Decoding in the Rank Metric: from Finite Fields to Finite Rings

Hervé Talé Kalachi
Lecturer (Chargé de cours)
University of Yaoundé I, Cameroon

Department of Computer Engineering
National Advanced School of Engineering of Yaounde (NASEY)
University of Yaoundé I

ETIS-ICI Seminar – CY Cergy Paris University, May 7, 2025

(This Talk is based on a work done with H. T. Kamche)

Plan de la présentation

Next

Linear code

1. $(\mathrm{R}^n, \|\cdot\|)$, R a finite field/ring and $\|\cdot\|$ a norm

2. Linear code $\mathscr{C}$ = free.sm of $(\mathrm{R}^n, \|\cdot\|)$

$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathrm{R}\ \vec{v}_i$$

where $\vec{v}_i$ are linearly independent.

3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ \cdot \\ \cdot \\ \cdot \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$

4. Decoding a word $\vec{w} \in \mathrm{R}^n$ = solving the closest vector problem (CVP)

Introduction

Linear code

1. $(\mathrm{R}^n, \|\cdot\|)$, R a finite field/ring and $\|\cdot\|$ a norm
2. Linear code $\mathscr{C}$ = free.sm of $(\mathrm{R}^n, \|\cdot\|)$

$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathrm{R}\ \vec{v}_i$$

where $\vec{v}_i$ are linearly independent.

3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ . \\ . \\ . \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$
4. Decoding a word $\vec{w} \in \mathrm{R}^n$ = solving the closest vector problem (CVP)

Introduction

Linear code

1. $(\mathrm{R}^n, \|\cdot\|)$, R a finite field/ring and $\|\cdot\|$ a norm
2. Linear code $\mathscr{C}$ = free.sm of $(\mathrm{R}^n, \|\cdot\|)$

$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathrm{R}\ \vec{v}_i$$

where $\vec{v}_i$ are linearly independent.

3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ . \\ . \\ . \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$
4. Decoding a word $\vec{w} \in \mathrm{R}^n$ = solving the closest vector problem (CVP)

Linear code

1. $(\mathrm{R}^n, \|\cdot\|)$, R a finite field/ring and $\|\cdot\|$ a norm

2. Linear code $\mathscr{C}$ = free.sm of $(\mathrm{R}^n, \|\cdot\|)$

$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathrm{R}\ \vec{v}_i$$

   where $\vec{v}_i$ are linearly independent.

3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ . \\ . \\ . \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$

4. Decoding a word $\vec{w} \in \mathrm{R}^n$ = solving the closest vector problem (CVP)

Introduction

Linear code

1. $(\mathrm{R}^n, \|\cdot\|)$, R a finite field/ring and $\|\cdot\|$ a norm

2. Linear code $\mathscr{C}$ = free.sm of $(\mathrm{R}^n, \|\cdot\|)$

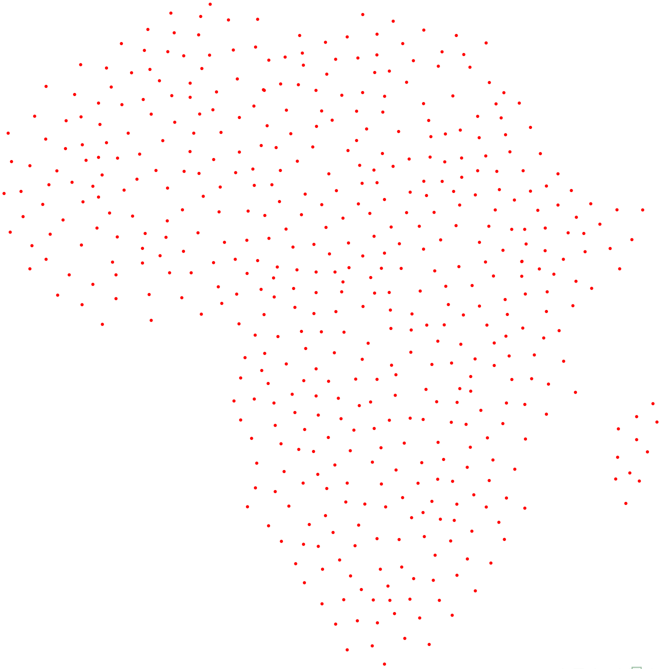
$$\mathscr{C} = \bigoplus_{i=1}^{k} \mathrm{R}\ \vec{v}_i$$

   where $\vec{v}_i$ are linearly independent.

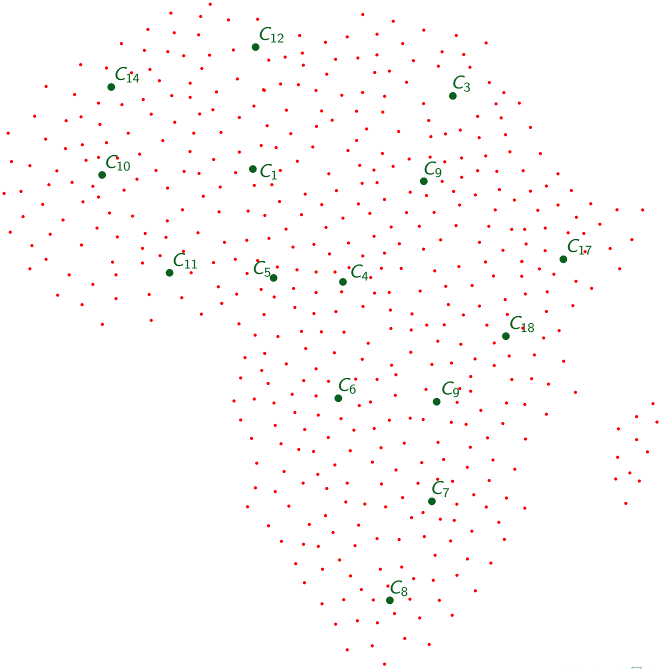
3. The matrix $\boldsymbol{G} = \begin{pmatrix} \vec{v}_1 \\ . \\ . \\ . \\ \vec{v}_k \end{pmatrix}$ is called a generator matrix of $\mathscr{C}$

4. Decoding a word $\vec{w} \in \mathrm{R}^n$ = solving the closest vector problem (CVP)

General Decoding Problem = Closest Vector Problem (CVP)



General Decoding Problem = Closest Vector Problem (CVP)



Hardness of decoding

- Decoding is NP-Hard for a "random" linear code
- For Hamming metric: Berlekamp-McEliece-Van Tilborg '78

Solving the decoding problem

- Information set decoding
- Introduced by Prange '62
- Complexity: $2^{at(1+o(1))}$

$$a = constante\left(\frac{k}{n}, \frac{t}{n}\right)$$

Hardness of decoding

- Decoding is NP-Hard for a "random" linear code
- For Hamming metric: Berlekamp-McEliece-Van Tilborg '78

Solving the decoding problem

- Information set decoding
- Introduced by Prange '62
- Complexity: $2^{at(1+o(1))}$

$$a = constante(\frac{k}{n}, \frac{t}{n})$$

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key = random basis
   - Private key = decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem

McEliece Cryptosystem ('78)

1. Based on linear codes equipped with an efficient decoding algorithm
   - Public key $=$ random basis
   - Private key $=$ decoding algorithm (good basis)
2. McEliece proposed binary Goppa codes

Security assumptions

- Indistinguishability of Goppa codes **Courtois-Finiasz-Sendrier '01**
- Hardness of decoding a "random" linear code

McEliece Cryptosystem ('78)

Advantages

1. Encryption and decryption are very fast
2. No efficient attack
3. Even for an attacker with a Quantum Computer

Drawbacks

1. Enormous size of the Public Key : More than 460 000 bits for a security level of only 80 bits.

McEliece Cryptosystem ('78)

Advantages

1. Encryption and decryption are very fast
2. No efficient attack
3. Even for an attacker with a Quantum Computer

Drawbacks

1. Enormous size of the Public Key : More than 460 000 bits for a security level of only 80 bits.

Rank Metric Vs Hamming Metric

Rank metric and Hamming metric

Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ and $\vec{x} = (x_1 \cdots x_n) \in \mathbb{F}_{q^m}^n \equiv \mathbb{F}_q^{m \times n}$.

$$\|\vec{x}\|_h = \#\{\ i\ :\ x_i \neq 0\}$$

$$\|\vec{x}\|_q = \dim\langle x_1, \cdots, x_n\rangle_{\mathbb{F}_q}$$

Example

- $\mathbb{F} = \mathbb{F}_{2^5} = \mathbb{F}_2 < w > = < 1, w, w^2, w^3, w^4 >_{\mathbb{F}_2}$
- $\vec{x} = (w, 0, 0, w)$

1. **Hamming metric:**
   - $\|\vec{x}\|_h = 2$
2. **Rank metric:**
   - $\|\vec{x}\|_2 = \dim\left(< w, w >_{\mathbb{F}_2}\right) = 1$

Rank Metric Vs Hamming Metric

Rank metric and Hamming metric

Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ and $\vec{x} = (x_1 \cdots x_n) \in \mathbb{F}_{q^m}^n \equiv \mathbb{F}_q^{m\times n}$.

$$\|\vec{x}\|_h = \#\{\ i\ :\ x_i \neq 0\}$$

$$\|\vec{x}\|_q = \dim\langle x_1, \cdots, x_n\rangle_{\mathbb{F}_q}$$

Example

- $\mathbb{F} = \mathbb{F}_{2^5} = \mathbb{F}_2 < w > = < 1, w, w^2, w^3, w^4 >_{\mathbb{F}_2}$
- $\vec{x} = (w, 0, 0, w)$

1. **Hamming metric:**
   - $\|\vec{x}\|_h = 2$
2. **Rank metric:**
   - $\|\vec{x}\|_2 = \dim\left(< w, w >_{\mathbb{F}_2}\right) = 1$

Rank Metric Vs Hamming Metric

Hardness of decoding

- For Hamming metric: Berlekamp-McEliece-Van Tilborg '78
- For Rank metric: Gaborit-Zémor '16

Complexity Comparison

Metric	Approach	Complexity
Hamming	• Information Set Decoding	$2^{at(1+o(1))}$, where $a = \text{const}\left(\frac{k}{n}, \frac{t}{n}\right)$
Rank	• Combinatorial attacks • Ourivski–Johannsson (2002)	$2^{tn+o(1)}$

Rank Metric Vs Hamming Metric

Hardness of decoding

* For Hamming metric: Berlekamp-McEliece-Van Tilborg '78
* For Rank metric: Gaborit-Zémor '16

Complexity Comparison

Metric	Approach	Complexity
Hamming	• Information Set Decoding	$2^{at(1+o(1))}$, where $a = \text{const}\left(\frac{k}{n}, \frac{t}{n}\right)$
Rank	• Combinatorial attacks • Ourivski–Johannsson (2002)	$2^{tn+o(1)}$

Rank-Based Cryptography

First Rank-Metric Encryption Scheme

- First proposal from at Eurocrypt'91 : GPT Cryptosystem
- Broken by Overbeck at Mycrypt'05

Recent Proposals

- New proposal at WCC'13 based on LRPC codes[a] (LDPC in the rank metric)
- Submissions to the NIST PQ competition (ROLLO, RQC)
  - ROLLO : Analogue of NTRU, uses LRPC codes
  - RQC : Security relying only on the CVP in the rank metric
  - Shorter public keys

[a] Gaborit, P., Murat, G., Ruatta, O., & Zemor, G. Low rank parity check codes and their application to cryptography. *WCC'13.*

Rank-Based Cryptography

First Rank-Metric Encryption Scheme

- First proposal from at Eurocrypt'91 : GPT Cryptosystem
- Broken by Overbeck at Mycrypt'05

Recent Proposals

- New proposal at WCC'13 based on LRPC codes[a] (LDPC in the rank metric)
- Submissions to the NIST PQ competition (ROLLO, RQC)
  - ROLLO : Analogue of NTRU, uses LRPC codes
  - RQC : Security relying only on the CVP in the rank metric
  - Shorter public keys

[a]Gaborit, P., Murat, G., Ruatta, O., & Zemor, G. Low rank parity check codes and their application to cryptography. *WCC'13.*

Rank-Based Cryptography

First Rank-Metric Encryption Scheme

- First proposal from at Eurocrypt'91 : GPT Cryptosystem
- Broken by Overbeck at Mycrypt'05

Recent Proposals

- New proposal at WCC'13 based on LRPC codes[a] (LDPC in the rank metric)
- Submissions to the NIST PQ competition (ROLLO, RQC)
  - ROLLO : Analogue of NTRU, uses LRPC codes
  - RQC : Security relying only on the CVP in the rank metric
  - Shorter public keys

[a] Gaborit, P., Murat, G., Ruatta, O., & Zemor, G. Low rank parity check codes and their application to cryptography. *WCC'13.*

