Solving Systems of Algebraic Equations Over Finite Commutative Rings and Applications

Hermann Tchatchiem Kamche
hermann.tchatchiem@unine.ch
University of Neuchatel, Switzerland

COGNAC 2023
CIRM

Outline

Motivation : Cryptography

The best attacks on rank metric code-based cryptosystems over fields use the following proposition.

Proposition 1

Let $\mathbf{A}$ *be a matrix with entries from a field* F*. Then,* $\forall \alpha \in F$, $\alpha \neq 0$.

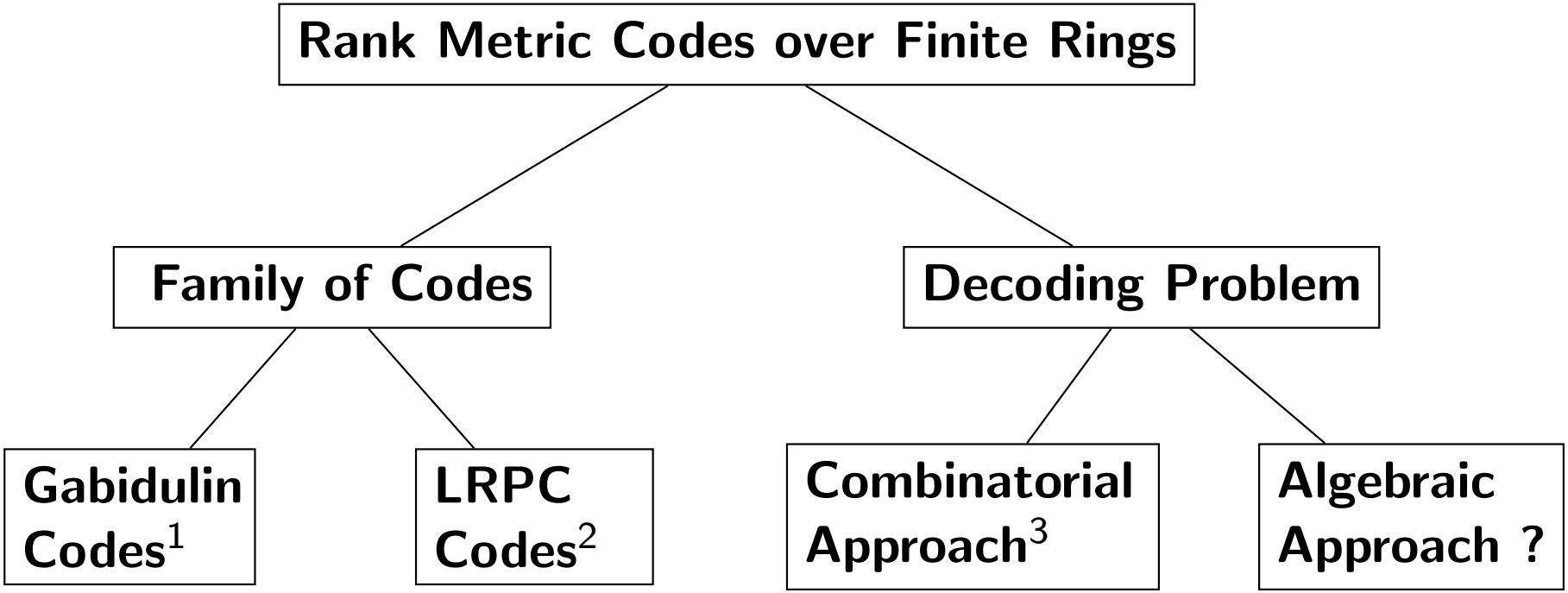
$$rank\,(\alpha \mathbf{A}) = rank\,(\mathbf{A})$$

The above proposition is not true over finite rings in general due to zero divisors.

Example 2

Over $\mathbb{Z}/4\mathbb{Z}$, if $\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ then, $2\mathbf{A} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$.

Thus, $rank\,(\mathbf{A}) = 2$ and $rank\,(2\mathbf{A}) = 1$.

