Applicable Algebra in Engineering, Communication and Computing
https://doi.org/10.1007/s00200-024-00652-8

ORIGINAL PAPER

Solving systems of algebraic equations over finite commutative rings and applications

Hermann Tchatchiem Kamche[1] · Hervé Talé Kalachi[2]

Received: 11 September 2023 / Revised: 16 January 2024 / Accepted: 19 February 2024

Abstract

Several problems in algebraic geometry and coding theory over finite rings are modeled by systems of algebraic equations. Among these problems, we have the rank decoding problem, which is used in the construction of public-key cryptosystems. A finite chain ring is a finite ring admitting exactly one maximal ideal and every ideal being generated by one element. In 2004, Nechaev and Mikhailov proposed two methods for solving systems of polynomial equations over finite chain rings. These methods used solutions over the residue field to construct all solutions step by step. However, for some types of algebraic equations, one simply needs partial solutions. In this paper, we combine two existing approaches to show how Gröbner bases over finite chain rings can be used to solve systems of algebraic equations over finite commutative rings. Then, we use skew polynomials and Plücker coordinates to show that some algebraic approaches used to solve the rank decoding problem and the MinRank problem over finite fields can be extended to finite principal ideal rings.

Keywords Finite commutative rings · Gröbner bases · MinRank problem · Rank decoding problem · Systems of algebraic equations

Mathematics Subject Classification 13M10 · 94B05 · 94A60

✉ Hervé Talé Kalachi
herve.tale@univ-yaounde1.cm

Hermann Tchatchiem Kamche
hermann.tchatchiem@gmail.com

[1] Institute of mathematics, University of Neuchatel, Neuchâtel, Switzerland

[2] Department of Computer Engineering, National Advanced School of Engineering of Yaoundé, Yaoundé, Cameroon

Published online: 24 April 2024

1 Introduction

Solving systems of algebraic equations has always been of high interest in algorithmic algebra. Indeed, many algebraic problems have their solution sets contained in those of systems of algebraic equations. A tangible example is the rank decoding problem [25], which has attracted a lot of attention this last decade in view of its application in cryptography. This problem is generally defined over finite fields and therefore, leads to the problem of solving systems of algebraic equations over finite fields when modeled appropriately. But it should be remembered that this latest problem has been studied for a long time and has a wide variety of algorithms that can be used to solve it and also estimate the solving complexities [14, 17, 20, 21, 26].

Most recently, the rank decoding problem has been extended to finite principal ideal rings in [29] where the authors, after having justified the interest of studying this problem over finite rings, show that it is at least as hard as the rank decoding problem over finite fields, and also provide a combinatorial type algorithm for solving this new problem. The translation of the rank decoding problem over finite rings as a system of algebraic equations naturally induces the problem of solving systems of algebraic equations over finite rings.

Contrary to the problem of solving systems of algebraic equations over finite fields, the previous problem over finite rings has not experienced much development. The most advanced and recent work is the paper of Mikhailov and Nechaev [40], who proposed two approaches for solving systems of polynomial equations over finite chain rings. One of these approaches uses canonical generating systems, which are not Gröbner bases in general. An algebraic modeling of the rank decoding problem over finite chain rings that we will use is a system of algebraic equations with some parameters, and we just need a partial solution. Note that Gröbner bases over fields are generally used to solve these kinds of systems. A natural question is therefore to know whether Gröbner bases can be used to solve systems of algebraic equations over finite chain rings in general, as in the case of finite fields.

Independently, Gröbner bases over finite chain rings have been much studied and implemented in some mathematical software systems like Magma [9], SageMath [51], etc. Indeed, similar to Buchberger's algorithm over fields [11], Norton and Salagean [45] gave an algorithm for computing Gröbner bases over finite chain rings. This algorithm has been improved in [28] by adding the product criterion and the chain criterion. In the Magma handbook [9], it was specified that the F_4 algorithm [20] was extended over Euclidean rings,[1] taking into account the elimination criteria given in [41]. Moreover, the elimination theorem, which is the main property used to solve systems of algebraic equations, can be extended over finite chain rings. However, the elimination theorem does not hold in general on other types of finite rings. But we must not forget that low-rank parity-check codes which are potential linear codes for rank-based cryptography have been extended to finite commutative rings [30, 32, 49]. Thus, it also

[1] Note that Euclidean rings in Magma also contain rings with zero divisors like Galois rings.

becomes necessary to tackle the resolution of systems of algebraic equations over finite commutative rings.

According to the structure theorem for finite commutative rings [39], every finite commutative ring is isomorphic to a product of finite commutative local rings. Thus, solving systems of algebraic equations over finite commutative rings is reduced to finite local rings. In [13], Bulyovszky and Horváth gave a good method for solving systems of linear equations over finite local rings. Indeed, they transformed systems of linear equations from local rings to Galois rings and used the Hermite normal form to solve it. In this work we show that this transformation can be applied to systems of algebraic equations, and we then use Gröbner bases to solve the resulting equation since Galois rings are specific cases of finite chain rings.

Before one can use Gröbner bases over finite chain rings to solve the rank decoding problem, it is first necessary to give an algebraic modeling. As specified in [29], some properties of the rank for matrices over fields do not extend to matrices over rings in general due to zero divisors. Therefore, the algebraic modeling of the rank decoding problem given in [5] using the MaxMinors cannot be directly applied to rings. However, in [25] other algebraic modeling using linearized polynomials has been given and some main properties of linearized polynomials have been extended in [31] over finite principal ideal rings. We will use these results to prove that the algebraic modeling done in [25] using linearized polynomials can be generalized over finite principal ideal rings. Furthermore, as the rank decoding problem reduces to the MinRank problem [23], we also study possible algebraic modelings of the MinRank problem over finite rings.

The MinRank problem have several algebraic modelings over fields. For example, the MaxMinors modeling [22], the Kipnis–Shamir modeling [34], or the Support-Minors modeling [5]. Over finite chain rings, the rank of a matrix is not generally equal to the order of the highest order non-vanishing minor. Thus, the MaxMinors modeling cannot directly extend over rings. However, we will use the rank decomposition and the Plücker coordinates to show that the Kipnis–Shamir modeling and the Support-Minors modeling can be extended to finite principal ideal rings.

The rest of the paper is organized as follows. In Sect. 2, we give some preliminary notions on Gröbner bases over finite chain rings, followed by the use of Gröbner bases for solving systems of algebraic equations over finite chain rings in Sect. 3. In Sect. 4 we show how to solve systems of algebraic equations over finite commutative local rings by decomposing them as a direct sum of cyclic modules over Galois rings. Section 5 uses the fact that the row span of a matrix is contained in a free module of the same rank to prove that the Kipnis–Shamir Modeling and the Support Minors Modeling of the MinRank problem can be extended to finite principal ideal rings. In Sect. 6, skew polynomials are used to give an algebraic modeling of the rank decoding problem over finite principal ideal rings, and to finish, we conclude the paper and give some perspectives in Sect. 7.

2 Preliminaries

2.1 Finite chain rings

A chain ring is a ring whose ideals are linearly ordered by inclusion, and a local ring is a ring with exactly one maximal ideal. By [39], a finite ring is a chain ring if and only if it is a local principal ideal ring, that is to say a finite ring admitting exactly one maximal ideal and every ideal being generated by one element. A basic example of finite chain rings is the ring $\mathbb{Z}_{p^k} = \mathbb{Z}/p^k\mathbb{Z}$ of integers modulo a power of a prime number p. Its maximal ideal is $p\mathbb{Z}_{p^k}$. Other examples of finite chain rings that we will use to give a representation of finite commutative local rings in Sect. 4 are Galois rings. A Galois ring of characteristic p^k and rank r, denoted by $GR\left(p^k, r\right)$, is the ring $\mathbb{Z}_{p^k}[X]/(f)$, where $f \in \mathbb{Z}_{p^k}[X]$ is a monic polynomial of degree r, irreducible modulo p, and (f) being the ideal of $\mathbb{Z}_{p^k}[X]$ generated by f. Thus, $GR\left(p^k, r\right)$ is a degree r Galois extension of $\mathbb{Z}_{p^k}$ and is a finite chain ring with maximal ideal generated by p and residue field $\mathbb{F}_{p^r} = GR\left(p^k, r\right)/pGR\left(p^k, r\right)$ [39].

In this section, we assume that R is a finite commutative chain ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}_q = R/\mathfrak{m}$. We denote by π a generator of $\mathfrak{m}$, and ν the nilpotency index of π, i.e., the smallest positive integer such that $\pi^\nu = 0$. An important property of finite chain rings is the structure of their ideals. Every ideal of R is of the form $\pi^i R$, for $i = 0, \dots, \nu$. A direct consequence is the following decomposition of any element from R. Let $a, b \in R$. We say that a is congruent to b modulo π and denote it by $a \equiv b(mod\ \pi)$, if there exists c in R such that $a = b + c\pi$. This relation is equivalent to $\varphi(a) = \varphi(b)$ where $\varphi : R \longrightarrow R/\mathfrak{m}$ is the canonical projection. Let Γ be a complete set of representatives of the equivalence classes of R under the congruence modulo π. As in [40], we have for example $\Gamma = \{a \in R : a^q = a\}$.

Proposition 1 *Let c in R, then c has a unique representation in the form*

$$c = \sum_{j=0}^{\nu-1} c_j \pi^j \tag{1}$$

where $c_j \in \Gamma$, for $j = 0, \dots, \nu - 1$.

The representation of c given by Eq. (1) is called the $\pi-$adic decomposition of c. Let $j \in \{0, \dots, \nu - 1\}$, and the map $\gamma_j : R \longrightarrow \Gamma$ given by $c \longmapsto c_j$, that is to say $\gamma_j(c) := c_j$ and $c = \sum_{j=0}^{\nu-1} \gamma_j(c)\pi^j$. For l in $\{1, \dots, \nu - 1\}$ we set $c^{[l]} = \sum_{j=0}^{l-1} \gamma_j(c)\pi^j$. The $\pi-$adic decomposition will be used is Sect. 3 to solve algebraic equations. Note that this decomposition depends on the choice of π.

Example 1 The ring $\mathbb{Z}_8$ is a finite chain ring where the maximal ideal is generated by 2, with nilpotency index 3. The residue field of $\mathbb{Z}_8$ is $\mathbb{F}_2 = \mathbb{Z}_8/2\mathbb{Z}_8$ and a complete set of representatives of the equivalence classes of $\mathbb{Z}_8$ under the congruence modulo

2 is $\Gamma = \{0, 1\}$. The 2–adic decomposition of 6 is $6 = 0 \times 2^0 + 1 \times 2^1 + 1 \times 2^2$. The maximal ideal is also generated by 6 and the 6–adic decomposition of 6 is $6 = 0 \times 6^0 + 1 \times 6^1 + 0 \times 6^2$.

2.2 Gröbner bases

The ring of polynomials with k indeterminates $x_1, \ldots, x_k$ and coefficients in R is denoted $R\left[x_1, \ldots, x_k\right]$. A monomial is an element of $R\left[x_1, \ldots, x_k\right]$ of the form $x^\alpha := x_1^{d_1} \cdots x_k^{d_k}$ where the d_i's are non-negative integers and $\alpha = \left(d_1, \ldots, d_k\right)$. If ">" is an admissible order on the set of monomials, then any element f in $R\left[x_1, \ldots, x_k\right] \backslash \{0\}$ can be written uniquely as $f = \sum_{i=1}^{s} c_i x^{\alpha_i}$ where each x^{α_i} is a monomial, $c_i \in R$, and $x^{\alpha_1} > \cdots > x^{\alpha_s}$. The leading term of f is defined by $lt(f) := c_1 x^{\alpha_1}$. For $W \subset R\left[x_1, \ldots, x_k\right]$, we denote by $lt(W)$ the ideal generated by $\{lt(w) \mid w \in W\}$. According to [46, Definition 3.8], we have the following definition.

Definition 1 Let I be an ideal in $R\left[x_1, \ldots, x_k\right]$ and G a subset of I.

(a) G is called a Gröbner basis for I if $lt(G) = lt(I)$.