Rank-Based Cryptography

First Rank-Metric Encryption Scheme

- First proposal from at Eurocrypt'91 : GPT Cryptosystem
- Broken by Overbeck at Mycrypt'05

Recent Proposals

- New proposal at WCC'13 based on LRPC codes[a] (LDPC in the rank metric)
- Submissions to the NIST PQ competition (ROLLO, RQC)
  - ROLLO : Analogue of NTRU, uses LRPC codes
  - RQC : Security relying only on the CVP in the rank metric
  - Shorter public keys

[a] Gaborit, P., Murat, G., Ruatta, O., & Zemor, G. Low rank parity check codes and their application to cryptography. *WCC'13.*

Rank Metric : Improvement of Algebraic Attacks in 2020

Solving the decoding problem in the rank metric

1. - Combinatorial attacks
   - Aragon-Gaborit-Hautville-Tillich '18

   $$2^{tn+o(1)}$$

2. - New algebraic attack
   - By Bardet et al. Eurocrypt'20

   $$2^{O(t\log_2(n))}$$

Consequenses

- Drastic reduction of security levels
- ROLLO−I−128/192/256 $\rightsquigarrow$ ROLLO−I−71/87/151
- RQC−256 $\rightsquigarrow$ RQC−188
- Elimination of ROLLO and RQC from the NIST competition

Rank Metric : Improvement of Algebraic Attacks in 2020

Solving the decoding problem in the rank metric

1.
- Combinatorial attacks
- Aragon-Gaborit-Hautville-Tillich '18

$$2^{tn+o(1)}$$

2.
- New algebraic attack
- By Bardet et al. Eurocrypt'20

$$2^{O(t\log_2(n))}$$

Consequenses

- Drastic reduction of security levels
- ROLLO$-$I$-$128/192/256 $\rightsquigarrow$ ROLLO$-$I$-$71/87/151
- RQC$-$256 $\rightsquigarrow$ RQC$-$188
- Elimination of ROLLO and RQC from the NIST competition

Rank Metric : Improvement of Algebraic Attacks in 2020

Solving the decoding problem in the rank metric

1. - Combinatorial attacks
   - Aragon-Gaborit-Hautville-Tillich '18

   $$2^{tn+o(1)}$$

2. - New algebraic attack
   - By Bardet et al. Eurocrypt'20

   $$2^{O(t\log_2(n))}$$

Consequenses

- Drastic reduction of security levels
- ROLLO−I−128/192/256 $\rightsquigarrow$ ROLLO−I−71/87/151
- RQC−256 $\rightsquigarrow$ RQC−188
- Elimination of ROLLO and RQC from the NIST competition

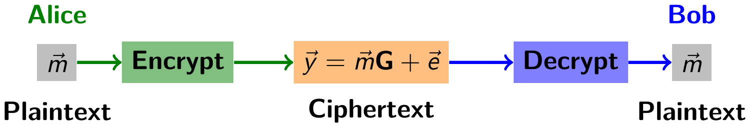
Excerpt from the NIST Report on the Second Round of the PQCS

"... Despite the development of algebraic attacks, NIST believes rank-based cryptography should continue to be researched. The rank metric cryptosystems offer a nice alternative to traditional hamming metric codes with comparable bandwidth... " [1]

[1] Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, **July 2020**

Starting Point for all Algebraic Attacks

- $\mathscr{C}$ is a $(n,k)_{\mathbb{F}_{q^m}}-$code generated by $\boldsymbol{G}$



Ourivski-Johannsson's Modelling

- $\mathscr{C}_{ext}$ the $(n,k+1)-$code generated by

$$\mathscr{C}_{ext} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_{\mathbb{F}_{q^m}} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{m}\boldsymbol{G} + \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}} = < \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}}$$

$$\Longrightarrow \exists \vec{c}\,' \in \mathscr{C}_{ext} \text{ s.t } \mathrm{Rank}_{\mathbb{F}_q}(\vec{c}\,') = r$$

- Each elt of the form $\lambda\vec{e}$, $\lambda \in \mathbb{F}_{q^m}^*$ is a good candidate

Starting Point of Recent Algebraic Attacks

- $\mathscr{C}$ is a $(n,k)_{\mathbb{F}_{q^m}}$ −code generated by $\boldsymbol{G}$

Alice — **Bob**

$\vec{m}$ → **Encrypt** → $\vec{y} = \vec{m}\mathbf{G} + \vec{e}$ → **Decrypt** → $\vec{m}$

Plaintext — **Ciphertext** — **Plaintext**

Ourivski-Johannsson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)$−code generated by

$$\mathscr{C}_{ext} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_{\mathbb{F}_{q^m}} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_{\mathbb{F}_{q^m}}$$

$$\Longrightarrow \exists \vec{c}\,' \in \mathscr{C}_{ext} \text{ s.t } \mathrm{Rank}_{\mathbb{F}_q}(\vec{c}\,') = r$$

- Each elt of the form $\lambda\vec{e}$, $\lambda \in \mathbb{F}_{q^m}^*$ is a good candidate

- $\mathscr{C}$ is a $(n, k)_S-$code generated by $\boldsymbol{G}$

Alice **Bob**

$\vec{m} \longrightarrow$ **Encrypt** $\longrightarrow \vec{y} = \vec{m}\mathbf{G} + \vec{e} \longrightarrow$ **Decrypt** $\longrightarrow \vec{m}$

Plaintext **Ciphertext** **Plaintext**

Ourivski-Johannsson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)-$code generated by

$$\mathscr{C}_{ext} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_S =< \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_S$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \mathrm{Rank}_R (\vec{c}') = r$$

- Each elt of the form $\lambda \vec{e}$, $\lambda \in S^*$ is a good candidate ?

Starting Point of Recent Algebraic Attacks

- $\mathscr{C}$ is a $(n,k)_S-$code generated by $\boldsymbol{G}$

Alice — **Bob**

$\vec{m} \longrightarrow$ **Encrypt** $\longrightarrow \vec{y} = \vec{m}\mathbf{G} + \vec{e} \longrightarrow$ **Decrypt** $\longrightarrow \vec{m}$

Plaintext — **Ciphertext** — **Plaintext**

Ourivski-Johannsson's Modelling

- $\mathscr{C}_{ext}$ the $(n, k+1)-$code generated by

$$\mathscr{C}_{ext} =< \begin{pmatrix} \boldsymbol{G} \\ \vec{y} \end{pmatrix} >_S =< \begin{pmatrix} \boldsymbol{G} \\ \vec{e} \end{pmatrix} >_S$$

$$\Longrightarrow \exists \vec{c}' \in \mathscr{C}_{ext} \text{ s.t } \mathrm{Rank}_R\,(\vec{c}') = r$$

- Each elt of the form $\lambda\vec{e}$, $\lambda \in S^*$ is a good candidate ?

Rank Decoding Problem over Finite Rings

Illustration with words viewed as matrices

- Let $R = \mathbb{Z}_6$ and $\boldsymbol{A} = \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix}$. $2\boldsymbol{A} = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$.
- We have

$$\mathrm{Rank}_{R}(\boldsymbol{A}) = 2, \text{ while } \mathrm{Rank}_{R}(2\boldsymbol{A}) = 1$$

- Ourivski-Johannsson's modelling is not applicable[2]
- All known algebraic attacks/costs are not applicable

[2] Kalachi & Kamche. On the rank decoding problem over finite principal ideal rings. *AMC'23*

Next

Finite Chain Rings

- A finite ring R is a finite chain ring if the set of its ideals forms a chain.
  * e.g. $\mathbb{Z}_{p^k} = \mathbb{Z}/p^k\mathbb{Z}$ with $k \in \mathbb{N}^*$ and p a prime number.

$$\{0\} \subset p^{k-1}\mathbb{Z}_{p^k} \subset p^{k-2}\mathbb{Z}_{p^k} \subset \cdots \subset p\mathbb{Z}_{p^k} \subset \mathbb{Z}_{p^k}$$

- Given a finite chain ring R, // e.g. $\mathbb{Z}_8 = \mathbb{Z}_{2^3} = \mathbb{Z}/2^3\mathbb{Z}$,
- $\mathfrak{m} = \pi R$ is the maximal ideal of R // $\mathfrak{m} = 2\mathbb{Z}_{2^3}$
- $\mathbb{F}_q = R/\mathfrak{m}$ is the residue field of R // $\mathbb{Z}_{2^3}/2\mathbb{Z}_{2^3} = \mathbb{F}_2$
- ν is the nilpotency index of π // $\nu = 3$

Finite Chain Rings

- A finite ring R is a finite chain ring if the set of its ideals forms a chain.
  * e.g. $\mathbb{Z}_{p^k} = \mathbb{Z}/p^k\mathbb{Z}$ with $k \in \mathbb{N}^*$ and p a prime number.

$$\{0\} \subset p^{k-1}\mathbb{Z}_{p^k} \subset p^{k-2}\mathbb{Z}_{p^k} \subset \cdots \subset p\mathbb{Z}_{p^k} \subset \mathbb{Z}_{p^k}$$

- Given a finite chain ring R, // e.g. $\mathbb{Z}_8 = \mathbb{Z}_{2^3} = \mathbb{Z}/2^3\mathbb{Z}$,
- $\mathfrak{m} = \pi R$ is the maximal ideal of R // $\mathfrak{m} = 2\mathbb{Z}_{2^3}$
- $\mathbb{F}_q = R/\mathfrak{m}$ is the residue field of R // $\mathbb{Z}_{2^3}/2\mathbb{Z}_{2^3} = \mathbb{F}_2$
- ν is the nilpotency index of π // $\nu = 3$

Finite Chain Rings

- A finite ring R is a finite chain ring if the set of its ideals forms a chain.
  * e.g. $\mathbb{Z}_{p^k} = \mathbb{Z}/p^k\mathbb{Z}$ with $k \in \mathbb{N}^*$ and p a prime number.

$$\{0\} \subset p^{k-1}\mathbb{Z}_{p^k} \subset p^{k-2}\mathbb{Z}_{p^k} \subset \cdots \subset p\mathbb{Z}_{p^k} \subset \mathbb{Z}_{p^k}$$

- Given a finite chain ring R, // e.g. $\mathbb{Z}_8 = \mathbb{Z}_{2^3} = \mathbb{Z}/2^3\mathbb{Z}$,
- $\mathfrak{m} = \pi R$ is the maximal ideal of R // $\mathfrak{m} = 2\mathbb{Z}_{2^3}$
- $\mathbb{F}_q = R/\mathfrak{m}$ is the residue field of R // $\mathbb{Z}_{2^3}/2\mathbb{Z}_{2^3} = \mathbb{F}_2$
- ν is the nilpotency index of π // $\nu = 3$

Finite Chain Rings

- A finite ring R is a finite chain ring if the set of its ideals forms a chain.
  * e.g. $\mathbb{Z}_{p^k} = \mathbb{Z}/p^k\mathbb{Z}$ with $k \in \mathbb{N}^*$ and p a prime number.

$$\{0\} \subset p^{k-1}\mathbb{Z}_{p^k} \subset p^{k-2}\mathbb{Z}_{p^k} \subset \cdots \subset p\mathbb{Z}_{p^k} \subset \mathbb{Z}_{p^k}$$

- Given a finite chain ring R, // e.g. $\mathbb{Z}_8 = \mathbb{Z}_{2^3} = \mathbb{Z}/2^3\mathbb{Z}$,
- $\mathfrak{m} = \pi R$ is the maximal ideal of R // $\mathfrak{m} = 2\mathbb{Z}_{2^3}$
- $\mathbb{F}_q = R/\mathfrak{m}$ is the residue field of R // $\mathbb{Z}_{2^3}/2\mathbb{Z}_{2^3} = \mathbb{F}_2$
- ν is the nilpotency index of π // $\nu = 3$

Finite Chain Rings

- A finite ring R is a finite chain ring if the set of its ideals forms a chain.
  * e.g. $\mathbb{Z}_{p^k} = \mathbb{Z}/p^k\mathbb{Z}$ with $k \in \mathbb{N}^*$ and p a prime number.

$$\{0\} \subset p^{k-1}\mathbb{Z}_{p^k} \subset p^{k-2}\mathbb{Z}_{p^k} \subset \cdots \subset p\mathbb{Z}_{p^k} \subset \mathbb{Z}_{p^k}$$

- Given a finite chain ring R, // e.g. $\mathbb{Z}_8 = \mathbb{Z}_{2^3} = \mathbb{Z}/2^3\mathbb{Z}$,
- $\mathfrak{m} = \pi R$ is the maximal ideal of R // $\mathfrak{m} = 2\mathbb{Z}_{2^3}$
- $\mathbb{F}_q = R/\mathfrak{m}$ is the residue field of R // $\mathbb{Z}_{2^3}/2\mathbb{Z}_{2^3} = \mathbb{F}_2$
- ν is the nilpotency index of π // $\nu = 3$

Galois Extension of a FCR : $\mathbb{Z}_8$

Let us take $R = \mathbb{Z}_8 = \mathbb{Z}_{2^3}$ and consider the polynomial

$$h(X) = X^3 + 6X^2 + 3X + 1 \in R[X].$$

Its projection modulo 2 is

$$\Psi(h)(X) = X^3 + X + 1,$$

which is irreducible in $\mathbb{F}_2[X]$.

