Information Set Decoding for Ring-Linear Codes

Giulia Cavicchioni[1,2], Alessio Meneghetti[1,3], Giovanni Tognolini[1]

[1]Department of Mathematics, University of Trento, Trento, Italy.
[2]Institute of Communication and Navigation, German Aerospace Center, Oberpfaffenhofen, Germany.
[3]Department of Mathematics, University of Bari Aldo Moro, Bari, Italy.

Contributing authors: giulia.cavicchioni@dlr.de; alessio.meneghetti@uniba.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 roblem 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 propose a general framework for decoding ring-linear codes that exploits the underlying ring structure to improve traditional approaches. The core idea is to project the decoding instance onto a smaller alphabet, which may enable more efficient decoding algorithms. Our framework is compatible with any coordinate-additive metric, including Hamming and Lee, and can also be adapted to the rank metric. However, we show that the effectiveness of this approach strongly depends on the chosen metric. We illustrate how this framework can be leveraged to design decoding algorithms for the two aforementioned problems in Hamming, rank, and Lee metrics, along with their range of effectiveness. For each case, we provide the average computational complexity of the resulting algorithms.

Keywords: Ring-linear code, Information Set Decoding, Hamming metric, Lee metric, Rank metric,

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 [49, 51].

Traditionally, linear codes are algebraic varieties living in a finite-dimensional vector space over a finite field equipped with the 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 [12, 43, 58, 66]. However, recent research in the coding community has investigated new directions, exploring different algebraic structure and metrics beyond traditional linear codes over finite fields with the Hamming metric. Notable applications of these developments include multiparty computation protocols over integer residue rings $\mathbb{Z}_{p^r}$ [1, 21, 24], digital signature schemes in the Lee metric, with FuLeeca being a prominent example [63] and McEliece-like cryptosystems in the rank metric [2, 39, 50]. Therefore ISD algorithms have been adapted to account for the new underlying algebraic structure or new metrics [5, 18, 20, 31, 35, 38, 44, 67].

Although some advances have been made, the problem of decoding codes over rings still 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. Specifically, our main contribution is to propose a general decoding strategy for ring-linear codes that transforms a decoding instance into a new one over a smaller alphabet, allowing for more efficient decoding. This idea is not entirely new in code-based cryptography. For example, folding techniques exploit a similar strategy by transforming a code into a shorter one over the same alphabet, preserving the rate while reducing the error weight. Originally introduced in [30], this strategy was formalized for structured codes in [25] and later extended to arbitrary codes with a nontrivial automorphism group and to codes over group rings in [17] and [14], respectively. The core of this approach is the *folding operation*, which is essentially a projection [14]. When working with rings, such projections naturally arise by quotienting the ring by one of its ideals. This projection can be lifted to codes, yielding a new code over a smaller alphabet.

However, the projection may alter the code's parameters, potentially resulting in an intractable decoding problem. In this paper, we show that this outcome depends on the underlying metric. For the Hamming and rank metrics, the projection preserves the code parameters, ensuring that a tractable decoding instance remains tractable. This is not the case for the Lee metric: although our framework fully applies to $\mathbb{Z}_4$-linear codes, for residue rings $\mathbb{Z}_{p^r}$ with $p^r > 4$, we can only identify sufficient conditions under which the framework can still be applied.

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 behavior 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 —along with the range of parameters for which it remains effective— in each of the metrics 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

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

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 $\mathbb{F}_p$;
- 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 [48]. 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 $\mathrm{GR}(p^r, m)$.

Alternatively to the additive representation, each element of $\mathrm{GR}(p^r, m)$ can be uniquely expressed in its *multiplicative*, or *p-adic*, form. Specifically, any $t \in \mathrm{GR}(p^r, m)$ admits a unique p-adic expansion

$$t = a_0 + a_1 p + \cdots + a_{r-1}p^{r-1}, \tag{1}$$

where each coefficient a_i, $0 \leq i < r$, lies in the Teichmüller set of $\mathrm{GR}(p^r, m)$ [48].

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

$$k \coloneqq \log_{|\mathcal{R}|} |\mathcal{C}|\ ,$$

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 $k_0 = K = k$. Finally the *rate* of the code is given by $R \coloneqq k/n$.

Similar to the finite field case, ring-linear codes can be represented through a generator matrix or a parity-check matrix [52].

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. *[52, 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:*

$$G = \begin{bmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \ldots & A_{0,r-1} & A_{0,r} \\ 0 & pI_{k_1} & pA_{1,2} & pA_{1,3} & \ldots & pA_{1,r-1} & pA_{1,r} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{2,3} & \ldots & p^2 A_{2,r-1} & p^2 A_{2,r} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & p^{r-1} I_{k_{r-1}} & p^{r-1} A_{r-1,r} \end{bmatrix} = \begin{bmatrix} A_0 \\ pA_1 \\ p^2 A_2 \\ \vdots \\ p^{r-1} A_{r-1}\ , \end{bmatrix} \tag{2}$$

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:

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

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.

Throughout this paper, we will frequently work with the *socle* of a linear code.

Definition 2.7. *Let $\mathcal{R} = \mathrm{GR}(p^r, m)$ be a Galois ring with maximal ideal $p\mathrm{GR}(p^r, m) = \langle p \rangle$ and let $\mathcal{C}$ be an $\mathcal{R}$-linear code. The* socle *of $\mathcal{C}$ is the largest $\mathcal{R}$-submodule of $\mathcal{C}$ annihilated by the maximal ideal of $\mathcal{R}$, that is,*

$$\mathrm{Soc}(\mathcal{C}) \coloneqq \{c \in \mathcal{C} \mid mc = 0 \text{ for all } m \in \langle p \rangle\} \ .$$

Since $\mathcal{R}$ is a local ring, the socle of any $\mathcal{R}$-linear code $\mathcal{C}$ is always nontrivial and forms a vector space over the residue field $\mathcal{R}/\langle p \rangle$. In our setting, where the maximal ideal consists of all multiples of p, the socle of $\mathcal{C}$ is given by $\mathcal{C} \cap \langle p^{r-1} \rangle$.

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. The amount of errors that a code can correct is measured using a metric, which is generally induced by a weight function.

Definition 2.8. *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 *coordinate-additive weight* and *coordinate-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 a coordinate-additive weight is the Hamming weight, introduced by Hamming in 1950 for codes over finite fields [34].

Definition 2.9. *Given a Galois ring $\mathcal{R}$, the* Hamming weight of an element $a \in \mathcal{R}$ *is given by*

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

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

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

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 coordinate-additive distance, when $\mathcal{R} = \mathbb{Z}_{p^r}$, is the Lee distance, first proposed in [42] as an extension of the Hamming distance for the binary field. It has recently garnered increasing attention in code-based cryptography [9, 10, 35, 67].

Definition 2.10. *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*

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

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

$$0 \leq \mathrm{wt}_{\mathsf{L}}(a) \leq \lfloor p^r/2 \rfloor \quad \text{and} \quad \mathrm{wt}_{\mathsf{H}}(x) \leq \mathrm{wt}_{\mathsf{L}}(x) \leq \lfloor p^r/2 \rfloor \mathrm{wt}_{\mathsf{H}}(x). \tag{3}$$

Another metric that has gained significant attention is the rank metric, which, unlike the Hamming and Lee metrics, is not coordinate-additive. Rank-metric codes over finite fields were first studied in connection with association schemes by Delsarte in 1978 [22]. They were also independently introduced by Gabidulin in [26], 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 [40]. 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 2.11. *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 $\mathrm{d}_{\mathsf{rk}}(0,x)$ 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 [7, 57]. The same holds for rank metric codes over finite fields [46, 47]. The GV bound for codes over rings was first explored in [45, 55], and later, in [16] it was proved that random codes over rings with a coordinate-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 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 2.12. (Gilbert-Varshamov bound for coordinate-additive distances, [55]) *For a positive integer n, assume $\mathcal{R}^n$ is equipped with a coordinate-additive distance* d. *The maximal size of a code in $\mathcal{R}^n$ having minimum distance d is*

$$A_{\mathsf{d}}(\mathcal{R}, n, d) \geq \frac{q^{rn}}{B_{\mathsf{d}}(\mathcal{R}, n, d-1)} \ . \tag{4}$$

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

Theorem 2.13 (Gilbert-Varshamov bound for rank distance, [46])**.** *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 2.14 (Volume of a Hamming-metric ball, [65])**.** *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 2.15 (Volume of a Lee-metric ball, [4, 65])**.** *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*

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

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

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 [16], this amount is given by

$$N_{n,\mathcal{R}}(k_0, \ldots, k_{r-1}) \coloneqq q^{\sum_{i=0}^{r-1}(n - \sum_{j=0}^{i} k_j)\sum_{j=0}^{i-1} k_j} \prod_{i=0}^{r-1} \begin{bmatrix} n - \sum_{j=0}^{i-1} k_j \\ k_i \end{bmatrix}_q . \tag{5}$$

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

$$W(\mathcal{R}, n, i) \coloneqq \sum_{(k_0, \ldots, k_{r-1}) \in C(r,i)} N_{n,\mathcal{R}}(k_0, \ldots, k_{s-1}) \ . \tag{6}$$

In the following, we compute the volume of a rank-metric ball in $\mathcal{R}^n$. To prove the next Proposition, it suffices to adapt the arguments of the proof of [6, Lemma 3.5] to Galois rings.

