powerful tools for decoding linear codes [3–6]. However, recent research in the coding community has investigated new directions, exploring different algebraic structure and metrics such as and the Rank metric [7, 8], the sum-rank metric [9] or Lee metric [10] over the integer ring $\mathbb{Z}_m$. Therefore ISD algorithms have been adapted to account for the new underlying algebraic structure or new metrics [8, 11–14].

Although preliminary work has been conducted in this direction, the problem of decoding over rings is relatively new, and the potential of these algorithms remains largely unexplored. This leaves ample space for developing new algorithms and gaining a deeper understanding of this emerging area of research. The question motivating our research is thus:

In the context of ring-linear codes, is it possible to construct decoding algorithms that outperform those obtained by simply adapting ISD?

Our Contribution

In this work, we answer this question by proposing new decoding algorithms for codes defined over rings, showing new promising approaches for the decoding problems. For each of the analyzed metrics, we propose new algorithms that mirror the previous ones, but derive additional advantages from the structure of the underlying ring.

This work is structured as follows. In Section 2 we introduce the notation used throughout the paper, briefly describing linear codes defined over a Galois ring, and then moving on to describe the Hamming, Lee, and rank metrics, as well as the behaviour of the Gilbert-Varshamov (GV) bound in each of these cases. Section 3 introduces the key problems around which our research hinges, namely SDP and CFP, describing the algorithms now in use to solve these problems, as well as the related complexities. Finally, we introduce a new framework for solving these problems and explore it in each metric mentioned above, respectively in Sections 4, 5 and 6. We draw some concluding remarks in Section 7.

2 Preliminaries

In this section we are going to focus on the preliminaries we need to state our result. In order to do this, we will start fixing the notation we are going to use in the remainder of the article. Afterwards, we are going to introduce some basics concerning codes over rings. We will then conclude by providing an overview on the GV bound for the three metrics under analysis.

2.1 Notation

Throughout this paper, we primarily consider codes as submodules over a Galois extension of the integer ring $\mathbb{Z}_{p^r} \coloneqq \mathbb{Z}/p^r\mathbb{Z}$, where p is a prime and r is a positive integer. From now on, given a Galois ring $\mathcal{R}$ and $t \in \mathcal{R}$, we will write $\langle t \rangle$ to refer either

to the ideal $t\mathcal{R}$ or the submodule $t\mathcal{R}^n$, depending on the context.
We will also denote the *q-binomial coefficient* by $\begin{bmatrix} n \\ k \end{bmatrix}_q$, defined as

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i} \ .$$

If q is a prime power, this value represents the number of k-dimensional subspaces of $\mathbb{F}_q^n$.

2.2 Codes over Galois rings

An interesting family of finite commutative rings is given by the Galois rings, as they both generalize finite fields and the rings of integers modulo p^r.

Definition 2.1. *Let p be a prime, and r, m positive integers. The* Galois ring $\mathrm{GR}(p^r, m)$ *of characteristic p^r and with p^{rm} elements is the Galois extension of $\mathbb{Z}_{p^r}$ of degree m.*

Example 2.1. The most basic examples of Galois rings are significant special cases.

- If $m = 1$, $\mathrm{GR}(p^r, 1)$ is the ring of integers $\mathbb{Z}_{p^r}$;
- If $r = m = 1$, $\mathrm{GR}(p, 1)$ is the prime field $\mathbb{Z}_p$;
- If $r = 1$, $\mathrm{GR}(p, m)$ is the Galois extension of $\mathbb{F}_p$ of degree m, namely $\mathbb{F}_{p^m}$.

As for the Galois fields, there exists a polynomial construction for Galois rings, which are indeed a Galois extension of a base ring [15]. More precisely, $\mathrm{GR}(p^r, m)$ is isomorphic to $\mathbb{Z}_{p^r}[x]/\langle f_m \rangle$, where f is a monic polynomial of degree m which is irreducible modulo p.

Galois rings are local rings, with principal maximal ideal $p\mathrm{GR}(p^r, m) = \langle p \rangle$. In fact, $\mathrm{GR}(p^r, m)$ is a finite chain ring and every non-zero ideal has the form $\langle p^i \rangle$, where $0 \leq i \leq r - 1$.

Remark 2.1. As for finite fields, any element $t \in \mathrm{GR}(p^r, m)$ can be written in its *additive representation*

$$t = t_0 + t_1\xi + \cdots + t_{m-1}\xi^{m-1}, \ t_i \in \mathbb{Z}_{p^r} \text{ for all } 0 \leq i \leq m-1 \ ,$$

where ξ is a primitive p^m-root of unity. As a consequence, $\mathrm{GR}(p^r, m)$ is a free $\mathbb{Z}_{p^r}$-module and $\{1, \xi, \ldots, \xi^{m-1}\}$ is a basis of $\mathrm{GR}(p^r, m)$.

Finite chain rings, and in particular, Galois rings are the most prominent alphabets in ring-linear coding theory. Throughout this section, we will denote with $\mathcal{R}$ the Galois ring $\mathrm{GR}(p^r, m)$.

Definition 2.2. *An $\mathcal{R}$-*linear code $\mathcal{C}$ *of length n is an $\mathcal{R}$-submodule of $\mathcal{R}^n$. The free module $\mathcal{R}^n$ is called the* ambient space *of $\mathcal{C}$, and the elements of $\mathcal{C}$ are called* codewords.

Unless otherwise specified, from now on, we consider any code to be $\mathcal{R}$-linear. The *$\mathcal{R}$-dimension* of the code, defined as

$$k := \log_{|\mathcal{R}|} |\mathcal{C}| \ ,$$

is an analog of the dimension for codes over finite fields. However, the $\mathcal{R}$-dimension does not fully describe the dimension of a ring-linear code. As a consequence of the

fundamental Theorem of finite abelian groups, any $\mathcal{R}$-linear code $\mathcal{C}$ is isomorphic to the following direct sum of $\mathcal{R}$-modules

$$\mathcal{C} \cong (\mathcal{R}/p^r\mathcal{R})^{k_0} \times (\mathcal{R}/p^{r-1}\mathcal{R})^{k_1} \times \ldots \times (\mathcal{R}/p\mathcal{R})^{k_{r-1}}.$$

The unique r-tuple $(k_0, k_1, \ldots, k_{r-1})$ is called the *subtype* of $\mathcal{C}$. In addition k_0 is called the *free-rank* of $\mathcal{C}$. A code $\mathcal{C} \subseteq \mathcal{R}^n$ can be represented by a *generating set* representing a subset of codewords that generates $\mathcal{C}$ as an $\mathcal{R}$-submodule. We call a generating set *minimal generating set* if it is minimal with respect to inclusion.

Definition 2.3. *For an $\mathcal{R}$-linear code $\mathcal{C}$, the* rank *of $\mathcal{C}$ is the cardinality of a minimal generating set of $\mathcal{C}$. More generally, the* rank of an $\mathcal{R}$-module *is defined as the size of a minimal generating set for that module.*

Notice that the rank K of a module $\mathcal{C}$ of subtype $(k_0, k_1, \ldots, k_{r-1})$ is equal to $\sum_{i=0}^{r-1} k_i$ and hence, it follows $0 \leq k_0 \leq k \leq K \leq n$. In particular, a code is said to be *free* if its $\mathcal{R}$-dimension is equal to its rank, and in this case $k_0 = K$. Finally the *rate* of the code is given by $R \coloneqq k/n$. Notice also that, if $\mathcal{R}$ is a field, then $k_0 = k = K$ and $k_i = 0$ for every $i \in \{1, \ldots, r-1\}$.

Similar to the finite field case, ring-linear codes can be represented through a generator matrix or a parity-check matrix [16].

Definition 2.4. *Given a linear code $\mathcal{C} \subseteq \mathcal{R}^n$, a matrix $G \in \mathcal{R}^{K \times n}$ whose rows form a generating set of $\mathcal{C}$ is called a* generator matrix *of the code. A matrix $H \in \mathcal{R}^{(n-k_0)\times n}$ whose kernel coincides with $\mathcal{C}$ is called a* parity-check matrix *of $\mathcal{C}$.*

For our purposes, it is convenient to consider generator and parity-check matrices in standard form, which are defined as follows.

Proposition 2.5. *[16, Proposition 3.2] Let $\mathcal{R}$ be a finite chain ring and let $\mathcal{C} \subseteq \mathcal{R}^n$ be a linear code of length n and subtype $(k_0, \ldots, k_{r-1})$. Then $\mathcal{C}$ is permutation equivalent to a code having the following generator matrix in standard form:*

$$G = \begin{bmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \ldots & A_{0,r-1} & A_{0,r} \\ 0 & pI_{k_1} & pA_{1,2} & pA_{1,3} & \ldots & pA_{1,r-1} & pA_{1,r} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{2,3} & \ldots & p^2 A_{2,r-1} & p^2 A_{2,r} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & p^{r-1} I_{k_{r-1}} & p^{r-1} A_{r-1,r} \end{bmatrix},$$

where $A_{i,r} \in (\mathcal{R}/p^{r-i}\mathcal{R})^{k_i \times (n-K)}$ and $A_{i,j} \in (\mathcal{R}/p^{r-i}\mathcal{R})^{k_i \times k_j}$ for $j < r$. Moreover $\mathcal{C}$ is permutation equivalent to a code having a parity-check matrix in standard form:

$$H = \begin{bmatrix} B_{0,0} & B_{0,1} & \ldots & B_{0,s-1} & I_{n-K} \\ pB_{1,0} & pB_{1,1} & \ldots & pI_{k_{r-1}} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ p^{r-1}B_{r-1,0} & p^{r-1}I_{k_1} & \ldots & 0 & 0 \end{bmatrix},$$

where $B_{0,j} \in (\mathcal{R}/p^r\mathcal{R})^{(n-K)\times k_j}, B_{i,j} \in (\mathcal{R}/p^{r-i}\mathcal{R})^{k_{r-i}\times k_j}$, for $j > 1$.

Given an $\mathcal{R}$-linear code $\mathcal{C}$, for any subset $I \subset \{1, \ldots, n\}$ of the coordinates, we denote by $\mathcal{C}_I$ the code obtained by deleting in each codeword all but the coordinates indexed in I.

Definition 2.6. *Let $\mathcal{C}$ be an $\mathcal{R}$-linear code of rank K. An* information set *for $\mathcal{C}$ is a subset $I \subseteq \{1, \ldots, n\}$ of the coordinates of size K such that $|\mathcal{C}_I| = |\mathcal{C}|$.*

Using the parity check matrix in standard form, one can find an information set for the code in the first K columns of H.

2.3 Different ambient spaces and metrics

One of the most important parameters of a code is its minimum distance, as it is related to the code's error correction capability. Errors are measured using a metric, which is generally induced by a weight function.

Definition 2.7. *Given $\mathcal{R} = \mathrm{GR}(p^r, m)$, a* weight *over $\mathcal{R}$ is a function* $\mathrm{wt}\colon \mathcal{R} \to \mathbb{N}$ *satisfying*

1. $\mathrm{wt}(0) = 0$ *and* $\mathrm{wt}(x) > 0$ *for all* $x \neq 0$*;*
2. $\mathrm{wt}(x) = \mathrm{wt}(-x)$*;*
3. $\mathrm{wt}(x + y) \leq \mathrm{wt}(x) + \mathrm{wt}(y)$.

A weight function induces a *distance* defined as $\mathrm{d}\colon \mathcal{R} \times \mathcal{R} \to \mathbb{N}$, where $\mathrm{d}(x, y) := \mathrm{wt}(x - y)$. We may extend the weight and distance functions coordinate-wise, and these extensions will also be referred to as *(additive) weight* and *(additive) distance*, respectively. In particular, given $x \in \mathcal{R}^n$, we define

$$\mathrm{wt}(x) := \sum_{i=1}^{n} \mathrm{wt}(x_i) \ .$$

In coding theory, one of the most classical and important examples of an additive weight is the Hamming weight, introduced by Hamming in 1950 for codes over finite fields [17].

Definition 2.8. *Given a Galois ring $\mathcal{R}$, the* Hamming weight of an element $a \in \mathcal{R}$ *is given by*

$$\mathrm{wt}_{\mathsf{H}}(a) := \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{otherwise} \ . \end{cases}$$

We define the Hamming weight of an n-tuple $x \in \mathcal{R}^n$ *additively by*

$$\mathrm{wt}_{\mathsf{H}}(x) := \sum_{i=1}^{n} \mathrm{wt}_{\mathsf{H}}(x_i) \ .$$

The *Hamming support* of a vector $x \in \mathcal{R}^n$ is defined as the set of coordinates where x is non-zero, namely

$$\mathrm{supp}(x) := \{1 \leq j \leq n \mid x_j \neq 0\} \ .$$

Note that the Hamming weight of a vector $x \in \mathcal{R}^n$ is equal to the cardinality of its support, that is, $\mathrm{wt}_{\mathsf{H}}(x) = |\mathrm{supp}(x)|$. As an alternative to the classical Hamming metric, we can endow the ambient space with other metrics. A notable example of additive distance, when $\mathcal{R} = \mathbb{Z}_{p^r}$, is the Lee distance, first proposed in [18] as an extension of the Hamming metric for the binary field. It has recently garnered increasing attention in code-based cryptography [12, 14, 19, 20].

Definition 2.9. *The* Lee weight of an element $a \in \mathbb{Z}_{p^r}$ *is given by*

$$\mathrm{wt}_{\mathsf{L}}(a) \coloneqq \min\{a, |p^r - a|\} \ .$$

Similarly, we define the Lee weight of an n-tuple $x \in \mathbb{Z}_{p^r}^n$ *additively by*

$$\mathrm{wt}_{\mathsf{L}}(x) := \sum_{i=1}^{n} \mathrm{wt}_{\mathsf{L}}(x_i) \ .$$

The following bounds hold for any $a \in \mathbb{Z}_{p^r}$ and $x \in \mathbb{Z}_{p^r}^n$.

$$0 \leq \mathrm{wt}_{\mathsf{L}}(a) \leq \lfloor p^r/2 \rfloor \quad \text{and} \quad \mathrm{wt}_{\mathsf{H}}(x) \leq \mathrm{wt}_{\mathsf{L}}(x) \leq \lfloor p^r/2 \rfloor \mathrm{wt}_{\mathsf{H}}(x). \tag{1}$$

Another metric that has gained significant attention is the rank metric, which, unlike the Hamming and Lee metrics, is not additive. Rank-metric codes over finite fields were first studied in connection with association schemes by Delsarte in 1978 [21]. They were also independently introduced by Gabidulin in [22], where rank-metric codes are described as $\mathbb{F}_q$-linear spaces of vectors over an extension field. In other words, codewords are matrices and the distance between two codewords is the rank of their difference.

Rank-metric codes can also be extended to principal ideal rings [23]. Given $\mathcal{R} = \mathbb{Z}_{p^r}$, let $\mathcal{S} = \mathrm{GR}(p^r, m)$ be the Galois extension of $\mathcal{R}$. In this framework, a rank-metric code over $\mathcal{S}$ is an $\mathcal{S}$-submodule of $\mathcal{S}^n$. As $\mathcal{S}$ is a free $\mathcal{R}$-module of rank m, see Remark 2.1, elements of $\mathcal{S}$ can be seen as vectors in $\mathcal{R}^m$. Therefore we can define rank of elements of $\mathcal{S}$.

Definition 2.10. *Given a vector $x = (x_1, \ldots, x_n) \in \mathcal{S}^n$ we define*

- *The* $\mathcal{R}$-support of x, $\langle x_1, \ldots, x_n \rangle_{\mathcal{R}}$, *is the $\mathcal{R}$-submodule of $\mathcal{S}$ generated by the entries of x, namely,* $\mathrm{supp}_{\mathcal{R}} x \coloneqq \langle x_1, \ldots, x_n \rangle_{\mathcal{R}}$;
- *The* rank *of x, $rk_{\mathcal{R}}(x)$ or $rk(x)$ if $\mathcal{R}$ is clear from the context, is the rank of the $\mathcal{R}$-support of x.*

Given $x, y \in \mathcal{S}^n$, the *rank-distance* of the vectors $x, y \in \mathcal{S}^n$ is the rank of their difference, namely $\mathrm{d}_{\mathsf{rk}}(x, y) \coloneqq rk_{\mathcal{R}}(x - y)$. In particular the *rank-weight* of x is given by $\mathrm{d}_{\mathsf{rk}}(x, 0) = rk(x)$. In the following, we will use either $\mathrm{d}_{\mathsf{rk}}(x)$ or $rk(x)$ to refer to the rank-weight of x.