Consider the ring

$$S = \mathbb{Z}_8[X]/(h(X))$$

S is said to be a Galois extension of degree 3 of $\mathbb{Z}_8$.

Galois Extension of a FCR : $\mathbb{Z}_8$

Let us take $R = \mathbb{Z}_8 = \mathbb{Z}_{2^3}$ and consider the polynomial

$$h(X) = X^3 + 6X^2 + 3X + 1 \in R[X].$$

Its projection modulo 2 is

$$\Psi(h)(X) = X^3 + X + 1,$$

which is irreducible in $\mathbb{F}_2[X]$.

Consider the ring

$$S = \mathbb{Z}_8[X]/(h(X))$$

S is said to be a Galois extension of degree 3 of $\mathbb{Z}_8$.

Galois Extension of a FCR : $\mathbb{Z}_8$

Let us take $R = \mathbb{Z}_8 = \mathbb{Z}_{2^3}$ and consider the polynomial

$$h(X) = X^3 + 6X^2 + 3X + 1 \in R[X].$$

Its projection modulo 2 is

$$\Psi(h)(X) = X^3 + X + 1,$$

which is irreducible in $\mathbb{F}_2[X]$.

Consider the ring

$$S = \mathbb{Z}_8[X]/(h(X))$$

S is said to be a Galois extension of degree 3 of $\mathbb{Z}_8$.

Rank Metric

Definition 1

Let S be a Galois extension of degree m over a finite chain ring R. Let $\beta = (\beta_1, \ldots, \beta_m)$ be an R-basis of S. Any vector $\vec{x} = (x_1, \ldots, x_n) \in S^n$ can be uniquely represented as a matrix over R:

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

So that $\vec{x} = \beta \boldsymbol{X}$. The **rank of** $\vec{x}$, denoted $\mathrm{Rank}_R(\vec{x})$, is defined as:

$$\mathrm{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}).$$

The **support** of $\vec{x}$, denoted $\mathrm{supp}_R(\vec{x})$, is the R-submodule of $R^m \equiv S$ generated by the columns of $\boldsymbol{X}$:

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

Rank Metric

Definition 1

Let S be a Galois extension of degree m over a finite chain ring R. Let $\beta = (\beta_1, \ldots, \beta_m)$ be an R-basis of S. Any vector $\vec{x} = (x_1, \ldots, x_n) \in S^n$ can be uniquely represented as a matrix over R:

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

So that $\vec{x} = \beta \boldsymbol{X}$. The **rank of** $\vec{x}$, denoted $\mathrm{Rank}_R(\vec{x})$, is defined as:

$$\mathrm{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}).$$

The **support** of $\vec{x}$, denoted $\mathrm{supp}_R(\vec{x})$, is the R-submodule of $R^m \equiv S$ generated by the columns of $\boldsymbol{X}$:

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

Rank Metric

Definition 1

Let S be a Galois extension of degree m over a finite chain ring R. Let $\beta = (\beta_1, \ldots, \beta_m)$ be an R-basis of S. Any vector $\vec{x} = (x_1, \ldots, x_n) \in S^n$ can be uniquely represented as a matrix over R:

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

So that $\vec{x} = \beta \boldsymbol{X}$. The **rank of** $\vec{x}$, denoted $\mathtt{Rank}_R(\vec{x})$, is defined as:

$$\mathtt{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}).$$

The **support** of $\vec{x}$, denoted $\mathrm{supp}_R(\vec{x})$, is the R-submodule of $R^m \equiv S$ generated by the columns of $\boldsymbol{X}$:

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

Rank Metric

Definition 1

Let S be a Galois extension of degree m over a finite chain ring R. Let $\beta = (\beta_1, \ldots, \beta_m)$ be an R-basis of S. Any vector $\vec{x} = (x_1, \ldots, x_n) \in S^n$ can be uniquely represented as a matrix over R:

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

So that $\vec{x} = \beta \boldsymbol{X}$. The **rank of** $\vec{x}$, denoted $\mathtt{Rank}_R(\vec{x})$, is defined as:

$$\mathtt{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}).$$

The **support** of $\vec{x}$, denoted $\mathrm{supp}_R(\vec{x})$, is the R-submodule of $R^m \equiv S$ generated by the columns of $\boldsymbol{X}$:

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

Rank Metric

Example

Consider the finite chain ring $R = \mathbb{Z}_4$ and the extension

$$S = \frac{\mathbb{Z}_4[X]}{(X^3 + 3X + 1)} = \frac{\mathbb{Z}_4[X]}{(f(X))},$$

of degree $m = 3$ over R.

- $a := X \mod f(X)$
- $S = R[a] = \langle 1, a, a^2 \rangle_R$.
- $\vec{x} = (1 + 2a + 3a^2,\ 2 + 2a^2,\ 2a,\ 0) \in S^4$

Its matrix representation over R is:

$$\boldsymbol{X} = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 3 & 2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Thus, $\mathrm{Rank}_R(\vec{x}) = 2$.

Rank Metric

Example

Consider the finite chain ring $R = \mathbb{Z}_4$ and the extension

$$S = \frac{\mathbb{Z}_4[X]}{(X^3 + 3X + 1)} = \frac{\mathbb{Z}_4[X]}{(f(X))},$$

of degree $m = 3$ over R.

- $a := X \mod f(X)$
- $S = R[a] = \langle 1, a, a^2 \rangle_R$.
- $\vec{x} = (1 + 2a + 3a^2,\ 2 + 2a^2,\ 2a,\ 0) \in S^4$

Its matrix representation over R is:

$$\boldsymbol{X} = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 3 & 2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Thus, $\mathrm{Rank}_R(\vec{x}) = 2$.

Rank Metric

Example

Consider the finite chain ring $R = \mathbb{Z}_4$ and the extension

$$S = \frac{\mathbb{Z}_4[X]}{(X^3 + 3X + 1)} = \frac{\mathbb{Z}_4[X]}{(f(X))},$$

of degree $m = 3$ over R.

- $a := X \mod f(X)$
- $S = R[a] = \langle 1, a, a^2 \rangle_R$.
- $\vec{x} = (1 + 2a + 3a^2,\ 2 + 2a^2,\ 2a,\ 0) \in S^4$

Its matrix representation over R is:

$$\boldsymbol{X} = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 3 & 2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Thus, $\mathrm{Rank}_R(\vec{x}) = 2$.

Rank Metric

Example

Consider the finite chain ring $R = \mathbb{Z}_4$ and the extension

$$S = \frac{\mathbb{Z}_4[X]}{(X^3 + 3X + 1)} = \frac{\mathbb{Z}_4[X]}{(f(X))},$$

of degree $m = 3$ over R.

- $a := X \mod f(X)$
- $S = R[a] = \langle 1, a, a^2 \rangle_R$.
- $\vec{x} = (1 + 2a + 3a^2,\ 2 + 2a^2,\ 2a,\ 0) \in S^4$

Its matrix representation over R is:

$$\boldsymbol{X} = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 3 & 2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Thus, $\mathrm{Rank}_R(\vec{x}) = 2$.

Rank Metric

Example

Consider the finite chain ring $R = \mathbb{Z}_4$ and the extension

$$S = \frac{\mathbb{Z}_4[X]}{(X^3 + 3X + 1)} = \frac{\mathbb{Z}_4[X]}{(f(X))},$$

of degree $m = 3$ over R.

- $a := X \mod f(X)$
- $S = R[a] = \langle 1, a, a^2 \rangle_R$.
- $\vec{x} = (1 + 2a + 3a^2,\ 2 + 2a^2,\ 2a,\ 0) \in S^4$

Its matrix representation over R is:

$$\boldsymbol{X} = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 3 & 2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Thus, $\mathtt{Rank}_R(\vec{x}) = 2$.

Next

Rank Decoding Problem over Finite Chain Rings

- R is a finite chain ring
- S is a Galois extension of R

Definition 2 (Rank Decoding Problem $\mathcal{RD}$)

- Let $\mathcal{C}$ be a (n, k)-linear code over S
- $\vec{y} \in S^n$ and $t \in \mathbb{N}^*$

The *Rank Decoding Problem* is to find $\vec{e} \in S^n$ and $\vec{c} \in \mathcal{C}$ such that :

$$\vec{y} = \vec{c} + \vec{e} \text{ and } \mathtt{Rank}_R(\vec{e}) \leqslant t$$

- Let $\mathbf{H} \in S^{(n-k)\times n}$, be a parity check matrix of $\mathcal{C}$

$$\text{i.e. } \forall \vec{c} \in \mathcal{C},\ \vec{c}\boldsymbol{H}^\top = \vec{0}$$

- We have

$$\vec{y}\boldsymbol{H}^\top = (\vec{c} + \vec{e})\boldsymbol{H}^\top = \vec{c}\boldsymbol{H}^\top + \vec{e}\boldsymbol{H}^\top = \vec{e}\boldsymbol{H}^\top$$

Rank Decoding Problem over Finite Chain Rings

- R is a finite chain ring
- S is a Galois extension of R

Definition 2 (Rank Decoding Problem $\mathcal{RD}$)

- Let $\mathcal{C}$ be a (n, k)-linear code over S
- $\vec{y} \in S^n$ and $t \in \mathbb{N}^*$

The *Rank Decoding Problem* is to find $\vec{e} \in S^n$ and $\vec{c} \in \mathcal{C}$ such that :

$$\vec{y} = \vec{c} + \vec{e} \text{ and } \mathrm{Rank}_R(\vec{e}) \leqslant t$$

- Let $\mathbf{H} \in S^{(n-k)\times n}$, be a parity check matrix of $\mathcal{C}$

$$\text{i.e. } \forall \vec{c} \in \mathcal{C},\ \vec{c}\boldsymbol{H}^{\top} = \vec{0}$$

- We have

$$\vec{y}\boldsymbol{H}^{\top} = (\vec{c} + \vec{e})\boldsymbol{H}^{\top} = \vec{c}\boldsymbol{H}^{\top} + \vec{e}\boldsymbol{H}^{\top} = \vec{e}\boldsymbol{H}^{\top}$$

Rank Decoding Problem over Finite Chain Rings

- R is a finite chain ring
- S is a Galois extension of R

Definition 2 (Rank Decoding Problem $\mathcal{RD}$)

- Let $\mathcal{C}$ be a (n, k)-linear code over S
- $\vec{y} \in S^n$ and $t \in \mathbb{N}^*$

The *Rank Decoding Problem* is to find $\vec{e} \in S^n$ and $\vec{c} \in \mathcal{C}$ such that :

$$\vec{y} = \vec{c} + \vec{e} \text{ and } \mathrm{Rank}_R(\vec{e}) \leqslant t$$

- Let $\mathbf{H} \in S^{(n-k)\times n}$, be a parity check matrix of $\mathcal{C}$

$$\text{i.e. } \forall \vec{c} \in \mathcal{C},\ \vec{c}\boldsymbol{H}^\top = \vec{0}$$

- We have

$$\vec{y}\boldsymbol{H}^\top = (\vec{c} + \vec{e})\boldsymbol{H}^\top = \vec{c}\boldsymbol{H}^\top + \vec{e}\boldsymbol{H}^\top = \vec{e}\boldsymbol{H}^\top$$

Rank Decoding Problem over Finite Chain Rings

- R is a finite chain ring
- S is a Galois extension of R

Definition 2 (Rank Decoding Problem $\mathcal{RD}$)

- Let $\mathcal{C}$ be a (n, k)-linear code over S
- $\vec{y} \in S^n$ and $t \in \mathbb{N}^*$

The *Rank Decoding Problem* is to find $\vec{e} \in S^n$ and $\vec{c} \in \mathcal{C}$ such that :

$$\vec{y} = \vec{c} + \vec{e} \text{ and } \mathrm{Rank}_R(\vec{e}) \leqslant t$$

- Let $\mathbf{H} \in S^{(n-k)\times n}$, be a parity check matrix of $\mathcal{C}$

$$\text{i.e. } \forall \vec{c} \in \mathcal{C},\ \vec{c}\boldsymbol{H}^\top = \vec{0}$$