(b) G is called a strong Gröbner basis for I if for all $f \in I$ there exists $g \in G$ such that $lt(g)$ divides $lt(f)$, that is to say $lt(f) = cx^\alpha lt(g)$ where $c \in R$ and x^α is a monomial.

In [46, Proposition 3.9] a connection between Gröbner bases and strong Gröbner bases was given over finite chain rings.

Proposition 2 *A subset of $R\left[x_1, \ldots, x_k\right]$ is a Gröbner basis if and only if it is a strong Gröbner basis.*

Similar to Buchberger's algorithm over fields, Norton and Salagean gave an algorithm in [45, Algorithme 3.9] to compute Gröbner bases over finite chain rings. This algorithm has been improved in [28] by adding the product criterion and the chain criterion. An algorithm for computing Gröbner bases on certain classes of finite rings has been implemented in Magma [9] and SageMath [51].

Example 2 A Gröbner basis for the ideal generated by $\{4x^2y + y^3 + 2y + 4, 4xy^2\}$ in $\mathbb{Z}_8[x, y]$ with lexicographic order $x > y$ can be computed using SageMath, and we get $\{4x^2y + y^3 + 2y + 4, 4xy^2, y^4 + 2y^2 + 4y, 2y^3 + 4y\}$.

3 Solving systems of algebraic equations over finite chain rings

In this section, we assume as in Sect. 2 that R is a finite commutative chain ring with maximal ideal $\mathfrak{m}$ generated by π, residue field $\mathbb{F}_q = R/\mathfrak{m}$, and that ν is the nilpotency index of π. In order to solve systems of polynomial equations, Mikhailov and Nechaev [40] used the lifting approach, which consists of using solutions in the residue field $R/\mathfrak{m}$ to construct solutions in the ring R. However, in some cases this approach is not appropriate in practice, specifically for parametric systems. As an illustration, consider the following system over $\mathbb{Z}_8$:

$$\begin{cases} 4x^2y + y^3 + 2y + 4 = 0 \\ 4xy^2 = 0 \end{cases} \tag{2}$$

This system has 16 solutions. So when we use the lifting approach to solve it, we have to compute each solution step by step, and this is computationally tedious. We will see in this section that one can easily obtain all these solutions using Gröbner bases (see Example 3). The following proposition from [54, Theorem 244], called the elimination theorem, is a direct consequence of Proposition 2.

Proposition 3 *Let G be a Gröbner basis for an ideal I in $R\left[x_1, \dots, x_k\right]$ with the lexicographic order $x_1 > \cdots > x_k$. Then, for all i in $\{1, \dots, k\}$, $G \cap R\left[x_i, \dots, x_k\right]$ is a Gröbner basis of $I \cap R\left[x_i, \dots, x_k\right]$.*

The elimination theorem makes it possible to iteratively solve algebraic systems by eliminating variables. Indeed, consider a system of polynomial equations of the form

$$f_i\left(x_1, \dots, x_k\right) = 0, \quad i = 1, \dots, d. \tag{3}$$

where $f_i\left(x_1, \dots, x_k\right) \in R\left[x_1, \dots x_k\right]$. By Proposition 3, if we compute a Gröbner basis G of the ideal $I = \left(f_1, \dots, f_d\right)$ associated to (3) with the lexicographic order $x_1 > \cdots > x_k$, then G will be of the form $G = G_1 \cup G_2 \cup \cdots \cup G_k$, where $G_1 = \left\{g_{1,1}\left(x_k\right), \dots, g_{1,j_1}\left(x_k\right)\right\}$, $G_2 = \left\{g_{2,1}\left(x_{k-1}, x_k\right), \dots, g_{2,j_2}\left(x_{k-1}, x_k\right)\right\}$, …, $G_k = \left\{g_{k,1}\left(x_1, \dots, x_k\right), \dots, g_{k,j_k}\left(x_1, \dots, x_k\right)\right\}$. So, (3) is equivalent to:

$$\begin{cases} g_{1,1}\left(x_k\right) = \cdots = g_{1,j_1}\left(x_k\right) = 0 \\ g_{2,1}\left(x_{k-1}, x_k\right) = \cdots = g_{2,j_2}\left(x_{k-1}, x_k\right) = 0 \\ \vdots \\ g_{k,1}\left(x_1, \dots, x_k\right) = \cdots = g_{k,j_k}\left(x_1, \dots, x_k\right) = 0 \end{cases} \tag{4}$$

If for all i in $\{1, \dots, k\}$ there exists an element in the Gröbner basis G whose the leading monomial is a pure power of x_i, then each G_i is non-empty and, solving (4) is reduced to successively solving systems of univariate polynomial equations. Recall that this process is similar to the case of fields for zero-dimensional algebraic systems [12, 36]. Note in our case that one can always add some univariate polynomial equations to the system using the following remark.

Remark 1 In [42, Theorem 5.14], the monic polynomial F_m with smaller degree satisfying $F_m(x) = 0$ for all x in R, has been defined. Thus, as in the case of finite fields, to simplify the resolution of (3), one can add the following equations $F_m\left(x_1\right) = \cdots = F_m\left(x_k\right) = 0$. For illustration, see Example 4.

We will now show how to use Gröbner bases over finite chain rings to solve systems of univariate polynomial equations. Recall that a Gröbner basis G is called minimal if no proper subset of G is a Gröbner basis for the ideal generated by G. In [45, Theorem 4.2], a characterization of minimal Gröbner bases in one variable over finite chain rings has been given.

Proposition 4 *Let $G \subset R[x] \backslash \{0\}$. Then G is a minimal Gröbner basis if and only if $G = \left\{u_0\pi^{a_0}g_0, \dots, u_s\pi^{a_s}g_s\right\}$ for some $0 \le s \le \nu - 1$, $u_i \in R$ and $g_i \in R[x]$ for $i = 0, \dots, s$ and such that*:

(i) $0 \le a_0 < a_1 < \cdots < a_s \le \nu - 1$ *and for $i = 0, \dots, s$, u_i is a unit*;
(ii) *for $i = 0, \dots, s$, g_i is monic*;
(iii) $\deg\left(g_i\right) > \deg\left(g_{i+1}\right)$ *for any $i \in \{0, \dots, s-1\}$*;
(iv) *for $i = 0, \dots, s-1$, $\pi^{a_{i+1}}g_i$ is in the ideal generated by $\left\{\pi^{a_{i+1}}g_{i+1}, \dots, \pi^{a_s}g_s\right\}$.*

As specified in [40], a minimal Gröbner basis in one variable over finite chain rings is a canonical generating system. Therefore, according to Proposition 4, we can use [40, Algorithm 2] to solve systems of univariate polynomial equations over finite chain rings using Gröbner bases. Specifically, consider a system of univariate polynomial equations of the form

$$f_i(x) = 0, \qquad i = 1, \dots, r \tag{5}$$

where $f_i(x) \in R[x]$. Assume that a minimal Gröbner basis of the ideal generated by $\left\{f_1(x), \dots, f_r(x)\right\}$ is $G = \left\{u_0\pi^{a_0}g_0, \dots, u_s\pi^{a_s}g_s\right\}$ as in Proposition 4. As specified in [40, page 64] we can assume that $a_0 = 0$. Set $h_j = g_i$, for $0 \le i \le s$ and $a_i \le j < a_{i+1}$, where $a_{s+1} = \nu$. Then, Eq. (5) is equivalent to the following system of polynomial equations:

$$\pi^j h_j(x) = 0, \qquad j = 0, \dots, \nu - 1. \tag{6}$$

Like in [40, Theorem 8] and [40, Equation (54)], we will use the derivation $Dh_j(x)$ of $h_j(x)$ to solve Eq. (6). As specified in Proposition 1, every element c in R, has a unique $\pi-$adic decomposition $c = \sum_{j=0}^{\nu-1} \pi^j\gamma_j(c)$ where $\gamma_j(c) \in \Gamma$.

Proposition 5 *An element c in R, is a solution of (6) if and only if $\gamma_0(c)$ is a solution in Γ of the polynomial equation*

$$h_{\nu-1}(x) \equiv 0 \ (mod\ \pi),$$

and for $j \in \{1, \dots, \nu - 1\}$, $\gamma_j(c)$ is a solution in Γ of the linear equation:

$$Dh_{\nu-j-1}\left(\gamma_0(c)\right)x \equiv -\gamma_j\left(h_{\nu-j-1}\left(c^{[j]}\right)\right) \ \ (mod\ \pi).$$

According to Propositions 3 and 5, to solve a system of multivariate polynomial equations over finite chain rings, we can compute a Gröbner basis of the associated system with the lexicographic order and find the solutions by successively solving the resulting systems of univariate polynomial equations. We will see in Sects. 5 and 6 that this approach is appropriate for some systems of algebraic equations when we just need a partial solution.

Example 3 Let us solve System (2) over $\mathbb{Z}_8$ using Gröbner bases. According to Example 2, a Gröbner basis with the lexicographic order $x > y$ of the ideal I generated by $\left\{4x^2y + y^3 + 2y + 4, 4xy^2\right\}$ is $G = \left\{g_{1,1}, g_{1,2}, g_{2,1}, g_{2,2}\right\}$ where $g_{1,1}(y) = y^4 + 2y^2 + 4y$, $g_{1,2}(y) = 2y^3 + 4y$, $g_{2,1}(x, y) = 4x^2y + y^3 + 2y + 4$, $g_{2,2}(x, y) = 4xy^2$. By Proposition 3, a Gröbner basis of $I \cap R\left[y\right]$ is $G_1 = G \cap R\left[y\right] = \left\{g_{1,1}(y), g_{1,2}(y)\right\}$. So, we can use G_1 to find the partial solution y of (2). The system

$$g_{1,1}(y) = g_{1,2}(y) = 0$$

is equivalent to

$$h_{1,1}(y) = 2h_{1,2}(y) = 4h_{1,3}(y) = 0 \tag{7}$$

where $h_{1,1}(y) = g_{1,1}(y)$ and $h_{1,2}(y) = h_{1,3}(y) = y^3 + 2y$. Let c be a solution of (7). We have $c = \gamma_0(c) + 2\gamma_1(c) + 4\gamma_2(c)$ where $\gamma_j(c) \in \Gamma = \{0, 1\}$ for $j \in \{0, 1, 2\}$. By Proposition 5, $\gamma_0(c)$ is a solution in Γ of the equation $h_{1,3}(c) \equiv 0\ (mod\ 2)$. So, $\gamma_0(c) = 0$. By Proposition 5, $\gamma_1(c)$ is a solution in Γ of the equation $Dh_{1,2}\left(\gamma_0(c)\right)y \equiv -\gamma_1\left(h_{1,2}\left(c^{[1]}\right)\right)\ (mod\ 2)$. We have $c^{[1]} = \gamma_0(c) = 0$, $h_{1,2}\left(c^{[1]}\right) = 0$, $\gamma_1\left(h_{1,2}\left(c^{[1]}\right)\right) = 0$, $Dh_{1,2}(y) = 3y^2 + 2$, and $Dh_{1,2}\left(\gamma_0(c)\right) = 2$. Therefore, $\gamma_1(c)$ is a solution of $2y \equiv 0\ (mod\ 2)$. So, $\gamma_1(c) \in \{0, 1\}$. Using the same reasoning, for $\gamma_1(c) = 0$ or $\gamma_1(c) = 1$, we compute $\gamma_2(c) \in \{0, 1\}$. Therefore, $c \in \{0, 2, 4, 6\}$. Thus, the partial solution y of (2) is in $\{0, 2, 4, 6\}$. To find the partial solution x corresponding for example to $y = 0$, we must first compute a Gröbner basis of $\left\{g_{2,1}(x, 0), g_{2,2}(x, 0)\right\}$. But for all x in $\mathbb{Z}_8$, $g_{2,1}(x, 0) = 4 \neq 0$, $g_{2,1}(x, 4) = 4 \neq 0$, $g_{2,1}(x, 2) = g_{2,2}(x, 2) = 0$, and $g_{2,1}(x, 6) = g_{2,2}(x, 6) = 0$. Thus, y is in $\{2, 6\}$ and the solution set of (2) is $\left\{(t, 2), (t, 6), t \in \mathbb{Z}_8\right\}$.

As noted in Remark 1, in certain cases it is necessary to add some equations to solve the system. The following example is an illustration.