2.4 The Gilbert-Varshamov bound

In coding theory, the Gilbert-Varshamov (GV) bound is a fundamental result that provides a lower bound on the maximum size of a code, given its length and minimum

distance. In the Hamming metric over finite fields, it is well known that random linear codes asymptotically achieve the GV bound [24, 25]. The same holds for rank metric codes over finite fields [26, 27]. The GV bound for codes over rings was first explored in [28], and later, in [29] it was proved that random codes over rings with an additive weight also attain the GV bound.

Throughout this section, given $q = p^m$, let $\mathcal{R} = \mathrm{GR}(p^r, m)$ be the Galois ring with residue field $\mathbb{F}_q$ and nilpotency index r. Moreover, assume that the ambient space $\mathcal{R}^n$ is equipped with a translation-invariant distance d. Note that the (closed) ball of center x and radius ℓ in $\mathcal{R}^n$, namely $\{y \in \mathcal{R}^n \mid \mathrm{d}(x, y) \leq \ell\}$ has the same size for any center x. Thus, in the following, we will not specify the center of the ball and we will set

$$B_{\mathsf{d}}(\mathcal{R}, n, \ell) \coloneqq |\{y \in \mathcal{R}^n \mid \mathrm{d}(0, y) \leq \ell\}| \ ,$$

that is, given a translation invariant distance, $B_{\mathrm{d}}(\mathcal{R}, n, \ell)$ is the volume of the (closed) ball of radius ℓ in $\mathcal{R}^n$. Therefore the volumes of the the Hamming, Lee and rank metric balls in $\mathcal{R}^n$ are respectively denoted by $B_{\mathsf{H}}(\mathcal{R}, n, \ell)$, $B_{\mathsf{L}}(\mathcal{R}, n, \ell)$ and $B_{\mathsf{rk}}(\mathcal{R}, n, \ell)$. Finally, given a translation invariant distance d, we will denote by $A_{\mathrm{d}}(\mathcal{R}, n, d)$ the maximum number of codewords of a code in $\mathcal{R}^n$ with minimum distance d. That is, $A_{\mathsf{H}}(\mathcal{R}, n, d)$, $A_{\mathsf{L}}(\mathcal{R}, n, d)$ and $A_{\mathsf{rk}}(\mathcal{R}, n, d)$ represent the maximum number of codewords of a code in $\mathcal{R}^n$ with minimum distance d in the Hamming, Lee and rank metric respectively.

Theorem 2.11. (Gilbert-Varshamov bound for additive distances, [29]) *For a positive integer n, assume $\mathcal{R}^n$ is equipped with an additive distance* d. *The maximal size of a code in $\mathcal{R}^n$ having minimum distance d is*

$$A_{\mathsf{d}}(\mathcal{R}, n, d) \geq \frac{q^{rn}}{B_{\mathsf{d}}(\mathcal{R}, n, d-1)} \ . \tag{2}$$

An analogue of the Gilbert-Varshamov bound also holds for rank-metric codes.

Theorem 2.12 (Gilbert-Varshamov bound for rank distance, [26])**.** *Given a positive integer n, the maximal size of a code in $\mathcal{R}^n$ having minimum rank distance d is*

$$A_{\mathrm{rk}}(\mathcal{R}, n, d) \geq \frac{q^{rn}}{B_{\mathsf{rk}}(\mathcal{R}, n, d-1)} \ .$$

If $\mathcal{C}$ is a linear code in $\mathcal{R}^n$ equipped with a translation invariant distance d, we will say that $\mathcal{C}$ *lies on the GV bound* if

$$|\mathcal{C}| - 1 < \frac{q^{rn}}{B_{\mathrm{d}}(\mathcal{R}, n, d-1)} \leq |\mathcal{C}| \ .$$

In the following, we will specify the volume of the n-dimensional balls for each of the three metrics considered in this work: Hamming, Lee, and rank.

Proposition 2.13 (Volume of a Hamming-metric ball, [30]). *Given n, w positive integers, the volume of the n-dimensional Hamming ball of radius w in $\mathcal{R}^n$ is*

$$B_{\mathsf{H}}(\mathcal{R}, n, w) = \sum_{i=0}^{w} \binom{n}{i} (q-1)^i.$$

Proposition 2.14 (Volume of a Lee-metric ball, [30, 31]). *Let n, w be positive integers. The volume of a radius w Lee-ball in $\mathbb{Z}_{p^r}^n$, is $B_{\mathsf{L}}(\mathbb{Z}_{p^r}, n, w) = \sum_{i=0}^{w} 2^i \binom{n}{i}\binom{w}{i}$, for $p^r \geq 2w+1$. Otherwise, for $p^r < 2w+1$ the volume of the n-dimensional Lee ball is*

$$B_{\mathsf{L}}(\mathbb{Z}_{p^r}, n, w) = \sum_{i=0}^{w} 2^i \binom{n}{i} \sum_{\ell=0}^{i} (-1)^\ell \binom{i}{\ell} \binom{w-\ell M}{i} \quad \text{for } p^r = 2M+1,$$

$$B_{\mathsf{L}}(\mathbb{Z}_{p^r}, n, w) = \sum_{i=0}^{\lfloor \frac{w}{M} \rfloor} (-1)^i \binom{n}{i} B_{\mathsf{L}}(\mathbb{Z}_{p^r}, n, w - Mi) \quad \text{for } p^r = 2M.$$

To compute the volume of a rank-metric ball in $\mathcal{R}^n$, where $\mathcal{R}$ is a Galois ring with residue field of size q, we need to introduce some additional notations. We define the *set of compositions of K into r parts*, denoted by $C(r, K)$, as

$$C(r, K) \coloneqq \left\{ (k_0, \ldots, k_{r-1}) \mid 0 \leq k_i \leq K, \ \sum_{i=0}^{r-1} k_i = K \right\}.$$

Moreover, given a free $\mathcal{R}$-module $\mathcal{F}$ of rank n, we denote by $N_{n,\mathcal{R}}(k_0, \ldots, k_{r-1})$ the number of submodules of $\mathcal{F}$ with subtype $(k_0, \ldots, k_{r-1})$. As shown in [29], this amount is given by

$$N_{n,\mathcal{R}}(k_0, \ldots, k_{r-1}) \coloneqq q^{\sum_{i=0}^{r-1}(n - \sum_{j=0}^{i} k_j)\sum_{j=0}^{i-1} k_j} \prod_{i=0}^{r-1} \begin{bmatrix} n - \sum_{j=0}^{i-1} k_j \\ k_i \end{bmatrix}_q . \tag{3}$$

Finally, we denote by $W(\mathcal{R}, n, i)$ the number of $\mathcal{R}$-submodules of rank i of the free $\mathcal{R}$-module $\mathcal{F}$ of rank n , which is given by

$$W(\mathcal{R}, n, i) \coloneqq \sum_{(k_0, \ldots, k_{r-1}) \in C(r,i)} N_{n,\mathcal{R}}(k_0, \ldots, k_{s-1}) . \tag{4}$$

A proof of the following Proposition is provided in [32] for finite fields, and it can be generalized to Galois rings as well.

Proposition 2.15 (Volume of a Rank-metric ball). *Given n, m, w positive integers, the volume of a rank metric ball of radius w in $\mathrm{GR}(p^r, m)^n$ is equal to the number of $m \times n$ matrices of rank less or equal than w in $\mathbb{Z}_{p^r}$. In particular, for every*

$w \in \{0, \ldots, \min\{n, m\}\}$, $B_{\mathsf{rk}}(\mathrm{GR}(p^r, m), n, w)$ *is equal to*

$$\sum_{i=0}^{w} W(\mathbb{Z}_{p^r}, n, i) \left(\sum_{(k_0,\ldots,k_{r-1}) \in C(r,i)} \prod_{\ell=0}^{r-1} \left(\prod_{j=0}^{k_\ell - 1} (p^{m(r-\ell)} - p^{m(r-\ell)(j+\sum_{t=0}^{\ell-1} k_t)}) \right) \right),$$

where $W(\mathbb{Z}_{p^r}, n, i)$ represents the number of $\mathbb{Z}_{p^r}$-submodules of $\mathbb{Z}_{p^r}^n$ of rank i.

For completeness, we explicitly provide the volume of the rank-metric ball for finite fields.

Proposition 2.16 (Volume of a Rank-metric ball over finite fields, [26])**.** *The volume of a rank metric ball of radius w in $\mathbb{F}_{q^m}^n$ is equal to the number of $m \times n$ matrices of rank less or equal than w in $\mathbb{F}_q$. In particular, for every $w \in \{0, \ldots, \min\{n, m\}\}$,*

$$B_{\mathsf{rk}}(\mathbb{F}_{q^m}, n, w) = \sum_{i=0}^{w} \left(\prod_{j=0}^{i-1} \frac{(q^n - q^j)(q^m - q^j)}{q^i - q^j} \right).$$

In its asymptotic form, the GV bound offers a lower limit on the rate of the code, rather than its cardinality.

Let $\mathcal{R} = \mathrm{GR}(p^r, m)$ be a Galois ring with $|\mathcal{R}| = q^r$ and d be a distance on $\mathcal{R}^n$, which can be either an additive distance or the rank distance. In what follows, we denote by N the maximum weight of an element in $\mathcal{R}^n$. Note that, if d is an additive distance in $\mathcal{R}^n$ and M is the maximum weight of an element in $\mathcal{R}$, then $N = nM$. On the other hand, if is the rank metric, then $N = \min\{n, m\}$. Moreover, let δ be the relative distance of the code, that is $d = \delta N$. We have that

$$\lim_{n\to\infty} \frac{1}{n} \log_{q^r}(A_{\mathrm{d}}(\mathcal{R}, n, d)) \geq 1 - \lim_{n\to\infty} \frac{1}{n} \log_{q^r}(B_{\mathrm{d}}(, \mathcal{R}, n, d)). \tag{5}$$

It has been proven that the limit in the right-hand side of the previous equation exists for an arbitrary additive distance and varies depending on the metric used. For instance, if d is the Hamming metric the limit in the right hand side of (5) is in particular the q^r-ary entropy function $h_{q^r}(\delta)$. For the Lee distance, the values of this limit, along with additional details, can be found in [14, 33]. Finally, the asymptotic behaviour of rank metric over finite fields is studied in [26, 27].

It is well known that random codes equipped with an additive metric lie on the GV bound with high probability [29], as do rank metric codes over finite fields [26, 27]. However, to the best of our knowledge, it remains unknown whether a random ring-linear code with rank metric achieves the GV bound.

3 Hard problems in Coding Theory

In this work, we will focus on two computationally-hard problems in coding theory, which are at the basis of many code-based cryptosystems: the Codeword Finding Problem (CFP) and the Syndrome Decoding Problem (SDP). These problems are known

to be NP-complete for codes over fields equipped with the Hamming metric [34, 35], and this result extends to codes over rings equipped with an additive metric as well [14]. Finally, the computational complexity of syndrome decoding and codeword finding in the rank metric was studied in [36]. In the following, we will present the decisional variant of these two problems for ring-linear codes equipped with a translation-invariant metric. Throughout this section, assume that $\mathcal{R} = \mathrm{GR}(p^r, m)$ and d is a translation invariant distance in $\mathcal{R}^n$.

Problem 3.1 (d-**Syndrome Decoding Problem over** $\mathcal{R}$ – $\mathsf{SDP}_{\mathrm{d}}(\mathcal{R}, H, s, w)$)**.** *Given $H \in \mathcal{R}^{(n-k)\times n}$, $s \in \mathcal{R}^{n-k}$ and $w \in \mathbb{N}$, decide if there exists a vector $e \in \mathcal{R}^n$ such that $\mathrm{wt}_{\mathrm{d}}(e) \leq w$ and $He^\top = s$.*

Problem 3.2 (d-**Codeword Finding Problem over** $\mathcal{R}$ – $\mathsf{CFP}_{\mathrm{d}}(\mathcal{R}, H, w)$)**.** *Given $H \in \mathcal{R}^{(n-k)\times n}$ and $w \in \mathbb{N}$, decide if there exists a vector $c \in \mathcal{R}^n$ such that $\mathrm{wt}_{\mathrm{d}}(c) \leq w$ and $Hc^\top = 0$.*

In the following, we will refer to generic problems with $\mathsf{SDP}_{\mathrm{d}}$ over $\mathcal{R}$ and $\mathsf{CFP}_{\mathrm{d}}$ over $\mathcal{R}$, or, for short, simply with SDP and CFP. For the aims of this work, we will assume that a solution of fixed weight w always exists for the system $Hx^\top = s^\top$. For this reason, in the remainder of the paper, we will deal with the search variant of the problems, where it is asked to find a vector solving the given instance. For random codes in $\mathcal{R}^n$, we can easily estimate the expected number of solutions to these problems, as follows.

Proposition 3.3. *Let $\mathcal{C} \subseteq \mathcal{R}^n$ be a linear code of subtype $(k_0, \ldots, k_{r-1})$ and rate R. If $H \in \mathcal{R}^{(n-k_0)\times n}$ is a parity-check for $\mathcal{C}$, $s \in \mathcal{R}^{n-k_0}$, and $w \in \mathbb{N}$, consider the syndrome decoding problem $\mathsf{SDP}_{\mathsf{d}}(\mathcal{R}, H, s, w)$. Denote with S the set made up of all the solutions to this instance, that is, $S \coloneqq \{x \in \mathcal{R} \ : \ xH^\top = s, \mathrm{wt}_{\mathsf{d}}(x) \leq w\}$. Then, on average*

$$|S| = \frac{B_{\mathsf{d}}(\mathcal{R}, n, w)}{(q^r)^{n-k}}.$$

Proof. The number of expected solutions is given by

$$\begin{aligned}
\mathbb{E}(|S|) &= \mathbb{E}(|\{x \in \mathcal{R}^n \ : \ xH^\top = s, \ \mathrm{wt}_{\mathsf{d}}(x) \leq w\}|) \\
&= \sum_{i=0}^{w} \mathbb{E}(|\{x \in \mathcal{R}^n \ : \ xH^\top = s, \ \mathrm{wt}_{\mathsf{d}}(x)\}|) \\
&= B_{\mathsf{d}}(\mathcal{R}, n, w)/(q^r)^{n-k}.
\end{aligned}$$

□

Note that, if $r = 1$, one get the expected number of solutions to the syndrome decoding problem for random codes over finite fields. This result allows us to estimate a value for which we expect the syndrome decoding problem to have only one solution.

Definition 3.4 (Uniqueness bound)**.** *Given $\mathcal{C} \subseteq \mathcal{R}^n$ with rate R, the SDP Uniqueness Bound corresponds to*

$$w^* := \max_{w \in \mathbb{N}} \left\{ \frac{B_{\mathsf{d}}(\mathcal{R}, n, w)}{(q^r)^{n-k}} \leq 1 \right\}.$$

Notice that $w^* = \delta N$, where δ is the relative distance of the code. Sometimes, this expression is referred to (with abuse of notation) GV bound; however, this is not

exactly correct: even if these two quantities coincide, they are semantically different as the GV bound regards the existence of codes with some guaranteed minimum distance.

3.1 ISD algorithms for additive metrics

To the best of our knowledge, papers that directly address ISD for ring-linear codes [12, 14, 19, 20] all focus on ISD with the Lee metric. Although these works only consider the Lee metric, adapting their algorithms to the Hamming metric is quite straightforward. The syndrome decoding problem has also been studied in its equivalent LPN formulation for lattices over $\mathbb{Z}_{2^\lambda}$ with the Hamming metric in [13], which we will see in more detail in Section 4.