- We have

$$\vec{y}\boldsymbol{H}^\top = (\vec{c} + \vec{e})\boldsymbol{H}^\top = \vec{c}\boldsymbol{H}^\top + \vec{e}\boldsymbol{H}^\top = \vec{e}\boldsymbol{H}^\top$$

Rank Decoding Problem over Finite Chain Rings

- R is a finite chain ring
- S is a Galois extension of R

Definition 2 (Rank Decoding Problem $\mathcal{RD}$)

- Let $\mathcal{C}$ be a (n,k)-linear code over S
- $\vec{y} \in S^n$ and $t \in \mathbb{N}^*$

The *Rank Decoding Problem* is to find $\vec{e} \in S^n$ and $\vec{c} \in \mathcal{C}$ such that :

$$\vec{y} = \vec{c} + \vec{e} \text{ and } \mathrm{Rank}_R(\vec{e}) \leqslant t$$

- Let $\mathbf{H} \in S^{(n-k)\times n}$, be a parity check matrix of $\mathcal{C}$

$$\text{i.e. } \forall \vec{c} \in \mathcal{C},\ \vec{c}\boldsymbol{H}^\top = \vec{0}$$

- We have

$$\vec{y}\boldsymbol{H}^\top = (\vec{c}+\vec{e})\boldsymbol{H}^\top = \vec{c}\boldsymbol{H}^\top + \vec{e}\boldsymbol{H}^\top = \vec{e}\boldsymbol{H}^\top$$

Rank Decoding Problem over Finite Chain Rings

- R is a finite chain ring
- S is a Galois extension of R

Definition 2 (Rank Decoding Problem $\mathcal{RD}$)

- Let $\mathcal{C}$ be a (n, k)-linear code over S
- $\vec{y} \in S^n$ and $t \in \mathbb{N}^*$

The *Rank Decoding Problem* is to find $\vec{e} \in S^n$ and $\vec{c} \in \mathcal{C}$ such that :

$$\vec{y} = \vec{c} + \vec{e} \text{ and } \mathrm{Rank}_R(\vec{e}) \leqslant t$$

- Let $\mathbf{H} \in S^{(n-k)\times n}$, be a parity check matrix of $\mathcal{C}$

$$\text{i.e. } \forall \vec{c} \in \mathcal{C},\ \vec{c}\boldsymbol{H}^\top = \vec{0}$$

- We have

$$\vec{y}\boldsymbol{H}^\top = (\vec{c} + \vec{e})\boldsymbol{H}^\top = \vec{c}\boldsymbol{H}^\top + \vec{e}\boldsymbol{H}^\top = \vec{e}\boldsymbol{H}^\top$$

Rank Decoding Problem over Finite Chain Rings

- R is a finite chain ring
- S is a Galois extension of R

Definition 2 (Rank Decoding Problem $\mathcal{RD}$)

- Let $\mathcal{C}$ be a (n, k)-linear code over S
- $\vec{y} \in S^n$ and $t \in \mathbb{N}^*$

The *Rank Decoding Problem* is to find $\vec{e} \in S^n$ and $\vec{c} \in \mathcal{C}$ such that :

$$\vec{y} = \vec{c} + \vec{e} \text{ and } \mathrm{Rank}_R(\vec{e}) \leqslant t$$

- Let $\mathbf{H} \in S^{(n-k)\times n}$, be a parity check matrix of $\mathcal{C}$

$$\text{i.e. } \forall \vec{c} \in \mathcal{C},\ \vec{c}\boldsymbol{H}^\top = \vec{0}$$

- We have

$$\vec{y}\boldsymbol{H}^\top = (\vec{c} + \vec{e})\boldsymbol{H}^\top = \vec{c}\boldsymbol{H}^\top + \vec{e}\boldsymbol{H}^\top = \vec{e}\boldsymbol{H}^\top$$

Rank Decoding Problem over Finite Chain Rings

- R is a finite chain ring
- S is a Galois extension of R

Definition 2 (Rank Decoding Problem $\mathcal{RD}$)

- Let $\mathcal{C}$ be a (n, k)-linear code over S
- $\vec{y} \in S^n$ and $t \in \mathbb{N}^*$

The *Rank Decoding Problem* is to find $\vec{e} \in S^n$ and $\vec{c} \in \mathcal{C}$ such that :

$$\vec{y} = \vec{c} + \vec{e} \text{ and } \mathtt{Rank}_R(\vec{e}) \leqslant t$$

- Let $\mathbf{H} \in S^{(n-k)\times n}$, be a parity check matrix of $\mathcal{C}$

$$\text{i.e. } \forall \vec{c} \in \mathcal{C},\ \vec{c}\boldsymbol{H}^\top = \vec{0}$$

- We have

$$\vec{y}\boldsymbol{H}^\top = (\vec{c} + \vec{e})\boldsymbol{H}^\top = \vec{c}\boldsymbol{H}^\top + \vec{e}\boldsymbol{H}^\top = \vec{e}\boldsymbol{H}^\top$$

Rank Syndrome Decoding Problem over Finite Chain Rings

- Let $\mathbf{H} \in S^{(n-k)\times n}$, be a parity check matrix of $\mathcal{C}$

$$\text{i.e. } \forall \vec{c} \in \mathcal{C},\ \vec{c}\boldsymbol{H}^\top = \vec{0}$$

- We have

$$\vec{y}\boldsymbol{H}^\top = (\vec{c}+\vec{e})\boldsymbol{H}^\top = \vec{c}\boldsymbol{H}^\top + \vec{e}\boldsymbol{H}^\top = \vec{e}\boldsymbol{H}^\top = \vec{s}$$

Definition 3 (Rank Syndrome Decoding Problem $\mathcal{RSD}$)

- $\mathbf{H} \in S^{(n-k)\times n}$,
- $\vec{s} \in S^{n-k}$ and $t \in \mathbb{N}^*$

The *Rank Syndrome Decoding Problem* is to find $\vec{e}$ in S^n such that

$$\vec{s} = \vec{e}\boldsymbol{H}^\top \text{ and } \mathrm{Rank}_R(\vec{e}) \leqslant t$$

- Let $\mathbf{H} \in S^{(n-k)\times n}$, be a parity check matrix of $\mathcal{C}$

$$\text{i.e. } \forall \vec{c} \in \mathcal{C},\ \ \vec{c}\boldsymbol{H}^\top = \vec{0}$$

- We have

$$\vec{y}\boldsymbol{H}^\top = (\vec{c} + \vec{e})\boldsymbol{H}^\top = \vec{c}\boldsymbol{H}^\top + \vec{e}\boldsymbol{H}^\top = \vec{e}\boldsymbol{H}^\top = \vec{s}$$

Definition 3 (Rank Syndrome Decoding Problem $\mathcal{RSD}$)

- $\mathbf{H} \in S^{(n-k)\times n}$,
- $\vec{s} \in S^{n-k}$ and $t \in \mathbb{N}^*$

The *Rank Syndrome Decoding Problem* is to find $\vec{e}$ in S^n such that

$$\vec{s} = \vec{e}\boldsymbol{H}^\top \text{ and } \mathtt{Rank}_R(\vec{e}) \leqslant t$$

Rank Syndrome Decoding Problem (example)

Setup

- Let $R = \mathbb{Z}_8$ and $S = R[a]$, where a is a root of the polynomial $h(x) = x^3 + 6x^2 + 3x + 1$.
- Then $\mathbf{b} = (1, a, a^2)$ forms an R-basis of S.
- Consider the $[3, 1, 3]$-linear code $\mathcal{C} \subset S^3$ generated by the matrix:

$$\boldsymbol{G} = \begin{pmatrix} 1 & a^2 + 5 & a^2 + a + 1 \end{pmatrix}$$

- Let

$$\vec{y} = (6a^2 + 3,\ \ 5a^2 + 1,\ \ 3a^2 + a + 7) \in S^3$$

- A parity check matrix of $\mathscr{C}$ is

$$\boldsymbol{H} = \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}$$

- And we have

$$\vec{s} = \vec{y}\boldsymbol{H}^\top = (6a^2 + 2a + 6,\ \ 2a + 6) \neq \vec{0}$$

Rank Syndrome Decoding Problem (example)

Setup

- Let $R = \mathbb{Z}_8$ and $S = R[a]$, where a is a root of the polynomial $h(x) = x^3 + 6x^2 + 3x + 1$.
- Then $\mathbf{b} = (1, a, a^2)$ forms an R-basis of S.
- Consider the $[3, 1, 3]$-linear code $\mathcal{C} \subset S^3$ generated by the matrix:

$$\boldsymbol{G} = \begin{pmatrix} 1 & a^2 + 5 & a^2 + a + 1 \end{pmatrix}$$

- Let

$$\vec{y} = \left(6a^2 + 3,\ 5a^2 + 1,\ 3a^2 + a + 7\right) \in S^3$$

- A parity check matrix of $\mathscr{C}$ is

$$\boldsymbol{H} = \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}$$

- And we have

$$\vec{s} = \vec{y}\boldsymbol{H}^\top = \left(6a^2 + 2a + 6,\ 2a + 6\right) \neq \vec{0}$$

Rank Syndrome Decoding Problem (example)

Setup

- Let $R = \mathbb{Z}_8$ and $S = R[a]$, where a is a root of the polynomial $h(x) = x^3 + 6x^2 + 3x + 1$.
- Then $\mathbf{b} = (1, a, a^2)$ forms an R-basis of S.
- Consider the $[3, 1, 3]$-linear code $\mathcal{C} \subset S^3$ generated by the matrix:

$$\boldsymbol{G} = \begin{pmatrix} 1 & a^2 + 5 & a^2 + a + 1 \end{pmatrix}$$

- Let

$$\vec{y} = (6a^2 + 3,\ 5a^2 + 1,\ 3a^2 + a + 7) \in S^3$$

- A parity check matrix of $\mathscr{C}$ is

$$\boldsymbol{H} = \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}$$

- And we have

$$\vec{s} = \vec{y}\boldsymbol{H}^\top = (6a^2 + 2a + 6,\ 2a + 6) \neq \vec{0}$$

Rank Syndrome Decoding Problem (example)

Setup

- Let $R = \mathbb{Z}_8$ and $S = R[a]$, where a is a root of the polynomial $h(x) = x^3 + 6x^2 + 3x + 1$.
- Then $\mathbf{b} = (1, a, a^2)$ forms an R-basis of S.
- Consider the $[3, 1, 3]$-linear code $\mathcal{C} \subset S^3$ generated by the matrix:

$$\boldsymbol{G} = \begin{pmatrix} 1 & a^2 + 5 & a^2 + a + 1 \end{pmatrix}$$

- Let

$$\vec{y} = \left(6a^2 + 3,\ \ 5a^2 + 1,\ \ 3a^2 + a + 7\right) \in S^3$$

- A parity check matrix of $\mathscr{C}$ is

$$\boldsymbol{H} = \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}$$

- And we have

$$\vec{s} = \vec{y}\boldsymbol{H}^\top = \left(6a^2 + 2a + 6,\ \ 2a + 6\right) \neq \vec{0}$$

Rank Syndrome Decoding Problem (example)

Setup

- Let $R = \mathbb{Z}_8$ and $S = R[a]$, where a is a root of the polynomial $h(x) = x^3 + 6x^2 + 3x + 1$.
- Then $\mathbf{b} = (1, a, a^2)$ forms an R-basis of S.
- Consider the $[3, 1, 3]$-linear code $\mathcal{C} \subset S^3$ generated by the matrix:

$$\boldsymbol{G} = \begin{pmatrix} 1 & a^2 + 5 & a^2 + a + 1 \end{pmatrix}$$

- Let

$$\vec{y} = \left(6a^2 + 3,\ \ 5a^2 + 1,\ \ 3a^2 + a + 7\right) \in S^3$$

- A parity check matrix of $\mathscr{C}$ is

$$\boldsymbol{H} = \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}$$

- And we have

$$\vec{s} = \vec{y}\boldsymbol{H}^\top = \left(6a^2 + 2a + 6,\ \ 2a + 6\right) \neq \vec{0}$$

Rank Syndrome Decoding Problem (example)

Setup

- Let $R = \mathbb{Z}_8$ and $S = R[a]$, where a is a root of the polynomial $h(x) = x^3 + 6x^2 + 3x + 1$.
- Then $\mathbf{b} = (1, a, a^2)$ forms an R-basis of S.
- Consider the $[3, 1, 3]$-linear code $\mathcal{C} \subset S^3$ generated by the matrix:

$$\boldsymbol{G} = \begin{pmatrix} 1 & a^2 + 5 & a^2 + a + 1 \end{pmatrix}$$

- Let

$$\vec{y} = \left(6a^2 + 3,\ \ 5a^2 + 1,\ \ 3a^2 + a + 7\right) \in S^3$$

- A parity check matrix of $\mathscr{C}$ is

$$\boldsymbol{H} = \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}$$

- And we have

$$\vec{s} = \vec{y}\boldsymbol{H}^\top = \left(6a^2 + 2a + 6,\ \ 2a + 6\right) \neq \vec{0}$$

Rank Syndrome Decoding Problem (example)

Setup

- Let $R = \mathbb{Z}_8$ and $S = R[a]$, where a is a root of the polynomial $h(x) = x^3 + 6x^2 + 3x + 1$.
- Then $\mathbf{b} = (1, a, a^2)$ forms an R-basis of S.
- Consider the $[3, 1, 3]$-linear code $\mathcal{C} \subset S^3$ generated by the matrix:

$$\boldsymbol{G} = \begin{pmatrix} 1 & a^2 + 5 & a^2 + a + 1 \end{pmatrix}$$

- Let

$$\vec{y} = \left(6a^2 + 3,\ \ 5a^2 + 1,\ \ 3a^2 + a + 7\right) \in S^3$$

- A parity check matrix of $\mathscr{C}$ is

$$\boldsymbol{H} = \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}$$

- And we have

$$\vec{s} = \vec{y}\boldsymbol{H}^\top = \left(6a^2 + 2a + 6,\ \ 2a + 6\right) = \vec{e}\boldsymbol{H}^\top \neq \vec{0}$$

So, $\vec{y} \notin \mathscr{C}$, and the problem here is to find $\vec{e} \in S^3$ so that $\vec{e}\boldsymbol{H}^\top = \vec{s}$ and $\mathtt{Rank}_R(\vec{e}) = 1$.