Proposition 2.16 (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 $w \in \{0, \dots, \min\{n, m\}\}$, $B_{\mathsf{rk}}(\mathrm{GR}(p^r, m), n, w)$ is equal to*

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

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 2.17 (Volume of a rank-metric ball over finite fields, [46])**.** *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 $w \in \{0, \dots, \min\{n, m\}\}$,*

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

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 with residue field of size $q \coloneqq p^m$ and d be a distance on $\mathcal{R}^n$, which can be either a coordinate-additive distance or the rank distance. In what follows, we let d denote the product of the code's relative distance δ and the maximum weight of an element in $\mathcal{R}^n$.

$$\lim_{n\to\infty} \frac{1}{n} \log_{q^r}(A_{\mathrm{d}}(\mathcal{R}, n, d)) \geq 1 - \lim_{n\to\infty} \frac{1}{n} \log_{q^r}(B_{\mathrm{d}}(\mathcal{R}, n, d)). \tag{7}$$

It has been proven that the limit in the right-hand side of the previous equation exists for an arbitrary coordinate-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 (7) 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 [29, 67]. Finally, the asymptotic behaviour of rank metric over finite fields is studied in [46, 47].

It is well known that random codes equipped with a coordinate-additive distance lie on the GV bound with high probability [16], as do rank-metric codes over finite fields [46, 47]. 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 [8, 13], and this result extends to codes over rings equipped with a coordinate-additive metric as well [67]. Finally, the computational complexity of syndrome decoding and codeword finding in the rank metric was studied in [27]. 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, let $\mathcal{R} = \mathrm{GR}(p^r, m)$ be a Galois ring with residue field of size $q \coloneqq p^m$, and let d be 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* $(k_0, \dots, k_{r-1})$ *and* $\mathcal{R}$*-dimension* k*. 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

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

□

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 $\mathcal{R}$-dimension k, the SDP Uniqueness Bound corresponds to*

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

Note that w^* coincides with the product of the relative distance δ and the maximum possible weight of an element in $\mathcal{R}^n$. Sometimes, this expression is referred to as the GV radius, or (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 coordinate-additive distances

The problem of decoding ring-linear codes in the Hamming metric has been investigated since the early 2000s, with [5, 18, 31] providing some notable examples. More recently, this problem has also been considered in its equivalent LPN formulation [44], which we will discuss in more detail in Section 4. On the other hand, decoding random Lee-metric codes is a more recent and still challenging problem [9, 10, 35, 67], driven by growing interest in their applications in code-based cryptography.

In the following, we generalize the two-blocks algorithm presented in [67] for Lee metric, allowing the code to be equipped with any coordinate-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 coordinate-additive metric, taking in mind that the Lee and Hamming metrics are special cases of this more general setting.

Let $\mathcal{R} = \mathrm{GR}(p^r, m)$ be a Galois ring with residue field of size $q \coloneqq p^m$, and consider a coordinate-additive distance d over $\mathcal{R}$. Given 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. 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 $\mathrm{wt}_{\mathsf{d}}(e_J) = w - v$ 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 $\mathrm{GR}(p^{r-1}, m)$. In what follows, M will denote the maximum weight of an element in $\mathcal{R}$ with respect to the distance d.

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

Input: The $(n - k_0) \times n$ parity-check matrix H over $\mathcal{R}$, the syndrome $s \in \mathcal{R}^{n-k_0}$, the code's rank K, $w \in \mathbb{N}, v \leq \min\{M \cdot K, w\}$
Output: Vector $e \in \mathcal{R}^n$ such that $\mathrm{wt}_{\mathsf{d}}(e) \leq w$ 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 $P \coloneqq \left\{e_1 \in \mathcal{R}^K \ : \ \mathrm{wt}_{\mathsf{d}}(e_1) = v,\ pBe_1^\top = ps_2\right\}$;
4 **for** $e_1 \in P$ **do**
5 **if** $\mathrm{wt}_{\mathsf{d}}(s_1 - Ae_1^\top) \leq w - v$ **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 generalization of the one shown in [67], 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: $k(n) = \log_{|\mathcal{R}|}(|\mathcal{C}|)$ 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 coordinate-additive distance d over $\mathcal{R}$, the surface of an n-dimensional sphere of radius v is given by:

$$F_{\mathrm{d}}(\mathcal{R}, n, v) \coloneqq \left|\{x \in \mathcal{R}^n \mid \mathrm{wt}_{\mathtt{d}}(x) = v\}\right|. \tag{8}$$

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 a coordinate-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 a coordinate-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 coordinate-additive metric

Input: The $(n-k_0)\times n$ parity-check matrix H over $\mathcal{R}$, the syndrome $s\in\mathcal{R}^{n-k_0}$, the code's rank K, $w\in\mathbb{N}$

Output: Vector $e\in\mathcal{R}^n$ such that $\mathrm{wt}_{\mathsf{d}}(e)\leq w$ and $He^\top = s^\top$

1 Choose an information set $I\subseteq[n]$ of size K and define $J \coloneqq [n]\setminus I$;

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** $\mathrm{wt}_{\mathsf{d}}(s_1)\leq w$ **then**

4 ⌊ **return** e such that $e_I=(0,\dots,0)$, $e_J=s_1$;

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 [67, Theorem 4.1]) *The asymptotic average complexity of Algorithm 2 applied to an $\mathcal{R}$-linear code equipped with a coordinate-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 coordinate-additive and therefore requires a different approach.
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 [19] and then improved in [3, 28, 54]. In particular, [28] proposes an algorithm that, generalizing classical ISD algorithms, aims to find the support of an error vector. While for codes equipped with a coordinate-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 [38]. As solving the syndrome decoding problem over finite principal ideal rings reduces to solving the same problem over finite chain rings [38, Proposition 2.9], our focus will be exclusively on finite chain rings, and especially on Galois rings.

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 [38].

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 $\mathsf{SDP}_{\mathsf{rk}}(\mathcal{S}, H, s, w)$*

$$He^\top = s^\top, \tag{9}$$

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 $j \in \{1, \ldots, n\}$,

$$e_j = \sum_{i=1}^{u} x_{i,j} f_i. \tag{10}$$

Then, Equation (9) 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 [38, 39], we will set $u = \lfloor (n-k_0)m/n \rfloor$.

Algorithm 3: Error support attack

Input: The $(n-k_0) \times n$ parity-check matrix H over $\mathcal{S}$, the syndrome $s \in \mathcal{S}^{n-k_0}$, $w \in \mathbb{N}$.