In the following, we generalize the two-blocks algorithm presented in [14], allowing the code to be equipped with any additive weight, and we analyze the resulting algorithms. To help account for the asymptotic computational complexity, we focus on Lee-Brickell and Prange's ISD variants. Given an instance of SDP or CFP as input, the Lee-Brickell algorithm aims to find an information set of the code that contains v errors, and $w - v$ errors outside the information set. Prange is a special case of Lee-Brickell when v is set to 0. Below we describe these algorithms for codes over Galois rings equipped with any additive metric, taking in mind that the Lee and Hamming metrics are special cases of this more general setting.

Given a Galois ring $\mathcal{R} = \mathrm{GR}(p^r, m)$, an additive distance d over $\mathcal{R}$, let M be the maximum weight that an element of $\mathcal{R}$ can assume. Moreover, for a vector $x \in \mathcal{R}^n$, we will denote by $\mathrm{wt}_\mathsf{d}(x)$ the weight of x with respect to the distance d. Finally, throughout this section, let $q \coloneqq |\mathcal{R}| = p^{mr}$. Let $\mathcal{C} \subseteq \mathcal{R}^n$ be a linear code of rank K and subtype $(k_0, k_1, \ldots, k_{r-1})$ and with parity check matrix H. Assume I is an information set for $\mathcal{C}$ and, for convenience, say it consists of the first K columns, that is, $I = \{1, \ldots, K\}$. Set $J \coloneqq I^C = \{K + 1, \ldots, n\}$. The algorithm involves bringing $H \in \mathcal{R}^{(n-k_0)\times n}$ into systematic form by multiplying by an invertible matrix $U \in \mathcal{R}^{(n-k_0)\times(n-k_0)}$, so that

$$(UH)e^\top = \begin{pmatrix} A & 1 \\ pB & 0 \end{pmatrix} e^\top = Us^\top.$$

The algorithm is based on the hope that the solution vector e has weight v in the information set, and $w - v$ in the remaining columns. We can therefore rewrite the error vector as $e = (e_I, e_J)$, and the previous equation as

$$(UH)e^\top = \begin{pmatrix} A & 1 \\ pB & 0 \end{pmatrix} \begin{pmatrix} e_I^\top \\ e_J^\top \end{pmatrix} = \begin{pmatrix} s_1^\top \\ ps_2^\top \end{pmatrix},$$

from which we obtain the following equations:

$$\begin{cases} Ae_I^\top + e_J^\top = s_1^\top \\ pBe_I^\top = ps_2^\top \end{cases}.$$

We then compute the set P given by all vectors of weight v satisfying $pBe_I^\top = ps_2^\top$. For each $e_I \in P$ we therefore define $e_J \coloneqq s_1 - Ae_I^\top$. If $\mathrm{wt}_{\mathtt{d}}(e_J) = w - v$ then we have successfully reconstructed the error vector, otherwise we start again from scratch by selecting a new information set. The algorithm is schematically described in Algorithm 1. Here $\mathcal{T}$ denotes the Galois ring $\mathrm{GR}(p^{r-1}, m)$

Algorithm 1: Lee-Brickell for ring-linear codes with additive distance

Input: $H \in \mathcal{R}^{(n-k_0)\times n}$, $s \in \mathcal{R}^{n-k_0}$ $w \in \mathbb{N}, v \leq \min\{M \cdot K, w\}$
Output: Vector $e \in \mathcal{R}^n$ such that $\mathrm{wt}_{\mathtt{d}}(e) \leq w$ and $He^\top = s^\top$

1 Choose an information set $I \subseteq [n]$ of size K and define $J \coloneqq [n] \setminus J$;
2 Compute a square matrix $U \in \mathcal{R}^{(n-k_0)\times(n-k_0)}$ such that:

$$(UH)_I = \begin{pmatrix} A \\ pB \end{pmatrix} \quad (UH)_J = \begin{pmatrix} 1_{n-K} \\ 0_{(K-k_0)\times(n-K)} \end{pmatrix} \quad Us^\top = \begin{pmatrix} s_1^\top \\ ps_2^\top \end{pmatrix},$$

where $A \in \mathcal{R}^{(n-K)\times K}, B \in \mathcal{R}^{(K-k_0)\times K}, s_1 \in \mathcal{R}^{(n-K)}, s_2 \in \mathcal{T}^{(K-k_0)}$;
3 Compute the set $P \coloneqq \left\{e_1 \in \mathcal{R}^K \ : \ \mathrm{wt}_{\mathtt{d}}(e_1) = v,\ pBe_1^\top = ps_2\right\}$;
4 **for** $e_1 \in P$ **do**
5 **if** $\mathrm{wt}_{\mathtt{d}}(s_1 - Ae_1^\top) \leq w - v$ **then**
6 **return** e such that $e_I = e_1$, $e_J = s_1 - Ae_1^\top$;
7 Start over with Step 1 and a new selection of I.

In the following we derive the time complexity of Algorithm 1. We stress that this algorithm is a special case of the one shown in [10], and that the complexity we obtain is simply a particularization of the formulas already present in it. Let us recall the parameters that characterize the code, assuming they are functions of n: $k(n) = \log_q(|\mathcal{C}|)$ is the $\mathcal{R}$-dimension of $\mathcal{C}$, $k_0(n)$ is the free rank, $K(n) = \sum_i k_i$ is the rank. Since we are interested in estimating the asymptotic computational complexity, we will work with the following quantities:

$$R \coloneqq \lim_{n\to\infty} \frac{k(n)}{n}, \quad R_0 \coloneqq \lim_{n\to\infty} \frac{k_0(n)}{n}, \quad R_I \coloneqq \lim_{n\to\infty} \frac{K(n)}{n}.$$

Finally, regarding the algorithm parameters, $w(n)$ represents the solution weight, while $v(n)$ is the algorithm's internal parameter. We will also use the following notation:

$$W \coloneqq \lim_{n\to\infty} \frac{w(n)}{n}, \quad V \coloneqq \lim_{n\to\infty} \frac{v(n)}{n}.$$

Recall that, given any additive distance d over $\mathcal{R}$, the surface of an n-dimensional sphere of radius v is given by:

$$F_{\mathrm{d}}(\mathcal{R}, n, v) \coloneqq |\{x \in \mathcal{R}^n \mid \mathrm{wt}_{\mathtt{d}}(x) = v\}|.$$

To lighten the asymptotic notation we further denote the asymptotic volume of this ball as

$$S_{\mathrm{d}}(\mathcal{R}, R, V) \coloneqq \lim_{n\to\infty} \frac{1}{n} \log(F_{\mathrm{d}}(\mathcal{R}, k, v)) = R \lim_{k\to\infty} \frac{1}{k} \log(F_{\mathrm{d}}(\mathcal{R}, k, v)).$$

Proposition 3.5 (Complexity of Lee-Brickell)**.** *The asymptotic average complexity of Algorithm 1 applied to an $\mathcal{R}$-linear code equipped with an additive distance* d *is*

$$S_{\mathrm{d}}(\mathcal{R}, 1, W) - S_{\mathrm{d}}(\mathcal{R}, 1 - R_I, W - V).$$

Proof. We can obtain the asymptotic complexity by computing the time required to construct the set P and the time required to reconstruct the vector e in the last phase of the algorithm. The construction of P requires constructing a sphere of radius v in $\mathcal{R}^K$. The number of elements we need to test is therefore given by

$$F_{\mathrm{d}}(\mathcal{R}, K, v) \xrightarrow{n\to\infty} S_{\mathrm{d}}(\mathcal{R}, R_I, V)$$

For Lee-Brickell, the number of iterations needed for the last part of the algorithm is given by $F_{\mathrm{d}}(\mathcal{R}, n, w)\big(F_{\mathrm{d}}(\mathcal{R}, K, v) \cdot F_{\mathrm{d}}(\mathcal{R}, n-K, w-v)\big)^{-1}$, which grows asymptotically as

$$S_{\mathrm{d}}(\mathcal{R}, 1, W) - S_{\mathrm{d}}(\mathcal{R}, R_I, V) - S_{\mathrm{d}}(\mathcal{R}, 1 - R_I, W - V).$$

Putting everything together, the thesis follows.

□

In the following we also present Prange's algorithm for the case of ring-linear codes equipped with an additive metric. We stress that Prange is a specific instance of the Lee-Brickell algorithm described above, obtained by setting the internal parameter v in the algorithm to zero.

Algorithm 2: Prange's ISD for ring-linear codes with additive metric

Input: $H \in \mathcal{R}^{(n-k_0)\times n}$, $s \in \mathcal{R}^{n-k_0}$ $w \in \mathbb{N}$
Output: Vector $e \in \mathcal{R}^n$ such that $\mathrm{wt}_{\mathtt{d}}(e) \leq w$ and $He^\top = s^\top$

1 Choose an information set $I \subseteq [n]$ of size K and define $J \coloneqq [n] \setminus J$;
2 Compute a square matrix $U \in \mathcal{R}^{(n-k_0)\times(n-k_0)}$ such that:

$$(UH)_I = \begin{pmatrix} A \\ pB \end{pmatrix} \quad (UH)_J = \begin{pmatrix} 1_{n-K} \\ 0_{(K-k_0)\times(n-K)} \end{pmatrix} \quad Us^\top = \begin{pmatrix} s_1^\top \\ 0_{(K-k_0)\times 1} \end{pmatrix},$$

where $A \in \mathcal{R}^{(n-K)\times K}, B \in \mathcal{R}^{(K-k_0)\times K}, s_1 \in \mathcal{R}^{(n-K)}$;
3 **if** $\mathrm{wt}_{\mathtt{d}}(s_1) \leq w$ **then**
4 **return** e such that $e_I = (0, \ldots, 0)$, $e_J = s_1$;
5 Start over with Step 1 and a new selection of I.

As a consequence of Proposition 3.5, we obtain the following asymptotic time complexity for Prange's algorithm.

Proposition 3.6. (Complexity of Prange [14, Theorem 4.1]) *The asymptotic average complexity of Algorithm 2 applied to an $\mathcal{R}$-linear code equipped with an additive distance* d *is*

$$S_{\mathrm{d}}(\mathcal{R}, 1, W) - S_{\mathrm{d}}(\mathcal{R}, 1 - R_I, W).$$

3.2 Algorithms in the rank metric

In the following, we will focus on the rank metric case. Unlike the previous cases, this metric is not additive and therefore requires a different approach.
Information set decoding algorithms heavily exploit the additivity of the metric, therefore they cannot be directly transposed in a context where the code is equipped with the rank metric. In the case of rank-metric codes over finite fields, it is still possible to find a sort of generalization, in which the algorithm searches for a set of positions that contain error support. This generalization was introduced in [37] and then improved in [7, 38, 39]. In particular, [7] proposes an algorithm that, generalizing classical ISD algorithms, aims to find the support of an error vector. While for codes equipped with an additive metric, finding the error support coincides with finding the indices for which the entries of the error vector are non-zero, in the rank-metric case, it translates into finding the submodule generated by the coordinates of the vector. In this sense, a solving algorithm tries to guess the subspace defined by the error support and subsequently solves a system of linear equations to find the coordinates of that error.

In a recent paper, two new algorithms were introduced to extend the standard ones to codes over finite principal ideal rings [8]. As solving the Syndrome Decoding Problem over finite principal ideal rings reduces to solve the same problem over finite chain rings [8, Proposition 2.9], our focus will be exclusively on finite chain rings, and especially on Galois rings. The substantial difference between the two new proposals

lies in the use cases, i.e. when n is greater or less than m. For this work, we consider only the first case and report below the results necessary to understand the algorithm.

Throughout this section, given positive integers n, m and $q = p^m$, assume that $n \geq m$ and $\mathcal{S} = \mathrm{GR}(p^r, m)$ is the Galois ring with residue field $\mathbb{F}_q$ and nilpotency index r. Note that $\mathcal{S}$ is a Galois extension of $\mathcal{R} \coloneqq \mathbb{Z}_{p^r}$ and, in particular, it is a free $\mathcal{R}$-module of rank m. The following result is taken from [8].

Proposition 3.7. *Let $\mathcal{C} \subseteq \mathcal{S}^n$ be a linear code of subtype $(k_0, \ldots, k_{r-1})$ and let H be a parity-check for $\mathcal{C}$. Given $s \in \mathcal{S}^{n-k_0}$, we want to solve the rank-syndrome decoding problem $\mathsf{SDP}_{\mathsf{rk}}(\mathcal{S}, H, s, w)$*

$$He^\top = s^\top, \tag{6}$$

where $e = (e_1, \ldots, e_n) \in \mathcal{S}^n$ and $rk(e) = w$. Let $\mathcal{F}$ be a free $\mathcal{R}$-submodule of $\mathcal{S}$ of rank u. Assume that $\mathrm{supp}_{\mathcal{R}}(e) \subseteq \mathcal{F}$. Let $\{f_1, \ldots, f_u\}$ be a basis of $\mathcal{F}$ and $x_{i,j} \in \mathcal{R}$ such that, for all $j \in \{1, \ldots, n\}$,

$$e_j = \sum_{i=1}^{u} x_{i,j} f_i. \tag{7}$$

Then, Equation (6) with unknown e can be transformed into a system of linear equations over $\mathcal{R}$ (that we denote with $\mathcal{E}_1$) with $m(n-k_0)$ equations and $n \times u$ unknowns $x_{i,j}$.

Proposition 3.7 allows to describe a decoding algorithm that generalizes ISD also for codes in the rank metric. We report this algorithm below. In line with [8, 40], we will set $u = \lfloor (n-k_0)m/n \rfloor$.

Algorithm 3: Error support attack

Input: $H \in \mathcal{S}^{(n-k_0)\times n}$, $w \in \mathbb{N}$, $s \in \mathcal{S}^{n-k_0}$.
Output: Vector $e \in \mathcal{S}^n$ such that $rk(e) \leq w$ and $He^\top = s^\top$

```
Choose a free R-submodule F of S of rank u
  Choose a basis {f_1, ..., f_u} of F
  Solve Equation (E_1) of Prop. 3.7
  if E_1 admits a solution then
2   Use a solution of E_1 to compute e as in Eq. 7
      if rk(e) ≤ w then
3       return e
4 Start over with Step 1 and a new selection of F.
```

Below we also report the analysis of the asymptotic complexity of Algorithm 3. Accordingly to Equations (3) and (4), the number of submodule of rank i of a free $\mathcal{R}$-module of rank n is given by $W(\mathcal{R}, n, i)$, which is equal to

$$\sum_{(k_0,\ldots,k_{r-1})\in C(r,i)} q^{\sum_{i=0}^{r-1}(n-\sum_{j=0}^{i}k_j)\sum_{j=0}^{i-1}k_j} \prod_{i=0}^{r-1} \begin{bmatrix} n-\sum_{j=0}^{i-1}k_j \\ k_i \end{bmatrix}_q, \tag{8}$$

where q is the size of the residue field of $\mathcal{R}$ and r is its nilpotency index.

Proposition 3.8. (Complexity of error support attack, [8, Theorem 5.4]) *On average, the complexity of Algorithm 3 is given by*

$$O\left(m(n-k)n^2u^2 \cdot \frac{W(\mathcal{R},m,w)}{W(\mathcal{R},u,w)}\right),$$

where $W(\mathcal{R},u,w)$ and $W(\mathcal{R},m,w)$ are defined as in Eq. (8), and

$$\frac{W(\mathcal{R},m,w)}{W(\mathcal{R},u,w)} \approx |\mathcal{R}|^{r\lfloor \frac{mk_0}{n} \rfloor} .$$

3.3 Solving SDP using subcodes

In this section, we will introduce the fundamental tools for designing new algorithms for both CFP and SDP, in all the metrics presented previously. The main idea is to work with subcodes rather than the entire code. This technique results in smaller instances than the original problem, which can affect the algorithm's efficiency. In fact, given a ring-linear code $\mathcal{C} \subseteq R^n$ of rank K, it is natural to consider a chain of subcodes, all of which have rank K, namely the filtration subcodes.