Example 4 Consider again the system (2) over $\mathbb{Z}_8$. A Gröbner basis with the lexicographic order $y > x$ of the ideal I generated by $\left\{4x^2y + y^3 + 2y + 4, 4xy^2\right\}$ is once again the set $\left\{4x^2y + y^3 + 2y + 4, 4xy^2\right\}$. Consequently, $I \cap \mathbb{Z}_8[x] = \{0\}$. So, we cannot solve Eq. (2) directly by using only Proposition 5 with the lexicographic order $y > x$. However, according to [42, Theorem 5.14], the monic polynomial F_m for the ring $\mathbb{Z}_8$ is defined by $F_m(x) = \left(x^2 - x\right)^2 - 2\left(x^2 - x\right)$. A Gröbner basis with the lexicographic order $y > x$ of the ideal generated by $\left\{4x^2y + y^3 + 2y + 4, 4xy^2, F_m(x), F_m(y)\right\}$ is $\left\{y^2 + 4, 2y + 4, F_m(x)\right\}$. Therefore, (2) is equivalent to $y^2 + 4 = 2y + 4 = 0$. We solve the system $y^2 + 4 = 2y + 4 = 0$ using

Proposition 5, and we obtain $y = 2$ or $y = 6$. Thus, the solutions of (2) are the elements of $\left\{(t,2),(t,6), t \in \mathbb{Z}_8\right\}$.

4 Solving systems of algebraic equations over finite commutative local rings

In the previous section, we have used Gröbner bases to show how one can solve systems of algebraic equations over finite chain rings. We will now show that solving systems of algebraic equations over finite commutative rings can be reduced to finite chain rings. According to [39, Theorem VI.2], if R is a finite commutative ring, then R can be decomposed as a direct sum of local rings, that is to say $R \cong R_{(1)} \times \cdots \times R_{(\rho)}$ where for $j = 1,\dots,\rho$, $R_{(j)}$ is a finite commutative local ring. Thus, the problem of solving systems of algebraic equations over R can be reduced to solving systems of algebraic equations over the various $R_{(j)}$. However, Grö bner basis are not generally equal to strong Gröbner bases over local rings. Therefore, we will use Galois rings, which are specific classes of finite chain rings to represent finite local rings. As specified in [1, 7], finite rings have several representations (the table representation, the basis representation, and the polynomial representation). Galois rings can be used to give the basis representation and the polynomial representation of finite commutative local rings [39, Theorems XVI.2 and XVII.1]. In [13], Bulyovszky and Horváth used the basis representation to give a good method for solving systems of linear equations over finite local rings. We are going to extend this method to systems of multivariate polynomial equations.

In this section, we assume that R is a finite commutative local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}_q = R/\mathfrak{m}$. Set $q = p^\mu$ where p is a prime number. Then the characteristic of R is p^ς where ς is a non-negative integer and by [39, Theorem XVII.1] there is a sub-ring R_0 of R such that R_0 is isomorphic to the Galois ring of characteristic p^ς and cardinality $p^{\mu\varsigma}$. Considering R as a R_0−module, there exist $\theta_1,\dots,\theta_\gamma$ in R such that

$$R = R_0\theta_1 \oplus \cdots \oplus R_0\theta_\gamma. \tag{8}$$

Let j in $\{1,\dots,\gamma\}$. Since every ideal in R_0 is generated by a power of p, then there is ς_j in $\{1,\dots,\varsigma\}$ such that

$$p^{\varsigma_j}R_0 = Ann\left(\theta_j\right) = \left\{a \in R_0 \,:\, a\theta_j = 0\right\}.$$

According to [13, Subsection 2.2] we have the following lemma.

Lemma 1 *Let u in R and u_j in R_0 such that $u = \sum_{j=1}^{\gamma} u_j\theta_j$. The following statements are equivalent*:

(a) $u = 0$;

(b) *for all* $j \in \{1, \ldots, \gamma\}$, $\theta_j u_j = 0$;
(c) *for all* $j \in \{1, \ldots, \gamma\}$, $p^{\varsigma - \varsigma_j} u_j = 0$.

Moreover, each element u_j is unique modulo p^{ς_j}.

Lemma 1 and the basis decomposition (8) can be used to transform a system of multivariate polynomial equations over finite local rings to Galois rings. Specifically, we have the following:

Theorem 1 *Consider a system of polynomial equations of the form*

$$f_r\Big(\big(x_i\big)_{1\leq i\leq k}\Big) = 0, \;\; r = 1, \ldots, d \tag{9}$$

where f_r *are multivariate polynomial functions with coefficients in* R *and* $\big(x_i\big)_{1\leq i\leq k} \in R^k$. *Set*

$$x_i = \sum_{j=1}^{\gamma} x_{i,j}\theta_j, \;\; i = 1, \ldots, k$$

where $x_{i,j} \in R_0$ *and*

$$f_r\Big(\big(x_i\big)_{1\leq i\leq k}\Big) = \sum_{s=1}^{\gamma} f_{r,s}\Big(\big(x_{i,j}\big)_{1\leq i\leq k, 1\leq j\leq \gamma}\Big)\theta_s, \;\; r = 1, \ldots, d$$

where $f_{r,s}$ *are multivariate polynomial functions with coefficients in* R_0. *Then Eq.* (9) *is equivalent to*

$$p^{\varsigma - \varsigma_s} f_{r,s}\Big(\big(x_{i,j}\big)_{1\leq i\leq k, 1\leq j\leq \gamma}\Big) = 0, \;\; r = 1, \ldots, d, \; s = 1, \ldots, \gamma. \tag{10}$$

Since Galois rings are specific cases of finite chain rings, we can use the methods described in Sect. 3 to solve (10).

Example 5 In this example we consider a local ring of size 16 which is not a finite chain ring. As specified in [38], we can choose $R = \mathbb{Z}_8[X]/I$ where I is the ideal generated by $X^2 + 4$ and $2X$. Then R is a local ring with the maximal ideal generated by $2 + I$ and $X + I$. Set $\theta = X + I$, then a maximal Galois sub-ring of R is $R_0 = \mathbb{Z}_8$ and we have $R = \theta_1 R_0 \oplus \theta_2 R_0$ where $\theta_1 = 1$ and $\theta_2 = \theta$. Moreover, $Ann\big(\theta_1\big) = \{0\} = 2^3 R_0$ and $Ann\big(\theta_2\big) = 2R_0$. We would like to find the roots of the polynomial function defined over R by

$$P(x) = x^3 + 2x + 4.$$

The residue field of R is $\mathbb{F}_2$ and the projection over $\mathbb{F}_2$ of $P(x)$ is $\overline{P}(x) = x^3$ which is not square-free. Therefore, we are not able to find the roots of P using methods based on the Hensel's lemma [39, Theorem XIII.4] or the Newton-Hensel's lemma [24, Proposition 2.1.9]. Thus, an alternative method is to use Theorem 1. Set $x = x_1 + x_2\theta$ where x_1 and x_2 are in R_0. Then,

$$P\left(x_1 + x_2\theta\right) = x_1^3 + 4x_1x_2^2 + 2x_1 + 4 + \theta x_1^2x_2.$$

Therefore, equation

$$x^3 + 2x + 4 = 0$$

is equivalent to the system

$$\begin{cases} x_1^3 + 4x_1x_2^2 + 2x_1 + 4 = 0 \\ 4x_1^2x_2 = 0 \end{cases} \tag{11}$$

Thanks to Example 3, we deduce that the solutions of (11) are the couples $\left(x_1, x_2\right)$ in $\left\{(2, t), (6, t), t \in \mathbb{Z}_8\right\}$. As $2\theta = 0$ and $x = x_1 + x_2\theta$, then x_2 is unique modulo 2. We can therefore choose x_2 in $\{0, 1\}$. Thus, the roots of P are 2, 6, $2 + \theta$, and $6 + \theta$.

Example 5 gave a method for finding the roots of polynomials over finite local rings. Another type of local rings are valuation rings, and some methods based on the truncation orders have been described in [8, 43] for the univariate case and in [15, 35, 52] for the multivariate case.

5 MinRank problem over finite principal ideal rings

In this section, we first justify the interest of studying the algebraic resolution of the MinRank problem over finite principal ideal rings by establishing the fact that it is an NP-complete problem. We then extend some known algebraic modelings of the classical MinRank problem to the MinRank problem over finite principal ideal rings. In what follow, we assume that R is a finite commutative principal ideal ring. The set of all $m \times n$ matrices with entries in the ring R will be denoted by $R^{m\times n}$. Let $\mathbf{A} \in R^{m\times n}$, we denote by $row(\mathbf{A})$ the $R-$submodule of R^n generated by the row vectors of $\mathbf{A}$. The transpose of $\mathbf{A}$ is denoted by $\mathbf{A}^\top$ and the $k \times k$ identity matrix is denoted by $\mathbf{I}_k$.

5.1 MinRank problem

Definition 2 Let $\mathbf{A} \in R^{m\times n}$. The *rank* of $\mathbf{A}$, denoted by $rk_R(\mathbf{A})$ or simply by $rk(\mathbf{A}\ )$ is the smallest number of elements in $row(\mathbf{A})$ which generate $row(\mathbf{A})$ as a $R-$module.

As specified in [31, Proposition 3.4], the Smith normal form can be used to compute the rank of a matrix. Moreover, as in the case of fields, the map $R^{m\times n} \times R^{m\times n} \to \mathbb{N}$, given by $(\mathbf{A{,}B}) \mapsto rk(\mathbf{A} - \mathbf{B})$ is a metric. However, some properties of the rank of a matrix over fields generally do not extend to rings due to zero divisors.

Example 6 Consider the matrix $\mathbf{A} = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$ over $\mathbb{Z}_8$. Then, $rk(\mathbf{A}) = 2$, $rk(6\mathbf{A}) = 1$ and $det(\mathbf{A}) = 0$. Thus, $rk(\mathbf{A}) \neq rk(6\mathbf{A})$ and $rk(\mathbf{A})$ is not equal to the order of the highest-order non-vanishing minor.

The MinRank Problem over the ring R can then be defined as follows.

Definition 3 Let $\mathbf{M}_0, \mathbf{M}_1, \cdots, \mathbf{M}_k$ in $R^{m\times n}$ and r in $\mathbb{N}^*$. The *MinRank problem* is to find $x_1, \dots, x_k$ in R such that $rk(\mathbf{M}_0 + \sum_{i=1}^{k} x_i\mathbf{M}_i) \leq r$. The *homogeneous MinRank problem* corresponds to the case where $\mathbf{M}_0 = \mathbf{0}$.

In general, an instance of the MinRank problem has several solutions. But if r is not greater than the error correction capability of the R–linear code generated by $\mathbf{M}_1, \dots, \mathbf{M}_k$ (assuming $\mathbf{M}_1, \dots, \mathbf{M}_k$ are R–linearly independent), then the problem has a unique solution $\left(x_1, \dots, x_k\right)$. In the homogeneous case, for any solution $\left(x_1, \dots, x_k\right)$ and for any $\alpha \in R$, $\left(\alpha x_1, \dots, \alpha x_k\right)$ is also a solution. Thus, if R is a field, one of the components of a non-zero solution of the homogeneous MinRank problem can always be assumed to be 1. However, if R is not a field, this assumption is not true in some cases (see Example 8).

In [16] Nicolas Courtois used a connection between the Hamming metric and the rank metric to prove that the MinRank problem over fields is NP-complete. We will extend this result to finite principal ideal rings. As in Sect. 4, the finite principal ideal ring R can be decomposed as a direct sum of finite chain rings. So, assume that $R = R_{(1)} \times \cdots \times R_{(\rho)}$ where $R_{(j)}$ is a finite chain ring for $j \in \{1, \dots, \rho\}$. We denote by $\Phi_{(j)}$ the j-th projection map from R to $R_{(j)}$. We also extend $\Phi_{(j)}$ coefficient-by-coefficient as a map from $R^{m\times n}$ to $R_{(j)}^{m\times n}$. We have the following result from [18].