Output: Vector $e \in \mathcal{S}^n$ such that $rk(e) \leq w$ and $He^\top = s^\top$

```
1 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. 10
       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 (5) and (6), the number of submodules of rank i of a free $\mathcal{R}$-module of rank n is given by $W(\mathcal{R}, n, i)$, which is equal to

$$\sum_{(k_0,\ldots,k_{r-1}) \in C(r,i)} q^{\sum_{i=0}^{r-1}(n-\sum_{j=0}^{i} k_j)\sum_{j=0}^{i-1} k_j} \prod_{i=0}^{r-1} \begin{bmatrix} n-\sum_{j=0}^{i-1} k_j \\ k_i \end{bmatrix}_q, \tag{11}$$

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, [38, 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. (11)*, 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 $\mathcal{C} \subseteq \mathcal{R}^n$ of rank K, it is natural to consider a chain of subcodes of $\mathcal{C}$, all of which have rank K, namely the filtration subcodes.

Throughout this section, let $\mathcal{R} = \mathrm{GR}(p^r, m)$ be a Galois ring with residue field of size $q \coloneqq p^m$ 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

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

According to Definition 2.7, the $r-1$ filtration subcode is the socle of the code.

Lemma 3.10. ([52, Lemma 2.9]) *For any $0 \leq i \leq r-1$, the map $\varphi^{(i)} \colon p^i\mathcal{R}^n \to (\mathcal{R}/p^{r-i}\mathcal{R})^n$ given by $\varphi(p^i c) = (c_1 + p^{r-i}\mathcal{R}, \ldots, c_n + p^{r-i}\mathcal{R})$ for any $c = (c_1, \ldots, c_n)$ is an isomorphism of $\mathcal{R}$ and $(\mathcal{R}/p^{r-i}\mathcal{R})$-modules. In particular $p^{r-1}\mathcal{R}^n$ and $\mathbb{F}_q^n$ are isomorphic as $\mathbb{F}_q$-vector spaces.*

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

Definition 3.11. *Given $\mathcal{R} \coloneqq \mathrm{GR}(p^r, m)$, we define the* i-th projection onto *$\mathcal{T}_{r-i}$ as*

$$\pi^{(i)} \colon \mathcal{R} \longrightarrow \mathcal{T}_{r-i}, \quad z \mapsto \overline{z}^{(i)} \coloneqq \pi^{(i)}(z) = \varphi^{(i)}(p^i z) , \tag{12}$$

that is, $\overline{z}^{(i)}$ is the image of $p^i z \in p^i\mathcal{R}$ under the map $\varphi^{(i)}$.

The i-th canonical projection naturally extends component-wise to vectors over $\mathcal{R}$. In particular, given a vector $x = (x_1, \ldots, x_n) \in \mathcal{R}^n$, we define $\pi^{(i)}(x) \coloneqq \big(\pi^{(i)}(x_1), \ldots, \pi^{(i)}(x_n)\big) \in \mathcal{T}_{r-i}^n$, i.e., by applying the i-canonical projection each entry of x.

Later on with the discussion, to keep the notations simple, we will write $\overline{x}^{(i)}$ to denote $\pi^{(i)}(x) \in \mathcal{T}_{r-i}^n$. Moreover, we will write $\overline{x}$ to denote $\overline{x}^{(r-1)}$ and, for a subset $\mathcal{C}$ of $\mathcal{R}^n$, we will set $\overline{\mathcal{C}}^{(i)} \coloneqq \{\, \overline{c}^{(i)} \mid c \in \mathcal{C} \,\}$.

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 $\overline{\mathcal{C}}_i$. Finally, we will set $\overline{\mathcal{C}} = \overline{\mathcal{C}}_{r-1}$.

If d is a coordinate-additive metric or the rank metric, consider a linear code $\mathcal{C} \subseteq \mathcal{R}^n$ of subtype $(k_0, \ldots, k_{r-1})$ with parity-check matrix H. Following the uniqueness bound 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 $\overline{H}^{(i)} {\overline{e}^{(i)}}^{\top} = {\overline{s}^{(i)}}^{\top}$ where $\overline{H}^{(i)}$ is a parity-check matrix for the i-th filtration subcode identified through $\varphi^{(i)}$ with a code over $\mathcal{T}_{r-i}$ and ${\overline{s}^{(i)}}^{\top}$ is as a vector with coordinates in $\mathcal{T}_{r-i}$. Hence, $\overline{e}^{(i)}$ 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 and 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 by 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 the codeword finding and the syndrome decoding problem for Hamming metric codes. We begin by reviewing known decoding algorithm for Hamming-metric codes over Galois rings. We then introduce a general framework that leverages the ring structure to project the original decoding instance onto a smaller alphabet. For this approach to be effective, the resulting instance must remain tractable. To this end, we analyze how the projection affects the error weight and the code parameters. This analysis enables us to identify the conditions under which the framework leads to a speed-up in the decoding.

We begin by explicitly analyzing the computational complexity of Algorithms 1 and 2 in the Hamming metric.

As a consequence of Proposition 3.5, we can determine the complexity of Algorithm 1 in the Hamming metric case. Throughout this section, let $\mathcal{R} = \mathrm{GR}(p^r, m)$ with residue field of size $q \coloneqq p^m$ and nilpotency index r.

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:

$$\lim_{n\to\infty} \frac{1}{n} \log \left(\frac{q^{r h_{q^r}(\frac{w}{n})n}}{q^{r h_{q^r}(\frac{v}{K})K} q^{r h_{q^r}(\frac{w-v}{n-K})(n-K)}} \right). \tag{13}$$

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

$$B_{\mathsf{H}}(\mathcal{R}, n, t) \approx q^{r h_{q^r}(\frac{t}{n})n} - q^{r h_1(\frac{t-1}{n})n} \approx q^{r h_{q^r}(\frac{t}{n})n}.$$

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

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

Asymptotically, the complexity is therefore given by

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

□

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:*

$$\lim_{n\to\infty} \frac{1}{n} \log \left(\frac{q^{h_q(\frac{w}{n})n}}{q^{h_q(\frac{w}{n-K})(n-K)}} \right). \tag{14}$$

4.1 Overview of decoding algorithms over Galois Rings

Before introducing our framework, we briefly review existing decoding algorithms for ring-linear codes equipped with the Hamming metric. In the late 1990s and early 2000s, researchers developed numerous decoding algorithms for linear codes over Galois rings, focusing particularly on structured families including BCH, Reed–Solomon, and alternant codes [15, 37, 60]. Meanwhile, a general decoding framework was introduced that exploits the algebraic structure of the Galois ring $\mathrm{GR}(p^r, m)$ and, specifically, the p-adic representation of its elements. This framework enables the lifting of decoding algorithms from the residue field to the ring. Initially proposed for free codes in [32], this method was later extended to non-free codes in [5]. It was subsequently generalized to arbitrary finite chain rings in [31] and later combined with the Rosenthal algorithm for convolutional codes [64] to decode ring-linear convolutional codes [18]. The core idea

is to reformulate the decoding problem over a Galois ring $\mathrm{GR}(p^r, m)$ as a sequence of r decoding problems over the base field, whose solutions are then combined to reconstruct a solution to the original problem. We now provide a brief overview of the framework proposed in [5]. Although we adopt a slightly different notation, the core idea remains unchanged. Rather than decoding directly over the Galois ring $\mathcal{R} \coloneqq \mathrm{GR}(p^r, m)$, the authors leverage the p-adic expansion of elements in $\mathcal{R}$ to reduce the problem to r decoding instances over the base field $\mathbb{F}_q$, where $q \coloneqq p^m$. These instances are obtained from successive projections of a tower of supercodes containing the original code $\mathcal{C} \subseteq \mathcal{R}^n$. To formalize this process, for any $\mathcal{R}$-linear code $\mathcal{C}$ and any $t \in \mathcal{R}$, $(\mathcal{C} \colon t)$ denote the *submodule quotient* $(\mathcal{C} \colon t) = \{x \in \mathcal{R}^n \mid tx \in \mathcal{C}\}$. In line with the notation introduced in Definition 3.11, we denote by $\overline{(\mathcal{C} : t)}$ the projection of $(\mathcal{C} : t)$ onto the residue field $\mathbb{F}_q$. To any code $\mathcal{C} \subseteq \mathcal{R}^n$ we associate the tower of supercodes of $\mathcal{C}$ as

$$\mathcal{C} = (\mathcal{C} : p^0) \subseteq \cdots \subseteq (\mathcal{C} : p^i) \subseteq \cdots \subseteq (\mathcal{C} : p^{r-1}) \ ;$$

and its projection over $\mathbb{F}_q$,

$$\overline{\mathcal{C}} = \overline{(\mathcal{C} : p^0)} \subseteq \cdots \subseteq \overline{(\mathcal{C} : p^i)} \subseteq \cdots \subseteq \overline{(\mathcal{C} : p^{r-1})} \ .$$