Through this section, let $\mathcal{R} = \mathrm{GR}(p^r, m)$ be the Galois ring with residue field $\mathbb{F}_q$ and nilpotency index r. Recall that $\mathcal{R}$ is local and its unique maximal ideal is $\langle p \rangle = p\mathrm{GR}(p^r, m)$.

Definition 3.9. *Given an $\mathcal{R}$-linear code $\mathcal{C}$, for each $0 \leq i \leq r-1$ we define the i-th* filtration subcode *$\mathcal{C}_i$ of $\mathcal{C}$ as*

$$\mathcal{C}_i \coloneqq \mathcal{C} \cap \langle p^i \rangle .$$

The filtration subcodes form a chain, namely

$$\mathcal{C}_{r-1} \subseteq \mathcal{C}_{r-2} \subseteq \cdots \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_0 = \mathcal{C} .$$

The $r-1$ filtration subcode is referred to as the *socle* of the code.

Lemma 3.10. ([16, Lemma 2.9]) *For any $0 \leq i \leq r-1$ there exists an isomorphism of $(\mathcal{R}/p^{r-i}\mathcal{R})$-modules $\varphi^{(i)} \colon p^i\mathcal{R}^n \to (\mathcal{R}/p^{r-i}\mathcal{R})^n$. In particular $p^{r-1}\mathcal{R}^n$ and $\mathbb{F}_q^n$ are isomorphic as $\mathbb{F}_q$-vector spaces.*

In the following, we will write $\mathcal{T}_{r-i}$ to denote the ring $\mathcal{R}/p^{r-i}\mathcal{R} = \mathrm{GR}(p^{r-i}, m)$.

Remark 3.1. Consider an $\mathcal{R}$-linear code $\mathcal{C} \subseteq \mathcal{R}^n$ and let $\mathcal{C}_i$ be the i-th filtration subcode. From the Lemma 3.10 follows that $\mathcal{C}_i$ can be identified with a code over $\mathcal{T}_{r-i}$,which will be denoted with $\overline{\mathcal{C}}_i$.

In order to make the syndrome decoding problem more feasible, the idea is to reduce the weight of the solution, which can be done by multiplying by appropriate scalars. Suitable choices of scalars, not only lead to a reduction in the weight of the solution but also allow us to transform the instance into a new instance over a smaller alphabet.

In the following, we formally define this framework.

Definition 3.11. *Given a positive integer n, we define the i-*th *projection onto $\mathcal{T}_{r-1}$ as*

$$\pi^{(i)} \colon \mathcal{R}^n \longrightarrow \mathcal{T}_{r-i}^n, \quad z \mapsto \overline{z}^{(i)} \coloneqq \pi^{(i)}(z) \ ,$$

where $\overline{z}^{(i)}$ is the unique element in $\mathcal{T}_{r-i}$ such that $p^i z = p^i \overline{z}^{(i)}$.

Later on with the discussion, to keep the notations simple, we will write $\overline{x}^{(i)}$ to denote $\pi^{(i)}(x)$. Moreover we will set $\overline{x} \coloneqq \overline{x}^{(r-1)}$ and $\overline{\mathcal{C}} = \overline{\mathcal{C}}_{r-1}$.

If d is an additive metric or the rank metric, consider a linear code $\mathcal{C} \subseteq \mathcal{R}^n$ of subtype $(k_0, \dots, k_{r-1})$ with parity check matrix H. Following the uniqueness bond 3.4, assume e is the unique solution to $\mathsf{SDP}_{\mathrm{d}}(\mathcal{R}, H, s, w)$. Then $\overline{e}^{(i)}$, the projection of e onto $\mathcal{T}_{r-i}$, satisfies $p^i H \overline{e}^{(i)^\top} = p^i s^\top$. Notice that $p^i H$ is the parity-check of the i-th filtration subcode identified through $\varphi^{(i)}$ with a code over $\mathcal{T}_{r-i}$. In what follows, we will denote the parity-check of $\overline{\mathcal{C}}_i$ with $\overline{H}^{(i)}$. Moreover $p^i s$ can be also seen as a vector with coordinates in $\mathcal{T}_{r-i}$. Hence, we find that $\overline{e}^{(i)}$ is a solution of the Syndrome Decoding Problem $\mathsf{SDP}_{\mathrm{d}}(\overline{H}^{(i)}, \overline{s}^{(i)}, w)$ with input $\overline{\mathcal{C}}_i$. In the following, we will refer to the latter problem as the projected problem or to the instance over the smaller alphabet as the projected instance. In the following sections, we will see that, for specific choices of the metric, such as Hamming or rank, $\overline{e}^{(i)}$ is the unique solution to the Syndrome Decoding Problem with input $\overline{\mathcal{C}}_i$. In the case of the Lee metric, this is not always true and may require additional assumptions. In particular, if the uniqueness is preserved, we can exploit the information obtained from solving the projected instance to speed up the decoding of the original problem.

4 Hamming Case

In this section, we study the practical hardness of solving the codeword finding problem and the syndrome decoding problem for linear codes equipped with the Hamming metric. In particular, we will study how the Hamming weight of a vector decreases when projected onto a smaller ring. We then introduce a new algorithm that speeds up decoding for codes over rings. The underlying idea is similar to that presented in [13], but we describe it in terms of linear codes rather than lattices.

Throughout this section, given $q = p^m$, let $\mathcal{R} = \mathrm{GR}(p^r, m)$ be the Galois ring with residue field $\mathbb{F}_q$ and nilpotency index r.

As a consequence of Proposition 3.5, we can determine the complexity of Algorithm 1 in the Hamming metric case.

Corollary 4.1 (Complexity of Lee-Brickell with the Hamming metric)**.** *The asymptotic average complexity of Algorithm 1 applied to an $\mathcal{R}$-linear code equipped with the Hamming metric is given by:*

$$\lim_{n\to\infty} \frac{1}{n} \log \left(\frac{q^{r h_{q^r}(\frac{w}{n})n}}{q^{r h_{q^r}(\frac{v}{K})K} q^{r h_{q^r}(\frac{w-v}{n-K})(n-K)}} \right). \tag{9}$$

Proof. In the Hamming metric, the asymptotic volume of an n-dimensional ball of radius t over $\mathcal{R}$ can be estimated as $B_{\mathsf{H}}(\mathcal{R}, n, t) \approx q^{rh_{q^r}(\frac{t}{n})n}$, from which

$$B_{\mathsf{H}}(\mathcal{R}, n, t) \approx q^{rh_{q^r}(\frac{t}{n})n} - q^{rh_1(\frac{t-1}{n})n} \approx q^{rh_{q^r}(\frac{t}{n})n}.$$

Therefore, when considering the Hamming metric, Algorithm 1 requires approximately $F_{\mathsf{H}}(\mathcal{R}, K, v) \approx q^{rh_{q^r}(\frac{v}{K})K}$ operations to construct set P. Similarly, the number of iterations needed to execute the last part of the algorithm is given by

$$\frac{F_{\mathsf{H}}(\mathcal{R}, n, w)}{(F_{\mathsf{H}}(\mathcal{R}, K, v) \cdot F_{\mathsf{H}}(\mathcal{R}, n-K, t-v))} \approx \frac{q^{rh_{q^r}(\frac{w}{n})n}}{q^{rh_{q^r}(\frac{v}{K})K} q^{rh_{q^r}(\frac{w-v}{n-K})(n-K)}}.$$

Asymptotically, the complexity is therefore given by

$$\lim_{n\to\infty} \frac{1}{n} \log \left(\frac{q^{rh_{q^r}(\frac{w}{n})n}}{q^{rh_{q^r}(\frac{v}{K})K} q^{rh_{q^r}(\frac{w-v}{n-K})(n-K)}} \right).$$

□

The following holds as a consequence of the previous result.

Corollary 4.2 (Complexity of Prange with the Hamming metric)**.** *The asymptotic average complexity of Algorithm 2 applied to an $\mathcal{R}$-linear code equipped with the Hamming metric is given by:*

$$\lim_{n\to\infty} \frac{1}{n} \log \left(\frac{q^{h_q(\frac{w}{n})n}}{q^{h_q(\frac{w}{n-K})(n-K)}} \right). \tag{10}$$

4.1 Weights and projections

Assume the ambient space is endowed with the Hamming metric, and x is a vector in $\mathcal{R}^n$. When we project x onto $\mathcal{T}_{r-i}^n$, $0 \leq i \leq r-1$, it is clear that the Hamming weight of the projected vector decreases. In the following, we will provide an estimate of how the Hamming weight of a vector is reduced when projected onto $\mathcal{T}_{r-i}$.

Proposition 4.3. *Given a random vector $e \in \mathcal{R}^n$ of Hamming weight w, let $\overline{e}^{(i)}$ be the projection of e onto $\mathcal{T}_{r-i}$. The Hamming weight of $\overline{e}^{(i)}$ is, on average, reduced to*

$$\overline{w}^{(i)} \coloneqq w\left(1 - \frac{q^i - 1}{q^r - 1}\right).$$

Proof. In order to find the average weight $\overline{w}^{(i)}$ of $\overline{e}^{(i)} \in \mathcal{T}_{r-i}$, we need to find $\mathbb{E}\left[\mathrm{wt}_{\mathsf{H}}(\overline{e}^{(i)})|\ \mathrm{wt}_{\mathsf{H}}(e) = w\right]$. Since the coordinates of e are i.i.d. random variables, it its sufficient to compute $\sum_{j=1}^{n} \mathbb{E}\left[\mathrm{wt}_{\mathsf{H}}\left(\overline{e}_j^{(i)}\right)|\ \mathrm{wt}_{\mathsf{H}}(e) = w\right]$. When we project onto $\mathcal{T}_{r-i}$,

the q^i elements lying in $p^{r-i}\mathcal{R}$ are mapped to zero. Therefore, we obtain

$$\overline{w}^{(i)} = n \cdot \frac{w}{n} \cdot \left(\frac{q^r - 1 - (q^i - 1)}{q^r - 1} \right) ,$$

and hence, the claim follows. □

Corollary 4.4. *Given a random vector $e \in \mathcal{R}^n$ of Hamming weight w, let $\overline{e}$ be the projection of e onto its base field $\mathcal{R}/p\mathcal{R}$. The Hamming weight of $\overline{e}$ is, on average, reduced to*

$$\overline{w} \coloneqq w \left(1 - \frac{q^{r-1} - 1}{q^r - 1} \right) .$$

Here is an example illustrating how the weight of a random vector over an integer residue ring decreases when projected onto its base field.

Example 4.1. Given $n = 70$ and $w \in \mathbb{N}$, consider a vector $e \in \mathbb{Z}_{5^3}^n$ of Hamming weight w. We have just shown that the Hamming weight of e projected onto the base field decreases linearly in the weight of the initial vector. Figure 1 provides a graphical representation of this fact.

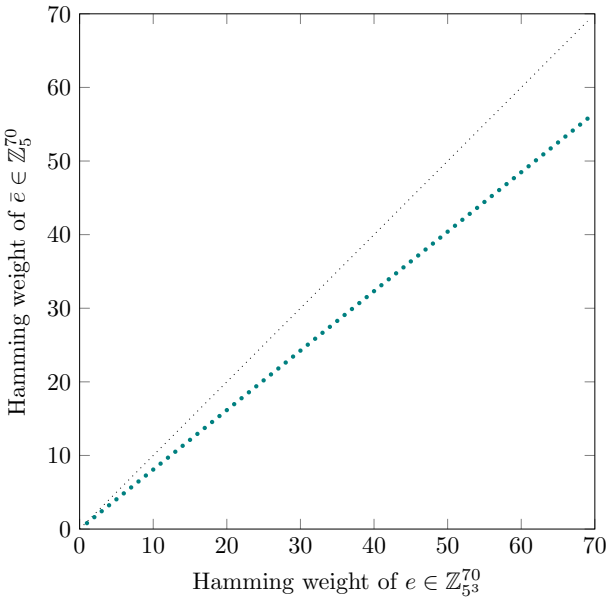

Fig. 1: On the x-axis we put the Hamming weights that a vector can assume, while on the y-axis we draw (in teal) the expected weight that the same vector will have once projected on the base field.

4.2 Solving CFP

In this following, we will show that algorithms for solving the codeword finding problem over rings are more efficient than algorithms over fields of the same size.
For both problems, we are interested in instances for which the solution is unique, and consequently we will just consider weights obtained from the uniqueness bound, or equivalently from the GV bound.

Let $\mathbb{F}_{p^m}$ be the Galois field with p^m elements and let $\mathcal{C}$ be a linear code in $\mathbb{F}_{p^m}^n$ equipped with the Hamming metric. We estimate the minimum distance of $\mathcal{C}$ using the GV bound over finite fields, that is, we will set $w = \delta N = \delta n$, where δ is the relative distance of the code. Given a random instance $\mathsf{CFP}_{\mathsf{H}}(\mathbb{F}_{p^m}, H, w)$, Proposition 4.1 provides an estimates of the asymptotic complexity of Lee-Brickell's algorithm in this context.

We now turn to the codeword finding problem over finite rings. Given $\mathcal{R} = \mathrm{GR}(p^r, m)$ with residue field $\mathbb{F}_{p^m}$, let $\mathcal{C}$ be an $\mathcal{R}$-linear code equipped with the Hamming metric.
Remark 4.1. Given $x \in \mathcal{R}^n$, for any $1 \leq i \leq r-1$, it holds that $\mathrm{wt}_{\mathsf{H}}(p^i x) \leq \mathrm{wt}_{\mathsf{H}}(x)$. As a result, we can always find minimum Hamming-weight codewords in the socle.

Accordingly to Remark 3.1, as the socle can be identified with a linear code over $\mathbb{F}_{p^m}$, one can simply look for the minimum weight codeword in the code $\overline{\mathcal{C}}$, taking values in $\mathbb{F}_{p^m}$. In other words, we have that the complexity to solve $\mathsf{CFP}_{\mathsf{H}}$ over $\mathcal{R}$ is the same as solving $\mathsf{CFP}_{\mathsf{H}}$ over $\mathbb{F}_{p^m}$. In particular, increasing r does not lead to modifications for the time complexity of Lee-Brickell over the rings, since it only depends on the size of its residue field. As before, Proposition 4.1 returns the complexity of this algorithm.

4.3 Solving SDP

In this section, we study the practical hardness of the syndrome decoding problem, focusing on instances with a unique solution. In this regime, for both codes over fields and rings, we will compute the complexity of algorithms that solve this problem. As shown in Proposition 4.1, Algorithm 1 applied to codes over rings or fields results in the same level of complexity. However, in the ring case, we can leverage the optimizations detailed in the previous section, thereby significantly improving upon the "naive" approach. This results in a more refined and efficient solution, enhancing performance and reducing computational overhead compared to a straightforward, unoptimized approach.

To the best of our knowledge, the approach we propose is not known to the coding community. However, an analogue formulation for lattices defined as $\mathbb{Z}_{2^\lambda}$ has been recently proposed in [13]. In this sense, in this specific metric, our work is not new and merely offers a different vocabulary to describe the same technique. We describe this approach in the following.

From now on, let $\mathcal{R} = \mathrm{GR}(p^r, m)$ and $\mathcal{T}_{r-i} = \mathcal{R}/p^i\mathcal{R}$. In line with Definition 3.11, let $\pi^{(i)}$ be the i-th projection over $\mathcal{T}_{r-i}$. Given a linear code $\mathcal{C} \subseteq \mathcal{R}^n$, let $\overline{\mathcal{C}}_i$ the i-th filtration subcode identified with a code over $\mathcal{T}_{r-i}$. If $H \in \mathcal{R}^{(n-k_0)\times n}$ is a parity-check

for $\mathcal{C}$, we will denote with $\overline{H}^{(i)}$ a parity-check for $\overline{\mathcal{C}}_i$.

In what follows, we will extensively use the following facts.