Lemma 2 *Let* $\mathbf{A}$ *in* $R^{m\times n}$, *then*

$$rk_R(\mathbf{A}) = \max_{1\leq j\leq \rho} \left\{ rk_{R_{(j)}}\left(\Phi_{(j)}(\mathbf{A})\right) \right\}.$$

Since $R_{(j)}$ is a finite chain ring, if a and b are in $R_{(j)}$ then a divides b, or b divides a. Therefore, according to [31, Proposition 3.4], we have the following:

Lemma 3 *Let* $\mathbf{x} = \left(x_r\right)_{1\leq r\leq n} \in R_{(j)}^n$, *and* $\mathbf{D}_\mathbf{x}$ *the* $n \times n$ *diagonal matrix with the entries of* $\mathbf{x}$ *on the diagonal, that is,* $\mathbf{D}_\mathbf{x} = \left(d_{r,s}\right)$ *where* $d_{r,r} = x_r$ *and* $d_{r,s} = 0$ *if* $r \neq s$. *Then, the Hamming weight*[2] *of* $\mathbf{x}$ *is equal to the rank of* $\mathbf{D}_\mathbf{x}$.

Proposition 6 *The MinRank problem over finite commutative principal ideal rings is NP-complete.*

[2] The Hamming weight of $\mathbf{x}$ is the number of r such that $x_r \neq 0$.

Proof From Lemma 2, the MinRank Problem over the principal ideal ring R is equivalent to the same problem over the finite chain rings $R_{(j)}$, for $j \in \{1, \dots, \rho\}$. By Lemma 3 the decoding problem in the Hamming metric[3] over $R_{(j)}$ is reduced to the MinRank Problem. According to [6] or [53] the decoding problem in Hamming metric over $R_{(j)}$ is NP-complete.[4] Thus, the result follows. □

Since the MinRank problem over finite principal ideal rings is a hard problem, the study of its algebraic resolution deserves attention for cryptographic applications. From a modelling perspective, the MinRank problem over finite fields can be transformed into a system of algebraic equations using the maximum minors while over finite principal ideal rings, the rank of a matrix is usually not equal to the order of the highest order non-vanishing minor. As a consequence, the MaxMinor modelling does not apply in general when dealing with rings. In the following subsections, we will prove that the Kipnis–Shamir Modelling and the Support Minors Modelling can be extended over finite principal ideal rings. A natural consequence is that the methods proposed above for solving systems of algebraic equations over finite commutative rings can be applied to solve the MinRank Problem Over Finite Principal Ideal Rings.

5.2 Kipnis–Shamir modeling

We start with some lemmas which will be used to give the Kipnis–Shamir modeling over finite principal ideal rings. According to [31, Proposition 3.2], we have the following:

Lemma 4 *Let* $\mathbf{E} \in R^{m\times n}$ *such that* $rk(\mathbf{E}) \leq r$. *Then, there exists a rank* r *free submodule* F *of* R^n *such that* $row(\mathbf{E}) \subset F$.

Remark 2 Let $\mathbf{E}$ and F as in Lemma 4. If $row(\mathbf{E})$ is a free module and $rk(\mathbf{E}) = r$ then F is unique and $row(\mathbf{E}) = F$. But if $row(\mathbf{E})$ is not a free module, then F is generally not unique.

Example 7 Consider the matrix $\mathbf{E} = \begin{pmatrix} 2 & 0 & 4 \end{pmatrix}$ over $\mathbb{Z}_8$. Then $rk(\mathbf{E}) = 1$ and there exist four free submodules F of $\mathbb{Z}_8^3$ of rank 1 such that $row(\mathbf{E}) \subset F$. These four submodules are respectively generated by $(1, 0, 2)$, $(1, 4, 2)$, $(1, 0, 6)$, and $(1, 4, 6)$.

Let F be a free submodule of R^n of rank r and $F^{\perp}$ the dual of F with respect to the canonical inner-product of R^n. Then, by [19, Proposition 2.9], $F^{\perp}$ is also a free module of rank $n - r$ and $\left(F^{\perp}\right)^{\perp} = F$. Thus, we have the following:

[3] The decoding problem in the Hamming metric can be defined as in Definition 5 using the Hamming metric weight instead of the rank weight.

[4] Note that the decoding problem is equivalent to the syndrome decoding problem.

Lemma 5 *A subset F of R^n is a free submodule of R^n of rank r if and only if there exists $\mathbf{Z} \in R^{n\times(n-r)}$ with linearly independent column vectors and satisfying*:

$$\forall\, \mathbf{y} \in R^n,\ \mathbf{y} \in F \iff \mathbf{yZ} = \mathbf{0}. \tag{12}$$

Proof Assume that F is a free submodule of R^n of rank r. Then, by [19, Proposition 2.9], $F^{\perp}$ is a free module of rank $n-r$. Let $\mathbf{Z} \in R^{n\times(n-r)}$ such that the rows of $\mathbf{Z}^{\top}$ generates $F^{\perp}$. Then the column vectors of $\mathbf{Z}$ are linearly independent and (12) holds.

Conversely, assume that there exists $\mathbf{Z} \in R^{n\times(n-r)}$ with linearly independent column vectors. Let $F = \{\mathbf{y} \in R^n : \mathbf{yZ} = \mathbf{0}\}$. Then, by [19, Proposition 2.9], F is a free module of rank r. □

If a and b are two elements of a finite chain ring, then a divides b or b divides a. This property was used in [44, Proposition 3.2] to prove the existence of the generator matrices in standard form over finite chain rings. So, we have the following:

Lemma 6 *Assume that R is a finite chain ring. Let $\mathbf{Z} \in R^{n\times(n-r)}$ with column vectors that are linearly independent. Then there exists a size n permutation matrix $\mathbf{P}$, an invertible matrix $\mathbf{Q} \in R^{(n-r)\times(n-r)}$, and a matrix $\mathbf{Z}' \in R^{r\times(n-r)}$ such that*

$$\mathbf{Z} = \mathbf{P}\begin{pmatrix} \mathbf{I}_{n-r} \\ \mathbf{Z}' \end{pmatrix}\mathbf{Q}.$$

The above Lemma 6 is not generally true when R is not a finite chain ring. Indeed, consider the matrix

$$\mathbf{Z} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

over $\mathbb{Z}_6$. The column vector of $\mathbf{Z}$ is $\mathbb{Z}_6$–linearly independent. But $\mathbf{Z}$ cannot be decomposed as in Lemma 6. Lemmas 4, 5 and 6 allow to extend the Kipnis–Shamir Modeling to finite principal ideal rings.

Theorem 2 *Let $\mathbf{M}_0$, $\mathbf{M}_1, \dots, \mathbf{M}_k$ in $R^{m\times n}$, $x_1, \dots, x_k$ in R and r in $\mathbb{N}^*$. For $M_x = \mathbf{M}_0 + \sum_{i=1}^{k} x_i\mathbf{M}_i$, the following statements are equivalent.*

(i) $rk(\mathbf{M}_x) \leq r$.

(ii) *There exists $\mathbf{Z} \in R^{n\times(n-r)}$, with column vectors that are linearly independent and such that*

$$\mathbf{M}_x\mathbf{Z} = \mathbf{0}. \tag{13}$$

Moreover, if R is a finite chain ring then, up to a permutation of columns of $\mathbf{M}_x$, we can assume that $\mathbf{Z}$ is into the form

$$\mathbf{Z} = \begin{pmatrix} \mathbf{I}_{n-r} \\ \mathbf{Z}' \end{pmatrix}$$

where $\mathbf{Z}' \in R^{r\times(n-r)}$.

Proof The proof is similar to the case of fields. Indeed, assume that $rk(\mathbf{M}_{\,x}) \leq r$. Then, by Lemma 4, there exists a free submodule F of R^n of rank r such that $row\big(\mathbf{M}_x\big) \subset F$. Thus, by Lemma 5, there is $\mathbf{Z} \in R^{n\times(n-r)}$, with column vectors that are linearly independent and such that (13) holds. Conversely, assume that (ii) holds. Then, by Lemma 5, all row vectors of $\mathbf{M}_x$ are in a free module of rank r. Therefore, by [31, Proposition 3.2], $rk(\mathbf{M}_x) \leq r$. □

As specified in Remark 2, the free submodule F is generally not unique. Therefore, $\mathbf{Z}'$ is generally not unique.

Example 8 Consider the following MinRank problem that is to find x_1, x_2 and x_3 in $\mathbb{Z}_8$ such that

$$rk\big(x_1\mathbf{M}_1 + x_2\mathbf{M}_2 + x_3\mathbf{M}_3\big) \leq 1 \tag{14}$$

with

$$M_1 = \begin{pmatrix} 0&0&0&7 \\ 1&0&0&5 \\ 0&1&0&2 \\ 0&0&1&4 \end{pmatrix},\ M_2 = \begin{pmatrix} 0&0&7&4 \\ 0&0&5&3 \\ 1&0&2&5 \\ 0&1&4&2 \end{pmatrix},\ M_3 = \begin{pmatrix} 2&2&0&4 \\ 4&2&0&6 \\ 0&4&2&4 \\ 0&6&6&0 \end{pmatrix}.$$

Since $r = 1$, by Theorem 2, (14) is equivalent to

$$\big(x_1\mathbf{M}_1 + x_2\mathbf{M}_2 + x_3\mathbf{M}_3\big)\begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \\ z_1&z_2&z_3 \end{pmatrix} = \mathbf{0} \tag{15}$$

A Gröbner basis associated to (15) with the lexicographic order $z_1 > z_2 > z_3 > x_1 > x_2 > x_3$ is $2z_1x_3 + 6x_3$, $2z_2x_3 + 6x_3$, $2z_3x_3 + 6x_3$, $x_1 + 2x_3$, $x_2 + 2x_3$, $4x_3$. According to Proposition 5, the solutions of the system $x_1 + 2x_3 = x_2 + 2x_3 = 4x_3 = 0$ are the triples $\big(x_1, x_2, x_3\big)$ in $\{(0,0,0), (4,4,2), (0,0,4), (4,4,6)\}$. Furthermore, each of these solutions satisfies Eq. (14). So we conclude that we have exactly four solutions.

In the simulations, we observe that in some cases, to simplify the resolution of (13) it is necessary to add some equations as specified in Remark 1.

Example 9 Consider the MinRank problem that is to find x_1, x_2, x_3 in $\mathbb{Z}_8$ such that

$$rk(\mathbf{M}_x) \leq 1 \tag{16}$$

where $\mathbf{M}_x = \mathbf{M}_0 + \sum_{i=1}^{3} x_i \mathbf{M}_i$ and

$$\mathbf{M}_0 = \begin{pmatrix} 5 & 2 & 3 \\ 5 & 1 & 4 \\ 4 & 3 & 6 \end{pmatrix}, \quad \mathbf{M}_1 = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 3 \\ 0 & 2 & 1 \end{pmatrix}, \quad \mathbf{M}_2 = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 3 \\ 0 & 5 & 5 \end{pmatrix}, \quad \mathbf{M}_3 = \begin{pmatrix} 0 & 5 & 5 \\ 0 & 1 & 0 \\ 1 & 2 & 5 \end{pmatrix}$$

According to Theorem 2, (16) is equivalent to

$$\mathbf{M}_x \mathbf{Z} = \mathbf{0}. \tag{17}$$

When we choose $\mathbf{Z}$ in the form $\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ z_1 & z_2 \end{pmatrix}$ we do not get the solution. Thus, it is necessary to choose the switchable permutation. In our simulations, we observed that we can choose $\mathbf{Z} = \begin{pmatrix} z_1 & z_2 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$. In this case, when we compute a Gröbner basis associated to (17) with the lexicographic order $z_1 > z_2 > x_1 > x_2 > x_3$, the resolution requires a search for the solution among several potential candidates. But when we add the polynomial expressions $F_m(z_1)$, $F_m(z_2)$, $F_m(x_1)$, $F_m(x_2)$, $F_m(x_3)$ as in Example 4, we get the Gröbner basis $z_1^4 - z_1^2$, $2z_1$, $z_2^4 + 3z_2^2 + 4$, $2z_2 + 4$, $x_1 + 7$, $x_2 + 5$, $x_3 + 2$. Thus, we directly obtain the solution of (16) which is $x_1 = 1, x_2 = 3, x_3 = 6$.

5.3 Support-minors modeling

In this subsection, we will show that the Support-Minors modeling of the MinRank problem given in [3] over fields can be extended to finite principal ideal rings.