Let $c \in \mathcal{C}$ be a codeword, and suppose the word $y = c + e$ is received, where e is the error vector. Following (1), let $e = e_0 + e_1 p + \cdots + e_{r-1} p^{r-1}$with $e_i \in \mathbb{F}_q^n$ be the p-adic decomposition of e . The decoding procedure proposed in [5, 32] recovers each coefficient e_i separately, by solving a decoding problem over the residue field for the projected instance $\overline{(\mathcal{C} : p^i)}$. Suppose that the decoding algorithm $\mathcal{A}$ corrects all error patterns of weight up to $w \in \mathbb{N}$. Then the layered procedure is able to recover any error pattern $e \in \mathcal{R}^n$ whose p-adic expansion satisfies $\mathrm{wt}_{\mathsf{H}}(e_i) \leq w$ for all $0 \leq i \leq r-1$.
We now go one step further with respect to [5, 32]. We assume that w is chosen according to the uniqueness bound 3.4 and that the error vector e has Hamming weight w. Then, any ISD algorithm over $\mathcal{R}$, including Lee–Brickell (Algorithm 1) or Prange (Algorithm 2) algorithms, recovers the error with high probability. The same holds for the layered decoding procedure described above. Indeed, since the minimum distance of $\mathcal{C}$ coincides with that of $\overline{(\mathcal{C} : p^{r-1})}$ [53, Theorem 4.2], the minimum distance of each projected code $\overline{(\mathcal{C} : p^i)}$ is lower bounded by that of $\mathcal{C}$. Furthermore, the Hamming weight of each e_i in the p-adic decomposition satisfies $w_{\mathsf{H}}(e_i) \leq w$. Consequently, at each level, the algorithm solves a decoding problem with potentially reduced error weight and improved error correction capability. Once a syndrome decoding algorithm over the residue field is fixed, the overall decoding complexity is determined by that of the chosen algorithm. In particular, Corollaries 4.1 and 4.2 provide the average computational cost of the procedure when Lee–Brickell's or Prange's algorithm over $\mathbb{F}_q$ is employed at each layer. It should be noted that the algorithm decodes a tower of codes whose dimensions grow according to the subtype of the code. Nevertheless, the complexity of the layered procedure is determined solely by the dimension of the largest code in the tower, which coincides with the rank of the original code. As a result, the procedure has the same computational cost for both free and non-free codes. In the following, we present a decoding framework that leverages a different chain of

subcodes, namely the filtration subcodes. This technique enables us to design decoding algorithms that outperform those obtained by transposing classical ISD techniques.

4.2 Weights and projections

The aim of this section is to estimate the weight of an error vector after its projection onto a smaller alphabet. 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, for any $0 \leq i \leq r-1$ we will denote by $\mathcal{T}_{r-i}$ the ring $\mathcal{R}/p^{r-i}\mathcal{R} = \mathrm{GR}(p^{r-i}, m)$. Finally, accordingly to Definition 3.11 we set $\pi^{(i)}$ to be the i-th projection onto $\mathcal{T}_{r-i}$.

Assume that the ambient space is equipped 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 $\mathcal{T}_{r-i}$.
For any $w \in \{0, \ldots, n\}$, according to the notation in (8), we denote by

$$F_{\mathsf{H}}(w) \coloneqq |\{x \in \mathcal{R}^n \mid \mathrm{wt}_{\mathsf{H}}(x) = w\}| \ ,$$

the size of an Hamming sphere of radius w in $\mathcal{R}^n$. Moreover, if $\overline{x}^{(i)}$ denotes the projection of $x \in \mathcal{R}^n$ over $\mathcal{T}_{r-i}^n$, we define

$$F_{\mathsf{H}}^{(i)}(w,t) \coloneqq \left| \left\{ x \in \mathcal{R}^n \;\middle|\; \mathrm{wt}_{\mathsf{H}}(x) = w,\ \mathrm{wt}_{\mathsf{H}}(\overline{x}^{(i)}) = t \right\} \right|$$

to be the number of vectors in $\mathcal{T}_{r-i}$ of Hamming weight w that are projected to vectors of Hamming weight t.

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*

$$\overline{w}^{(i)} \coloneqq \frac{\sum_{t=0}^{w} t\binom{w}{t}(q^r - q^{r-i})^t (q^{r-i}-1)^{w-t}}{(q^r-1)^w} \ .$$

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

$$\mathbb{E}[\mathrm{wt}_{\mathsf{H}}(\overline{e}^{(i)}) \ \mid \ \mathrm{wt}_{\mathsf{H}}(e) = w] = \sum_{t=0}^{w} t \cdot \mathbb{P}[\mathrm{wt}_{\mathsf{H}}(\overline{e}^{(i)}) = t \ \mid \ \mathrm{wt}_{\mathsf{H}}(e) = w] \ .$$

Thus, it is sufficient to determine the probability that a vector of Hamming weight w is projected onto a vector of Hamming weight $t \leq w$, which is given by the ratio $\frac{F_{\mathsf{H}}^{(i)}(w,t)}{F_{\mathsf{H}}(w)}$. We observe that the volume of the Hamming sphere of radius w, $F_{\mathsf{H}}(w)$, can be directly deduced from Proposition 2.14. On the other hand, if $x \in \mathcal{R}^n$ with Hamming weight w belongs to $F_{\mathsf{H}}^{(i)}(w,t)$, then when x is projected through $\pi^{(i)}$, exactly $w-t$ of its non-zero entries are mapped to zero. According to Definition 3.11, this is equivalent to saying

that $w - t$ non-zero positions of x lie in $p^i\mathcal{R}$, while the remaining t non-zero positions lie in $\mathcal{R} \setminus p^i\mathcal{R}$. Since $\left|\mathcal{R} \setminus p^i\mathcal{R}\right| = q^r - q^{r-i}$ and $\left|p^i\mathcal{R} \setminus \{0\}\right| = q^{r-i} - 1$, it follows that

$$\mathbb{P}[\mathrm{wt}_{\mathsf{H}}(\overline{e}^{(i)}) = t \mid \mathrm{wt}_{\mathsf{H}}(e) = w] = \frac{\binom{n}{w}\binom{w}{t}(q^r - q^{r-i})^t(q^{r-i} - 1)^{w-t}}{\binom{n}{w}(q^r - 1)^w} \ ,$$

and the claim follows. □

In our setting, we consider a channel model where the error vector is drawn uniformly at random from the set of vectors in $\mathcal{R}^n$ with fixed Hamming weight. A commonly used alternative is the memoryless channel model, where the error vector entries are assumed to be independent and identically distributed random variables. This assumption often simplifies the analysis. Notably, their channel laws coincide in the asymptotic regime, as their marginal distributions converge [45]. In the following, we derive a formula for the expected weight of a projected error vector in the memoryless channel model.

Proposition 4.4. *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 is 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 4.5. *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 residue field. The expected weight is computed using the formulas from Propositions 4.3 and 4.4, which, as desired, yield the same expectation.

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.

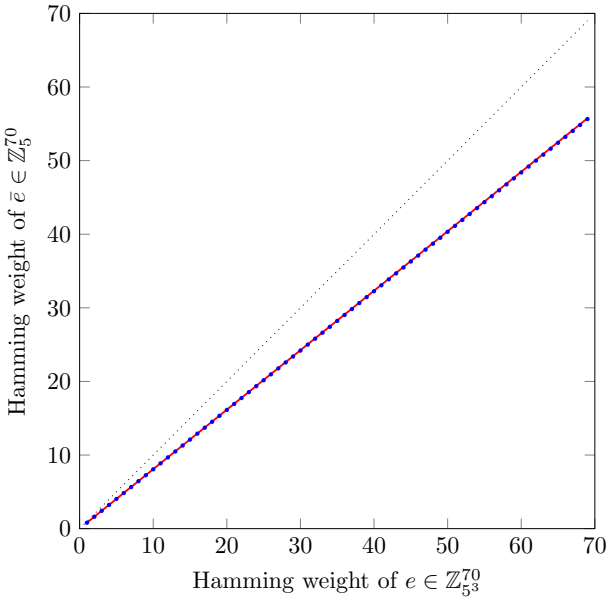

Fig. 1: On the x-axis, we plot the possible Hamming weights of a vector, while on the y-axis we draw the corresponding expected projected weight over the base field. The expected values are computed using Proposition 4.3 (teal dots) and Proposition 4.4 (red continuous line), respectively. To better illustrate how the weight decreases after the projection, the dashed black line represents the Hamming weight of e before projection.

4.3 Solving CFP

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.
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.

Given a prime p and a positive integer m, let $q \coloneqq p^m$. Let $\mathbb{F}_q$ be the Galois field with q elements and consider a linear code $\mathcal{C}$ in $\mathbb{F}_q^n$ 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 $w = \delta n$, where δ is the relative distance of the code. Given a random instance $\mathsf{CFP}_{\mathsf{H}}(\mathbb{F}_q, H, w)$, Proposition 4.1 provides an estimate 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 $\mathbb{F}_q$, 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 $\mathbb{F}_q$, one can simply look for the minimum weight codeword in the code $\overline{\mathcal{C}}$, taking values in $\mathbb{F}_q$. 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 $\mathbb{F}_q$. In particular, increasing r does not lead to modifications for the time complexity of Lee-Brickell over rings, since it only depends on the size of its residue field. As before, Proposition 4.1 returns the complexity of this algorithm.

4.4 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. An analog formulation has been recently proposed for the LPN problem over $\mathbb{Z}_{2^\lambda}$ [44]. Since LPN is known to be equivalent to the syndrome decoding problem, our contribution to the Hamming metric case is not entirely new; rather, it provides a different vocabulary to describe the same technique. Furthermore, our proposed strategy is reminiscent of the approach adopted in the folding attacks [17], where the decoding instance is reduced to a smaller one through quotienting operations. In the following, we transform a syndrome decoding problem into one defined over a smaller alphabet by performing a projection. However, a key distinction lies in the outcome of the transformation. While folding may result in an intractable decoding problem, the projection preserves the code parameters and yields a new instance that remains tractable. We now detail this framework.