Proposition 4.5. *Given a linear code $\mathcal{C} \subseteq \mathcal{R}^n$, for any $0 \leq i \leq r-1$ let $\mathcal{C}_i$ be the i-th filtration subcode. The minimum Hamming distance of $\mathcal{C}$ and $\mathcal{C}_i$ coincide.*

Proof. Let $d_{\mathsf{H}}(\mathcal{C})$ and $d_{\mathsf{H}}(\mathcal{C}_i)$ be the minimum hamming distance of $\mathcal{C}$ and $\mathcal{C}_i$ respectively. Since $\mathcal{C}_i$ is a subcode of $\mathcal{C}$, one get $d_{\mathsf{H}}(\mathcal{C}) \leq d_{\mathsf{H}}(\mathcal{C}_i)$. On the other hand, let $\tilde{c}$ be a minimum weight codeword in $\mathcal{C}$. From Remark 4.1 we get that $p^i\tilde{c}$ is a codeword in $\mathcal{C}_i$ whose weight is less or equal than the weight of $\tilde{c}$, and hence $d_{\mathsf{H}}(\mathcal{C}_i) \leq d_{\mathsf{H}}(\mathcal{C})$. □

Remark 4.2. Let d be the minimum distance of $\mathcal{C}$ and $\mathcal{C}_i$. Since the isomorphism $\varphi^{(i)}$ preserves the Hamming weight, the minimum distance of $\overline{\mathcal{C}}_i$ is d.

Let $\mathcal{C} \subseteq \mathcal{R}^n$ be a linear code of subtype $(k_0, \ldots, k_{r-1})$ and let $H \in \mathcal{R}^{(n-k_0)\times n}$ be a parity-check matrix for $\mathcal{C}$. Let $s \in \mathcal{R}^{n-k_0}$, $w \in \mathbb{N}$ obtained according to the uniqueness bound, and consider the syndrome decoding problem $\mathsf{SDP}_{\mathsf{H}}(\mathcal{R}, H, s, w)$. Below is an overview of the algorithm we will present.

- Consider the instance with input the i-th filtration subcode identified as a code over $\mathcal{T}_{r-i}$, namely $\mathsf{SDP}_{\mathsf{H}}(\mathcal{T}_{r-i}, \overline{H}^{(i)}, \overline{s}^{(i)}, \overline{w}^{(i)})$, where $\overline{H}^{(i)} \in \mathcal{R}^{(n-k_0-\sum_{j=1}^{i} k_j)\times n}$ and $\overline{s}^{(i)} \in \mathcal{T}_{r-i}^{n-k_0-\sum_{j=1}^{i} k_j}$.
- call ISD to find $\overline{e}^{(i)} \in \mathcal{T}_{r-i}^{n}$ with weight less or equal then w, such that $\overline{H}^{(i)}\overline{e}^{(i)^\top} = \overline{s}^{(i)}$;
- exploit $\overline{e}^{(i)}$ to reconstruct e.

The core intuition behind the procedure is that, if e is a solution of an instance of the form $\mathsf{SDP}_{\mathsf{H}}(\mathcal{R}, H, s, w)$, then $\overline{e}^{(i)}$ is the solution of $\mathsf{SDP}_{\mathsf{H}}(\mathcal{T}_{r-i}, \overline{H}^{(i)}, \overline{s}^{(i)}, \overline{w}^{(i)})$ instance.

From Remark 4.2, we know that the minimum distance of $\mathcal{C}$ and $\overline{\mathcal{C}}_i$ coincides. Hence, from uniqueness bound 3.4, it follows that, with high probability $\overline{e}^{(i)}$ is the unique vector with weight less or equal than w and with syndrome $\overline{s}^{(i)}$. After having recovered $\overline{e}^{(i)}$, we can retrieve e by considering that

$$\mathrm{Supp}(\overline{e}^{(i)}) \subseteq \mathrm{Supp}(e).$$

This information can be used to speed-up decoding in the final step. We give an example of the resulting algorithm, using Prange's ISD as a subroutine.

Algorithm 4: Improved Prange for ring linear codes, Hamming metric

Input: $H \in \mathcal{R}^{(n-k_0)\times n}$, $s \in \mathcal{R}^{n-k_0}$, $w \in \mathbb{N}$
Output: Vector $e \in \mathcal{R}^n$ such that $\mathrm{wt}_{\mathsf{H}}(e) \leq w$ and $He^\top = s^\top$

// Base case
if $r == 1$ **then**
  Call Algorithm 2 with input H, s, w to find e with weight $\leq w$, such that $He^\top = s^\top$;
  return e

// Recursive step
Compute $\overline{H}^{(1)} \in \mathcal{T}_{r-1i}^{(n-k_0-k_1)\times n}$;
Compute $\overline{s}^{(1)} = \mathcal{T}_{r-1}^{n-k_0-k_1}$;
Compute $\overline{w}^{(1)} = w\left(1 - \frac{q^i-1}{q^r-1}\right)$;
Call Algorithm 4 with input $\overline{H}^{(1)}, \overline{s}^{(1)}, \overline{w}^{(1)}$ to find $\overline{e}^{(1)}$ with weight $\leq \overline{w}^{(1)}$, such that $\overline{H}^{(1)}{\overline{e}^{(1)}}^\top = {\overline{s}^{(1)}}^\top$;

// Reconstruct solution
Set $J' = \mathrm{Supp}(\overline{e}^{(1)})$, $w' = \mathrm{wt}_{\mathsf{H}}(\overline{e}^{(1)})$;
while `True` **do**
  Sample $J'' \subseteq \{1, \ldots, n\} \setminus J'$, with size $(n - K - w')$;
  Set $J = J' \cup J''$;
  Compute a square matrix $U \in \mathcal{R}^{(n-k_0)\times(n-k_0)}$ such that:

$$(UH)_I = \begin{pmatrix} A \\ pB \end{pmatrix} \quad (UH)_J = \begin{pmatrix} 1_{n-K} \\ 0_{(K-k_0)\times(n-K)} \end{pmatrix} \quad Us^\top = \begin{pmatrix} s_1^\top \\ 0_{(K-k_0)\times 1} \end{pmatrix},$$

  where $A \in \mathcal{R}^{(n-K)\times K}, B \in \mathcal{R}^{(K-k_0)\times K}, s_1 \in \mathcal{R}^{(n-K)}$
  if $\mathrm{wt}_{\mathsf{H}}(s_1) \leq w$ **then**
    return e such that $e_I = (0, \ldots, 0)$, $e_J = s_1$.

Proposition 4.6. *Let $w \in \mathbb{N}$ be obtained according to the uniqueness bound. Then, Algorithm 4 runs in time*

$$\max_{i\in\{0,\ldots,r-1\}} \left\{ S_{\mathsf{H}}(\mathcal{T}_{r-i}, 1 - W^{(i+1)}, W^{(i)} - W^{(i+1)}) - S_{\mathsf{H}}(\mathcal{T}_{r-i}, 1 - R_I, W^{(i)} - W^{(i+1)}) \right\},$$

where $W^{(i)} = \lim_{n\to\infty}\left(\frac{\overline{w}^{(i)}(n)}{n}\right)$.

Proof. We observe that Algorithm 4, with input $\{H, s, w\}$, recursively reduces the initial problem into r subproblems. For $i \in \{1, \ldots, r\}$, we therefore denote by τ_i the complexity of the algorithm to solve the i-th level, with $i = r - 1$ as the base case. We also denote by $\{\overline{H}^{(i)}, \overline{s}^{(i)}, \overline{w}^{(i)}\}$ the inputs of these subproblems. Let's first consider

the base case. In what follows we will set $\overline{w}^{(r)} = 0$ In this case the complexity is the same as Algorithm 2, and can be estimated using Proposition 3.6 as

$$\tau_{r-1} := \frac{\binom{n}{\overline{w}^{(r-1)}}}{\binom{n-K}{\overline{w}^{(r-1)}}} = \frac{\binom{n}{\overline{w}^{(r-1)}-w^{(r)}}}{\binom{n-K}{\overline{w}^{(r-1)}-\overline{w}^{(r)}}},$$

which grows asymptotically as

$$S_{\mathsf{H}}(\mathcal{T}_1, 1, W^{(r-1)}) - S_{\mathsf{H}}(\mathcal{T}_1, 1 - R_I, W^{(r-1)}).$$

At this point, on average $\overline{w}^{(r-1)}$ positions of the support of the solution vector are known, which will therefore be excluded from the search in the subsequent steps of the algorithm. Let us consider the immediately higher level. In this case the complexity of the reconstruction algorithm is given by

$$\tau_{r-2} := \frac{\binom{n-\overline{w}^{(r-1)}}{\overline{w}^{(r-2)}-\overline{w}^{(r-1)}}}{\binom{(n-\overline{w}^{(r-1)})-(K-\overline{w}^{(r-1)})}{\overline{w}^{(r-2)}-\overline{w}^{(r-1)}}}.$$

The subsequent steps of the algorithm behave in the exact same way, therefore, for $i \in \{0, \dots, r-3\}$,

$$\tau_i = \frac{\binom{n-\overline{w}^{(i+1)}}{\overline{w}^{(i)}-\overline{w}^{(i+1)}}}{\binom{n-K}{\overline{w}^{(i)}-\overline{w}^{(i+1)}}},$$

which grows asymptotically as

$$S_{\mathsf{H}}(\mathcal{T}_{r-i}, 1 - W^{(i+1)}, W^{(i)} - W^{(i+1)}) - S_{\mathsf{H}}(\mathcal{T}_{r-i}, 1 - R_I, W^{(i)} - W^{(i+1)}).$$

The total complexity is therefore given by the sum of the individual complexities, which grows asymptotically as $\max_{i \in 0 \le i \le r-1} \{\tau_i\}$. □

5 Rank Case

In this section, we investigate both the codeword finding and syndrome decoding problems for rank-metric codes over Galois rings. Specifically, we examine how the rank of a vector reduces when mapped to a smaller ring. Following that, we propose a novel algorithm designed to accelerate the decoding process for codes over rings.

Throughout this section, given $q = p^m$, let $\mathcal{S} = \mathrm{GR}(p^r, m)$ be the Galois ring with residue field $\mathbb{F}_q$ and nilpotency index r. In particular, $\mathcal{S}$ is the Galois extension of $\mathcal{R} := \mathbb{Z}_{p^r}$. Moreover, for any $0 \le i \le r-1$ we will denote by $\mathcal{T}_{r-i}$ the ring $\mathcal{S}/p^i\mathcal{S} = \mathrm{GR}(p^{r-i}, m)$. Finally, accordingly to Definition 3.11 we set $\pi^{(i)}$ to be the i-th projection onto $\mathcal{T}_{r-i}$.

5.1 Weights and projections

If we project the vector $x \in \mathcal{S}^n$ onto $\mathcal{T}^n_{r-i}$, for $1 \leq i \leq r-1$, it is clear that its rank may decreases. In the following, we will provide an estimate of how the rank of a vector is reduced when projected onto $\mathcal{T}_{r-i}$.

Proposition 5.1. *Given a random vector $e \in \mathcal{S}^n$ with rank w, let $\overline{e}^{(i)}$ be the projection of e onto $\mathcal{T}_{r-i}$. The weight of $\overline{e}^{(i)}$ is, on average, reduced to*

$$\overline{w}^{(i)} = \sum_{t=0}^{w} \left(t \cdot \frac{\sum_{\substack{k_0+\cdots+k_{r-1-i}=t \\ k_{r-i}+\cdots+k_{r-1}=w-t}} N_{n,q}(k_0, k_1, \ldots, k_{r-1})}{\sum_{(k_0,\cdots,k_{r-1})\in C(r,w)} N_{n,q}(k_0, \ldots, k_{r-1})} \right).$$

Proof. In order to find the average weight $\overline{w}^{(i)}$ of $\overline{e}^{(i)} \in \mathbb{Z}_{p^{r-i}}$, we need to find

$$\mathbb{E}[rk(\overline{e}^{(i)})|\ rk(e) = w] = \mathbb{E}[rk(\langle \overline{e}^{(i)}_1, \ldots, \overline{e}^{(i)}_n \rangle_{\mathbb{Z}_{p^{r-i}}}) \mid rk(\langle e_1, \ldots, e_n \rangle_{\mathcal{R}}) = w] \ ,$$

which can be computed as

$$\sum_{t=0}^{w} t \cdot \mathbb{P}(rk(\langle \overline{e}^{(i)}_1, \ldots, \overline{e}^{(i)}_n \rangle_{\mathbb{Z}_{p^{r-i}}}) = t \mid rk(\langle e_1, \ldots, e_n \rangle_{\mathcal{R}}) = w] \ .$$

Assume that $(e_1, \ldots, e_n)$ is an $\mathcal{R}$-submodule of subtype $(k_0, \ldots, k_{r-1})$. Then the $\mathbb{Z}_{p^{r-i}}$-module $(\overline{e}^{(i)}_1, \ldots, \overline{e}^{(i)}_n)$ has rank $k_0 + \cdots + k_{r-1-i}$. Hence $(\overline{e}^{(i)}_1, \ldots, \overline{e}^{(i)}_n)$ has rank t if and only if $k_0 + \cdots + k_{r-1-i} = t$. As the number of submodules satisfying that condition is

$$\sum_{\substack{k_0+\cdots+k_{r-1-i}=t \\ k_{r-i}+\cdots+k_{r-1}=w-t}} N_{n,q}(k_0, k_1, \ldots, k_{r-1}),$$

the claim follows. □

Corollary 5.2. *Given a random vector $e \in \mathcal{S}^n$ of rank weight w, let $\overline{e}$ be the projection of e onto its base field $\mathcal{S}/p\mathcal{S}$. The weight of $\overline{e}$ is, on average, reduced to*

$$\overline{w}^{(r-1)} = \sum_{t=0}^{w} \left(t \cdot \frac{\sum_{k_1+\cdots+k_{r-1}=w-t} N_{n,q}(t, k_1, \ldots, k_{r-1})}{\sum_{(k_0,\cdots,k_{r-1})\in C(r,w)} N_{n,q}(k_0, \ldots, k_{r-1})} \right).$$

Example 5.1. Given $n = 70$, $\mathcal{S} = \mathrm{GR}(5^3, 40)$, and $w \in \mathbb{N}$, consider $e \in \mathcal{S}^n$ of rank weight w. We have just shown that the rank weight of x decreases (as a function of w) when projected onto its residue field. Figure 2 provides a graphical representation of this fact.

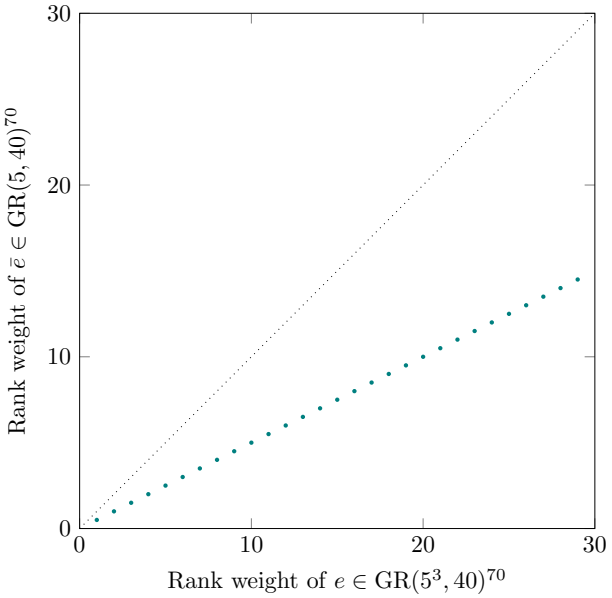

Fig. 2: On the x-axis we put the Hamming weights that a vector can assume, while on the y-axis we draw (in teal) the expected weight that the same vector will have once projected on the base field.

5.2 CFP

Analogously to the Hamming metric case, in this section, we will show that algorithms for solving the codeword finding problem over rings are more efficient than algorithms over fields of the same size.