Lemma 7 *Let* $\mathbf{A} \in R^{r\times n}$ *with row vectors that are linearly independent, and* $\mathbf{y} \in R^n$. *Then* $\mathbf{y} \in row(\mathbf{A})$ *if and only if*

$$Minors_{r+1}\begin{pmatrix} \mathbf{y} \\ \mathbf{A} \end{pmatrix} = \mathbf{0}, \tag{18}$$

where (18) *means that all minors of the matrix* $\begin{pmatrix} \mathbf{y} \\ \mathbf{A} \end{pmatrix}$ *of size* $r + 1$ *are equal to zero.*

Proof As the row vectors of $\mathbf{A}$ are linearly independent, by [19, Corollary 2.7] there is an invertible matrix $\mathbf{P} \in R^{n\times n}$ such that$\mathbf{A}\mathbf{P} = \begin{pmatrix} \mathbf{I}_r & \mathbf{0} \end{pmatrix}$. Set $\mathbf{P} = \begin{pmatrix} \mathbf{P}_1 & \mathbf{P}_2 \end{pmatrix}$ where $\mathbf{P}_1$ and $\mathbf{P}_2$ are submatrices of $\mathbf{P}$ of sizes $n \times r$ and $n \times (n - r)$, respectively. Assume that (18) holds. Then, using the Cauchy–Binet formula, we get

$$Minors_{r+1}\left(\begin{pmatrix} \mathbf{y} \\ \mathbf{A} \end{pmatrix}\mathbf{P}\right) = \mathbf{0},$$

that is to say,

$$Minors_{r+1}\begin{pmatrix} \mathbf{y}\mathbf{P}_1 & \mathbf{y}\mathbf{P}_2 \\ \mathbf{I}_r & \mathbf{0} \end{pmatrix} = \mathbf{0}.$$

For any entry u of $\mathbf{yP}_2$, the minor det $\begin{pmatrix} \mathbf{y}\,\mathbf{P}_1 & u \\ \mathbf{I}_r & \mathbf{0} \end{pmatrix}$ is equal to $(-1)^r u$, which is equal to 0 by the assumption. We then deduce that $\mathbf{yP}_2 = \mathbf{0}$. Thus, by Lemma 5, $\mathbf{y} \in row(\mathbf{A})$. Conversely, if $\mathbf{y} \in row(\mathbf{A})$ then (18) holds, since $\mathbf{y}$ is a linear combination of the rows of $\mathbf{A}$. □

Let $\mathbf{A}$ and $\mathbf{y}$ as in Lemma 7. For any sequence of r positive integers $1 \leq j_1 < \cdots < j_r \leq n$, let $a_{j_1,\ldots,j_r}$ be the determinant of the $r \times r$ submatrix of $\mathbf{A}$ with column index in $\{j_1, \ldots, j_r\}$. The set $\{a_{j_1,\ldots,j_r} : 1 \leq j_1 < \cdots < j_r \leq n\}$ is said to be a Plücker coordinates [10] of the free R–module $row(\mathbf{A})$. By [27, Remark 2.12], if $\mathbf{B} \in R^{r\times n}$ and $row(\mathbf{A}) = row(\mathbf{B})$, then there is an invertible matrix $\mathbf{Q} \in R^{r\times r}$ such that $\mathbf{B} = \mathbf{QA}$. Thus, as in the case of fields, the R–module $row(\mathbf{A})$ may admit several sets of Plücker coordinates, but they are all equal up to a unit multiplicative factor. Moreover, if R is a finite chain ring, then according to Lemma 6, at least one component in any Plücker coordinates is a unit. Furthermore, by setting $\mathbf{y} = \left(y_{j_\alpha}\right)_{1\leq\alpha\leq n}$ where $y_{j_\alpha} \in R$, and using the Laplace expansion along the first row, Eq. (18) is equivalent to

$$\sum_{\alpha=1}^{r+1} (-1)^{\alpha+1} y_{j_\alpha} a_{j_1,\ldots,j_{\alpha-1},j_{\alpha+1},\ldots,j_{r+1}} = 0, \tag{19}$$

for all sequence of $r + 1$ positive integers $1 \leq j_1 < \cdots < j_{r+1} \leq n$.

Notice that, when the row vectors of $\mathbf{A}$ are not linearly independent, the “only if” part of Lemma 7 may not be true. Indeed, consider the matrix $\mathbf{A} = \begin{pmatrix} 2 & 0 \end{pmatrix}$ over $\mathbb{Z}_4$. Then

$$Minors_2\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} = 0.$$

But $(0, 2) \notin row(\mathbf{A})$.

Similar to the Support-Minors modeling given in [3], we have the following:

Theorem 3 *Let* $\mathbf{M}_0, \mathbf{M}_1, \ldots, \mathbf{M}_k$ *in* $R^{m\times n}$, $x_1, \ldots, x_k$ *in* R *and* r *in* $\mathbb{N}^*$.

Set $\mathbf{M}_x = \mathbf{M}_0 + \sum_{l=1}^{k} x_l \mathbf{M}_l$. *Then, the following statements are equivalent.*

(i) $rk(\mathbf{M}_x) \leq r$.

(ii) *There exist Plücker coordinates* $\left\{z_{j_1,\dots,j_r} \,:\, 1 \le j_1 < \cdots < j_r \le n\right\}$ *of a free submodule of* R^n *of rank r such that*

$$\sum_{\alpha=1}^{r+1} (-1)^{\alpha+1} \mathbf{M}_x[i, j_\alpha] z_{j_1,\dots,j_{\alpha-1},j_{\alpha+1},\dots,j_{r+1}} = 0, \tag{20}$$

for all $i = 1, \dots, n$ and all sequences of $r+1$ positive integers $1 \le j_1 < \cdots < j_{r+1} \le n$, where $\mathbf{M}_x[i, j_\alpha]$ is the entry at the i^{th} row and j_α^{th} column of $\mathbf{M}_x$.

Proof Assume that $rk(\mathbf{M}_x) \le r$. Then, by Lemma 4, there exists a free submodule F of R^n of rank r such that $row\left(\mathbf{M}_x\right) \subset F$. Let $\left\{z_{j_1,\dots,j_r} \,:\, 1 \le j_1 < \cdots < j_r \le n\right\}$ be a Plücker coordinates of F. Then, by Lemma 7 and (19), we get (20).

Conversely, assume that (ii) holds. Then, by Lemma 7, all row vectors of $\mathbf{M}_x$ are in a free module of rank r. Therefore, by [31, Proposition 3.2], $rk(\mathbf{M}_x) \le r$. □

As stated in Remark 2, the free submodule F is generally not unique. Consequently, there are usually several Plücker coordinates associated to different free submodules, and which all satisfy Eq. (20). Equation (20) is a system of polynomial equations with unknowns x_l and $z_{j_1,\dots,j_r}$. Thus, as specified in the previous sections, we can use Gröbner bases to solve (20). But in some cases, it is possible to use linear algebra as in [3].

Example 10 Consider the MinRank problem (14) of Example 8. Since $r = 1$, then by Theorem 3, there exist Plücker coordinates $\left(z_1, z_2, z_3, z_4\right)$ of a free submodule of $\mathbb{Z}_8^4$ of rank 1 such that (14) is equivalent to

$$\begin{cases} \mathbf{M}_x[i,1]z_2 - \mathbf{M}_x[i,2]z_1 = 0 \\ \mathbf{M}_x[i,1]z_3 - \mathbf{M}_x[i,3]z_1 = 0 \\ \mathbf{M}_x[i,1]z_4 - \mathbf{M}_x[i,4]z_1 = 0 \\ \mathbf{M}_x[i,2]z_3 - \mathbf{M}_x[i,3]z_2 = 0 \\ \mathbf{M}_x[i,2]z_4 - \mathbf{M}_x[i,4]z_2 = 0 \\ \mathbf{M}_x[i,3]z_4 - \mathbf{M}_x[i,4]z_3 = 0 \end{cases}, \quad i = 1, ..., 4 \tag{21}$$

where $\mathbf{M}_x = x_1\mathbf{M}_1 + x_2\mathbf{M}_2 + x_3\mathbf{M}_3$. Since $\mathbb{Z}_8$ is a finite chain ring, at least one component of the Plücker coordinates $\left(z_1, z_2, z_3, z_4\right)$ is a unit. Without loss of generality, assume that z_4 is a unit, then in order to recover x_1, x_2 and x_3, we rewrite (21) as

$$\mathbf{AX} = \mathbf{0} \tag{22}$$

where $\mathbf{X}^\top = \left(x_1z_1 \; x_2z_1 \; x_3z_1 \; x_1z_2 \; x_2z_2 \; x_3z_2 \; x_1z_3 \; x_2z_3 \; x_3z_3 \; x_1z_4 \; x_2z_4 \; x_3z_4 \right)$ and $\mathbf{A}$ is a matrix with entries in $\mathbb{Z}_8$. Using SageMath [51], we can compute the row echelon form $\widetilde{\mathbf{A}}$ of $\mathbf{A}$ and get

$$\widetilde{\mathbf{A}} = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&0&2\\ 0&1&0&0&0&0&0&0&0&0&0&2\\ 0&0&2&0&0&0&0&0&0&0&0&2\\ 0&0&0&1&0&0&0&0&0&0&0&2\\ 0&0&0&0&1&0&0&0&0&0&0&2\\ 0&0&0&0&0&2&0&0&0&0&0&2\\ 0&0&0&0&0&0&1&0&0&0&0&2\\ 0&0&0&0&0&0&0&1&0&0&0&2\\ 0&0&0&0&0&0&0&0&2&0&0&2\\ 0&0&0&0&0&0&0&0&0&1&0&2\\ 0&0&0&0&0&0&0&0&0&0&1&2\\ 0&0&0&0&0&0&0&0&0&0&0&4 \end{pmatrix}$$

Therefore, (22) is equivalent to

$$\widetilde{\mathbf{A}}\mathbf{X} = \mathbf{0}$$

Thus, $x_1 z_4 + 2x_3 z_4 = x_2 z_4 + 2x_3 z_4 = 4x_3 z_4 = 0$. Since we assumed that z_4 is a unit, we get $\left(x_1, x_2, x_3\right) \in \{(0,0,0),(4,4,2),(0,0,4),(4,4,6)\}$.

In the case of fields, some conditions have been given in [3, 4] to solve (20) using linear algebra. It will be interesting to study if these conditions can be extended to rings.

It is important to note that, according to [31, Proposition 3.4], the rank of a matrix and its transpose are equal. Therefore, the MinRank problem defined with $\mathbf{M}_0$, $\mathbf{M}_1$, …, $\mathbf{M}_k$ shares the same solution set with the one defined with $\mathbf{M}_0^\top, \mathbf{M}_1^\top, \ldots, \mathbf{M}_k^\top$. Thus, in order to reduce the number of variables in the algebraic modeling, one can transpose the matrices before solving the MinRank problem, as stated for example in [2].

6 Rank decoding problems over finite principal ideal rings

In this section, we study the algebraic approach for solving the rank decoding problem over finite principal ideal rings. Note that this problem was recently shown in [29] to be at least as hard as the rank decoding problem over finite fields, and a combinatorial-like algorithm was also proposed for solving the problem. Over finite fields, the rank decoding problem has several algebraic modeling. As specified in [29, Section 4], the Ourivski-Johansson modeling [48] and the MaxMinors modeling [5] cannot extend directly to rings due to zero divisors. We show here that the Support-Minors modeling [4] and the modeling using linearized polynomials [25] can be extended in the case of finite principal ideal rings.