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 4.6. *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 $d_{\mathsf{H}}(\mathcal{C}_i)$ denote the minimum Hamming distance of $\mathcal{C}$ and $\mathcal{C}_i$, respectively. Since $\mathcal{C}_i \subseteq \mathcal{C}$, it follows immediately that

$$d_{\mathsf{H}}(\mathcal{C}) \leq d_{\mathsf{H}}(\mathcal{C}_i).$$

To prove the converse inequality, let $\tilde{c} \in \mathcal{C}$ be a codeword of minimum weight, that is, $\mathrm{wt}_{\mathsf{H}}(\tilde{c}) = d_{\mathsf{H}}(\mathcal{C})$. We consider two cases:

- If $\tilde{c} \in \mathcal{C}_i$, then clearly $d_{\mathsf{H}}(\mathcal{C}_i) \leq \mathrm{wt}_{\mathsf{H}}(\tilde{c}) = d_{\mathsf{H}}(\mathcal{C})$.
- If $\tilde{c} \notin \mathcal{C}_i$, then, since $\tilde{c}$ is a codeword, $\tilde{c} \in \mathcal{C}_j$ for some $0 \leq j < i$. Let $\overline{j}$ be the maximum such index., It follows that $p^{i-\overline{j}}\tilde{c}$ is a non-zero codeword in $\mathcal{C}_i$, and, by Remark 4.1, its Hamming weight satisfies

$$\mathrm{wt}_{\mathsf{H}}\left(p^{i-\overline{j}}\tilde{c}\right) \leq \mathrm{wt}_{\mathsf{H}}(\tilde{c}) = d_{\mathsf{H}}(\mathcal{C}) \ .$$

  Therefore, $d_{\mathsf{H}}(\mathcal{C}_i) \leq d_{\mathsf{H}}(\mathcal{C})$.

In both cases, we conclude that $d_{\mathsf{H}}(\mathcal{C}_i) \leq d_{\mathsf{H}}(\mathcal{C})$ and the thesis follows.

□

Remark 4.2. Let us consider the $(\mathcal{R}/p^{r-i}\mathcal{R})$-module homomorphism $\varphi^{(i)} \colon p^i\mathcal{R} \to \mathcal{R}/p^{r-i}\mathcal{R}$ defined in Lemma 3.10. Given $x \in p^i\mathcal{R}$, there exists $\tilde{x} \in \mathcal{R}$ such that $x = p^i\tilde{x}$, and, by definition

$$\varphi^{(i)}(x) = \varphi^{(i)}(p^i\tilde{x}) = \tilde{x} + p^{r-i}\mathcal{R} \ .$$

Since $\varphi^{(i)}$ is an isomorphism, it is injective. In particular, $\varphi^{(i)}(x) = 0$ if and only if $x = p^i\tilde{x} = 0$. Now, for any $n \geq 1$, we can extend $\varphi^{(i)}$ coordinate-wise to define a map $\varphi^{(i)} \colon p^i\mathcal{R}^n \to (\mathcal{R}/p^{r-i}\mathcal{R})^n$. This extension preserves the support of a vector: for any vector $x = (x_1, \ldots, x_n) \in p^i\mathcal{R}^n$, the j-th coordinate of $\varphi^{(i)}(x)$ is zero if and only if $x_j = 0$. Thus, $\varphi^{(i)}$ preserves the Hamming weight.
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 then or equal to 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 then or equal to w and with syndrome $\overline{s}^{(i)}$. Note that this also implies that if $\overline{s}^{(i)} = 0$ then $\overline{e}^{(i)} = 0$, hence it is possible to start the decoding procedure by searching for the smallest i for which $\overline{s}^{(i)} \neq 0$. 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. As in Algorithms 1 and 2, we bring the parity-check matrix $H \in \mathcal{R}^{(n-k_0)\times n}$ into systematic form by multiplying it with an invertible matrix $U \in \mathcal{R}^{(n-k_0)\times(n-k_0)}$ in line 12.

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

Input: The $(n-k_0)\times n$ parity-check matrix H over $\mathcal{R} = \mathrm{GR}(p^r, m)$, the syndrome $s \in \mathcal{R}^{n-k_0}$, the code's subtype $(k_0, \ldots, k_{r-1})$ and a positive integer w

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

// Base case

1 **if** $r == 1$ **then**

2 Call Algorithm 2 with input H, s, code's dimension k_0 and w to find e with weight $\leq w$, such that $He^\top = s^\top$;

3 **return** e

// Recursive step

4 Compute $\overline{H}^{(1)} \in \mathcal{T}_{r-1}^{(n-k_0-k_1)\times n}$;

5 Compute $\overline{s}^{(1)} = \mathcal{T}_{r-1}^{n-k_0-k_1}$;

6 Compute $\overline{w}^{(1)} = w\left(1 - \frac{q^{r-1}-1}{q^r-1}\right)$;

7 Call Algorithm 4 with input $\overline{H}^{(1)}, \overline{s}^{(1)}$, code's subtype $(k_0+k_1, \ldots, k_{r-1})$ and $\overline{w}^{(1)} \in \mathbb{N}$ 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

8 Set $J' = \mathrm{Supp}(\overline{e}^{(1)})$, $w' = \mathrm{wt}_{\mathsf{H}}(\overline{e}^{(1)})$;

9 **while** `True` **do**

10 Sample $J'' \subseteq \{1, \ldots, n\} \setminus J'$, with size $(n - K - w')$;

11 Set $J = J' \cup J''$;

12 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**

13 **return** e such that $e_I = (0, \ldots, 0)$, $e_J = s_1$.

Proposition 4.7. *Let $w \in \mathbb{N}$ be obtained according to the uniqueness bound. Then, Algorithm 4 runs in time*

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

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 $i \in \{1, \dots, r\}$, 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 $\max_{i\in 0\le i\le r-1} \{\tau_i\}$. □

Algorithm 4 recursively decodes the filtration subcodes of $\mathcal{C}$. The sizes of their parity-check matrix vary depending on the code's subtype. However, the proposed procedure is a lifting of the two-blocks algorithm (Algorithm 2), whose complexity depends only on the rank of the code rather than its subtype. Since all filtration

subcodes share the same rank, the overall complexity of the algorithm is determined solely by the rank of the code. As a result, the algorithm achieves the same time complexity for both free and non-free codes.

5 Rank Case

Although the rank metric was originally defined over finite fields, it has recently been extended to broader algebraic structures. In [40] the authors introduced rank-metric codes, particularly Gabidulin codes, over finite principal ideal rings. Decoding algorithms for ring-linear rank-metric codes have been proposed in [40, 59]. Low-Rank Parity-Check codes have been studied over Galois rings, along with decoding techniques [61, 62]. In [38], the authors introduced a combinatorial decoding algorithm that generalizes the rank Support Attack [28], initially designed for finite fields, to address the rank decoding problem over finite chain rings.
In this section, we build upon these developments and focus on the rank decoding problem over Galois rings, discussing 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 $\mathcal{R} \coloneqq \mathbb{Z}_{p^r}$. Moreover, for any $0 \leq i \leq r-1$ 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 $\mathcal{T}_{r-i}^n$, 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 $\overline{e}^{(i)} \in \mathcal{T}_{r-i}$, we need to find

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

which can be computed as

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

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 $(\overline{e}_1^{(i)}, \ldots, \overline{e}_n^{(i)})$ has rank $k_0 + \cdots + k_{r-1-i}$. Hence $(\overline{e}_1^{(i)}, \ldots, \overline{e}_n^{(i)})$ 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.

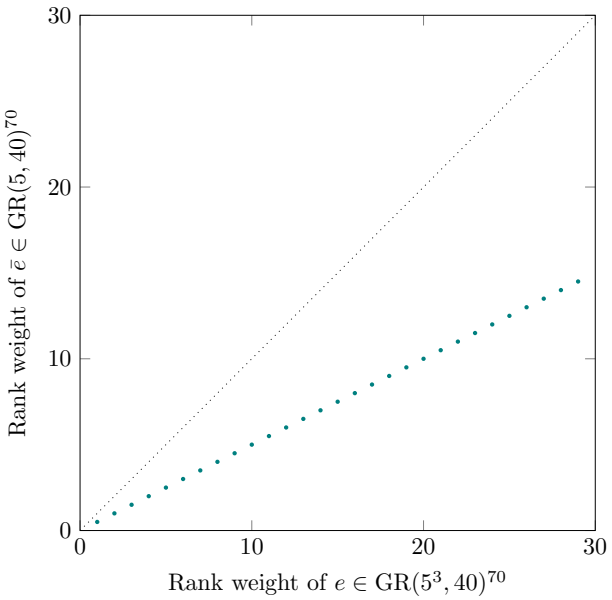

Fig. 2: On the x-axis we put the Hamming weights that a vector can assume, while on the y-axis we draw (in teal) the expected weight that the same vector will have once projected on the base field. To better illustrate how the weight decreases after the projection, the dashed black line represents the Hamming weight of e before projection.

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 a prime p and a positive integer m, let $q \coloneqq p^m$. Let $\mathbb{F}_q$ be the Galois field with q elements and consider a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with parity-check $H^{(n-k_0)\times n}$. In the following, we will study the codeword finding problem $\mathsf{CFP}_{\mathsf{rk}}(\mathbb{F}_q, H, w)$. Since a random code attains the GV bound with high probability [46, 47], 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 $\mathsf{CFP}_{\mathsf{rk}}(\mathbb{F}_q, H, w)$, 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 $\mathbb{F}_q$, one can simply look for the minimum weight codeword in the code $\overline{\mathcal{C}}$, taking values in $\mathbb{F}_q$. In other words, the complexity of solving $\mathsf{CFP}_{\mathsf{rk}}(\mathcal{S}, H, w)$ is equivalent to that of solving $\mathsf{CFP}_{\mathsf{rk}}(\mathbb{F}_q, \overline{H}, w)$. 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 $\mathcal{R} = \mathbb{Z}_{p^r}$ with residue field of size $q \coloneqq p^m$. For each $0 \leq i < r$, 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 4.6.