Next

Solving the RSD Problem over Finite Chain Rings

The following Lemma is from Kamche and Mouaha [3]

Lemma 4

- *Let S be a Galois extension of degree m of R*
- $\vec{e}$ *in* S^n *with* $\mathtt{Rank}_R(\vec{e}) = t$
- $u \in \mathbb{N}$ *such that* $t \leqslant u \leqslant m$

There exists a free submodule $F \subset S$ such that

$$supp(\vec{e}) = \langle e_1, \cdots, e_n \rangle_R \subset F \text{ and } \mathtt{Rank}_R(F) = u$$

Example (Keeping the previous setting)

Let $\vec{e} = (6a^2 + 2, \quad 4a^2 + 4, \quad 2a^2 + 6) \in S^3$, with $S = R[a]$ and $R = \mathbb{Z}_8$.

- We have $\mathtt{Rank}_R(\vec{e}) = 1$ and $m = 3$
- For $u = 2$, set

$$F = \langle 1, \quad a^2 \rangle_R$$

- One can see that F is free with rank 2 and $supp(\vec{e}) \subset F$.

[3] H. T. Kamche & C. Mouaha, Rank-metric codes over finite principal ideal rings and applications, *IEEE Tram. Inform. Theory, 2019.*

Solving the RSD Problem over Finite Chain Rings

The following Lemma is from Kamche and Mouaha [3]

Lemma 4

- *Let S be a Galois extension of degree m of R*
- *$\vec{e}$ in S^n with* $\texttt{Rank}_R(\vec{e}) = t$
- *$u \in \mathbb{N}$ such that $t \leqslant u \leqslant m$*

There exists a free submodule $F \subset S$ such that

$$supp(\vec{e}) = \langle e_1, \cdots, e_n \rangle_R \subset F \text{ and } \texttt{Rank}_R(F) = u$$

Example (Keeping the previous setting)

Let $\vec{e} = (6a^2 + 2, \quad 4a^2 + 4, \quad 2a^2 + 6) \in S^3$, with $S = R[a]$ and $R = \mathbb{Z}_8$.

- We have $\texttt{Rank}_R(\vec{e}) = 1$ and $m = 3$
- For $u = 2$, set

$$F = \langle 1, \quad a^2 \rangle_R$$

- One can see that F is free with rank 2 and $supp(\vec{e}) \subset F$.

[3] H. T. Kamche & C. Mouaha, Rank-metric codes over finite principal ideal rings and applications, *IEEE Tram. Inform. Theory, 2019.*

Solving the RSD Problem over Finite Chain Rings

The following Lemma is from Kamche and Mouaha [3]

Lemma 4

- *Let S be a Galois extension of degree m of R*
- $\vec{e}$ *in* S^n *with* $\mathrm{Rank}_R(\vec{e}) = t$
- $u \in \mathbb{N}$ *such that* $t \leqslant u \leqslant m$

There exists a free submodule $F \subset S$ such that

$$supp(\vec{e}) = \langle e_1, \cdots, e_n \rangle_R \subset F \text{ and } \mathrm{Rank}_R(F) = u$$

Example (Keeping the previous setting)

Let $\vec{e} = \left(6a^2 + 2, \quad 4a^2 + 4, \quad 2a^2 + 6\right) \in S^3$, with $S = R[a]$ and $R = \mathbb{Z}_8$.

- We have $\mathrm{Rank}_R(\vec{e}) = 1$ and $m = 3$
- For $u = 2$, set

$$F = \langle 1, \quad a^2 \rangle_R$$

- One can see that F is free with rank 2 and $supp(\vec{e}) \subset F$.

[3] H. T. Kamche & C. Mouaha, Rank-metric codes over finite principal ideal rings and applications, *IEEE Tram. Inform. Theory, 2019.*

Solving the RSD Problem over Finite Chain Rings

The following Lemma is from Kamche and Mouaha [3]

Lemma 4

- *Let S be a Galois extension of degree m of R*
- *$\vec{e}$ in S^n with $\mathtt{Rank}_R(\vec{e}) = t$*
- *$u \in \mathbb{N}$ such that $t \leqslant u \leqslant m$*

There exists a free submodule $F \subset S$ such that

$$supp(\vec{e}) = \langle e_1, \cdots, e_n \rangle_R \subset F \text{ and } \mathtt{Rank}_R(F) = u$$

Example (Keeping the previous setting)

Let $\vec{e} = \left(6a^2 + 2, \quad 4a^2 + 4, \quad 2a^2 + 6\right) \in S^3$, with $S = R[a]$ and $R = \mathbb{Z}_8$.

- We have $\mathtt{Rank}_R(\vec{e}) = 1$ and $m = 3$
- For $u = 2$, set

$$F = \langle 1, \quad a^2 \rangle_R$$

- One can see that F is free with rank 2 and $supp(\vec{e}) \subset F$.

[3] H. T. Kamche & C. Mouaha, Rank-metric codes over finite principal ideal rings and applications, *IEEE Tram. Inform. Theory, 2019.*

Problem Reminder

Setup

- Let $R = \mathbb{Z}_8$ and $S = R[a]$, where a is a root of the polynomial $h(x) = x^3 + 6x^2 + 3x + 1$.
- Then $\mathbf{b} = (1, a, a^2)$ forms an R-basis of S.
- Consider the $[3, 1, 3]$-linear code $\mathcal{C} \subset S^3$ generated by the matrix:

$$\boldsymbol{G} = \begin{pmatrix} 1 & a^2 + 5 & a^2 + a + 1 \end{pmatrix}$$

- Let

$$\vec{y} = \begin{pmatrix} 6a^2 + 3, & 5a^2 + 1, & 3a^2 + a + 7 \end{pmatrix} \in S^3$$

- A parity check matrix of $\mathscr{C}$ is

$$\boldsymbol{H} = \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}$$

- And we have

$$\vec{s} = \vec{y}\boldsymbol{H}^\top = \begin{pmatrix} 6a^2 + 2a + 6, & 2a + 6 \end{pmatrix} = \vec{e}\boldsymbol{H}^\top \neq \vec{0}$$

So, $\vec{y} \notin \mathscr{C}$, and the problem here is to find $\vec{e} \in S^3$ so that $\vec{e}\boldsymbol{H}^\top = \vec{s}$ and $\mathtt{Rank}_R(\vec{e}) = 1$.

Solving the RSD Problem over FCR.

We are looking for $\vec{e} \in S^n$ with $\texttt{Rank}_R(\vec{e}) = t$ satisfying $\quad //t = 1$ in our example

$$\vec{s} = \left(6a^2 + 2a + 6, \;\; 2a + 6\right) = \vec{e}\boldsymbol{H}^\top = (e_1, \quad e_2, \quad e_3) \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}^\top$$

- Let $u \in \mathbb{N}$ such that $t \leqslant u \leqslant m$ $\quad //t = 1$ and $m = 3$. So we choose $u = 2$
- F a rank u free $R-$s.m of S s.t $supp(\vec{e}) \subset F$ $\quad //$Let say $F = \langle 1, a^2 \rangle_R$
- $\vec{f} = (f_1, \cdots, f_u)$ a basis of F. $\quad //\vec{f} = (1, a^2)$
- There exists $\mathbf{X} \in R^{u \times n}$ s.t $\vec{e} = \vec{f}\mathbf{X}$ $\quad // \mathbf{X} \in R^{2\times 3}$
- That is to say $\vec{s} = \vec{f}\mathbf{X}\boldsymbol{H}^\top$ $\quad // \left(6a^2 + 2a + 6, \;\; 2a + 6\right) = \vec{f}\mathbf{X}\boldsymbol{H}^\top$
- So, we result on the system[4]

$$\left(\mathbf{H} \otimes \vec{f}\right) vec\left(\mathbf{X}\right) = vec\left(\vec{s}\right)$$

where $vec\left(\mathbf{X}\right)$ denotes the vectorization of the matrix $\mathbf{X}$

[4] Horn & Johnson. Topics in Matrix Analysis, *Cambridge University Press'91*

Solving the RSD Problem over FCR.

We are looking for $\vec{e} \in S^n$ with $\texttt{Rank}_R(\vec{e}) = t$ satisfying $\quad //t = 1$ in our example

$$\vec{s} = \left(6a^2 + 2a + 6, \ \ 2a + 6\right) = \vec{e}\boldsymbol{H}^\top = (e_1, \quad e_2, \quad e_3) \begin{pmatrix} 7a^2+3 & 1 & 0 \\ 7a^2+7a+7 & 0 & 1 \end{pmatrix}^\top$$

- Let $u \in \mathbb{N}$ such that $t \leqslant u \leqslant m$ $\qquad //t = 1$ and $m = 3$. So we choose $u = 2$
- F a rank u free $R-$s.m of S s.t $supp(\vec{e}) \subset F$ $\qquad //$Let say $F = \langle 1, a^2 \rangle_R$
- $\vec{f} = (f_1, \cdots, f_u)$ a basis of F. $\qquad //\vec{f} = (1, a^2)$
- There exists $\mathbf{X} \in R^{u \times n}$ s.t $\vec{e} = \vec{f}\mathbf{X}$ $\qquad // \mathbf{X} \in R^{2\times 3}$
- That is to say $\vec{s} = \vec{f}\mathbf{X}\boldsymbol{H}^\top$ $\qquad // (6a^2+2a+6, \ \ 2a+6) = \vec{f}\mathbf{X}\boldsymbol{H}^\top$
- So, we result on the system[4]

$$\left(\mathbf{H} \otimes \vec{f}\right) vec\left(\mathbf{X}\right) = vec\left(\vec{s}\right)$$

where $vec\left(\mathbf{X}\right)$ denotes the vectorization of the matrix $\mathbf{X}$

[4] Horn & Johnson. Topics in Matrix Analysis, *Cambridge University Press'91*

Solving the RSD Problem over FCR.

We are looking for $\vec{e} \in S^n$ with $\texttt{Rank}_R(\vec{e}) = t$ satisfying //$t = 1$ in our example

$$\vec{s} = \left(6a^2 + 2a + 6,\ \ 2a + 6\right) = \vec{e}\boldsymbol{H}^\top = (e_1,\quad e_2,\quad e_3)\begin{pmatrix} 7a^2+3 & 1 & 0 \\ 7a^2+7a+7 & 0 & 1 \end{pmatrix}^\top$$

- Let $u \in \mathbb{N}$ such that $t \leqslant u \leqslant m$ //$t = 1$ and $m = 3$. So we choose $u = 2$
- F a rank u free $R-$s.m of S s.t $supp(\vec{e}) \subset F$ //Let say $F = \langle 1, a^2\rangle_R$
- $\vec{f} = (f_1, \cdots, f_u)$ a basis of F. //$\vec{f} = (1, a^2)$
- There exists $\boldsymbol{X} \in R^{u\times n}$ s.t $\vec{e} = \vec{f}\boldsymbol{X}$ // $\boldsymbol{X} \in R^{2\times 3}$
- That is to say $\vec{s} = \vec{f}\boldsymbol{X}\boldsymbol{H}^\top$ // $(6a^2+2a+6,\ \ 2a+6) = \vec{f}\boldsymbol{X}\boldsymbol{H}^\top$
- So, we result on the system[4]

$$\left(\mathbf{H} \otimes \vec{f}\right) vec\left(\boldsymbol{X}\right) = vec\left(\vec{s}\right)$$

where $vec\left(\boldsymbol{X}\right)$ denotes the vectorization of the matrix $\boldsymbol{X}$

[4] Horn & Johnson. Topics in Matrix Analysis, *Cambridge University Press'91*

Solving the RSD Problem over FCR.