6.1 Rank decoding problem

To define the rank decoding problem, we must first recall the construction of a Galois extension of a finite principal ideal ring R. As we specified in Sect. 4, R can be decomposed into a direct sum of local rings. Thus, in the following, we assume that $R = R_{(1)} \times \cdots \times R_{(\rho)}$ where each $R_{(j)}$ is a finite chain ring with maximal ideal $\mathfrak{m}_{(j)}$ and residue field $\mathbb{F}_{q_{(j)}}$, for $j = 1, \ldots, \rho$. Let m be a non-zero positive integer and $h_{(j)} \in R_{(j)}[X]$ a monic polynomial of degree m such that its projection onto $\mathbb{F}_{q_{(j)}}[X]$ is irreducible. If we set $S_{(j)} = R_{(j)}[X]/\left(h_{(j)}\right)$ then, by [39], $S_{(j)}$ is a Galois extension of $R_{(j)}$ of degree m with Galois group that is cyclic of order m. Moreover, $S_{(j)}$ is also a finite chain ring with maximal ideal $\mathfrak{M}_{(j)} = \mathfrak{m}_{(j)}S_{(j)}$ and residue field $\mathbb{F}_{q^m_{(j)}}$. Let us denote by $\sigma_{(j)}$ a generator of the Galois group of $S_{(j)}$, $\sigma = \left(\sigma_{(j)}\right)_{1\le j\le \rho}$ and $S = S_{(1)} \times \cdots \times S_{(\rho)}$. Then, as specified in [31], S is a Galois extension of R of degree m with Galois group generated by σ. Moreover, there exists $h \in R[X]$ such that $S \cong R[X]/(h)$. An example of construction of a Galois extension of $\mathbb{Z}_{40}$ of degree 4 was given in [29, Example 2.2]. The following example shows how one can construct a generator of the Galois group in practice using the Hensel lifting of a primitive polynomial.

Example 11 Let us construct a degree 3 Galois extension of $R = \mathbb{Z}_8$, and its Galois group. The residue field of R is $\mathbb{F}_q = \mathbb{F}_2$ and the polynomial $g = X^3 + X + 1$ is a primitive polynomial in $\mathbb{F}_q[X]$. Using the Hensel's lemma, we can construct the polynomial $h = X^3 + 6X^2 + 5X + 7 \quad \in R[X]$, such that $\overline{h} = g$ and h divides $X^{q^m-1} - 1$. Therefore,$S = R[X]/(h) = R[\alpha]$ is a Galois extension of R of degree $m = 3$, where $\alpha = X + (h)$. Moreover, $\alpha^{q^m-1} = 1$ and $\alpha^i \neq 1$, for $0 < i < q^m - 1$. Thus, the Galois group is generated by the map $\sigma : S \to S$ given by $\alpha \mapsto \alpha^q$, that is to say, for all $x = \sum_{i=0}^{m-1} x_i\alpha^i$, where $x_i \in R$, $\sigma(x) = \sum_{i=0}^{m-1} x_i\alpha^{iq}$.

Definition 4 Let $\mathbf{u} = \left(u_1, \ldots, u_n\right) \in S^n$.

a) The **support** of $\mathbf{u}$, denoted by $supp(\mathbf{u})$, is the R−submodule of S generated by $\{u_1, \ldots, u_n\}$.
b) The **rank** of $\mathbf{u}$, denoted by $rk_R(\mathbf{u})$, or simply by $rk(\mathbf{u})$ is the smallest number of elements in $supp(\mathbf{u})$ which generate $supp(\mathbf{u})$ as a R−module.

Since S is a free R−module, computing the rank of a vector $\mathbf{u} \in S^n$ can be done by using its matrix representation in a R−basis of S as in the case of finite fields (for more details see [31, Proposition 3.13]).

Definition 5 Let $\mathcal{C}$ be a S−submodule of S^n, $\mathbf{y}$ an element of S^n and $r \in \mathbb{N}^*$. The rank decoding problem is to find (if there exist) $\mathbf{e}$ in S^n and $\mathbf{c}$ in $\mathcal{C}$ such that $\mathbf{y} = \mathbf{c} + \mathbf{e}$ with $rk(\mathbf{e}) \le r$.

Using the representation of elements in S^n as elements of $R^{m\times n}$, the rank decoding problem can be reduced to the MinRank problem, as in the case of finite fields [23].

Example 12 Let us consider the rings $R = \mathbb{Z}_8$ and $S = R[\alpha]$ as in Example 11. Let $\mathcal{C} \subset S^3$ be the S–linear code generated by:

$$\mathbf{g} = \left(1, 2\alpha^2 + \alpha + 2, \alpha^2 + 3\alpha\right).$$

Set $\mathbf{y} = \left(4\alpha^2 + 3\alpha + 3,\ 5\alpha^2 + 7\alpha + 6,\ 2\alpha^2 + 4\alpha + 5\right)$ and consider the instance of the rank decoding problem consisting of finding $\mathbf{c} \in \mathcal{C}$ such that

$$rk(\mathbf{y} - \mathbf{c}) \leq 1. \tag{23}$$

Eq. (23) is equivalent to finding x_1, x_2, x_3 in R such that

$$rk\left(\mathbf{y} - \left(x_1 + x_2\alpha + x_3\alpha^2\right)\mathbf{g}\right) \leq 1 \tag{24}$$

Since $\mathcal{C}$ is generated by $\mathbf{g}$, then the matrix representation of $\mathcal{C}$ in the basis $\left(1, \alpha, \alpha^2\right)$ is the R–linear code generated by $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3$ which are respectively the representation matrices of $\mathbf{g}, \alpha\mathbf{g}, \alpha^2\mathbf{g}$ in the basis $\left(1, \alpha, \alpha^2\right)$. Let $\mathbf{M}_0$ be the matrix representation of $-\mathbf{y}$ in the basis $\left(1, \alpha, \alpha^2\right)$. Then, the rank decoding problem (24) is equivalent to the MinRank problem (16) defined in Example 9. The solution of (16) is $x_1 = 1$, $x_2 = 3$, $x_3 = 6$. Thus, $\mathbf{c} = \left(1 + 3\alpha + 6\alpha^2\right)\mathbf{g}$.

6.2 Support-Minors modeling

According to [31, Proposition 3.14] we have the following:

Lemma 8 *For any $\mathbf{u} \in S^n$ with $rk(\mathbf{u}) \leq r$, there exists $\mathbf{b} \in S^r$ and $\mathbf{A} \in R^{r\times n}$ such that $row(\mathbf{A})$ is a free module of rank r and $\mathbf{u} = \mathbf{b}\mathbf{A}$.*

The following result is a generalization of the Support-Minors modeling for the rank decoding problem given in [4].

Theorem 4 *Let $\mathcal{C}$ be a S–submodule of S^n with a generator matrix $\mathbf{G} = \left(g_{i,j}\right)_{1\leq i\leq k, 1\leq j\leq n}$, $\mathbf{y} = \left(y_i\right)_{1\leq i\leq n} \in S^n$ and $r \in \mathbb{N}$. Assume that there exists $\mathbf{x} = \left(x_i\right)_{1\leq i\leq k} \in S^k$ such that $rk(\mathbf{y} - \mathbf{x}\mathbf{G}) \leq r$. Then, there exists a set $\left\{z_{j_1,\ldots,j_r} : 1 \leq j_1 < \cdots < j_r \leq n\right\}$ of Plücker coordinates of a free submodule of R^n of rank r such that*

$$\sum_{s=1}^{r+1} \sum_{i=1}^{k} (-1)^{s+1} \left(x_i g_{i,j_s} - y_{j_s}\right) z_{j_1,\ldots,j_{s-1},j_{s+1},\ldots,j_{r+1}} = 0, \tag{25}$$

for all sequence of $r + 1$ positive integers $1 \leq j_1 < \cdots < j_{r+1} \leq n$.

Proof Using Lemmas 7 and 8, the proof is similar to the one from [4, Section 3].

□

Equation (25) is a system of algebraic equations over S with unknowns $x_i \in S$ and $z_{j_1,\dots j_{s-1} j_{s+1},\dots j_{r+1}} \in R$. To solve this equation using Gröbner bases, we must first expand this equation to R.

Example 13 Consider the rank decoding problem (23) of Example 12. Set $\mathbf{g} = \left(g_{1,}g_2, g_3\right)$ and $\mathbf{y} = \left(y_{1,}y_2, y_3\right)$. Then, by Theorem 4, there are x in S and z_1, z_2, z_3 in R such that

$$\begin{cases} \left(xg_1 - y_1\right)z_2 - \left(xg_2 - y_2\right)z_1 = 0 \\ \left(xg_1 - y_1\right)z_3 - \left(xg_3 - y_3\right)z_1 = 0 \\ \left(xg_2 - y_2\right)z_3 - \left(xg_3 - y_3\right)z_2 = 0 \end{cases} \tag{26}$$

Since $R = \mathbb{Z}_8$ is a finite chain ring, at least one of the elements in the Plücker coordinates $\left(z_1, z_2, z_3\right)$ is a unit. Without loss of generality, assume that $z_1 = 1$. Set $x = x_0 + x_1\alpha + x_2\alpha^2$ where $x_i \in R$, for $i \in \{0, 1, 2\}$. Using SageMath [51], we substitute x and z_1 in (26) and expand the resulting equations over R using the basis $\left(1, \alpha, \alpha^2\right)$, then we obtain a system of equations of the form

$$\begin{cases} -z_2x_0 + 3z_2 + 2x_0 + 2x_1 + 5x_2 + 2 = 0 \\ -z_2x_1 + 3z_2 + x_0 + x_2 + 1 = 0 \\ -z_2x_2 + 4z_2 + 2x_0 + 5x_1 + 2x_2 + 3 = 0 \\ -z_3x_0 + 3z_3 + x_1 + 5x_2 + 3 = 0 \\ -z_3x_1 + 3z_3 + 3x_0 + 3x_1 + 4 = 0 \\ -z_3x_2 + 4z_3 + x_0 + 5x_1 + 5x_2 + 6 = 0 \\ z_2x_1 + 5z_2x_2 + 3z_2 + 6z_3x_0 + 6z_3x_1 + 3z_3x_2 + 6z_3 = 0 \\ 3z_2x_0 + 3z_2x_1 + 4z_2 - z_3x_0 - z_3x_2 - z_3 = 0 \\ z_2x_0 + 5z_2x_1 + 5z_2x_2 + 6z_2 + 6z_3x_0 + 3z_3x_1 + 6z_3x_2 + 5z_3 = 0 \end{cases} \tag{27}$$

As in Example 9, when we compute a Gröbner basis associated to (27) with the lexicographic order $z_2 > z_3 > x_0 > x_1 > x_2$, the resolution requires a search for the solution among several potential candidates. So, to simplify the resolution, we add the polynomial expressions $F_m\left(z_2\right)$, $F_m\left(z_3\right)$, $F_m\left(x_0\right)$, $F_m\left(x_1\right)$, $F_m\left(x_2\right)$ as in Example 4, and get the Gröbner basis: $z_2^4 - z_2^2$, $2z_2$, $z_3^4 + 3z_3^2 + 4$, $2z_3 + 4$, $x_0 + 7$, $x_1 + 5$, $x_2 + 2$. Thus, $x_0 = 1$, $x_1 = 3$, $x_2 = 6$.

6.3 Algebraic modeling with skew polynomials

Skew polynomials [47] generalize linearized polynomials, and some properties of linearized polynomials have been extended to skew polynomials in [31].

Definition 6 The *skew polynomial ring* over S with automorphism σ, denoted by $S[X, \sigma]$, is the ring of all polynomials in $S[X]$ such that

- the addition is defined to be the usual addition of polynomials;
- the multiplication is defined by the basic rule $Xa = \sigma(a)X$, for all $a \in S$.

Notation 5 (Evaluation Map) Let $f = a_0 + a_1X + \cdots + a_kX^k \in S[X, \sigma]$, $x \in S$ and $\mathbf{u} = \left(u_i\right)_{1\le i\le n} \in S^n$.

1. $f(x) := a_0x + a_1\sigma(x) + \cdots + a_k\sigma^k(x)$.
2. $f(\mathbf{u}) := \left(f\left(u_i\right)\right)_{1\le i\le n}$.

According to [31, Propositions 3.15, 3.16 and Corollary 2.7], we have the following proposition.

Proposition 7 *For all $\mathbf{u} \in S^n$, $rk(\mathbf{u}) \le r$ if and only if there exists a monic skew polynomial $f \in S[X, \sigma]$ of degree r such that, $f(\mathbf{u}) = \mathbf{0}$. Moreover, if supp$(\mathbf{u})$ is a free module and $rk(\mathbf{u}) = r$, then f is unique.*

Remark 3 To construct the skew polynomial *f* of Proposition 7, one generally uses a free R–submodule of S which contains *supp*$(\mathbf{u})$. Hence, as we pointed out in Remark 2, there are generally more than one free R–submodule of S which contains *supp*$(\mathbf{u})$. Thus, *f* is generally not unique.