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. The $(\mathcal{R}/p^{r-i}\mathcal{R})$-module isomorphism $\varphi^{(i)} \colon p^i\mathcal{R}^n \to (\mathcal{R}/p^{r-i}\mathcal{R})^n$ preserves both the Hamming weight (see Remark 4.2) and the rank weight. Let $M \subseteq p^i\mathcal{R}^n$ be a submodule of rank k, and suppose $M = \langle x_1, \ldots, x_k \rangle$, where each $x_j = p^i\tilde{x}_j$ for some $\tilde{x}_j \in \mathcal{R}^n$. Then the image $\varphi^{(i)}(M)$ is generated by $\{\varphi^{(i)}(x_1), \ldots, \varphi^{(i)}(x_k)\}$. Since $\varphi^{(i)}$ preserves the support of each x_j, all these images are non-zero. Suppose, by contradiction, that one of the elements in this set can be written as a linear combination of the others (for further details on linear dependencies for modules over rings, we refer the reader to [56]). Then there exist $b_1, \ldots, b_k \in \mathcal{R}/p^{r-i}\mathcal{R}$, not all zero divisors, such that

$$b_1\varphi^{(i)}(x_1) + \cdots + b_k\varphi^{(i)}(x_k) = 0.$$

Since $\varphi^{(i)}$ is an homomorphism,

$$\varphi^{(i)}(b_1x_1 + \cdots + b_kx_k) = \varphi^{(i)}(p^i(b_1\tilde{x}_1 + \cdots + b_k\tilde{x}_k)) = 0.$$

Since $\varphi^{(i)}$ is injective, it follows that $p^i(b_1\tilde{x}_1 + \cdots + b_k\tilde{x}_k) = 0$, which contradicts the assumption that the rank of M is k.

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 $(k_0, \ldots, k_{r-1})$ and let $H \in \mathcal{S}^{(n-k_0)\times n}$ be a parity-check matrix for $\mathcal{C}$. Let $s \in \mathcal{S}^{n-k_0}$, $w \in \mathbb{N}$ chosen accordingly to the uniqueness

bound, and consider the syndrome decoding problem $\mathsf{SDP}_{\mathsf{rk}}(\mathcal{S}, H, s, w)$.
As for the Hamming case, the main steps of the algorithm 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 or equal to 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 $\overline{e}^{(i)} = (\overline{e}_1^{(i)}, \ldots, \overline{e}_n^{(i)})$, 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 [38, 39], we will set $u = \lfloor \frac{(n-k_0)m}{n} \rfloor$.

Algorithm 5: Improved error support attack for ring linear codes

Input: The $(n-k_0)\times n$ parity-check matrix H over $\mathcal{S}=\mathrm{GR}(p^r,m)$, the syndrome $s\in\mathcal{S}^{n-k_0}$, the code's subtype $(k_0,\dots,k_{r-1})$ and a positive integer w

Output: Vector $e\in\mathcal{S}^n$ 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 $\overline{H}^{(1)},\overline{s}^{(1)}$ code's subtype $(k_0+k_1,\dots,k_{r-1})$ and $\overline{w}^{(1)}$ and 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 $\mathcal{R}$-submodule $\mathcal{F}$ of $\mathcal{S}$ of rank u such that $J\subseteq\mathcal{F}$;

  Choose a basis $\{f_1,\dots,f_u\}$ of $\mathcal{F}$

  Solve Equation $(\mathcal{E}_1)$ of Proposition 3.7

  if $\mathcal{E}_1$ *admits a solution* **then**

    Use a solution of $\mathcal{E}_1$ to compute e as in Eq. (10)

    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, where q is the size of the residue field of $\mathcal{R}$.*

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

Proof. Similarly to the proof of Proposition 4.2, notice that Algorithm 5, with input $\{H,s,w\}$, recursively reduces the initial problem into r subproblems. For $i\in\{0,\dots,r-1\}$, 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 $\{1,\dots,r-1\}$, 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 Proposition 5.1. The complexity here is the same as Algorithm 3, which can be estimated using Proposition 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 $\overline{e}^{(r-1)} = \left(\overline{e}_1^{(r-1)}, \ldots, \overline{e}_n^{(r-1)}\right)$ has rank $\overline{w}^{(r-1)}$. Without loss of generality, let us therefore assume that $\{\overline{e}_1^{(r-1)}, \ldots, \overline{e}_{\overline{w}^{(r-1)}}^{(r-1)}\}$ is a generating set for the support of $\overline{e}^{(i)}$, namely

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

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 $\overline{s}^{(r-2)} \in \mathcal{T}_2^{(n-K+k_{r-1})}$. Notice that

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

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

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

where each $\lambda_{(r-2,j)}$ is an element of the residue field $\mathbb{F}_q$, for each $j \in \{1, \ldots, \overline{w}^{(r-2)}\}$. 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 $\tau_i = q^{\overline{w}^{(i)}}$, therefore the total complexity can be expressed as

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

□

Similar to the Hamming metric case, the improved error support attack for the rank metric has the same time complexity for free and non-free codes, as the complexity depends only on the code's rank.

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. After their introduction in cryptography [35] and the first submission of a signature scheme in the Lee metric to the NIST competition [63], the problem of decoding Lee-metric codes has attracted significant attention [9, 10, 10, 36, 67]. In this work, we leverage the filtration subcodes to speed up the decoding process. The idea of leveraging the socle to improve the decoding is not entirely new. For instance, the s-blocks algorithm [67, Algorithm 2] exploits the code subtype and its socle to enhance decoding performance for non-free codes. In this section, we show that extending the techniques from Sections 4 and 5 to the Lee metric is not as immediate as it might seem. First, multiplying a codeword by p^{r-1} does not necessarily reduce its weight, meaning that we cannot always find minimal weight codewords in the socle. Furthermore, 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. However, we show that the framework applies $\mathbb{Z}_4$-linear codes, and we provide sufficient conditions for its applicability to rings of quadratic characteristics.

Proposition 6.1. (Complexity of Lee-Brickell in Lee metric [67, Theorem 4.1]) *The asymptotic average complexity of Algorithm 1 applied to a 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 [67, Theorem 4.1]) *The asymptotic average complexity of Algorithm 2 applied to a 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. In accordance with Definition 3.11, we denote by $\pi^{(i)}$ the i-th canonical projection, and given a vector $x \in \mathbb{Z}_{p^r}^n$, we denote by $\overline{x}^{(i)}$ its image under $\pi^{(i)}$.

In our channel model, an error vector of fixed Lee weight $w \in \mathbb{N}$ is added to the transmitted codeword. This error is chosen uniformly at random from the Lee sphere of radius w. To estimate its weight after projection, similarly to Hamming metric case, we denote by

$$F_{\mathsf{L}}(w) \coloneqq \left|\left\{x \in \mathbb{Z}_{p^r}^n \mid \mathrm{wt}_{\mathsf{L}}(x) = w\right\}\right|$$

the size of the Lee sphere of radius w. We also define

$$F_{\mathsf{L}}^{(i)}(w,t) \coloneqq \left| \left\{ x \in \mathbb{Z}_{p^r}^n \;\middle|\; \mathrm{wt}_{\mathsf{L}}(x) = w,\ \mathrm{wt}_{\mathsf{L}}(\overline{x}^{(i)}) = t \right\} \right|$$

to be the number of vectors of Lee weight w projected onto vectors in $\mathbb{Z}_{p^{r-i}}^n$ of Lee weight t. Note that knowing the Lee weight of a vector does not give information on the size of its support or the composition of its entries. Therefore, to compute the latter quantity, one should consider the *Lee-decomposition* of vectors in $\mathbb{Z}_{p^r}^n$. Given a vector $x = (x_1, \ldots, x_n) \in \mathbb{Z}_{p^r}^n$, its Lee-decomposition is the tuple $(\rho_0, \rho_1, \ldots, \rho_{\lfloor \frac{p^r}{2} \rfloor})$, where

$$\rho_i \coloneqq |\{j = 1, \ldots, n \mid x_j = \pm i\}| \ .$$

Specifically, to estimate the average weight of the projected vector, one must consider all possible Lee decompositions, determine their corresponding projected weights, and then average according to the probability distribution of the Lee decompositions, which can be found in [9, Chapter II.B]. Working with the Lee composition involves more complex computations. Therefore, following the approach used for the Hamming case, we adopt the memoryless Lee channel model, which simplifies the analysis. In [11], the authors show that, in the limit of large block length, the marginal conditional distributions of the constant Lee weight and memoryless Lee channel models converge. This allows us to treat the entries of the error vector as i.i.d. random variables. The distribution of the entries of a random vector with a fixed Lee weight has been studied in [9], which establish that, as $n \to \infty$, the following distribution holds for each coordinate x_i of x.

Lemma 6.3 ([9], 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 $j \in \mathbb{Z}_{p^r}$,*