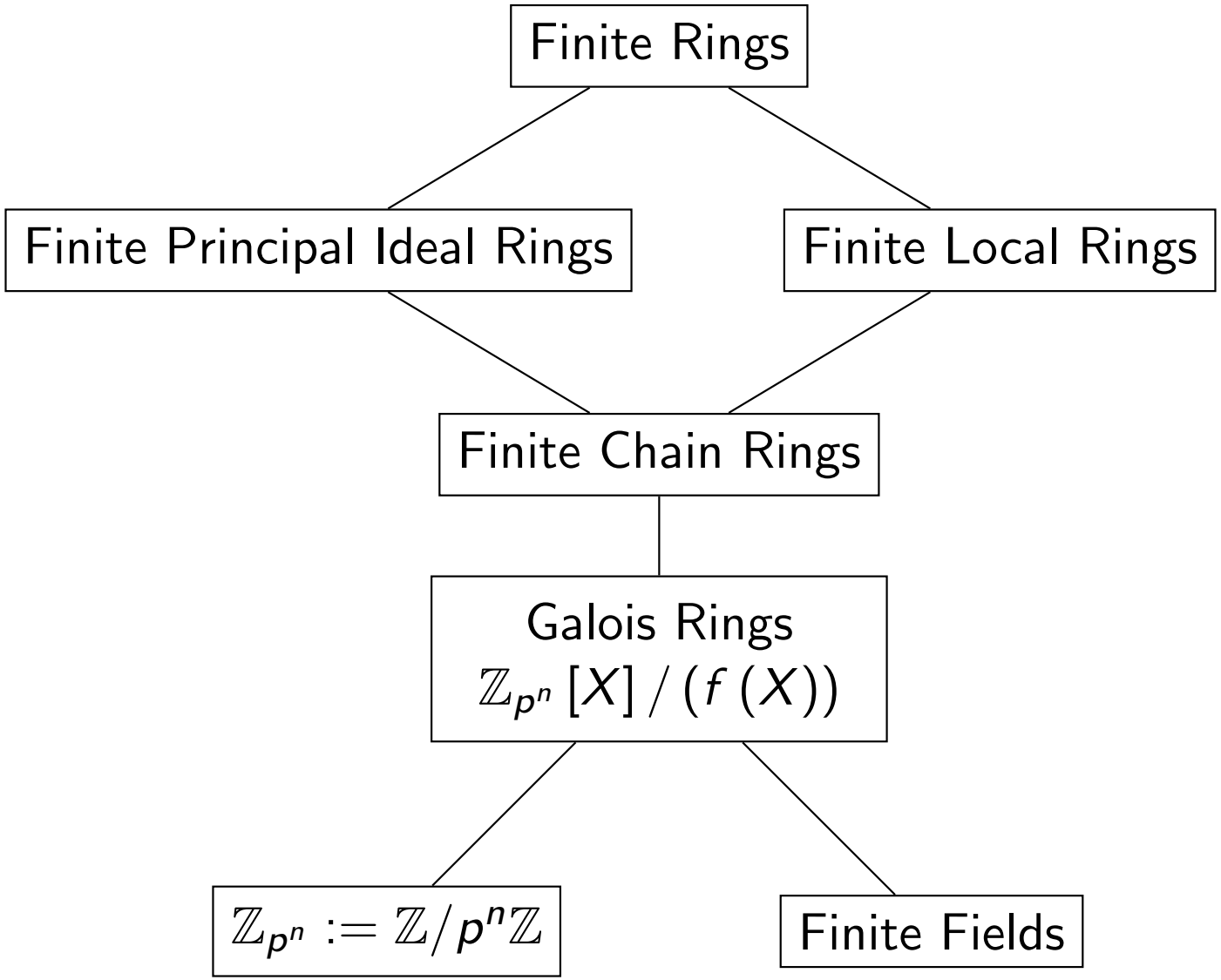


[1] **H. T. Kamche and C. Mouaha (2019)**, Rank-metric codes over finite principal ideal rings and applications

[2] **H.T. Kamche et al.**, Low-Rank Parity-Check codes over finite commutative rings, arXiv:2106.08712v2

[3] **H.T. Kalachi and H.T. Kamche (2023)**, On the rank decoding problem over finite principal ideal rings.

How to solve equations over finite commutative rings?