Example 14 Consider again $R = \mathbb{Z}_8$ and $S = R[\alpha]$ as in Example 11.

The rank of $\mathbf{u} = \left(2 + 6\alpha^2, 0, 4 + 4\alpha^2\right)$ is 1 and we would like to find all the monic skew polynomials $f \in S[X, \sigma]$ of degree 1 such that $f(\mathbf{u}) = \mathbf{0}$. So, $f = X + w$, where $w \in S$ and can be written as $w = w_0 + w_1\alpha + w_2\alpha^2$ with w_0, w_1, w_2 in R. When we solve the equation $f(\mathbf{u}) = \mathbf{0}$, we get $w_0 \in \{3, 7\}$, $w_1 \in \{0, 4\}$, $w_2 \in \{3, 7\}$. Thus, there are eight monic skew polynomials $f \in S[X, \sigma]$ with degree 1 such that $f(\mathbf{u}) = \mathbf{0}$.

Notation 6 If $\mathbf{B} = \left(b_{i,j}\right)$ is a matrix with entries in S and l is a positive integer then,

$$\sigma^l(\mathbf{B}) := \left(\sigma^l\left(b_{i,j}\right)\right).$$

The following result is a generalization of the result given in [25, Section V].

Theorem 7 *Let $\mathcal{C}$ be a S–submodule of S^n with generator matrix $\mathbf{G} = \left(g_{i,j}\right)_{1\le i\le k, 1\le j\le n}$, $r \in \mathbb{N}$ and $\mathbf{y} = \left(y_i\right)_{1\le i\le n} \in S^n$. The following statements are equivalent.*

(i) *There exists $\mathbf{c} \in \mathcal{C}$ such that $rk(\mathbf{y} - \mathbf{c}) \le r$.*
(ii) *There are $\left(z_l\right)_{0\le l\le r} \in S^{r+1}$, $z_r = 1$, and $\mathbf{x} = \left(x_i\right)_{1\le i\le k} \in S^k$ such that*

$$\sum_{l=0}^{r} z_l\sigma^l(\mathbf{y}) = \sum_{l=0}^{r} z_l\sigma^l(\mathbf{x}\mathbf{G}) \tag{28}$$

Moreover, if $\mathcal{C}$ is a free S−submodule of rank k and $r \leq t$, where t is the error correction capability of $\mathcal{C}$, then $\mathbf{x}$ is unique.

Proof By Proposition 7, $rk(\mathbf{y}-\mathbf{c}) \leq r$ if and only if there exists a monic skew polynomial $P = \sum_{l=0}^{r} z_l X^l \in S[X,\sigma]$ of degree r such that $P(\mathbf{y}-\mathbf{c}) = \mathbf{0}$. Since $\mathbf{c} \in \mathcal{C}$, then there exists $\mathbf{x} = \left(x_i\right)_{1\leq i\leq k} \in S^k$, such that $\mathbf{c} = \mathbf{x}\mathbf{G}$. Thus, the result follows. □

According to Remark 3, when the support of the error is not a free module, the unknowns z_i's, $i = 0,\dots,r-1$ are not unique, even if $\mathbf{x}$ is unique. So in general, (28) has many solutions. This is the main difference compared to the same result over finite fields. Note that to solve the rank decoding problem, we don't need the unknowns z_i. We just need $\mathbf{x}$, since we can use it to recover $\mathbf{c}$.

6.3.1 Solving by linearization

In this subsection, we will show that in some cases, the unknowns $\mathbf{x}$ in (28) can be recovered using linear algebra. Eq. (28) is equivalent to

$$\mathbf{A}\mathbf{u} = \mathbf{0} \tag{29}$$

where

$$\mathbf{A} = \begin{pmatrix} -\sigma^0\left(\mathbf{y}^\top\right) & \cdots & -\sigma^{r-1}\left(\mathbf{y}^\top\right) & \sigma^0\left(\mathbf{G}^\top\right) & \cdots & \sigma^r\left(\mathbf{G}^\top\right) & -\sigma^r\left(\mathbf{y}^\top\right) \end{pmatrix}$$

and

$$\mathbf{u}^\top = \begin{pmatrix} z_0 & \cdots & z_{r-1} & z_0\sigma^0(\mathbf{x}) & \cdots & z_r\sigma^r(\mathbf{x}) & z_r \end{pmatrix}.$$

In the same way as the row echelon form over fields, the matrix $\mathbf{A}$ can be decomposed as $\mathbf{A} = \mathbf{P}\mathbf{T}$ where $\mathbf{P}$ is an invertible matrix and $\mathbf{T} = \left(t_{i,j}\right)$ is an upper triangular matrix, that is to say $t_{i,j} = 0$ if $i > j$ [33, Theorem 3.5]. The matrix $\mathbf{T}$ is usually called the Hermite normal form of $\mathbf{A}$. One can compute the Hermite normal form using the same methods as the Gaussian elimination algorithm, see for example [13, 33, 50]. As $z_r = 1$, the following proposition shows that if $\mathbf{T}$ has a specific form, then $\mathbf{x}$ can be recovered.

Proposition 8 *With the above notations, assume that* (28) *has a solution and that* $\mathbf{T}$ *is of the form*

$$\mathbf{T} = \begin{pmatrix} \mathbf{T}_1 & \mathbf{T}_2 \\ \mathbf{0} & \mathbf{T}_3 \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \tag{30}$$

where $\mathbf{T}_1$ *is an* $r(k+1)\times r(k+1)$ *upper triangular matrix,* $\mathbf{T}_2$ *being a* $r(k+1)\times(k+1)$ *matrix and* $\mathbf{T}_3 = \begin{pmatrix} \mathbf{I}_k & \mathbf{b} \end{pmatrix}$ *where* $\mathbf{b}$ *is a* $k \times 1$ *matrix, then*

$$\mathbf{x} = -\sigma^{-r}\left(\mathbf{b}^\top\right).$$

Note that (29) is a homogeneous system of n linear equations with $(k+1)(r+1)$ unknowns. So, a necessary condition for **T** to have the form (30) is $n \geq (k+1)(r+1)-1$. The same condition was given in [25, Theorem 12] in the case of finite fields. With this condition, we observed in our simulations that, when $\mathcal{C}$ is a random free submodule, **x** can be recovered in many cases. It will be therefore interesting to study the probability of this observation.

Example 15 Consider the rank decoding problem of Example 12. Then there are $x \in S$ and $\mathbf{e}$ $\in S^3$ such that

$$\mathbf{y} = x\mathbf{g} + \mathbf{e} \tag{31}$$

with $rk(\mathbf{e}) = r = 1$. So, the skew polynomial $P \in S[X, \sigma]$, such that

$$P(\mathbf{e}) = \mathbf{0} \tag{32}$$

is of the form $P = z_0 + z_1 X$ where $z_0, z_1 \in S$ with $z_1 = 1$. By setting $\mathbf{g} = \left(g_{1,}g_2, g_3\right)$ and $\mathbf{y} = \left(y_{1,}y_2, y_3\right)$, (31) and (32) imply

$$z_0\left(xg_j - y_j\right) + z_1\sigma\left(xg_j - y_j\right) = 0, \quad j = 1, ..., 3. \tag{33}$$

which means that

$$\mathbf{A}\begin{pmatrix} z_0 \\ z_0 x \\ z_1\sigma(x) \\ z_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{34}$$

where

$$\mathbf{A} = \begin{pmatrix} -y_1 & g_1 & \sigma\left(g_1\right) & -\sigma\left(y_1\right) \\ -y_2 & g_2 & \sigma\left(g_2\right) & -\sigma\left(y_2\right) \\ -y_3 & g_3 & \sigma\left(g_3\right) & -\sigma\left(y_3\right) \end{pmatrix}.$$

Using Magma [9], we compute the row echelon form of **A** and get:

$$\mathbf{T} = \begin{pmatrix} 1 & \alpha^2+\alpha & 0 & 2\alpha^2+4 \\ 0 & 2 & 0 & 6\alpha^2+4\alpha \\ 0 & 0 & 1 & 3\alpha^2+6\alpha+3 \end{pmatrix}$$

Thus,

$$\begin{aligned} x &= -\sigma^{-1}\left(3\alpha^2+6\alpha+3\right) \\ &= 1+3\alpha+6\alpha^2 \end{aligned}$$

6.3.2 Solving with Gröbner bases

When S is a finite field, Eq. (28) is a system of multivariate polynomial equations in the variables z_l and x_i, and such a system was solved directly with Gröbner bases in [25, Section VII]. However, when S is not a field, the expression $\sigma^l\left(x_i g_{i,j}\right)$ is not a polynomial function in the variable x_i. So, to transform (28) into a system of multivariate polynomial equations, we will expand this equation in R. Let $\left(\beta_u\right)_{1\leq u\leq m}$ be a R–basis of S. Using the notations of Theorem 7, set $x_i = \sum_{u=1}^{m} x_{i,u}\beta_u$ and $z_l = \sum_{v=1}^{m} z_{l,v}\beta_v$ where $x_{i,u}$ and $z_{l,v}$ are in R. If we substitute x_i and z_l in (28) and expand the resulting equations over R using the basis $\left(\beta_u\right)_{1\leq u\leq m}$, then we obtain a system of equations of the form:

$$\left(\widetilde{\mathbf{x}} \otimes \widetilde{\mathbf{z}}\right)\mathbf{A} + \widetilde{\mathbf{x}}\mathbf{B} + \widetilde{\mathbf{z}}\mathbf{C} + \mathbf{D} = \mathbf{0} \tag{35}$$

where

$$\widetilde{\mathbf{x}} = \left(x_{1,1}, \dots x_{1,m}, \dots, x_{k,1}, \dots x_{k,m}\right), \widetilde{\mathbf{z}} = \left(z_{0,1}, \dots z_{0,m}, \dots, z_{r-1,1}, \dots z_{r-1,m}\right),$$

and $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ are matrices with mn columns and entries in R.

Assume that $\mathcal{C}$ is a free S–submodule and $r \leq t$, where t is the error correction capability of $\mathcal{C}$. Then, according to Theorem 7, Eq. (35) has a unique solution in the variables $\widetilde{\mathbf{x}}$ that we denote by $\widetilde{\mathbf{x}}_0$. Remember that when the support of the error is not a free module, Eq. (35) has many solutions in the variables $\widetilde{\mathbf{z}}$. But also note that we do not need all the solutions of (35). We just need the partial solution $\widetilde{\mathbf{x}}_0$. Therefore, to solve (35) we can use the elimination theorem as specified in Sect. 3 to simply find the partial solution $\widetilde{\mathbf{x}}_0$ using Gröbner bases.