Given the Galois field $\mathbb{F}_{p^m}$ with prime field $\mathbb{F}_p$, consider a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{p^m}^n$ with parity check $H^{(n-k_0)\times n}$. In the following, we will study the codeword finding problem $\mathsf{CFP}_{\mathsf{rk}}(\mathbb{F}_{p^m}, H, w)$. Since a random code attains the GV bound with high probability [26, 27], we estimate the minimum value of w for which the instance is not vacuous (i.e., at least one solution exists with high probability) using the GV bound. Given a random instance $\mathsf{CFP}_{\mathsf{rk}}(\mathbb{F}_{p^m}, H, w)$, Proposition 3.8 provides an estimates of the asymptotic complexity of the error support attack in this context.

We now turn to the codeword finding problem over rings. Let $\mathcal{S} = \mathrm{GR}(p^r, m)$ be the Galois extension of $\mathcal{R} = \mathbb{Z}_{p^r}$, and consider a linear code $\mathcal{C} \subseteq \mathcal{S}^n$ equipped with the rank-metric.

Remark 5.1. Given $x \in \mathcal{S}^n$, for any $1 \leq i \leq r-1$, we know that $rk_{\mathcal{R}}(p^i x) \leq rk_{\mathcal{R}}(x)$. As a result, we can always find minimum weight codewords in the socle.

Accordingly to Remark 3.1, as the socle can be identified with a linear code over $\mathbb{F}_{p^m}$, one can simply look for the minimum weight codeword in the code $\overline{\mathcal{C}}$, taking values in $\mathbb{F}_{p^m}$. In other words, the complexity of solving $\mathsf{CFP}_{\mathsf{rk}}(\mathcal{R}, H, w)$ is equivalent to that

of solving $\mathsf{CFP}_{\mathsf{rk}}(\mathbb{F}_{p^m}, \overline{H}, w)$. Notably, increasing r does not affect the time complexity of the error support attack on rings; instead, it is determined solely by the size of the residue field. As before, Proposition 3.8 returns the complexity of this algorithm.

5.3 SDP

In this section, we introduce a new algorithm for the syndrome decoding problem in rank metric over Galois rings. The main idea is to transform an SDP instance into an instance over a smaller alphabet and then solve the problem in this new setting. We describe the bigger picture of the algorithm in the following.

From now on, let $\mathcal{S} = \mathrm{GR}(p^r, m)$ be the Galois extension of $\mathcal{R} = \mathbb{Z}_{p^r}$ and let $\mathcal{T}_i \coloneqq \mathrm{GR}(p^{r-i}, m)$. In line with Definition 3.11, let $\pi^{(i)}$ be the i-th projection over $\mathcal{T}_{r-i}$. Given a linear code $\mathcal{C} \subseteq \mathcal{S}^n$, let $\overline{\mathcal{C}}_i$ the i-th filtration subcode identified with a code over $\mathcal{T}_{r-i}$. If $H \in \mathcal{S}^{(n-k_0)\times n}$ is a parity-check for $\mathcal{C}$, we will denote with $\overline{H}^{(i)}$ a parity-check for $\overline{\mathcal{C}}_i$.

Similar to the Hamming-metric case, our algorithm relies on the following fact, the proof of which follows the same steps as the proof of Proposition 4.5.

Proposition 5.3. *Given a linear code $\mathcal{C} \subseteq \mathcal{S}^n$, for any $0 \leq i \leq r-1$ let $\mathcal{C}_i$ be the i-th filtration subcode. The minimum rank distance of $\mathcal{C}$ and $\mathcal{C}_i$ coincide.*

Remark 5.2. Let d be the minimum rank-distance of $\mathcal{C}$ and $\mathcal{C}_i$. Since the isomorphism $\varphi^{(i)}$ preserves the rank weight, the minimum distance of $\overline{\mathcal{C}}_i$ is d.

Let $\mathcal{C} \subseteq \mathcal{S}^n$ be a linear code of subtype $(k_0, \dots, k_{r-1})$ and let $H \in \mathcal{S}^{(n-k_0)\times n}$ be a parity-check matrix for $\mathcal{C}$. Let $s \in \mathcal{R}^{n-k_0}$, $w \in \mathbb{N}$ chosen accordingly to the uniqueness bound, and consider the syndrome decoding problem $\mathsf{SDP}_{\mathsf{rk}}(\mathcal{R}, H, s, w)$.

As for the Hamming case, the main steps of the algorith are:

- Consider the instance with input the i-th filtration subcode identified as a code over $\mathcal{T}_{r-i}$, namely $\mathsf{SDP}_{\mathsf{rk}}(\mathcal{T}_{r-i}, \overline{H}^{(i)}, \overline{s}^{(i)}, \overline{w}^{(i)})$, where $\overline{H}^{(i)} \in \mathcal{R}^{(n-k_0-\sum_{j=1}^{i} k_j)\times n}$ and $\overline{s}^{(i)} \in \mathcal{T}_{r-i}^{n-k_0-\sum_{j=1}^{i} k_j}$.
- call ISD to find $\overline{e}^{(i)} \in \mathcal{T}_{r-i}^{n}$ with weight less then w, such that $\overline{H}^{(i)}\overline{e}^{(i)^\top} = \overline{s}^{(i)}$;
- exploit $\overline{e}^{(i)}$ to reconstruct e.

The core intuition behind the procedure is that, if e is a solution of the $\mathsf{SDP}_{\mathsf{rk}}(\mathcal{S}, H, s, w)$ instance over $\mathcal{S}$, then $\overline{e}^{(i)}$ is a solution of the $\mathsf{SDP}_{\mathsf{rk}}(\mathcal{T}_{r-i}, \overline{H}^{(i)}, \overline{s}^{(i)}, \overline{w}^{(i)})$ over $\mathcal{T}_{r-i}$.

From Remark 5.2, we know that the minimum distance of $\mathcal{C}$ and $\overline{\mathcal{C}}_i$ coincides. Therefore, from the uniqueness bound 3.4 it follows that, with high probability, $\overline{e}^{(i)}$ is the unique solution to the rank syndrome decoding problem $\overline{H}^{(i)}\overline{e}^{(i)^\top} = \overline{s}^{(i)^\top}$. After we find $\overline{e}^{(i)} = (\overline{e}_1^{(i)}, \dots, \overline{e}_n^{(i)})$, we can retrieve e by taking into account that the $\mathcal{R}$-support of e contains the $\mathbb{Z}_{p^{r-i}}$ support of $\overline{e}^{(i)}$. This information can be used to speed-up decoding in the final step.

We give an example of the resulting algorithm, using the error support attack with $n \geq m$ as a subroutine. In line with [8, 40], we will set $u = \lfloor \frac{(n-k_0)m}{n} \rfloor$.

Algorithm 5: Improved error support attack for ring linear codes

Input: $H \in S^{(n-k_0)\times n}$, $w \in \mathbb{N}$, $s \in S^{n-k_0}$
Output: Vector $e \in S^n$ such that $rk(e) \leq w$ and $He^\top = s^\top$

// Base case
if $r == 1$ **then**
  Call Algorithm 3 with input H, s, w to find e with weight $\leq w$, such that $He^\top = s^\top$;
  return e

// Recursive step
Compute $\overline{H}^{(1)} \in \mathcal{T}_{r-1}^{(n-k_0-k_1)\times n}$;
Compute $\overline{s}^{(1)} = \mathcal{T}_{r-1}^{n-k_0-k_1}$;
Compute $\overline{w}^{(1)}$ as in Equation (5.1) ;
Call Algorithm 5 with input $\overline{H}^{(1)}, \overline{s}^{(1)}, \overline{w}^{(1)}$ to find $\overline{e}^{(1)}$ with weight $\leq \overline{w}^{(1)}$, such that $\overline{H}^{(1)}\overline{e}^{(1)\top} = \overline{s}^{(1)\top}$;

// Reconstruct solution
Set $J = \mathrm{Supp}(\overline{e}^{(1)})$, $w' = rk(\overline{e}^{(1)})$;
while `True` **do**
  Choose a free R-submodule F of S of rank u such that $J \subseteq F^{(1)}$;
  Choose a basis $\{f_1, \ldots, f_u\}$ of F
  Solve Equation $(\mathcal{E}_1)$ of Prop. 3.7
  if $\mathcal{E}_1$ *admits a solution* **then**
    Use a solution of $\mathcal{E}_1$ to compute e as in Eq. (7)
    if $rk(e) \leq w$ **then**
      return e

Proposition 5.4. *Let $w \in \mathbb{N}$ be obtained according to the uniqueness bound. Then, Algorithm 5 runs in time*

$$\tau = \max\left\{q^w, m(n-K)n^2u^2q^{\overline{w}^{(r-1)}\lfloor mK/n\rfloor}\right\}.$$

Proof. Similarly to the proof of Prop. 4.2, notice that Algorithm 5, with input $\{H, s, w\}$, recursively reduces the initial problem into r subproblems. For $i \in \{0, \ldots, r-1\}$, we denote by τ_i the complexity of the algorithm to solve the i-th level, with $i = r-1$ as the base case and $i = 0$ as the last one. We also denote by $\{\overline{H}^{(i)}, \overline{s}^{(i)}, \overline{w}^{(i)}\}$ the inputs of these subproblems. We observe that, as i varies in the set $\{1, \ldots, r-1\}$, the dimensions of the inputs of the problem vary accordingly, in particular

$$\left(\overline{H}^{(i)}, \overline{s}^{(i)}\right) \in \left(\mathcal{T}_{r-i}^{\left(n-k_0+\sum_{j=1}^{i} k_j\right)\times n}, \mathcal{T}_{r-i}^{n-k_0+\sum_{j=1}^{i-1} k_j}\right).$$

Consider the base case, with input $\overline{H}^{(r-1)}, \overline{s}^{(r-1)}, \overline{w}^{(r-1)}$, where $\overline{w}^{(r-1)}$ has been obtained using Prop. 5.1. The complexity here is the same as Algorithm 3, which can be estimated using Prop. 3.8 as

$$\tau_{r-1} = m(n-K)n^2u^2\left(\frac{W(\mathcal{T}_1, u, \overline{w}^{(r-1)})}{W(\mathcal{T}_1, m, \overline{w}^{(r-1)})}\right) \approx m(n-K)n^2u^2q^{\overline{w}^{(r-1)}\lfloor mK/n \rfloor}.$$

Let $\overline{e}^{(r-1)}$ be the output produced by this subroutine. We know that $\overline{e}^{(r-1)} = \left(\overline{e}_1^{(r-1)}, \dots, \overline{e}_n^{(r-1)}\right)$ has rank $\overline{w}^{(r-1)}$. Without loss of generality, let us therefore assume that $\{\overline{e}_1^{(r-1)}, \dots, \overline{e}_{\overline{w}^{(r-1)}}^{(r-1)}\}$ is a generating set for the support of $\overline{e}^{(i)}$, namely

$$\langle \overline{e}_1^{(r-1)}, \dots, \overline{e}_n^{(r-1)} \rangle_{\mathbb{Z}_p} = \langle \overline{e}_1^{(r-1)}, \dots, \overline{e}_{\overline{w}^{(r-1)}}^{(r-1)} \rangle_{\mathbb{Z}_p}.$$

Let us consider the immediately higher level. We observe that the inputs of this subproblem are given by $\overline{H}^{(r-2)} \in \mathcal{T}_2^{(n-K+k_{r-1})\times n}$ and $\overline{s}^{(r-2)} \in \mathcal{T}_2^{(n-K+k_1)}$. Notice that

$$\overline{e}^{(r-2)} = \left(\overline{e}_1^{(r-1)} + \lambda_{(r-1,1)}p, \dots, \overline{e}_n^{(r-1)} + \lambda_{(r-1,n)}p\right).$$

When we are asked to find an error of weight $\overline{w}^{(r-2)}$ and syndrome $\overline{s}^{(r-2)}$, we must find a subspace that contains the support of the error vector. As seen at the level below, the support of $\overline{e}^{(r-2)}$ can be written as

$$\langle \overline{e}_1^{(r-1)} + \lambda_{(r-2,1)}p, \dots, \overline{e}_{\overline{w}^{(r-1)}}^{(r-1)} + \lambda_{(r-2,\overline{w}^{(r-1)})}p, \lambda_{(r-2,\overline{w}^{(r-1)}+1)}p, \dots, \lambda_{(r-2,\overline{w}^{(r-2)})}p \rangle_{\mathbb{Z}_2},$$

where each $\lambda_{(r-2,j)}$ is an element of the residue field $\mathbb{F}_q$, for each $j \in \{1, \dots, \overline{w}^{(r-2)}\}$. As a consequence, in at most $\tau_{r-2} = q^{\overline{w}^{(r-2)}}$ attempts we are able to solve the associated subproblem. The subsequent steps of the algorithm work in a similar way, with a complexity respectively given by $\tau_i = q^{w^{(i)}}$, therefore the total complexity can be expressed as

$$\tau = \max_{i\in\{1,\dots,r\}} \tau_i = \max\left\{q^w, m(n-K)n^2u^2q^{\overline{w}^{(r-1)}\lfloor mK/n \rfloor}\right\}.$$

□

6 Lee Case

In the case of the Lee metric, we consider codes over the integer residue ring $\mathbb{Z}_p^r$, where p is a prime and r is a positive integer. The Lee metric case is more complex than the Hamming and rank metric cases. Firstly, multiplying a codeword by p^{r-1} does not necessarily reduce its weight, meaning we cannot always find minimal weight codewords in the socle. Additionally, the coordinates of vectors with low Lee weight (i.e., those below the GV bound) are not uniformly distributed in $\mathbb{Z}_{p^r}$ as low Lee weight coordinates are more likely. For these reasons, we cannot fully apply the previous framework to the codeword finding problem or the syndrome decoding problem.

Proposition 6.1. (Complexity of Lee-Brickell in Lee metric [10, Theorem 4.1]) *The asymptotic average complexity of Algorithm 1 applied to an linear code in $\mathbb{Z}_{p^r}^n$ equipped with the Lee metric is given by:*

$$\lim_{n\to\infty} \frac{1}{n} \log\left(\frac{B_L(\mathbb{Z}_{p^r}, n, w)}{B_L(\mathbb{Z}_{p^r}, n-K, w)}\right).$$

Proposition 6.2. (Complexity of Prange in Lee metric [10, Theorem 4.1]) *The asymptotic average complexity of Algorithm 2 applied to an linear code in $\mathbb{Z}_{p^r}^n$ equipped with the Lee metric is given by:*

$$\lim_{n\to\infty} \frac{1}{n} \log\left(\frac{B_L(\mathbb{Z}_{p^r}, n, w)}{B_L(\mathbb{Z}_{p^r}, K, v) B_L(\mathbb{Z}_{p^r}, n-K, w-v)}\right).$$

6.1 Weights and projections

In this section, we will show how the Lee weight of a vector decreases when projected onto a ring with a smaller size.

We start by analyzing the composition of a randomly chosen vector from a Lee-sphere of a fixed radius.