π-adic decomposition over finite chain rings

	Finite Chain Ring	Example
Ring	R	$\mathbb{Z}_8 := \mathbb{Z}/8\mathbb{Z}$
Maximal Ideal	πR	$2\mathbb{Z}_8$
Residue Field	$\mathbb{F}_q = R/\pi R$	$\mathbb{F}_2 = \mathbb{Z}_8/2\mathbb{Z}_8$
Coset Representations	$\Gamma \subset R$	$\Gamma = \{0, 1\}$
π-adic decomposition	$c = \sum_{j=0}^{\nu-1} c_j \pi^j, \;\; c_j \in \Gamma$	$6 = 0.2^0 + 1.2^1 + 1.2^2$

Solving with lifting approach over finite chain rings[4]

- The lifting approach consists to use solutions in the residue field $\mathbb{F}_q = R/\pi R$ to construct solutions in the ring R.
- Consider for example the following system over $\mathbb{Z}_8$:

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

- 2-adic decomposition over $\mathbb{Z}_8$: $y = y_0 + 2y_1 + 4y_2,\ \ y_i \in \Gamma = \{0, 1\}$
- $y \equiv y_0\ mod 2$ and $y \equiv y_0 + 2y_1\ mod 4$

[4] **D. Mikhailov and A. A. Nechaev (2004)**, Solving systems of polynomial equations over Galois Eisenstein rings with the use of the canonical generating systems of polynomial ideals.

Solving with lifting approach over finite chain rings

- The lifting approach consists to use solutions in the residue field $\mathbb{F}_q = R/\pi R$ to construct solutions in the ring R.
- Consider for example the following system over $\mathbb{Z}_8$:

$$\begin{cases} y^4 + 2y^2 + 4y = 0 \\ 2y^3 + 4y = 0 \end{cases} \iff \begin{cases} y^4 + 2y^2 + 4y \equiv 0 \ mod 8 \\ 2y^3 \equiv 0 \ mod 4 \\ y^3 \equiv 0 \ mod 2 \end{cases}$$

- 2-adic decomposition over $\mathbb{Z}_8$: $y = y_0 + 2y_1 + 4y_2,\ y_i \in \Gamma = \{0, 1\}$
- $y \equiv y_0 \ mod 2$ and $y \equiv y_0 + 2y_1 \ mod 4$
- $y_0 = 0,\quad y_1 \in \{0, 1\},\quad y_2 = 1$
- $y = 4$ or $y = 6$

Solving with lifting approach over finite chain rings

- The lifting approach is not appropriate for some systems of **multivariate** polynomial equations.

- For example, the following system over $\mathbb{Z}_8$ has 16 solutions

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

- When we use the lifting approach, we calculate **each** solution **step by step.**

Gröbner Bases Over Finite Chain Rings

- $x^{\alpha} := x_1^{d_1} \cdots x_k^{d_k}$ a monomial in $R[x_1, \ldots, x_k]$
- $f = c_1 x^{\alpha_1} + \cdots + c_s x^{\alpha_s}, \qquad x^{\alpha_1} > \cdots > x^{\alpha_s}$
- leading term: $lt(f) := c_1 x^{\alpha_1}$
- $lt(W) =$ the ideal generated by $\{lt(w) \mid w \in W\}$

Definition 3

Let I be an ideal in $R[x_1, \ldots, x_k]$ and G a subset of I.
(a) G is called a **Gröbner basis** for I if $lt(G) = lt(I)$.

[5] **G. H. Norton and A. Salagean (2001)**, Strong Gröbner bases for polynomials over a principal ideal ring.

Gröbner Bases Over Finite Chain Rings

- $x^{\alpha} := x_1^{d_1} \cdots x_k^{d_k}$ a monomial in $R[x_1, \ldots, x_k]$
- $f = c_1 x^{\alpha_1} + \cdots + c_s x^{\alpha_s}, \qquad x^{\alpha_1} > \cdots > x^{\alpha_s}$
- leading term: $lt(f) := c_1 x^{\alpha_1}$
- $lt(W) =$ the ideal generated by $\{lt(w) \mid w \in W\}$

Definition 3

Let I be an ideal in $R[x_1, \ldots, x_k]$ 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 any $f \in I$ there exists $g \in G$ such that $lt(g)$ divides $lt(f)$.

Over finite chain rings, Gröbner bases $\Longleftrightarrow$ Strong Gröbner bases.[5]

[5] **G. H. Norton and A. Salagean (2001)**, Strong Gröbner bases for polynomials over a principal ideal ring.