Example 16 Consider Eq. (33) of Example 15. Set $x = x_0 + x_1\alpha + x_2\alpha^2$ and $z_0 = t_0 + t_1\alpha + t_2\alpha^2$ where x_i and t_i are in R for $i = 1, \dots, 3$. Using SageMath, we substitute x, z_0 and $z_1 = 1$ in (33) and expand the resulting equations over R using the basis $\left(1, \alpha, \alpha^2\right)$ to finally obtain a system of equations of the form

$$\begin{cases} x_0t_0 + x_2t_1 + x_1t_2 + 2x_2t_2 + x_0 + 2x_2 + 5t_0 + 4t_1 + 5t_2 + 5 = 0 \\ x_1t_0 + x_0t_1 + 3x_2t_1 + 3x_1t_2 - x_2t_2 - x_2 + 5t_0 + t_1 + 3t_2 + 4 = 0 \\ x_2t_0 + x_1t_1 + 2x_2t_1 + x_0t_2 + 2x_1t_2 - x_2t_2 + x_1 - x_2 + 4t_0 + 5t_1 + 3t_2 + 1 = 0 \\ 2x_0t_0 + 2x_1t_0 + 5x_2t_0 + 2x_0t_1 + 5x_1t_1 + 2x_2t_1 + 5x_0t_2 + 2x_1t_2 + 5x_2t_2 + 6x_0 + 4x_1 + x_2 + 2t_0 + 3t_1 - t_2 = 0 \\ x_0t_0 + x_2t_0 + x_1t_1 + 3x_2t_1 + x_0t_2 + 3x_1t_2 + x_2t_2 + 6x_0 + 3x_1 + 6x_2 + t_0 + 3t_1 + 5 = 0 \\ 2x_0t_0 + 5x_1t_0 + 2x_2t_0 + 5x_0t_1 + 2x_1t_1 + 5x_2t_1 + 2x_0t_2 + 5x_1t_2 + 5x_2t_2 - x_0 + 3x_1 - x_2 + 3t_0 - t_1 + t_2 + 6 = 0 \\ x_1t_0 + 5x_2t_0 + x_0t_1 + 5x_1t_1 + 5x_2t_1 + 5x_0t_2 + 5x_1t_2 + 2x_2t_2 + 2x_0 + 3x_1 - x_2 + 3t_0 + 6t_1 + 7 = 0 \\ 3x_0t_0 + 3x_1t_0 + 3x_0t_1 + 4x_2t_1 + 4x_1t_2 + 3x_2t_2 - x_0 + 3x_1 + 3x_2 + 4t_0 + 5t_1 + 6t_2 + 2 = 0 \\ x_0t_0 + 5x_1t_0 + 5x_2t_0 + 5x_0t_1 + 5x_1t_1 + 2x_2t_1 + 5x_0t_2 + 2x_1t_2 + 2x_0 + 6x_1 + 3x_2 + 6t_0 + 5t_2 + 6 = 0 \end{cases} \tag{36}$$

Using SageMath [51], we compute a Gröbner basis of (36) and get:

$$\left\{x_0 + 7, x_1 + 5, x_2 + 2, 2t_0 + 2, 2t_1, 2t_2 + 2\right\}.$$

Thus, $x = x_0 + x_1\alpha + x_2\alpha^2 = 1 + 3\alpha + 6\alpha^2$.

The SageMath code used for all the examples in this paper is available at https://github.com/hervekalachi/Ring_RSD-MinRank.

7 Conclusion

In this work, we have shown that solving systems of algebraic equations over finite commutative rings reduces to the same problem over Galois rings. Then, using the elimination theorem and some properties of canonical generating systems, we have also shown how Gröbner bases can be used to solve systems of algebraic equations over finite chain rings. As applications, these results have been used to give some algebraic approaches for solving the MinRank problem and the rank decoding problem over finite principal ideal rings.

The above work clearly opens the door to an important complexity question, namely the real coast of Gröbner bases computation over finite chain rings, or at least the cost when dealing with the MinRank and rank decoding problems over finite chain rings.

Another metric used in coding theory and cryptography is the Lee metric [37]. This metric is usually defined over integer residue rings, which are specific cases of finite principal ideal rings. Another interesting perspective will be to study the possibility of using algebraic techniques for solving the decoding problem in the Lee metric.

Funding The first author acknowledges the Swiss Government Excellence for the financial support under Grant ESKAS No. 2022.0689. The second author acknowledges the UNESCO-TWAS and the German Federal Ministry of Education and Research (BMBF) for the financial support under the SG-NAPI Grant Number 4500454079.

Data availability Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest The authors declare no conflicts of interest.

References

1. Agrawal, M., Saxena, N.: Automorphisms of finite rings and applications to complexity of problems. In: STACS 2005: 22nd Annual Symposium on Theoretical Aspects of Computer Science, Stuttgart, Germany, February 24–26, 2005. Proceedings 22, pp. 1–17. Springer (2005)
2. Bardet, M., Bertin, M.: Improvement of algebraic attacks for solving superdetermined minrank instances. In: Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings, pp. 107–123. Springer (2022)
3. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Neiger, V., Ruatta, O., Tillich, J.: An algebraic attack on rank metric code-based cryptosystems. In: A. Canteaut, Y. Ishai (eds.) Advances in Cryptology - EUROCRYPT, Lecture Notes in Computer Science, vol. 12107, pp. 64–93. Springer (2020)

4. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Tillich, J.: Revisiting algebraic attacks on MinRank and on the rank decoding problem. Des. Codes Cryptogr. **91**(11), 3671–3707 (2023)
5. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R.A., Smith-Tone, D., Tillich, J., Verbel, J.A.: Improvements of algebraic attacks for solving the rank decoding and minrank problems. In: Advances in Cryptology - ASIACRYPT, Lecture Notes in Computer Science, vol. 12491, pp. 507–536. Springer (2020)
6. Barg, S.: Some new NP-complete coding problems. Problemy Peredachi Informatsii **30**(3), 23–28 (1994)
7. Behboodi, M., Beyranvand, R., Hashemi, A., Khabazian, H.: Classification of finite rings: theory and algorithm. Czechoslov. Math. J. **64**, 641–658 (2014)
8. Berthomieu, J., Lecerf, G., Quintin, G.: Polynomial root finding over local rings and application to error correcting codes. Appl. Algebra Eng. Commun. Comput. **24**(6), 413–443 (2013)
9. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)
10. Bruns, W., Vetter, U.: Determinantal rings, Lecture Notes in Mathematics, vol. 1327. Springer (2006)
11. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. Universitat Innsbruck, Austria, Ph. D. Thesis (1965)
12. Buchberger, B.: Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory. Recent trends in multidimensional systems theory. Reidel Publishing Company, Dordrecht (1985)
13. Bulyovszky, B., Horváth, G.: Polynomial functions over finite commutative rings. Theoret. Comput. Sci. **703**, 76–86 (2017)
14. Caminata, A., Gorla, E.: Solving degree, last fall degree, and related invariants. J. Symb. Comput. **114**, 322–335 (2023)
15. Caruso, X., Roe, D., Vaccon, T.: p-adic stability in linear algebra. In: Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, pp. 101–108. Association for Computing Machinery, New York (2015)
16. Courtois, N.T.: Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In: Advances in Cryptology—ASIACRYPT 2001, pp. 402–421. Springer, Berlin (2001)
17. Courtois, N.T., Klimov, A., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: B. Preneel (ed.) Advances in Cryptology—EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding, Lecture Notes in Computer Science, vol. 1807, pp. 392–407. Springer (2000)
18. Dougherty, S.T., Kim, J.L., Kulosman, H.: MDS codes over finite principal ideal rings. Des. Codes Crypt. **50**(1), 77 (2009)
19. Fan, Y., Ling, S., Liu, H.: Matrix product codes over finite commutative Frobenius rings. Des. Codes Crypt. **71**(2), 201–227 (2014)
20. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases (F4). J. Pure Appl. Algebra **139**(1–3), 61–88 (1999)
21. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, pp. 75–83. Association for Computing Machinery (2002)
22. Faugère, J.-C., Safey El Din, M., Spaenlehauer, P.J.: Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, pp. 257–264. Association for Computing Machinery, New York, United States (2010)
23. Faugère, J.-C., Levy-dit Vehel, F., Perret, L.: Cryptanalysis of minrank. In: Advances in Cryptology–CRYPTO 2008: 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings 28, pp. 280–296. Springer (2008)
24. Felix, F.: Elliptic curves over rings with a point of view on cryptography and factoring. Ph.D. thesis, Carl von Ossietzky-Universität Oldenburg (2005). https://user.math.uzh.ch/fontein/diplom-fontein.pdf
25. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Trans. Inf. Theory **62**(2), 1006–1019 (2016)
26. Gianni, P., Mora, T.: Algebraic solution of systems of polynomial equations using Groebner bases. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 5th International Conference, AAECC-5 Menorca, Spain, June 15–19, 1987 Proceedings 5, pp. 247–257. Springer (1989)

27. Gorla, E., Ravagnani, A.: An algebraic framework for end-to-end physical-layer network coding. IEEE Trans. Inf. Theory **64**(6), 4480–4495 (2017)
28. Hashemi, A., Alvandi, P.: Applying Buchberger's criteria for computing Gröbner bases over finite-chain rings. J. Algebra Appl. **12**(07), 1350034 (2013)
29. Kalachi, H.T., Kamche, H.T.: On the rank decoding problem over finite principal ideal rings. Adv. Math. Commun. (2023)
30. Kamche, H.T., Kalachi, H.T., Djomou, F.R.K., Fouotsa, E.: Low-rank parity-check codes over finite commutative rings. Applicable Algebra Eng. Commun. Comput. **10**, 1–27 (2024)
31. Kamche, H.T., Mouaha, C.: Rank-metric codes over finite principal ideal rings and applications. IEEE Trans. Inf. Theory **65**(12), 7718–7735 (2019)
32. Kamwa Djomou, F.R., Kalachi, H.T., Fouotsa, E.: Generalization of low rank parity-check (LRPC) codes over the ring of integers modulo a positive integer. Arab. J. Math. **10**(2), 357–366 (2021)
33. Kaplansky, I.: Elementary divisors and modules. Trans. Am. Math. Soc. **66**(2), 464–491 (1949)
34. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Wiener, M. (ed.) Advances in Cryptology—CRYPTO' 99, pp. 19–30. Springer, Berlin Heidelberg, Berlin, Heidelberg (1999)
35. Kulkarni, A.: Solving p-adic polynomial systems via iterative eigenvector algorithms. Linear Multilinear Algebra **70**(4), 650–671 (2022)
36. Lazard, D.: Solving zero-dimensional algebraic systems. J. Symb. Comput. **13**(2), 117–131 (1992)
37. Lee, C.: Some properties of nonbinary error-correcting codes. IRE Trans. Inf. Theory **4**(2), 77–82 (1958)
38. Martınez-Moro, E., Szabo, S.: On codes over local Frobenius non-chain rings of order 16. Noncommutative rings and their applications. Contemp. Math **634**, 227–243 (2015)
39. McDonald, B.R.: Finite Rings with Identity, vol. 28. Marcel Dekker Incorporated, New York (1974)
40. Mikhailov, D., Nechaev, A.A.: Solving systems of polynomial equations over Galois–Eisenstein rings with the use of the canonical generating systems of polynomial ideals. Discrete Math. Appl. (2004)
41. Möller, H.M.: On the construction of Gröbner bases using syzygies. J. Symb. Comput. **6**(2–3), 345–359 (1988)
42. Nechaev, A.A.: Finite rings with applications. Handb. Algebra **5**, 213–320 (2008)
43. Neiger, V., Rosenkilde, J., Schost, É.: Fast computation of the roots of polynomials over the ring of power series. In: Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, pp. 349–356. Association for Computing Machinery, New York, United States (2017)
44. Norton, G.H., Sălăgean, A.: On the structure of linear and cyclic codes over a finite chain ring. Appl. Algebra Eng. Commun. Comput. **10**, 489–506 (2000)
45. Norton, G.H., Salagean, A.: Strong Gröbner bases and cyclic codes over a finite-chain ring. Electron. Notes Discrete Math. **6**, 240–250 (2001)
46. Norton, G.H., Salagean, A.: Strong Gröbner bases for polynomials over a principal ideal ring. Bull. Aust. Math. Soc. **64**(3), 505–528 (2001)
47. Ore, O.: Theory of non-commutative polynomials. Ann. Math., pp. 480–508 (1933)
48. Ourivski, A.V., Johansson, T.: New technique for decoding codes in the rank metric and its cryptography applications. Probl. Inf. Transm. **38**(3), 237–246 (2002)
49. Renner, J., Neri, A., Puchinger, S.: Low-rank parity-check codes over Galois rings. Des. Codes Crypt. **89**, 351–386 (2021)
50. Storjohann, A.: Algorithms for matrix canonical forms. Ph.D. thesis, ETH Zurich (2000)
51. The Sage Developers: SageMath, the Sage Mathematics Software System (2023). https://www.sagemath.org
52. Vaccon, T.: Matrix-F5 algorithms over finite-precision complete discrete valuation fields. In: Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation, pp. 397–404. Association for Computing Machinery, New York, United States (2014)
53. Weger, V., Khathuria, K., Horlemann, A.L., Battaglioni, M., Santini, P., Persichetti, E.: On the hardness of the Lee syndrome decoding problem. Adv. Math. Commun. (2022)
54. Yengui, I.: Constructive commutative algebra: projective modules over polynomial rings and dynamical Gröbner bases. Lecture Notes in Mathematics. Springer International Publishing (2015)

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