$$\mathbb{P}[x_i = j |\ \mathrm{wt}_{\mathsf{L}}(x) = w] = \frac{\exp(-\beta \mathrm{wt}_{\mathsf{L}}(j))}{\sum_{\ell \in \mathbb{Z}_{p^r}} \exp(-\beta \mathrm{wt}_{\mathsf{L}}(\ell))}, \tag{15}$$

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*

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

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 $\mathbb{E}\left[\mathrm{wt}_{\mathsf{L}}(\overline{e}^{(i)})|\ \mathrm{wt}_{\mathsf{L}}(e) = w\right]$. Since the coordinates of e are i.i.d. random variables, it is 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 $1 \leq j \leq n$,

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

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 $\mathbb{Z}_5$. 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.

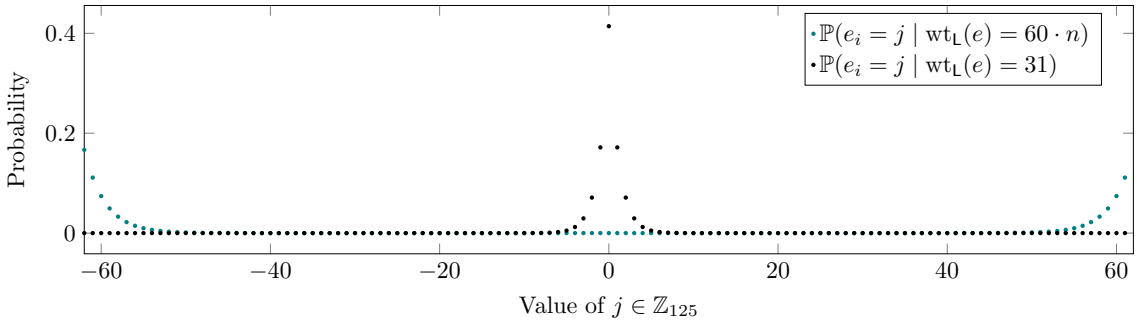

Fig. 3: Given the Lee weight of the vector e, the figure represents the marginal distribution of the i-th entry $e_i \in \mathbb{Z}_{125}$. The black dots represent the marginal distribution of the i-th entry of a vector e with a small Lee weight, while the green dots represent the marginal distribution 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 4.3 and 5.2 do not allow us to transform a CFP instance over $\mathbb{Z}_{p^r}$ into a CFP instance over its

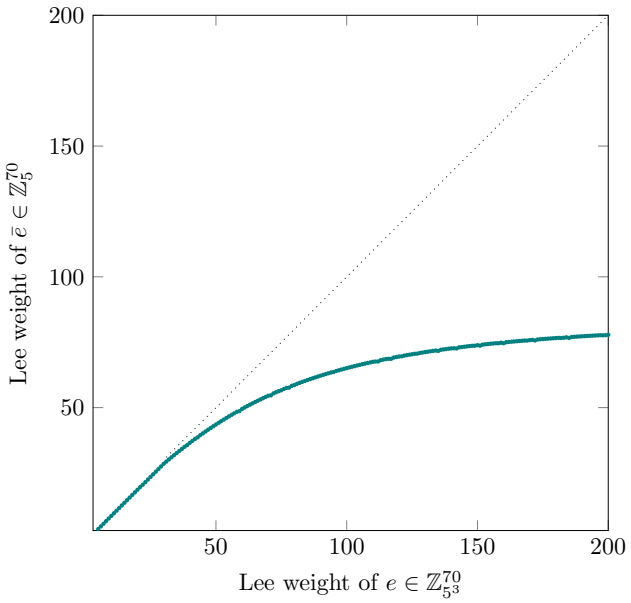

Fig. 4: On the x-axis we put the Lee weight that a vector can assume (truncating this value from above by 200), while on the y-axis we draw (in teal) the expected weight that the same vector will have once projected on the base field. To better illustrate how the weight decreases after the projection, the dashed black line represents the Hamming weight of e before projection.

residue 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 matrix 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 [16], 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 code $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^n$ with minimum distance $d(\mathcal{C})$ and let $\mathcal{C}_i$ be the i-th filtration subcode with minimum distance $d(\mathcal{C}_i)$. 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, $d(\mathcal{C}_i)$ and $d(\overline{\mathcal{C}}_i)$ differs, and, in particular $d(\overline{\mathcal{C}}_i) < d(\mathcal{C}_i)$. 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 weight 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 matrix $H \in \mathbb{Z}_4^{(n-k_0)\times n}$. Moreover, let $\mathcal{C}_1$ be the socle of $\mathcal{C}$ and denote with $d(\mathcal{C})$ and $d(\mathcal{C}_1)$ the minimum Lee 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 $\mathbb{Z}_2$. From Equation 3, we get $d(\mathcal{C}) \leq 2d_{\mathsf{H}}(\mathcal{C})$, where $d_{\mathsf{H}}(\mathcal{C})$ denotes minimum the Hamming distance of $\mathcal{C}$. Moreover, recall that, over $\mathbb{Z}_2$, the Lee metric coincides to the Hamming metric. Therefore, $d(\overline{\mathcal{C}}_1) = d_{\mathsf{H}}(\mathcal{C}_1) \geq d_{\mathsf{H}}(\mathcal{C})$ 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 $\overline{e}^{(1)}$ 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: the code's subtype (k_0, k_1), the $(n-k_0) \times n$ parity-check matrix H over $\mathbb{Z}_4$, $s \in \mathbb{Z}_4^{n-k_0}$, $w \in \mathbb{N}$

Output: Vector $e \in \mathbb{Z}_4^n$ such that $\mathrm{wt}_{\mathsf{L}}(e) \leq w$ 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 $\leq \overline{w}^{(1)}$ and code's dimension $k_0 + k_1$, 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 $\mathrm{wt}_{\mathsf{L}}(s_1) \leq w$ **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 $d(\overline{\mathcal{C}}) = 36$. 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 $\overline{\mathcal{C}}_1$.

The previous example considers a code whose length is smaller than the size of the alphabet, which may lead to behaviors that differ from those observed in other parameter regimes. 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 (4) we get that, for any $w < d$,

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

and hence,

$$p^{n-k} < \sqrt{B_{\mathsf{L}}(\mathbb{Z}_{p^2}, n, w)} \ . \tag{16}$$

Given, $w = \lfloor \frac{d-1}{2} \rfloor$, consider the SDP instance $\mathsf{SDP}_{\mathsf{L}}(\mathbb{Z}_{p^2}, H, s, w)$ 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 (16), it is sufficient to prove that

$$\sqrt{B_{\mathsf{L}}(\mathbb{Z}_{p^2}, n, d/2)} < B_{\mathsf{L}}(\mathbb{Z}_p, n, d/2) \ . \tag{17}$$

Therefore, if there exist values of n, p, and k for which Equation (17) 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 $\overline{e}^{(1)}$.*

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. In particular, the proposed algorithms leverage the filtration subcodes to achieve a speed-up in decoding. Specifically, for both the Hamming and rank metrics, we showed that projecting the problem onto a smaller alphabet, solving the projected instance, and then lifting the solution back is more efficient than applying ISD directly. Although a similar result holds for Lee-metric codes over $\mathbb{Z}_4$, the scenario becomes more complex for Lee-metric codes over $\mathbb{Z}_{p^r}$ with $p^r > 4$. Projecting too deeply into the filtration can lead to an intractable decoding problem. Therefore, an interesting direction for future work is to identify the optimal stopping point in the filtration, deep enough to reduce the decoding instance while still maintaining tractability.

Additionally, it is well known that non-free codes typically do not perform as well as free codes. For instance, non-free code requires larger generator matrices to span the same number of codewords. Furthermore, certain ISD algorithms take advantage of their additional algebraic structure to enhance decoding performance. A notable example is the s-blocks algorithm for the Lee metric [67], which leverages the subtype of the code, to speed up the decoding process. This strategy allows the algorithm to outperform all known decoding methods for non-free codes, achieving significantly

lower complexity for non-free codes compared to free codes with the same parameters. On the other hand, to the best of our knowledge, the ISD algorithms designed for the Hamming and rank metrics rely solely on the code's rank and do not consider its subtype. Consequently, they yield the same computational complexity for both free and non-free codes. As a future direction of work, it would be interesting to investigate whether the s-blocks strategy, which exploits the code's subtype, can be adapted to other metrics such as rank and Hamming. Moreover, it would be worth exploring whether the projection technique and the s-blocks approach can be combined to achieve an additional speed-up in decoding.
Finally, the problem of finding codewords of small Hamming weight has an analogue in the Euclidean lattice setting, namely the problem of finding a short vector with respect to the Euclidean norm. A key class of algorithms for this task in lattices are Sieving algorithms, and recent works [23, 33, 41] have adapted Sieving techniques from lattices to codes. A promising direction for future research is to investigate whether such techniques can be extended to the ring-linear setting. It would also be interesting to explore potential connections between the decoding strategies proposed in this work and existing sieving-style ISD algorithms.

Acknowledgments

The authors 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 also thank Hannes Bartz and Daniele De Bernardini for their 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 first and second authors are members of the INdAM Research Group GNSAGA. The first and second authors conducted the majority of this research at the University of Trento, Trento, Italy. The first author is currently affiliated with the Institute of Communication and Navigation, German Aerospace Center, Oberpfaffenhofen, Germany. The second author is currently affiliated with the University of Bari Aldo Moro, Bari, Italy. The authors thank the reviewers for their thorough comments and suggestions.

References

[1] M. Abspoel, R. Cramer, I. Damgård, D. Escudero, M. Rambaud, C. Xing, and C. Yuan. Asymptotically good multiplicative LSSS over Galois rings and applications to MPC over $\mathbb{Z}/p^k\mathbb{Z}$. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 151–180. Springer, 2020.

[2] C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, G. Zémor, A. Couvreur, and A. Hauteville. Rank quasi cyclic (RQC). *Second Round submission to NIST Post-Quantum Cryptography call*, 2020.