Elimination Theorem Over Finite Chain Rings[6]

Theorem 4

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

The elimination theorem makes it possible to iteratively solve algebraic systems by eliminating variables.

[6] **I. Yengui (2015)**, Constructive commutative algebra: projective modules over polynomial rings and dynamical Gröbner bases.

Elimination Theorem Over Finite Chain Rings[6]

Theorem 4

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

The elimination theorem makes it possible to iteratively solve algebraic systems by eliminating variables.

Example 5 ($\mathbb{Z}_8$, lexicographic order $x > y$)

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

[6] **I. Yengui (2015)**, Constructive commutative algebra: projective modules over polynomial rings and dynamical Gröbner bases.

Elimination Theorem Over Finite Chain Rings[6]

Theorem 4

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

The elimination theorem makes it possible to iteratively solve algebraic systems by eliminating variables.

Example 5 ($\mathbb{Z}_8$, lexicographic order $x > y$)

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

$y = 4$ or $y = 6$

[6] **I. Yengui (2015)**, Constructive commutative algebra: projective modules over polynomial rings and dynamical Gröbner bases.

Elimination Theorem Over Finite Chain Rings[6]

Theorem 4

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

The elimination theorem makes it possible to iteratively solve algebraic systems by eliminating variables.

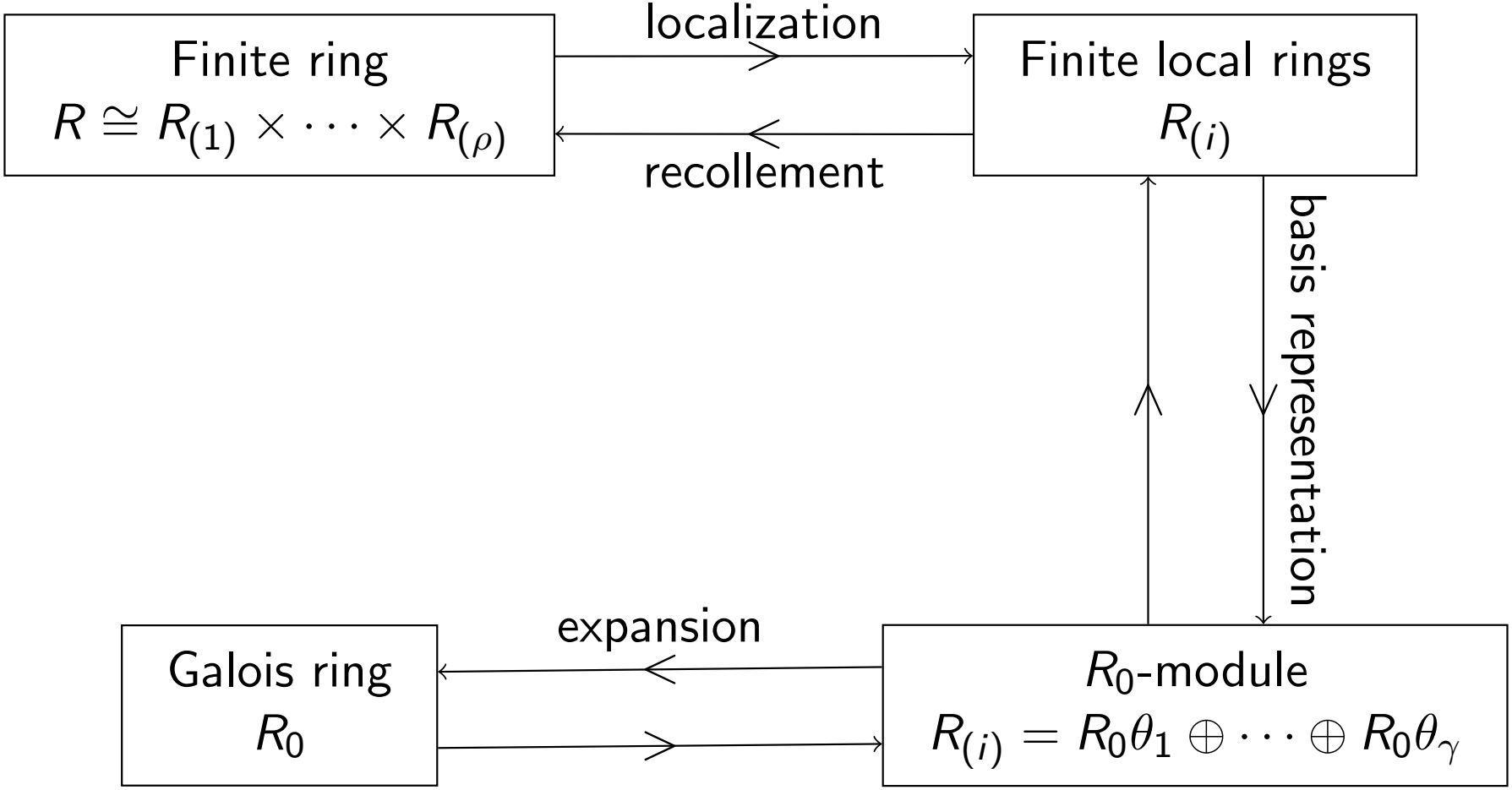
Example 5 ($\mathbb{Z}_8$, lexicographic order $x > y$)