We are looking for $\vec{e} \in S^n$ with $\texttt{Rank}_R(\vec{e}) = t$ satisfying $\quad //t = 1$ in our example

$$\vec{s} = \left(6a^2 + 2a + 6, \;\; 2a + 6\right) = \vec{e}\boldsymbol{H}^\top = (e_1, \quad e_2, \quad e_3) \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}^\top$$

- Let $u \in \mathbb{N}$ such that $t \leqslant u \leqslant m$ $\quad //t = 1$ and $m = 3$. So we choose $u = 2$
- F a rank u free $R-$s.m of S s.t $supp(\vec{e}) \subset F$ $\quad //$Let say $F = \langle 1, a^2 \rangle_R$
- $\vec{f} = (f_1, \cdots, f_u)$ a basis of F. $\quad //\vec{f} = (1, a^2)$
- There exists $\boldsymbol{X} \in R^{u \times n}$ s.t $\vec{e} = \vec{f}\boldsymbol{X}$ $\quad // \boldsymbol{X} \in R^{2\times 3}$
- That is to say $\vec{s} = \vec{f}\boldsymbol{X}\boldsymbol{H}^\top$ $\quad // (6a^2 + 2a + 6, \;\; 2a + 6) = \vec{f}\boldsymbol{X}\boldsymbol{H}^\top$
- So, we result on the system[4]

$$\left(\mathbf{H} \otimes \vec{f}\right) vec\left(\mathbf{X}\right) = vec\left(\vec{s}\right)$$

where $vec\left(\mathbf{X}\right)$ denotes the vectorization of the matrix $\mathbf{X}$

[4] Horn & Johnson. Topics in Matrix Analysis, *Cambridge University Press'91*

Solving the RSD Problem over FCR.

We are looking for $\vec{e} \in S^n$ with $\texttt{Rank}_R(\vec{e}) = t$ satisfying //$t = 1$ in our example

$$\vec{s} = \left(6a^2 + 2a + 6, \ \ 2a + 6\right) = \vec{e}\boldsymbol{H}^\top = (e_1, \quad e_2, \quad e_3) \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}^\top$$

- Let $u \in \mathbb{N}$ such that $t \leqslant u \leqslant m$ //$t = 1$ and $m = 3$. So we choose $u = 2$
- F a rank u free $R-$s.m of S s.t $supp(\vec{e}) \subset F$ //Let say $F = \langle 1, a^2 \rangle_R$
- $\vec{f} = (f_1, \cdots, f_u)$ a basis of F. //$\vec{f} = (1, a^2)$
- There exists $\boldsymbol{X} \in R^{u \times n}$ s.t $\vec{e} = \vec{f}\boldsymbol{X}$ // $\boldsymbol{X} \in R^{2\times 3}$
- That is to say $\vec{s} = \vec{f}\boldsymbol{X}\boldsymbol{H}^\top$ // $(6a^2 + 2a + 6, \ \ 2a + 6) = \vec{f}\boldsymbol{X}\boldsymbol{H}^\top$
- So, we result on the system[4]

$$\left(\mathbf{H} \otimes \vec{f}\right) vec\left(\mathbf{X}\right) = vec\left(\vec{s}\right)$$

where $vec\left(\mathbf{X}\right)$ denotes the vectorization of the matrix $\mathbf{X}$

[4] Horn & Johnson. Topics in Matrix Analysis, *Cambridge University Press'91*

Solving the RSD Problem over FCR.

We are looking for $\vec{e} \in S^n$ with $\mathtt{Rank}_R(\vec{e}) = t$ satisfying //$t = 1$ in our example

$$\vec{s} = \left(6a^2 + 2a + 6,\ \ 2a + 6\right) = \vec{e}\boldsymbol{H}^\top = (e_1,\quad e_2,\quad e_3) \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}^\top$$

- Let $u \in \mathbb{N}$ such that $t \leqslant u \leqslant m$ //$t = 1$ and $m = 3$. So we choose $u = 2$
- F a rank u free $R-$s.m of S s.t $supp(\vec{e}) \subset F$ //Let say $F = \langle 1, a^2 \rangle_R$
- $\vec{f} = (f_1, \cdots, f_u)$ a basis of F. //$\vec{f} = (1, a^2)$
- There exists $\boldsymbol{X} \in R^{u \times n}$ s.t $\vec{e} = \vec{f}\boldsymbol{X}$ // $\boldsymbol{X} \in R^{2\times 3}$
- That is to say $\vec{s} = \vec{f}\boldsymbol{X}\boldsymbol{H}^\top$ // $(6a^2 + 2a + 6,\ \ 2a + 6) = \vec{f}\boldsymbol{X}\boldsymbol{H}^\top$
- So, we result on the system[4]

$$\left(\mathbf{H} \otimes \vec{f}\right) vec\left(\mathbf{X}\right) = vec\left(\vec{s}\right)$$

where $vec\left(\mathbf{X}\right)$ denotes the vectorization of the matrix $\mathbf{X}$

[4] Horn & Johnson. Topics in Matrix Analysis, *Cambridge University Press'91*

Solving the RSD Problem over FCR.

We are looking for $\vec{e} \in S^n$ with $\texttt{Rank}_R(\vec{e}) = t$ satisfying //$t = 1$ in our example

$$\vec{s} = \begin{pmatrix} 6a^2 + 2a + 6, & 2a + 6 \end{pmatrix} = \vec{e}\boldsymbol{H}^\top = (e_1, \quad e_2, \quad e_3) \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}^\top$$

- Let $u \in \mathbb{N}$ such that $t \leqslant u \leqslant m$ //$t = 1$ and $m = 3$. So we choose $u = 2$
- F a rank u free $R-$s.m of S s.t $supp(\vec{e}) \subset F$ //Let say $F = \langle 1, a^2 \rangle_R$
- $\vec{f} = (f_1, \cdots, f_u)$ a basis of F. //$\vec{f} = (1, a^2)$
- There exists $\boldsymbol{X} \in R^{u \times n}$ s.t $\vec{e} = \vec{f}\boldsymbol{X}$ // $\boldsymbol{X} \in R^{2\times 3}$
- That is to say $\vec{s} = \vec{f}\boldsymbol{X}\boldsymbol{H}^\top$ // $(6a^2 + 2a + 6, \;\; 2a + 6) = \vec{f}\boldsymbol{X}\boldsymbol{H}^\top$
- So, we result on the system[4]

$$\left(\mathbf{H} \otimes \vec{f}\right) vec\left(\mathbf{X}\right) = vec\left(\vec{s}\right)$$

where $vec\left(\mathbf{X}\right)$ denotes the vectorization of the matrix $\mathbf{X}$

[4] Horn & Johnson. Topics in Matrix Analysis, *Cambridge University Press'91*

Solving the RSD Problem over FCR.

We are looking for $\vec{e} \in S^n$ with $\mathrm{Rank}_R(\vec{e}) = t$ satisfying $//t = 1$ in our example

$$\vec{s} = \left(6a^2 + 2a + 6, \;\; 2a + 6\right) = \vec{e}\boldsymbol{H}^\top = (e_1, \quad e_2, \quad e_3) \begin{pmatrix} 7a^2 + 3 & 1 & 0 \\ 7a^2 + 7a + 7 & 0 & 1 \end{pmatrix}^\top$$

- We resulted on the system

$$\left(\mathbf{H} \otimes \vec{f}\right) vec\left(\mathbf{X}\right) = vec\left(\vec{s}\right)$$

- Assume $\mathbf{X} = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \end{pmatrix} \in \mathbf{R}^{\mathbf{u} \times \mathbf{n}}$ and considering $\vec{f} = (1, a^2)$,
- The system $\mathscr{E}_1$ to be solved is then,

$$\left(\begin{array}{cc|cc|cc} 7a^2 + 3 & 2a^2 + 7a + 2 & 1 & a^2 & 0 & 0 \\ 7a^2 + 7a + 7 & 4a^2 + 2a + 3 & 0 & 0 & 1 & a^2 \end{array}\right) \begin{pmatrix} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 6a^2 + 2a + 6 \\ 2a + 6 \end{pmatrix}$$

Solving the RSD Problem over FCR.

We are looking for $\vec{e} \in S^n$ with $\texttt{Rank}_R(\vec{e}) = t$ satisfying $//t = 1$ in our example

$$\vec{s} = \left(6a^2 + 2a + 6,\ \ 2a + 6\right) = \vec{e}\boldsymbol{H}^\top = (e_1, \quad e_2, \quad e_3) \begin{pmatrix} 7a^2+3 & 1 & 0 \\ 7a^2+7a+7 & 0 & 1 \end{pmatrix}^\top$$

- We resulted on the system

$$\left(\mathbf{H} \otimes \vec{f}\right) vec\left(\mathbf{X}\right) = vec\left(\vec{s}\right)$$

- Assume $\mathbf{X} = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \end{pmatrix} \in \mathbf{R^{u \times n}}$ and considering $\vec{f} = (1, a^2)$,
- The system $\mathscr{E}_1$ to be solved is then,

$$\left(\begin{array}{cc|cc|cc} 7a^2+3 & 2a^2+7a+2 & 1 & a^2 & 0 & 0 \\ 7a^2+7a+7 & 4a^2+2a+3 & 0 & 0 & 1 & a^2 \end{array}\right) \begin{pmatrix} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 6a^2+2a+6 \\ 2a+6 \end{pmatrix}$$

Solving the RSD Problem over FCR.

- The system $\mathscr{E}_1$ is

$$\left(\begin{array}{cc|cc|cc} 7a^2+3 & 2a^2+7a+2 & 1 & a^2 & 0 & 0 \\ 7a^2+7a+7 & 4a^2+2a+3 & 0 & 0 & 1 & a^2 \end{array}\right)\begin{pmatrix} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 6a^2+2a+6 \\ 2a+6 \end{pmatrix}$$

- By expanding $\mathscr{E}_1$ in R, we get the linear system $\mathscr{E}_2$ given by

$$\left(\begin{array}{cccccc} 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 & 0 \\ 7 & 2 & 0 & 1 & 0 & 0 \\ \hline 7 & 3 & 0 & 0 & 1 & 0 \\ 7 & 2 & 0 & 0 & 0 & 0 \\ 7 & 4 & 0 & 0 & 0 & 1 \end{array}\right)\begin{pmatrix} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{pmatrix} = \left(\begin{array}{c} 6 \\ 2 \\ 6 \\ \hline 6 \\ 2 \\ 0 \end{array}\right)$$

- $\mathscr{E}_2$ has $(n-k)\times m$ equations and $u \times n$ unknowns.
- So, a nescessary condition to have at most one solution is $(n-k)\times m \geqslant u \times n$. That is to say, $u \leqslant \lfloor (n-k)m/n \rfloor$
- The max value for u is 2 in our example.

Solving the RSD Problem over FCR.

- The system $\mathscr{E}_1$ is

$$\begin{pmatrix} 7a^2+3 & 2a^2+7a+2 & 1 & a^2 & 0 & 0 \\ 7a^2+7a+7 & 4a^2+2a+3 & 0 & 0 & 1 & a^2 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{21} \\ x_{12} \\ x_{22} \\ x_{13} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 6a^2+2a+6 \\ 2a+6 \end{pmatrix}$$

- By expanding $\mathscr{E}_1$ in R, we get the linear system $\mathscr{E}_2$ given by

$$\begin{pmatrix} 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 & 0 \\ 7 & 2 & 0 & 1 & 0 & 0 \\ 7 & 3 & 0 & 0 & 1 & 0 \\ 7 & 2 & 0 & 0 & 0 & 0 \\ 7 & 4 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{21} \\ x_{12} \\ x_{22} \\ x_{13} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 6 \\ 2 \\ 6 \\ 6 \\ 2 \\ 0 \end{pmatrix}$$

- $\mathscr{E}_2$ has $(n-k) \times m$ equations and $u \times n$ unknowns.
- So, a nescessary condition to have at most one solution is $(n-k) \times m \geqslant u \times n$. That is to say, $u \leqslant \lfloor (n-k)m/n \rfloor$
- The max value for u is 2 in our example.

Solving the RSD Problem over FCR.