Lemma 6.3 ([19], Lemma 1)**.** *Consider a vector $x \in \mathbb{Z}_{p^r}^n$ chosen uniformly at random from the n-dimensional Lee sphere of radius w. For any $j \in \mathbb{Z}_{p^r}$,*

$$\mathbb{P}[x_i = j |\ \mathrm{wt_L}(x) = w] = \frac{\exp(-\beta \mathrm{wt_L}(j))}{\sum_{\ell \in \mathbb{Z}_{p^r}} \exp(-\beta \mathrm{wt_L}(\ell))}, \tag{11}$$

where, given $M = \lfloor p^r/2 \rfloor$, β is the unique real solution to the constraint

$$t/n = \left(\frac{M\exp\left((M+2))x\right) - (M+1)\exp((M+1)x) + \exp(x)}{(\exp(kx)-1)(\exp(x)-1)}\right).$$

Proposition 6.4. *Given a random vector $e \in \mathbb{Z}_{p^r}^n$ of Lee weight w, let $\overline{e}^{(i)}$ be the projection of e onto $\mathbb{Z}_{p^{r-i}}$. The Lee weight of $\overline{e}^{(i)}$ is, on average, reduced to*

$$\overline{w}^{(i)} := \frac{n}{\sum_{\ell \in \mathbb{Z}_{p^r}} \exp(-\beta \mathrm{wt_L}(\ell))} \sum_{j \in \mathbb{Z}_p} \exp(-\beta \mathrm{wt_L}(j)) \cdot \mathrm{wt_L}(\overline{j}^{(i)}).$$

where, given $M = \lfloor p^r/2 \rfloor$, β is the unique real solution to the constraint

$$t/n = \left(\frac{M\exp\left((M+2))x\right) - (M+1)\exp((M+1)x) + \exp(x)}{(\exp(kx)-1)(\exp(x)-1)}\right).$$

Proof. In order to find the average weight $\overline{w}^{(i)}$ of $\overline{e}^{(i)} \in \mathbb{Z}_{p^{r-i}}$, we need to find $\mathbb{E}\left[\mathrm{wt_L}(\overline{e}^{(i)})|\ \mathrm{wt_L}(e) = w\right]$. Since the coordinates of e are i.i.d. random variables, it its

sufficient to compute $\sum_{j=1}^{n} \mathbb{E}\left[\mathrm{wt}_{\mathsf{L}}\left(\overline{e}_j^{(i)}\right)|\ \mathrm{wt}_{\mathsf{L}}(e) = w\right]$. Since, for any $1 \leq j \leq n$,

$$\mathbb{E}\left[\mathrm{wt}_{\mathsf{L}}\left(\overline{e}_j^{(i)}\right)|\ \mathrm{wt}_{\mathsf{L}}(e) = w\right] = \sum_{\ell \in \mathbb{Z}_{p^s}} \mathbb{P}[e_j = \ell|\ \mathrm{wt}_{\mathsf{L}}(e) = w] \cdot \mathrm{wt}_{\mathsf{L}}(\ell^{(i)}) \ ,$$

the thesis follows from Lemma 6.3. □

Example 6.1. Given $n = 70$ and $w \in \mathbb{N}$, consider a vector in $\mathbb{Z}_{5^3}^n$ of Lee weight w. Figure 3 represents the marginal distribution of an entry of a random vector for two different values of w. For vectors with small weights, particularly those below the GV bound, entries with low Lee weight are much more likely to appear, while larger values are rarely seen. In contrast, for vectors with high Lee weights, the opposite occurs: entries with larger Lee weights become more frequent, and smaller values appear with probability close to zero. Additionally, figure 4 illustrates how the weight of a random vector in $\mathbb{Z}_{5^3}^n$ of weight w changes when projected onto the prime field $\mathbb{Z}_p$. In particular, it shows that for vectors with low weight, the weight of the projected vector decreases only slightly, while for vectors with high Lee weight, the weight of the projected vector drops significantly.

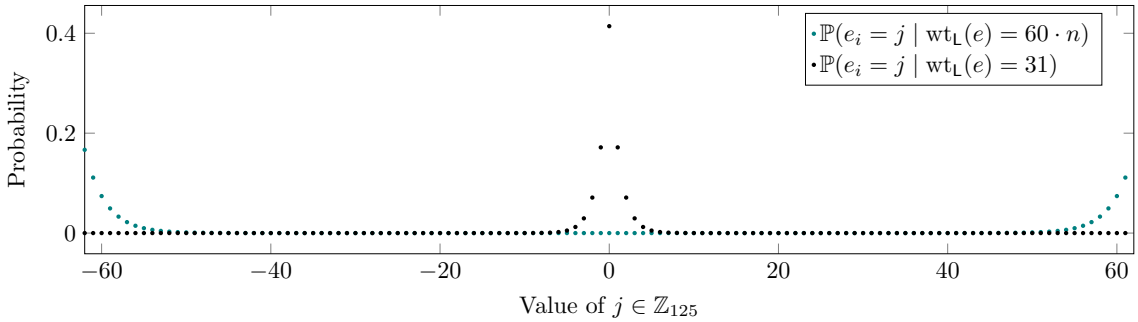

Fig. 3: Given the Lee weight of the vector e, the figure represents the marginal distribution of the i-th entry $e_i \in \mathbb{Z}_{125}$. The black dots represent the marginal distribution of the i-th entry of a vector e with a small Lee weight, while the green dots represent the marginal distribution of the i-th entry of a vector e with Lee weight $60 \cdot n$, which is close to the maximum possible Lee weight of a vector in $\mathbb{Z}_{5^3}^n$.

6.2 CFP

In the following, we will see that the techniques introduced in Sections 4.2 and 5.2 do not allow us to transform a CFP instance over $\mathbb{Z}_{p^r}$ into a CFP instance over its residue field.

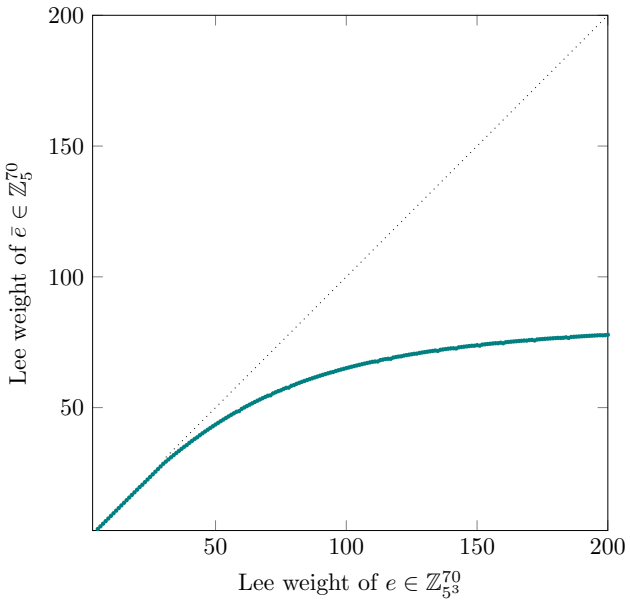

Fig. 4: On the x-axis we put the Lee weight that a vector can assume (truncating this value from above by 200), while on the y-axis we draw (in teal) the expected weight that the same vector will have once projected on the base field.

Given positive integers n and k, let $\mathcal{C} \subseteq \mathbb{Z}_p^n$ be a Lee-metric code of dimension k. Given $H^{(n-k)\times n}$ a parity check for $\mathcal{C}$, let $s \in \mathbb{Z}_p^{n-k}$. In the following, we will focus on the codeword finding problem $\mathsf{CFP}_{\mathsf{L}}(\mathbb{Z}_p, H, w)$. Since a random code attains the GV bound with high probability [29], we estimate the minimum value of w for which the instance is not vacuous (i.e., at least one solution exists with high probability) using the GV bound. Given a random instance $\mathsf{CFP}_{\mathsf{L}}(\mathbb{Z}_p, H, w)$, Proposition 6.1 provides an estimates of the asymptotic complexity of the Lee-Breekel algorithm in the Lee-metric case.

We now turn to the codeword finding problem over rings. Given a positive integer n, we consider a linear code $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^n$ equipped with the Lee-metric. The main difference compared to the Hamming and rank metric cases is that we cannot always find a minimum-weight codeword in the socle of the code. Unlike the previous cases, when multiplying a vector $x \in \mathbb{Z}_{p^r}^n$ by p^{r-1}, we cannot make any deduction on the weight of the vector $p^{r-1}x$: its weight can either increase, decrease, or remain the same.

Example 6.2.
- The linear code $\langle (1,3) \rangle \subseteq \mathbb{Z}_9^2$ has all its minimum weight codewords lying in the socle. In fact, its minimum Lee distance is 3 and it is attained by the codewords $(3,0)$ and $(6,0)$, all lying in the socle.
- The linear code $\langle (1,2) \rangle \subseteq \mathbb{Z}_9^2$ has all its minimum weight codewords outside the socle. In fact, its minimum Lee distance is 3 and it is attained by the codewords

$(1,2)$ and $(8,7)$, all lying outside the socle. Notice that, the codewords lying in the socle, namely $(3,6)$ and $(6,3)$ have Lee-weight equal to 6.

- The linear code $\langle(1,2,3)\rangle \subseteq \mathbb{Z}_9^3$ has some minimum weight codewords lying in the socle and some minimum weight codewords lying outside the socle. In fact, its minimum distance is 6 which is attained by the codewords $(3,6,0)$ and $(6,3,0)$ lying in the socle, and $(1,2,3)$ and $(8,7,6)$ lying outside the socle.

Therefore, unlike in the previous cases, we cannot simply restrict our search to a minimum-weight codeword within the socle, and hence, we cannot conclude that the complexity of solving CFP over a ring is the same as solving it over its base field.

6.3 SDP

The main idea of both improved ISD and improved error support attack algorithms lies in the observation that, if e is the solution to the Syndrome Decoding Problem, then its projection $\overline{e}^{(i)}$ is a solution of the instance with input the i-th filtration subcode, identified as a code over a smaller alphabet. Furthermore, if e is (with high probability) the unique solution to the original problem, $\overline{e}^{(i)}$ is the unique solution to the projected instance. In fact, the weight of the solution of the projected instance can only decrease, while the minimum distances of the code and the i-th filtration subcode as a code over a smaller alphabet coincide. This leads to the conclusion that $\overline{e}^{(i)}$ is the unique solution to the projected instance with high probability. We will now discuss when we can apply this idea in the Lee-metric case.

For a positive integer n, consider a Lee-metric $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^n$ with minimum distance $d(\mathcal{C})$ and let $\mathcal{C}_i$ be the i-th filtration subcode with minimum distance $d(\mathcal{C}_1)$. Moreover, let $\overline{\mathcal{C}}_i$ be the i-th filtration subcode identified with a code over $\mathbb{Z}_{p^{r-i}}$. Notice that the isomorphism $\varphi^{(i)}$ defined in 3.10 does not preserves the Lee weight. Hence, $d(\mathcal{C}_1)$ and $d(\overline{\mathcal{C}}_1)$ differs, and, in particular $d(\overline{\mathcal{C}}_1) < d(\mathcal{C}_1)$. Recall that the uniqueness bound 3.4 states that the solution of the syndrome decoding problem is unique if its weight is sufficiently small (i.e., below the GV bound). As seen in Section 6.1, when projecting a vector with a low Lee weight, its weight decreases very slightly. The reduction in distance is not sufficient to compensate for the decrease in the minimum distance of the projected instance. In certain situations, this causes the weight of the projected solution to exceed the uniqueness bound. As a result, we cannot conclude that the projection of the solution is the unique solution to the projected problem. The following example illustrates this concept.

Example 6.3. Given $p = 3$ and $r = 4$, consider the code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ of length $n = 350$ and $\mathbb{Z}_{p^r}$-dimension $k = 250$ and parity check H. Let $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ be respectively the 1st, 2nd filtration subcode and the socle of $\mathcal{C}$. We estimate the minimum Lee distance of $\mathcal{C}$ and of the filtration subcodes identified as codes over smaller alphabets using the GV bound. In particular, we obtain $d(\mathcal{C}) = 64$, $d(\overline{\mathcal{C}}_1) = 56$, $d(\overline{\mathcal{C}}_2) = 44$ and $d(\overline{\mathcal{C}}_3) = 27$. If $w = \lfloor \frac{d(C)-1}{2} \rfloor = 31$, acoordingly to the uniqueness bound 3.4, the SDP problem $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{3^4}, H, s, w)$ has a unique solution e. Accordingly to Proposition 6.4 $\overline{w}^{(1)} \approx 31$, $\overline{w}^{(2)} \approx 31$ and $\overline{w}^{(3)} \approx 29.5$. From the uniqueness bound 3.4 we get that, with high probability, $\overline{e}^{(1)}$ is the unique solution to $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{3^3}, \overline{H}^{(1)}, \overline{s}^{(1)}, \overline{w}^{(1)})$, as well as $\overline{e}^{(2)}$

is the unique solution to $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{3^2}, \overline{H}^{(2)}, \overline{s}^{(2)}, \overline{w}^{(2)})$. On the other hand, we cannot conclude that $\overline{e}^{(3)}$ is the unique solution of $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_3, \overline{H}^{(3)}, \overline{s}^{(3)}, \overline{w}^{(3)})$.

The previous example shows that the approach described at the beginning of this section cannot be applied to every linear code over $\mathbb{Z}_{p^r}$. Therefore, we start by considering some special cases, such as linear codes over $\mathbb{Z}_4$.

Let $\mathcal{C} \subseteq \mathbb{Z}_4^n$ be a linear code of subtype (k_0, k_1) and parity-check $H \in \mathbb{Z}_4^{(n-k_0)\times n}$. Moreover, let $\mathcal{C}_1$ be the socle of $\mathcal{C}$ and denote with $d(\mathcal{C})$ and $d(\mathcal{C}_1)$ the minimum distance of $\mathcal{C}$ and $\mathcal{C}_1$ respectively. Given $w = \lfloor \frac{d(\mathcal{C})-1}{2} \rfloor$ and $s \in \mathbb{Z}_4^{n-k_0}$, we consider the Syndrome Decoding Problem $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_4, H, s, w)$, whose unique solution will be denoted by e. We now show that, with high probability, $\overline{e}^{(1)}$ is the unique solution of the SDP instance $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_2, \overline{H}^{(1)}, \overline{s}^{(1)}, \overline{w}^{(1)})$ with input $\overline{\mathcal{C}}_1$, which is the socle of the code identified as a code over $\mathbb{Z}_2$. In fact, from Equation 1, we get $d(\mathcal{C}) \leq 2d_{\mathsf{H}}(\mathcal{C})$, where $d_{\mathsf{H}}(\mathcal{C})$ denotes minimum the Hamming distance of $\mathcal{C}$. Since, $d(\overline{\mathcal{C}}_1) = d_{\mathsf{H}}(\mathcal{C}_1) \geq d_{\mathsf{H}}(\mathcal{C})$ and

$$\overline{w}^{(1)} \leq w = \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor \leq \left\lfloor \frac{2d_{\mathsf{H}}(\mathcal{C})-1}{2} \right\rfloor \leq d_{\mathsf{H}}(\mathcal{C}) \leq d(\mathcal{C}_1) \ .$$

From the uniqueness bound 3.4, we get that $\overline{e}^{(i)}$ is, with high probability, the unique solution to $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_2, \overline{H}^{(1)}, \overline{s}^{(1)}, \overline{w}^{(1)})$. Therefore we can improve Algorithm 1 for linear codes over $\mathbb{Z}_4$ equipped with the Lee metric.

Algorithm 6: Improved Prange for ring linear codes, Lee metric

Input: $H \in \mathbb{Z}_4^{(n-k_0)\times n}$, $s \in \mathbb{Z}_4^{n-k_0}$, $w \in \mathbb{N}$
Output: Vector $e \in \mathbb{Z}_4^n$ such that $\mathrm{wt_L}(e) \leq w$ and $He^\top = s^\top$

// Project and solve
Compute $\overline{H}^{(1)} \in \mathbb{Z}_2^{(n-k_0)\times n}$;
Compute $\overline{s}^{(1)} = \mathbb{Z}_2^{n-k_0}$;
Compute $\overline{w}^{(1)}$ according to Prop. 6.4 ;
Call Algorithm 2 with input $\overline{H}^{(1)}, \overline{s}^{(1)}, \overline{w}^{(1)}$ to find $\overline{e}^{(1)}$ with weight $\leq \overline{w}^{(1)}$, such that $\overline{H}^{(1)}{\overline{e}^{(1)}}^\top = {\overline{s}^{(1)}}^\top$;

// Reconstruct solution
Set $J' = \mathrm{Supp}(\overline{e}^{(1)})$, $w' = \mathrm{wt}(\overline{e}^{(1)})$;
while `True` **do**
  Sample $J'' \subseteq \{1, \ldots, n\} \setminus J'$, with size $(n - K - w')$;
  Set $J = J' \cup J''$;
  Compute a square matrix $U \in \mathbb{Z}_4^{(n-k_0)\times(n-k_0)}$ such that:

$$(UH)_I = \begin{pmatrix} A \\ pB \end{pmatrix} \quad (UH)_J = \begin{pmatrix} 1_{n-K} \\ 0_{(K-k_0)\times(n-K)} \end{pmatrix} \quad Us^\top = \begin{pmatrix} s_1^\top \\ 0_{(K-k_0)\times 1} \end{pmatrix},$$

  where $A \in \mathbb{Z}_4^{(n-K)\times K}, B \in \mathbb{Z}_4^{(K-k_0)\times K}, s_1 \in \mathbb{Z}_4^{(n-K)}$
  if $\mathrm{wt_L}(s_1) \leq w$ **then**
    return e such that $e_I = (0, \ldots, 0)$, $e_J = s_1$.