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

$$y = 4 \quad \text{or} \quad y = 6 \quad \Rightarrow \quad (x, y) \in \{(t, 2), (t, 6), t \in \mathbb{Z}_8\}.$$

[6] **I. Yengui (2015)**, Constructive commutative algebra: projective modules over polynomial rings and dynamical Gröbner bases.

Local-Global Principle & Basis Representation[7]



[7] **B. R. McDonald (1974)**, Finite rings with identity.

Basis Representation of Finite Local Rings

- R_0 is a maximal Galois ring contained in the local ring R.
- Considering R as an R_0-module, there are $\theta_1, \ldots, \theta_\gamma$ in R such that

$$R = R_0\theta_1 \oplus \cdots \oplus R_0\theta_\gamma.$$

- For all j in $\{1, \ldots, \gamma\}$ there is ς_j in $\{1, \ldots, \varsigma\}$ such that

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

Lemma 6

$u = \sum_{j=1}^{\gamma} u_j\theta_j$, where u_j in R_0. The following statements are equivalent:
(a) $u = 0$;
(b) for all $j \in \{1, \ldots, \gamma\}$, $\theta_j u_j = 0$;
(c) for all $j \in \{1, \ldots, \gamma\}$, $p^{\varsigma - \varsigma_j} u_j = 0$.

$$R = R_0\theta_1 \oplus \cdots \oplus R_0\theta_\gamma.$$

Theorem 7

Consider a system of multivariate polynomial equations over R:

$$f_r\left((x_i)_{1\le i\le k}\right) = 0, \quad r = 1, \ldots, d \tag{1}$$

Set $x_i = \sum_{j=1}^{\gamma} x_{i,j}\theta_j$,

and $f_r\left((x_i)_{1\le i\le k}\right) = \sum_{s=1}^{\gamma} f_{r,s}\left((x_{i,j})_{1\le i\le k, 1\le j\le \gamma}\right)\theta_s$.

Then (1) is equivalent to

$$p^{\varsigma-\varsigma_s} f_{r,s}\left((x_{i,j})_{1\le i\le k, 1\le j\le \gamma}\right) = 0, \quad r = 1, \ldots, d,\ s = 1, \ldots, \gamma. \tag{2}$$

We can use Gröbner bases over finite chain rings, to solve (2).

Example

- $R = \mathbb{Z}_8[X]/I$ where I is the ideal generated by $X^2 + 4X$ and $2X$.
- A maximal Galois subring of R is $R_0 = \mathbb{Z}_8$.
- $R = \mathbb{Z}_8 \oplus \theta\mathbb{Z}_8$ where $\theta = X + I$.

Example

- $R = \mathbb{Z}_8[X]/I$ where I is the ideal generated by $X^2 + 4X$ and $2X$.
- A maximal Galois subring of R is $R_0 = \mathbb{Z}_8$.
- $R = \mathbb{Z}_8 \oplus \theta\mathbb{Z}_8$ where $\theta = X + I$.

- For finding roots over R of the polynomial: $P(z) = z^3 + 2z + 4$.
- Set $z = y + x\theta$, where $y, x \in \mathbb{Z}_8$.
- $$P(y + x\theta) = 4yx^3 + y^3 + 2y + 4 + \theta y^2 x.$$
- $$P(y + x\theta) = 0 \iff \begin{cases} 4x^3y + y^3 + 2y + 4 = 0 \\ 4y^2x = 0 \end{cases}$$

- The roots of P are 2, 6, $2 + \theta$, and $6 + \theta$.