- The system $\mathscr{E}_1$ is

$$\left(\begin{array}{cc|cc|cc} 7a^2+3 & 2a^2+7a+2 & 1 & a^2 & 0 & 0 \\ 7a^2+7a+7 & 4a^2+2a+3 & 0 & 0 & 1 & a^2 \end{array}\right)\begin{pmatrix} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 6a^2+2a+6 \\ 2a+6 \end{pmatrix}$$

- By expanding $\mathscr{E}_1$ in R, we get the linear system $\mathscr{E}_2$ given by

$$\left(\begin{array}{cccccc} 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 & 0 \\ 7 & 2 & 0 & 1 & 0 & 0 \\ \hline 7 & 3 & 0 & 0 & 1 & 0 \\ 7 & 2 & 0 & 0 & 0 & 0 \\ 7 & 4 & 0 & 0 & 0 & 1 \end{array}\right)\begin{pmatrix} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{pmatrix} = \left(\begin{array}{c} 6 \\ 2 \\ 6 \\ \hline 6 \\ 2 \\ 0 \end{array}\right)$$

- $\mathscr{E}_2$ has $(n-k)\times m$ equations and $u \times n$ unknowns.
- So, a nescessary condition to have at most one solution is $(n-k)\times m \geqslant u \times n$. That is to say, $u \leqslant \lfloor (n-k)m/n \rfloor$
- The max value for u is 2 in our example.

Solving the RSD Problem over FCR.

- The system $\mathscr{E}_1$ is

$$\left(\begin{array}{cc|cc|cc} 7a^2+3 & 2a^2+7a+2 & 1 & a^2 & 0 & 0 \\ 7a^2+7a+7 & 4a^2+2a+3 & 0 & 0 & 1 & a^2 \end{array}\right)\left(\begin{array}{c} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{array}\right) = \begin{pmatrix} 6a^2+2a+6 \\ 2a+6 \end{pmatrix}$$

- By expanding $\mathscr{E}_1$ in R, we get the linear system $\mathscr{E}_2$ given by

$$\left(\begin{array}{cccccc} 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 & 0 \\ 7 & 2 & 0 & 1 & 0 & 0 \\ \hline 7 & 3 & 0 & 0 & 1 & 0 \\ 7 & 2 & 0 & 0 & 0 & 0 \\ 7 & 4 & 0 & 0 & 0 & 1 \end{array}\right)\left(\begin{array}{c} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{array}\right) = \left(\begin{array}{c} 6 \\ 2 \\ 6 \\ \hline 6 \\ 2 \\ 0 \end{array}\right)$$

- $\mathscr{E}_2$ has $(n-k)\times m$ equations and $u \times n$ unknowns.
- So, a nescessary condition to have at most one solution is $(n-k)\times m \geqslant u \times n$. That is to say, $u \leqslant \lfloor (n-k)m/n \rfloor$
- The max value for u is 2 in our example.

Solving the RSD Problem over FCR.

- The system $\mathscr{E}_1$ is

$$\begin{pmatrix} 7a^2+3 & 2a^2+7a+2 & 1 & a^2 & 0 & 0 \\ 7a^2+7a+7 & 4a^2+2a+3 & 0 & 0 & 1 & a^2 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{21} \\ x_{12} \\ x_{22} \\ x_{13} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 6a^2+2a+6 \\ 2a+6 \end{pmatrix}$$

- By expanding $\mathscr{E}_1$ in R, we get the linear system $\mathscr{E}_2$ given by

$$\begin{pmatrix} 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 & 0 \\ 7 & 2 & 0 & 1 & 0 & 0 \\ 7 & 3 & 0 & 0 & 1 & 0 \\ 7 & 2 & 0 & 0 & 0 & 0 \\ 7 & 4 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{21} \\ x_{12} \\ x_{22} \\ x_{13} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 6 \\ 2 \\ 6 \\ 6 \\ 2 \\ 0 \end{pmatrix}$$

- $\mathscr{E}_2$ has $(n-k) \times m$ equations and $u \times n$ unknowns.
- So, a nescessary condition to have at most one solution is $(n-k) \times m \geqslant u \times n$. That is to say, $u \leqslant \lfloor (n-k)m/n \rfloor$
- The max value for u is 2 in our example.

Solving the RSD Problem over FCR.

- By expanding $\mathscr{E}_1$ in R, we get the linear system $\mathscr{E}_2$ given by

$$\left(\begin{array}{cccccc} 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 & 0 \\ 7 & 2 & 0 & 1 & 0 & 0 \\ \hline 7 & 3 & 0 & 0 & 1 & 0 \\ 7 & 2 & 0 & 0 & 0 & 0 \\ 7 & 4 & 0 & 0 & 0 & 1 \end{array}\right) \left(\begin{array}{c} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{array}\right) = \left(\begin{array}{c} 6 \\ 2 \\ 6 \\ \hline 6 \\ 2 \\ 0 \end{array}\right)$$

- $\mathscr{E}_2$ has $(n-k) \times m$ equations and $u \times n$ unknowns.
- So, a nescessary condition to have at most one solution is $(n-k) \times m \geqslant u \times n$. That is to say, $u \leqslant \lfloor (n-k)m/n \rfloor$
- By solving $\mathscr{E}_2$ we get the unique solution $\begin{pmatrix} 2 \\ 6 \\ 4 \\ 4 \\ 6 \\ 2 \end{pmatrix}$
- That is to say $\boldsymbol{X} = \begin{pmatrix} 2 & 4 & 6 \\ 6 & 4 & 2 \end{pmatrix}$ and $\vec{e} = \vec{f}\boldsymbol{X} = (1, a^2)\boldsymbol{X} = (6a^2+2, \; 4a^2+4, \; 2a^2+6)$

Solving the RSD Problem over FCR.

- By expanding $\mathscr{E}_1$ in R, we get the linear system $\mathscr{E}_2$ given by

$$\left(\begin{array}{cccccc} 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 & 0 \\ 7 & 2 & 0 & 1 & 0 & 0 \\ \hline 7 & 3 & 0 & 0 & 1 & 0 \\ 7 & 2 & 0 & 0 & 0 & 0 \\ 7 & 4 & 0 & 0 & 0 & 1 \end{array}\right) \left(\begin{array}{c} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{array}\right) = \left(\begin{array}{c} 6 \\ 2 \\ 6 \\ \hline 6 \\ 2 \\ 0 \end{array}\right)$$

- $\mathscr{E}_2$ has $(n-k) \times m$ equations and $u \times n$ unknowns.
- So, a nescessary condition to have at most one solution is $(n-k) \times m \geqslant u \times n$. That is to say, $u \leqslant \lfloor (n-k)m/n \rfloor$
- By solving $\mathscr{E}_2$ we get the unique solution $\begin{pmatrix} 2 \\ 6 \\ 4 \\ 4 \\ 6 \\ 2 \end{pmatrix}$
- That is to say $\boldsymbol{X} = \begin{pmatrix} 2 & 4 & 6 \\ 6 & 4 & 2 \end{pmatrix}$ and $\vec{e} = \vec{f}\boldsymbol{X} = (1, a^2)\boldsymbol{X} = (6a^2+2,\ \ 4a^2+4,\ \ 2a^2+6)$

Solving the RSD Problem over FCR.

- By expanding $\mathscr{E}_1$ in R, we get the linear system $\mathscr{E}_2$ given by

$$\begin{pmatrix} 3 & 2 & 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 & 0 \\ 7 & 2 & 0 & 1 & 0 & 0 \\ \hline 7 & 3 & 0 & 0 & 1 & 0 \\ 7 & 2 & 0 & 0 & 0 & 0 \\ 7 & 4 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{21} \\ \hline x_{12} \\ x_{22} \\ \hline x_{13} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 6 \\ 2 \\ 6 \\ \hline 6 \\ 2 \\ 0 \end{pmatrix}$$

- $\mathscr{E}_2$ has $(n-k) \times m$ equations and $u \times n$ unknowns.
- So, a nescessary condition to have at most one solution is $(n-k) \times m \geqslant u \times n$. That is to say, $u \leqslant \lfloor (n-k)m/n \rfloor$
- By solving $\mathscr{E}_2$ we get the unique solution $\begin{pmatrix} 2 \\ 6 \\ 4 \\ 4 \\ 6 \\ 2 \end{pmatrix}$
- That is to say $\boldsymbol{X} = \begin{pmatrix} 2 & 4 & 6 \\ 6 & 4 & 2 \end{pmatrix}$ and $\vec{e} = \vec{f}\boldsymbol{X} = (1, a^2)\boldsymbol{X} = (6a^2 + 2, \; 4a^2 + 4, \; 2a^2 + 6)$

Algorithm Complexity

- Proccess of the Algorithm :
  1. guess a free s.m. $F \subset S$ of rank $u = \lfloor (n-k)m/n \rfloor$ and s.t. $\mathrm{supp}(\vec{e}) \subset F$
  2. For each guess, solve a linear system $(\mathscr{E}_2)$ with $(n-k) \times m$ equations and $u \times n$ unknowns.
  3. Choose a new F if there is no solution to $\mathscr{E}_2$
- Complexity :
  1. Dominated by the probability P_d that $\mathrm{supp}(\mathbf{e}) \subset F$
  2. $P_1 \approx \frac{1}{q^{ur\lceil mk/n \rceil}}$ [5]

$$\mathcal{O}\left(m(n-k)\,u^2 n^2 / P_1\right) \approx \mathcal{O}\left(m(n-k)\,u^2 n^2 q^{ur\lceil mk/n \rceil}\right)$$

[5] Kalachi & Kamche. On the rank decoding problem over finite principal ideal rings. AMC'22

Algorithm Complexity

- Proccess of the Algorithm :
  1. guess a free s.m. $F \subset S$ of rank $u = \lfloor (n-k)m/n \rfloor$ and s.t. $\mathrm{supp}(\vec{e}) \subset F$
  2. For each guess, solve a linear system $(\mathscr{E}_2)$ with $(n-k) \times m$ equations and $u \times n$ unknowns.
  3. Choose a new F if there is no solution to $\mathscr{E}_2$
- Complexity :
  1. Dominated by the probability P_d that $\mathrm{supp}(\mathbf{e}) \subset F$
  2. $P_1 \approx \frac{1}{q^{\nu r \lfloor mk/n \rfloor}}$ [5]

$$\mathcal{O}\left(m\left(n-k\right)u^2n^2/P_1\right) \approx \mathcal{O}\left(m\left(n-k\right)u^2n^2q^{\nu r\lfloor mk/n \rfloor}\right)$$

[5] Kalachi & Kamche. On the rank decoding problem over finite principal ideal rings. AMC'22

Algorithm Complexity

- Proccess of the Algorithm :
  1. guess a free s.m. $F \subset S$ of rank $u = \lfloor (n-k)m/n \rfloor$ and s.t. $\mathrm{supp}(\vec{e}) \subset F$
  2. For each guess, solve a linear system $(\mathscr{E}_2)$ with $(n-k) \times m$ equations and $u \times n$ unknowns.
  3. Choose a new F if there is no solution to $\mathscr{E}_2$
- Complexity :
  1. Dominated by the probability P_d that $\mathrm{supp}(\mathbf{e}) \subset F$
  2. $P_1 \approx \frac{1}{q^{\nu r \lfloor mk/n \rfloor}}$ [5]

$$\mathcal{O}\left(m(n-k)u^2n^2/P_1\right) \approx \mathcal{O}\left(m(n-k)u^2n^2q^{\nu r\lfloor mk/n \rfloor}\right)$$

[5] Kalachi & Kamche. On the rank decoding problem over finite principal ideal rings. AMC'23

Algorithm Complexity

- Proccess of the Algorithm :
  1. guess a free s.m. $F \subset S$ of rank $u = \lfloor (n-k)m/n \rfloor$ and s.t. $\mathrm{supp}(\vec{e}) \subset F$
  2. For each guess, solve a linear system $(\mathscr{E}_2)$ with $(n-k) \times m$ equations and $u \times n$ unknowns.
  3. Choose a new F if there is no solution to $\mathscr{E}_2$
- Complexity :
  1. Dominated by the probability P_d that $\mathrm{supp}(\mathbf{e}) \subset F$
  2. $P_1 \approx \frac{1}{q^{\nu r \lfloor mk/n \rfloor}}$ [5]

$$\mathcal{O}\left(m(n-k)u^2n^2/P_1\right) \approx \mathcal{O}\left(m(n-k)u^2n^2q^{\nu r \lfloor mk/n \rfloor}\right)$$

[5] Kalachi & Kamche. On the rank decoding problem over finite principal ideal rings. *AMC'23*

Algorithm Complexity

- Proccess of the Algorithm :
  1. guess a free s.m. $F \subset S$ of rank $u = \lfloor (n-k)m/n \rfloor$ and s.t. $\mathrm{supp}(\vec{e}) \subset F$
  2. For each guess, solve a linear system $(\mathscr{E}_2)$ with $(n-k) \times m$ equations and $u \times n$ unknowns.
  3. Choose a new F if there is no solution to $\mathscr{E}_2$
- Complexity :
  1. Dominated by the probability P_d that $\mathrm{supp}(\mathbf{e}) \subset F$
  2. $P_1 \approx \frac{1}{q^{\nu r \lfloor mk/n \rfloor}}$ [5]

$$\mathcal{O}\left(m\,(n-k)\,u^2 n^2 / P_1\right) \approx \mathcal{O}\left(m\,(n-k)\,u^2 n^2 q^{\nu r \lfloor mk/n \rfloor}\right)$$

[5] Kalachi & Kamche. On the rank decoding problem over finite principal ideal rings. *AMC'23*

Key Points

- The most costly part in the first approach is the reseach of $F \subset S \equiv \mathbb{R}^m$ s.t $supp(\vec{e}) \subset F$
- This view is based on how we defined the rank end the support of a vector $\vec{x} \in S^n$

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

$$\mathrm{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- An equivalent definition :

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{1*}, \boldsymbol{X}_{2*}, \ldots, \boldsymbol{X}_{m*} \rangle_R \subset R^n$$

$$\mathrm{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- When $n < m$, it is then easier to look for a support in R^n.