Proposition 6.5 (Complexity of improved Prange with the Lee metric)**.** *Let $w \in \mathbb{N}$ be obtained according to the uniqueness bound. The asymptotic average complexity of Algorithm 6 applied to a $\mathbb{Z}_4$-linear code equipped with the Lee metric is given by:*

$$\max_{i\in[2]} \left\{ S_{\mathsf{L}}\left(\mathbb{Z}_{2^i}, 1 - W^{(i+1)}, W^{(i)} - W^{(i+1)}\right) - S_{\mathsf{L}}\left(\mathbb{Z}_{2^i}, 1 - R_I, W^{(i)} - W^{(i+1)}\right) \right\},$$

Here, for $i \in \{0, 1\}$, $W^{(i)} := \lim_{n\to\infty} \frac{w^{(i)}(n)}{n}$, where $w^{(i)}$ is obtained according to Proposition 6.4 and we set $W^{(2)} = 0$.

Proof. We observe that Algorithm 6, with input $\{H, s, w\}$, reduces the initial problem to one over $\mathbb{Z}_2$. Denote by τ_1 the complexity of the algorithm to solve this subproblem, and denote with $\{\overline{H}^{(1)}, \overline{s}^{(1)}, \overline{w}^{(1)}\}$ its input. In this case the complexity can be estimated using Proposition 3.6 as

$$\tau_1 = \frac{B_{\mathsf{L}}(\mathbb{Z}_2, n, w)}{B_{\mathsf{L}}(\mathbb{Z}_2, n - K, w)} \xrightarrow{n\to\infty} S_{\mathsf{L}}(\mathbb{Z}_2, 1, W^{(1)}) - S_{\mathsf{L}}(\mathbb{Z}_2, 1 - R_I, W^{(1)}) \ .$$

At this point, on average $\overline{w}^{(1)}$ positions of the support of the solution vector are known, which will therefore be excluded from the search in the subsequent step of the algorithm. Let us consider the higher level. In this case the complexity of the reconstruction algorithm is given by

$$\tau_0 = \frac{B_{\mathsf{L}}(\mathbb{Z}_4, n - w^{(1)}, w - \overline{w}^{(1)})}{B_{\mathsf{L}}(\mathbb{Z}_4, n - K, w - w^{(1)})}$$

which grows asymptotically as

$$S_{\mathsf{L}}(\mathbb{Z}_4, 1 - W^{(1)}, W - W^{(1)}) - S_{\mathsf{L}}(\mathbb{Z}_4, 1 - R_I, W - W^{(1)}),$$

The total complexity is therefore given by the sum of the individual complexities, which grows asymptotically as the maximum of these values. □

The following example demonstrates that Algorithm 6 over $\mathbb{Z}_4$ cannot be generalized to any integer rings with quadratic characteristics.

Example 6.4. Given $p = 17$ and $r = 2$, consider the code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ of length $n = 250$ and $\mathbb{Z}_{p^s}$-dimension $k = 180$. Moreover, let $\mathcal{C}_1$ be the socle of $\mathcal{C}$ and $\overline{\mathcal{C}}_1$ be $\mathcal{C}_1$ identified with a code over $\mathbb{Z}_{17}$. Using the GV bound we estimate the minimum Lee distance of $\mathcal{C}$ and $\overline{\mathcal{C}}_1$ which are respectively $d(\mathcal{C}) = 146$ and $d(\overline{\mathcal{C}}_1) = 36$. If $w = \lfloor \frac{d(\mathcal{C})-1}{2} \rfloor = 72$ and $s \in \mathbb{Z}_p^{n-k}$, from the uniqueness bound 3.4 follows that $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{17^2}, H, s, w)$ has a unique solution e. On the other hand, accordingly to Proposition 6.4 $\overline{w}^{(1)} \approx 72$ and hence $\overline{e}^{(1)}$ is not the unique solution, with high probability, of $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{17}, \overline{H}^{(1)}, \overline{s}^{(1)}, w^{(1)})$ with input $\overline{\mathcal{C}}_i$.

The previous example is quite pathological, as the length of the code is smaller than the size of the alphabet. Therefore, we will try to identify sufficient conditions under which Algorithm 6 can be generalized to integer rings of quadratic characteristic.

Let $\mathcal{C} \subseteq \mathbb{Z}_{p^2}^n$ be a linear code of subtype (k_0, k_1) and $\mathbb{Z}_{p^2}$-dimension k. If d is the minimum Lee-distance of $\mathcal{C}$, from the GV bound (2) we get that, for any $w < d$,

$$\frac{p^{2n}}{p^{2k} B_{\mathsf{L}}(\mathbb{Z}_{p^2}, n, w)} < 1 \ ,$$

and hence,

$$p^{n-k} < \sqrt{B_{\mathsf{L}}(\mathbb{Z}_{p^2}, n, w)} \ . \tag{12}$$

Given, $w = \lfloor \frac{d-1}{2} \rfloor$, consider the SDP instance $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{p^r}, H, s, w)$ with unique solution e. Let $\mathcal{C}_1$ denotes the socle of $\mathcal{C}$ and $\overline{\mathcal{C}}_1$ be $\mathcal{C}_1$ identified with a code over $\mathbb{Z}_p$. Assume $\overline{\mathcal{C}}_1$ has minimum distance $\overline{d}$. The uniqueness bound 3.4 states that, if $\overline{d} \geq d/2$, then $\overline{e}^{(1)}$ is the unique solution of $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_p, \overline{H}^{(1)}, \overline{s}^{(1)}, \overline{w}^{(1)})$ with input $\overline{\mathcal{C}}_1$. Since $|\mathcal{C}_1| \leq p^k$,

a sufficient condition to ensure that $\overline{d} \geq d/2$ is

$$p^{n-k} < B_{\mathsf{L}}(\mathbb{Z}_p, n, d/2) \ .$$

Finally, from Equation (13), it is sufficient to prove that

$$\sqrt{B_{\mathsf{L}}(\mathbb{Z}_{p^2}, n, d/2)} < B_{\mathsf{L}}(\mathbb{Z}_p, n, d/2) \ . \tag{13}$$

Therefore, if there exist values of n, p, and k for which Equation (13) is satisfied, then Algorithm 6 extends to a larger class of instances.

Open problem 6.6. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^2}$ be a Lee-metric code of subtype (k_0, k_1) with parity-check H. Given $s \in \mathbb{Z}_{p^2}^{n-k_0}$, assume that $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{p^2}, H, s, w)$ has a unique solution e. Find sufficient conditions on $p, n.k_0, k_1$ for which the projected instance $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_p, \overline{H}^{(1)}, \overline{s}^{(1)}, \overline{w}^{(1)})$ has a unique solution, which is exactly $\overline{e}^{(i)}$.*

Generalizing this idea, as Example 6.3 also suggests, we may exploit only few filtration subcodes, rather than the whole filtration, to speed up the decoding.

Open problem 6.7. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^r}$ be a Lee-metric code of subtype $(k_0, \ldots, k_{r-1})$ with parity-check H. Given $s \in \mathbb{Z}_{p^r}^{n-k_0}$, assume that $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{p^r}, H, s, w)$ has a unique solution e. Find sufficient conditions on $p, n.k_0, \ldots, k_r$ for which the instance $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{p^{r-i}}, \overline{H}^{(i)}, \overline{s}^{(i)}, \overline{w}^{(i)})$ with input the i-th filtration subcode has a unique solution, which is exactly $\overline{e}^{(i)}$. In particular, find the maximum $i \in \{1, \ldots, r-1\}$ such that $\overline{e}^{(i)}$ is the unique solution of $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{p^{r-i}}, \overline{H}^{(i)}, \overline{s}^{(i)}, \overline{w}^{(i)})$.*

7 Conclusions

In this paper, we have introduced new decoding algorithms for codes defined over rings, addressing the challenge of whether it is possible to construct algorithms that outperform those derived from the transposition of classical ISD. The results we presented show that ISD algorithms, if appropriately generalized, not only maintain their effectiveness, but also offer new perspectives for improving efficiency.

Acknowledgments

The authors would like to express their sincere gratitude to Marco Baldi and Paolo Santini for suggesting the idea of investigating this research direction, providing an initial spark for the study, and always being helpful with any questions. The authors would also like to thank Daniele De Bernardini for his precious help.

This publication was created with the co-financing of the European Union FSE-REACT-EU, PON Research and Innovation 2014-2020 DM1062/2021. The author acknowledge support from Ripple's University Blockchain Research Initiative. The first and second author are members of the INdAM Research Group GNSAGA.

References

[1] McEliece, R.J.: A public-key cryptosystem based on algebraic. Coding Thv **4244**, 114–116 (1978)

[2] Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Prob. Contr. Inform. Theory **15**(2), 157–166 (1986)

[3] Becker, A., Joux, A., May, A., Meurer, A.: Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In: Advances in Cryptology–EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings 31, pp. 520–536 (2012). Springer

[4] Lee, P.J., Brickell, E.F.: An observation on the security of mceliece's public-key cryptosystem. In: Advances in Cryptology—EUROCRYPT'88: Workshop on the Theory and Application of Cryptographic Techniques Davos, Switzerland, May 25–27, 1988 Proceedings 7, pp. 275–280 (1988). Springer

[5] Prange, E.: The use of information sets in decoding cyclic codes. IRE Transactions on Information Theory **8**(5), 5–9 (1962)

[6] Stern, J.: A method for finding codewords of small weight. Coding theory and applications **388**, 106–113 (1989)

[7] Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Transactions on Information Theory **62**(2), 1006–1019 (2015)

[8] Kalachi, H.T., Kamche, H.T.: On the rank decoding problem over finite principal ideal rings. arXiv preprint arXiv:2106.11569 (2021)

[9] Puchinger, S., Renner, J., Rosenkilde, J.: Generic decoding in the sum-rank metric. In: 2020 IEEE International Symposium on Information Theory (ISIT), pp. 54–59 (2020). https://doi.org/10.1109/ISIT44484.2020.9174497

[10] Weger, V., Khathuria, K., Horlemann, A.-L., Battaglioni, M., Santini, P., Persichetti, E.: On the hardness of the lee syndrome decoding problem. arXiv preprint arXiv:2002.12785 (2020)

[11] Chailloux, A., Debris-Alazard, T., Etinski, S.: Classical and quantum algorithms for generic syndrome decoding problems and applications to the lee metric. In: Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings 12, pp. 44–62 (2021). Springer

[12] Horlemann-Trautmann, A.-L., Weger, V.: Information set decoding in the lee metric with applications to cryptography. Advances in Mathematics of

Communications **15**(4), 677–699 (2020)

[13] Liu, H., Wang, X., Yang, K., Yu, Y.: The hardness of lpn over any integer ring and field for pcg applications. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 149–179 (2024). Springer

[14] Weger, V., Khathuria, K., Horlemann, A.-L., Battaglioni, M., Santini, P., Persichetti, E.: On the hardness of the lee syndrome decoding problem. Advances in Mathematics of Communications **18**(1), 233–266 (2024)

[15] McDonald, B.R.: Finite Rings with Identity. Lecture notes in pure and applied mathematics. M. Dekker, ??? (1974). https://books.google.it/books?id=1PenAAAAIAAJ

[16] Norton, G., Sălăgean, A.: On the structure of linear and cyclic codes over a finite chain ring. Applicable Algebra in Engineering, Communication and Computing **10**, 489–506 (2000) https://doi.org/10.1007/PL00012382

[17] Hamming, R.W.: Error detecting and error correcting codes. The Bell system technical journal **29**(2), 147–160 (1950)

[18] Lee, C.: Some properties of nonbinary error-correcting codes. IRE Transactions on Information Theory **4**(2), 77–82 (1958)

[19] Bariffi, J., Bartz, H., Liva, G., Rosenthal, J.: On the properties of error patterns in the constant lee weight channel. arXiv preprint arXiv:2110.01878 (2021)

[20] Bariffi, J., Khathuria, K., Weger, V.: Information set decoding for lee-metric codes using restricted balls. In: Code-Based Cryptography Workshop, pp. 110–136 (2022). Springer

[21] Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. Journal of combinatorial theory, Series A **25**(3), 226–241 (1978)

[22] Gabidulin, E.M.: Theory of codes with maximum rank distance. Problemy peredachi informatsii **21**(1), 3–16 (1985)

[23] Kamche, H.T., Mouaha, C.: Rank-metric codes over finite principal ideal rings and applications. IEEE Transactions on Information Theory **65**(12), 7718–7735 (2019)

[24] Barg, A., Forney, G.D.: Random codes: Minimum distances and error exponents. IEEE Transactions on Information Theory **48**(9), 2568–2573 (2002)

[25] Pierce, J.: Limit distribution of the minimum distance of random linear codes. IEEE Transactions on Information Theory **13**(4), 595–599 (1967)

[26] Loidreau, P.: Properties of codes in rank metric. arXiv preprint cs/0610057 (2006)

[27] Loidreau, P.: Asymptotic behaviour of codes in rank metric over finite fields. Designs, codes and cryptography **71**, 105–118 (2014)

[28] Ozbudak, F., Solé, P.: Gilbert-varshamov type bounds for linear codes over finite chain rings. Adv. Math. Commun. **1**(1), 99–109 (2007)

[29] Byrne, E., Horlemann, A.-L., Khathuria, K., Weger, V.: Density of free modules over finite chain rings. Linear Algebra and its Applications **651**, 1–25 (2022)

[30] Roth, R.M.: Introduction to coding theory. IET Communications **47**(18-19), 4 (2006)

[31] Astola, H., Tabus, I.: Bounds on the size of lee-codes. In: 2013 8th International Symposium on Image and Signal Processing and Analysis (ISPA), pp. 471–476 (2013). IEEE

[32] Stanley, R.P.: Enumerative combinatorics volume 1 second edition. Cambridge studies in advanced mathematics (2011)

[33] Gardy, D., Solé, P.: Saddle point techniques in asymptotic coding theory. In: Workshop on Algebraic Coding, pp. 75–81 (1991). Springer

[34] Berlekamp, E., McEliece, R., Van Tilborg, H.: On the inherent intractability of certain coding problems (corresp.). IEEE Transactions on Information theory **24**(3), 384–386 (1978)

[35] Barg, S.: Some new np-complete coding problems. Probl. Inf. Transm. **30**(3), 209–214 (1994)

[36] Gaborit, P., Zémor, G.: On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Transactions on Information Theory **62**(12), 7245–7252 (2016)

[37] Chabaud, F., Stern, J.: The cryptographic security of the syndrome decoding problem for rank distance codes. In: Advances in Cryptology—ASIACRYPT'96: International Conference on the Theory and Applications of Cryptology and Information Security Kyongju, Korea, November 3–7, 1996 Proceedings, pp. 368–381 (1996). Springer

[38] Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.-P.: A new algorithm for solving the rank syndrome decoding problem. In: 2018 IEEE International Symposium on Information Theory (ISIT), pp. 2421–2425 (2018). IEEE

[39] Ourivski, A.V., Johansson, T.: New technique for decoding codes in the rank metric and its cryptography applications. Problems of Information Transmission **38**, 237–246 (2002)

[40] Kamche, H.T., Kalachi, H.T.: On the generalizations of the rank metric over finite

chain rings. In: International Conference on Cryptology in Africa, pp. 201–221 (2024). Springer