[3] N. Aragon, P. Gaborit, A. Hauteville, and J.-P. Tillich. A new algorithm for solving the rank syndrome decoding problem. In *2018 IEEE International Symposium on*

Information Theory (ISIT), pages 2421–2425. IEEE, 2018.

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

[5] N. S. Babu and K.-H. Zimmermann. Decoding of linear codes over Galois rings. *IEEE Transactions on Information Theory*, 47(4):1599–1603, 2001.

[6] A. Barg. Complexity issues in coding theory. *Handbook of Coding theory*, 1: 649–754, 1998.

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

[8] S. Barg. Some new NP-complete coding problems. *Probl. Inf. Transm.*, 30(3): 209–214, 1994. ISSN 0032-9460.

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

[10] J. Bariffi, K. Khathuria, and V. Weger. Information set decoding for Lee-metric codes using restricted balls. In *Code-Based Cryptography Workshop*, pages 110–136. Springer, 2022.

[11] J. Bariffi, H. Bartz, G. Liva, and J. Rosenthal. Error-correction performance of regular ring-linear LDPC codes over Lee channels. *IEEE Transactions on Information Theory*, 2024.

[12] A. Becker, A. Joux, A. May, and A. Meurer. 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*, pages 520–536. Springer, 2012.

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

[14] M. Bombar, D. Bui, G. Couteau, A. Couvreur, C. Ducros, and S. Servan-Schreiber. FOLEAGE: $\mathbb{F}_4$ OLE-based multi-party computation for Boolean Circuits. *Cryptology ePrint Archive*, 2024.

[15] E. Byrne and P. Fitzpatrick. Hamming metric decoding of alternant codes over Galois rings. *IEEE Transactions on Information Theory*, 48(3):683–694, 2002.

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

[17] R. Canto-Torres and J.-P. Tillich. Speeding up decoding a code with a non-trivial automorphism group up to an exponential factor. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 1927–1931. IEEE, 2019.

[18] Á. L. M. Castañeda, N. Decastro-García, and M. V. Carriegos. Decoding convolutional codes over finite rings. A linear dynamical systems approach. *arXiv preprint arXiv:2411.18316*, 2024.

[19] F. Chabaud and J. Stern. 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*, pages 368–381. Springer, 1996.

[20] A. Chailloux, T. Debris-Alazard, and S. Etinski. 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*, pages 44–62. Springer, 2021.

[21] R. Cramer, M. Rambaud, and C. Xing. Asymptotically-good arithmetic secret sharing over $\mathbb{Z}/p^{\ell}\mathbb{Z}$ with strong multiplication and its applications to efficient MPC. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part III 41*, pages 656–686. Springer, 2021.

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

[23] L. Ducas, A. Esser, S. Etinski, and E. Kirshanova. Asymptotics and improvements of sieving for codes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 151–180. Springer, 2024.

[24] D. Escudero, C. Hong, H. Liu, C. Xing, and C. Yuan. Degree-d reverse multiplication-friendly embeddings: Constructions and applications. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 106–138. Springer, 2023.

[25] J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc, and J.-P. Tillich. Folding alternant and Goppa Codes with non-trivial automorphism groups. *IEEE Transactions on Information Theory*, 62(1):184–198, 2015.

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

[27] P. Gaborit and G. Zémor. On the hardness of the decoding and the minimum distance problems for rank codes. *IEEE Transactions on Information Theory*, 62

(12):7245–7252, 2016.

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

[29] D. Gardy and P. Solé. Saddle point techniques in asymptotic coding theory. In *Workshop on Algebraic Coding*, pages 75–81. Springer, 1991.

[30] C. Gentry. Key recovery and message attacks on NTRU-composite. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 182–194. Springer, 2001.

[31] J. Gómez-Torrecillas, F. Lobillo, and G. Navarro. Decoding Linear Codes over Chain Rings given by Parity Check Matrices. *Mathematics*, 9(16):1878, 2021.

[32] M. Greferath and U. Vellbinger. Efficient decoding of $\mathbb{Z}_{p^k}$-linear codes. *IEEE Transactions on Information Theory*, 44(3):1288–1291, 1998.

[33] Q. Guo, T. Johansson, and V. Nguyen. A new sieving-style information-set decoding algorithm. *IEEE Transactions on Information Theory*, 2024.

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

[35] A.-L. Horlemann-Trautmann and V. Weger. Information set decoding in the Lee metric with applications to cryptography. *Advances in Mathematics of Communications*, 15(4):677–699, 2020.

[36] F. Hörmann and W. van Woerden. FuLeakage: breaking Fuleeca by learning attacks. In *Annual International Cryptology Conference*, pages 253–286. Springer, 2024.

[37] J. C. Interlando, R. Palazzo, and M. Elia. On the decoding of Reed-Solomon and BCH codes over integer residue rings. *IEEE Transactions on Information Theory*, 43(3):1013–1021, 1997.

[38] H. T. Kalachi and H. T. Kamche. On the rank decoding problem over finite principal ideal rings. *Advances in Mathematics of Communications*, 18(5):1492–1513, 2024. ISSN 1930-5346.

[39] H. T. Kamche and H. T. Kalachi. On the Generalizations of the Rank Metric over Finite chain rings. In *International Conference on Cryptology in Africa*, pages 201–221. Springer, 2024.

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

[41] E. Kirshanova and T. Laarhoven. Lower bounds on lattice sieving and information set decoding. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part II 41*, pages 791–820. Springer, 2021.

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

[43] P. J. Lee and E. F. Brickell. 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*, pages 275–280. Springer, 1988.

[44] H. Liu, X. Wang, K. Yang, and Y. Yu. 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*, pages 149–179. Springer, 2024.

[45] H.-A. Loeliger. An upper bound on the volume of discrete spheres. *IEEE transactions on information theory*, 40(6):2071–2073, 1994.

[46] P. Loidreau. Properties of codes in rank metric. *arXiv preprint cs/0610057*, 2006.

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

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

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

[50] C. A. Melchor, N. Aragon, M. Bardet, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, A. Otmani, et al. Rollo-rank-Ouroboros, Lake & Locker. *Round-2 submission to the NIST PQC project*, 2019.

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

[52] G. Norton and A. Sălăgean. On the Structure of Linear and Cyclic Codes over a Finite Chain Ring. *Applicable Algebra in Engineering, Communication and Computing*, 10:489–506, 07 2000.

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

[54] A. V. Ourivski and T. Johansson. New technique for decoding codes in the rank metric and its cryptography applications. *Problems of Information Transmission*,

38:237–246, 2002.

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

[56] Y. H. Park. Modular independence and generator matrices for codes over. *Designs, codes and Cryptography*, 50(2):147–162, 2009.

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

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

[59] S. Puchinger, J. Renner, A. Wachter-Zeh, and J. Zumbrägel. Efficient decoding of Gabidulin codes over Galois rings. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 25–30. IEEE, 2021.

[60] B. S. Rajan and M. Siddiqi. Transform decoding of BCH codes over $\mathbb{Z}_m$. *International Journal of Electronics Theoretical and Experimental*, 75(6):1043–1054, 1993.

[61] J. Renner, S. Puchinger, A. Wachter-Zeh, C. Hollanti, and R. Freij-Hollanti. Low-rank parity-check codes over the ring of integers modulo a prime power. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 19–24. IEEE, 2020.

[62] J. Renner, A. Neri, and S. Puchinger. Low-rank parity-check codes over Galois rings. *Designs, Codes and Cryptography*, 89(2):351–386, 2021.

[63] S. Ritterhoff, G. Maringer, S. Bitzer, V. Weger, P. Karl, T. Schamberger, J. Schupp, and A. Wachter-Zeh. FuLeeca: a Lee-based signature scheme. In *Code-Based Cryptography Workshop*, pages 56–83. Springer, 2023.

[64] J. Rosenthal. An algebraic decoding algorithm for convolutional codes. In *Dynamical Systems, Control, Coding, Computer Vision: New Trends, Interfaces, and Interplay*, pages 343–360. Springer, 1999.

[65] R. M. Roth. Introduction to Coding Theory. *IET Communications*, 47(18-19):4, 2006.

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

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