Solving the RSD Problem over FCR (a second Approach)

Key Points

- The most costly part in the first approach is the reseach of $F \subset S \equiv \mathbb{R}^m$ s.t $supp(\vec{e}) \subset F$
- This view is based on how we defined the rank end the support of a vector $\vec{x} \in S^n$

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

$$\mathrm{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- An equivalent definition :

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{1*}, \boldsymbol{X}_{2*}, \ldots, \boldsymbol{X}_{m*} \rangle_R \subset R^n$$

$$\mathrm{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- When $n < m$, it is then easier to look for a support in R^n.

Solving the RSD Problem over FCR (a second Approach)

Key Points

- The most costly part in the first approach is the reseach of $F \subset S \equiv \mathbb{R}^m$ s.t $supp(\vec{e}) \subset F$
- This view is based on how we defined the rank end the support of a vector $\vec{x} \in S^n$

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

$$\mathrm{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- An equivalent definition :

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{1*}, \boldsymbol{X}_{2*}, \ldots, \boldsymbol{X}_{m*} \rangle_R \subset R^n$$

$$\mathrm{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- When $n < m$, it is then easier to look for a support in R^n.

Solving the RSD Problem over FCR (a second Approach)

Key Points

- The most costly part in the first approach is the reseach of $F \subset S \equiv \mathbb{R}^m$ s.t $supp(\vec{e}) \subset F$
- This view is based on how we defined the rank end the support of a vector $\vec{x} \in S^n$

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

$$\mathtt{Rank}_{R}(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- An equivalent definition :

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{1*}, \boldsymbol{X}_{2*}, \ldots, \boldsymbol{X}_{m*} \rangle_R \subset R^n$$

$$\mathtt{Rank}_{R}(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- When $n < m$, it is then easier to look for a support in R^n.

Key Points

- The most costly part in the first approach is the reseach of $F \subset S \equiv \mathbb{R}^m$ s.t $supp(\vec{e}) \subset F$
- This view is based on how we defined the rank end the support of a vector $\vec{x} \in S^n$

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

$$\mathtt{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- An equivalent definition :

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{1*}, \boldsymbol{X}_{2*}, \ldots, \boldsymbol{X}_{m*} \rangle_R \subset R^n$$

$$\mathtt{Rank}_R(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- When $n < m$, it is then easier to look for a support in R^n.

Key Points

- The most costly part in the first approach is the reseach of $F \subset S \equiv \mathbb{R}^m$ s.t $supp(\vec{e}) \subset F$
- This view is based on how we defined the rank end the support of a vector $\vec{x} \in S^n$

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

$$\text{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

$$\texttt{Rank}_R(\vec{x}) := \text{rank}_R(\boldsymbol{X}) = \dim(\text{supp}_R(\vec{x})).$$

- An equivalent definition :

$$\text{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{1*}, \boldsymbol{X}_{2*}, \ldots, \boldsymbol{X}_{m*} \rangle_R \subset R^n$$

$$\texttt{Rank}_R(\vec{x}) := \text{rank}_R(\boldsymbol{X}) = \dim(\text{supp}_R(\vec{x})).$$

- When $n < m$, it is then easier to look for a support in R^n.

Solving the RSD Problem over FCR (a second Approach)

Key Points

- The most costly part in the first approach is the reseach of $F \subset S \equiv \mathbb{R}^m$ s.t $supp(\vec{e}) \subset F$
- This view is based on how we defined the rank end the support of a vector $\vec{x} \in S^n$

$$\vec{x} \longleftrightarrow \boldsymbol{X} = (X_{ij}) = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & \vdots & & \vdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \in R^{m \times n},$$

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{*1}, \boldsymbol{X}_{*2}, \ldots, \boldsymbol{X}_{*n} \rangle_R \subset R^m \equiv S.$$

$$\mathtt{Rank}_{\,R}\,(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- An equivalent definition :

$$\mathrm{supp}_R(\vec{x}) := \langle \boldsymbol{X}_{1*}, \boldsymbol{X}_{2*}, \ldots, \boldsymbol{X}_{m*} \rangle_R \subset R^n$$

$$\mathtt{Rank}_{\,R}\,(\vec{x}) := \mathrm{rank}_R(\boldsymbol{X}) = \dim(\mathrm{supp}_R(\vec{x})).$$

- When $n < m$, it is then easier to look for a support in R^n.

Principal Ideal Rings $\longrightarrow$ Finite Chain Rings

Theorem 5 (McDonald, 1974)

If R is a principal ring, then

$$A \cong A_{(1)} \times \cdots \times A_{(\rho)}$$

where each $A_{(j)}$ is a finite chain ring.

Ring of Integers Modulo n (CRT)

- Let $p_1, \ldots, p_d$ be distinct prime numbers and $k_1, \ldots, k_d \in \mathbb{N}^*$,
- Define $n = p_1^{k_1} \cdots p_d^{k_d}$

Then:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_d^{k_d}}$$

Conclusion

Key Takeaways

- The **rank metric** is a powerful alternative to the classical Hamming metric.
- Recent algebraic attacks motivate to explore **finite rings**, where *torsion* breaks field-based assumptions.
- We analyzed **combinatorial attacks**[a] on the RSD problem over finite principal ideal rings.
- Complexity increases due to ring structure: the **nilpotency index** ν appears in the exponent.

[a] Gaborit, Ruatta & Schrek. On the complexity of the rank syndrome decoding problem. *IEEE IT'16*

Modeling Strategy	Over Fields	Over Rings
First Modeling	$\mathcal{O}\left(m^3(n-k)^3 q^{rk}\right)$	$\mathcal{O}\left(m^3(n-k)^3 q^{\nu rk}\right)$
Second Modeling	$\mathcal{O}\left(m(n-k)u^2 n^2 q^{r\lfloor \frac{mk}{n} \rfloor}\right)$	$\mathcal{O}\left(m(n-k)u^2 n^2 q^{\nu r\lfloor \frac{mk}{n} \rfloor}\right)$

Conclusion

Key Takeaways

- The **rank metric** is a powerful alternative to the classical Hamming metric.
- Recent algebraic attacks motivate to explore **finite rings**, where *torsion* breaks field-based assumptions.
- We analyzed **combinatorial attacks**[a] on the RSD problem over finite principal ideal rings.
- Complexity increases due to ring structure: the **nilpotency index** ν appears in the exponent.

[a] Gaborit, Ruatta & Schrek. On the complexity of the rank syndrome decoding problem. *IEEE IT'16*

Modeling Strategy	Over Fields	Over Rings
First Modeling	$\mathcal{O}\left(m^3(n-k)^3 q^{rk}\right)$	$\mathcal{O}\left(m^3(n-k)^3 q^{\nu rk}\right)$
Second Modeling	$\mathcal{O}\left(m(n-k)u^2 n^2 q^{r\lfloor \frac{mk}{n} \rfloor}\right)$	$\mathcal{O}\left(m(n-k)u^2 n^2 q^{\nu r\lfloor \frac{mk}{n} \rfloor}\right)$

Conclusion

Key Takeaways

- The **rank metric** is a powerful alternative to the classical Hamming metric.
- Recent algebraic attacks motivate to explore **finite rings**, where *torsion* breaks field-based assumptions.
- We analyzed **combinatorial attacks**[a] on the RSD problem over finite principal ideal rings.
- Complexity increases due to ring structure: the **nilpotency index** ν appears in the exponent.

[a] Gaborit, Ruatta & Schrek. On the complexity of the rank syndrome decoding problem. *IEEE IT'16*

Modeling Strategy	Over Fields	Over Rings
First Modeling	$\mathcal{O}\left(m^3(n-k)^3 q^{rk}\right)$	$\mathcal{O}\left(m^3(n-k)^3 q^{\nu rk}\right)$
Second Modeling	$\mathcal{O}\left(m(n-k)u^2 n^2 q^{r\lfloor \frac{mk}{n} \rfloor}\right)$	$\mathcal{O}\left(m(n-k)u^2 n^2 q^{\nu r\lfloor \frac{mk}{n} \rfloor}\right)$

Conclusion

Key Takeaways

- The **rank metric** is a powerful alternative to the classical Hamming metric.
- Recent algebraic attacks motivate to explore **finite rings**, where *torsion* breaks field-based assumptions.
- We analyzed **combinatorial attacks**[a] on the RSD problem over finite principal ideal rings.
- Complexity increases due to ring structure: the **nilpotency index** ν appears in the exponent.

[a] Gaborit, Ruatta & Schrek. On the complexity of the rank syndrome decoding problem. *IEEE IT'16*

Modeling Strategy	Over Fields	Over Rings
First Modeling	$\mathcal{O}\left(m^3(n-k)^3q^{rk}\right)$	$\mathcal{O}\left(m^3(n-k)^3q^{\nu rk}\right)$
Second Modeling	$\mathcal{O}\left(m(n-k)u^2n^2q^{r\lfloor\frac{mk}{n}\rfloor}\right)$	$\mathcal{O}\left(m(n-k)u^2n^2q^{\nu r\lfloor\frac{mk}{n}\rfloor}\right)$

Perspectives

Research Directions

- Explore **improvements** of existing combinatorial algorithms over finite rings.

- Several enhancements exist for combinatorial attacks,
  - but they all rely on the **Ourivski-Johannsson** model,
  - which **fails in the presence of torsion**.

- Developping an **efficient algebraic modeling over rings** remains an open problem

- *First steps* in this direction were initiated by **Kamche and Kalachi**[a].

- These studies could have an impact on several other problems such as MinRank and VSF[b]

[a] Kamche & Kalachi. Solving systems of algebraic equations over finite commutative rings and applications. *AAECC'24*

[b] P. Gaborit, M. Haiech & R. Neveu. A digital signature scheme based on the vector space factorization problem and the MPC-in-the-Head paradigm. *AMC'25*

$\Longrightarrow$ *Extending rank decoding theory beyond fields is a rich and promising area.*

Perspectives

Research Directions

- Explore **improvements** of existing combinatorial algorithms over finite rings.
- Several enhancements exist for combinatorial attacks,
  - ➠ but they all rely on the **Ourivski-Johannsson** model,
  - ➠ which **fails in the presence of torsion**.
- Developping an **efficient algebraic modeling over rings** remains an open problem
- *First steps* in this direction were initiated by **Kamche and Kalachi**[a].
- These studies could have an impact on several other problems such as MinRank and VSF[b]

[a] Kamche & Kalachi. Solving systems of algebraic equations over finite commutative rings and applications. *AAECC'24*

[b] P. Gaborit, M. Haiech & R. Neveu. A digital signature scheme based on the vector space factorization problem and the MPC-in-the-Head paradigm. *AMC'25*

$\Longrightarrow$ *Extending rank decoding theory beyond fields is a rich and promising area.*

Perspectives

Research Directions

- Explore **improvements** of existing combinatorial algorithms over finite rings.
- Several enhancements exist for combinatorial attacks,
  - ➠ but they all rely on the **Ourivski-Johannsson** model,
  - ➠ which **fails in the presence of torsion**.
- Developping an **efficient algebraic modeling over rings** remains an open problem
- *First steps* in this direction were initiated by **Kamche and Kalachi**[a].
- These studies could have an impact on several other problems such as MinRank and VSF[b]

[a] Kamche & Kalachi. Solving systems of algebraic equations over finite commutative rings and applications. *AAECC'24*

[b] P. Gaborit, M. Haiech & R. Neveu. A digital signature scheme based on the vector space factorization problem and the MPC-in-the-Head paradigm. *AMC'25*

$\Longrightarrow$ *Extending rank decoding theory beyond fields is a rich and promising area.*