MinRank Problem Over Finite Principal Ideal Rings R

- Let a matrix $\mathbf{A} \in R^{m \times n}$. The **rank** of $\mathbf{A}$, is the smallest number of elements in $col(\mathbf{A})$ which generate $col(\mathbf{A})$ as an R-module.

- Let $\mathbf{M}_0, \mathbf{M}_1, \ldots, \mathbf{M}_k$ in $R^{m \times n}$ and r in $\mathbb{N}^*$.
- The **MinRank problem** is to find $x_1, \ldots, x_k$ in R such that $rank(\mathbf{M}_0 + \sum_{i=1}^{k} x_i \mathbf{M}_i) \leq r$.

MinRank Problem Over Finite Principal Ideal Rings R

- Let a matrix $\mathbf{A} \in R^{m \times n}$. The **rank** of $\mathbf{A}$, is the smallest number of elements in $col(\mathbf{A})$ which generate $col(\mathbf{A})$ as an R-module.

- Let $\mathbf{M}_0, \mathbf{M}_1, \ldots, \mathbf{M}_k$ in $R^{m \times n}$ and r in $\mathbb{N}^*$.
- The **MinRank problem** is to find $x_1, \ldots, x_k$ in R such that $rank(\mathbf{M}_0 + \sum_{i=1}^{k} x_i \mathbf{M}_i) \leq r$.

Theorem 8 (Kipmis-Shamir Modeling)

The MinRank problem is equivalent to find $x_1, \ldots, x_k$ in R and $\mathbf{Z} \in R^{r \times (n-r)}$, such that

$$\left((\mathbf{M}_0 + \sum_{i=1}^{k} x_i \mathbf{M}_i) \right) \begin{pmatrix} \mathbf{I}_{n-r} \\ \mathbf{Z} \end{pmatrix} = \mathbf{0}$$

Rank Decoding Problem Over Finite Principal Ideal Rings

- S is a Galois Extension of R of degree m.
- σ a generator of the Galois group
- Let $\mathcal{C}$ be an S-submodule of S^n a generator matrix $\mathbf{G}$.
- $\mathbf{y}$ is an element of S^n and $r \in \mathbb{N}^*$.
- The **rank decoding problem** is to find $\mathbf{e}$ in S^n and $\mathbf{c}$ in $\mathcal{C}$ such that $\mathbf{y} = \mathbf{c} + \mathbf{e}$ with $rank(\mathbf{e}) \leq r$.

Rank Decoding Problem Over Finite Principal Ideal Rings

- S is a Galois Extension of R of degree m.
- σ a generator of the Galois group
- Let $\mathcal{C}$ be an S-submodule of S^n a generator matrix $\mathbf{G}$.
- $\mathbf{y}$ is an element of S^n and $r \in \mathbb{N}^*$.
- The **rank decoding problem** is to find $\mathbf{e}$ in S^n and $\mathbf{c}$ in $\mathcal{C}$ such that $\mathbf{y} = \mathbf{c} + \mathbf{e}$ with $rank(\mathbf{e}) \leq r$.

Theorem 9 (Algebraic Modeling with Skew Polynomials)

The rank decoding problem is equivalent to find $(z_l)_{0 \leq l \leq r} \in S^{r+1}$, $z_r = 1$, *and* $\mathbf{x} = (x_i)_{1 \leq i \leq k} \in S^k$ *such that*

$$\sum_{l=0}^{r} z_l \sigma^l(\mathbf{y}) = \sum_{l=0}^{r} z_l \sigma^l(\mathbf{xG})$$

Problem

- Some methods have been used to give an upper bound on the complexity of computing Gröbner bases over fields.[8]

- Can these methods be extended to rings?

[8] **A. Caminata and E. Gorla (2023)**, Solving degree, last fall degree, and related invariants.

Problem

- Some methods have been used to give an upper bound on the complexity of computing Gröbner bases over fields.[8]

- Can these methods be extended to rings?

Thank You!

[8] **A. Caminata and E. Gorla (2023)**, Solving degree, last fall degree, and related invariants.