# Algebraic attacks for the Rank Decoding Problem

Magali Bardet

LITIS, University of Rouen Normandie, France
magali.bardet@univ-rouen.fr

OpeRa 2024,
February 14th, 2024

# NIST call for proposals



## Post-Quantum Cryptography standardization process

- KEM + Signature.
- 4 Rounds since 2017.
- 1 KEM + 3 Signatures selected for standardization in 2022, based on Lattices and Hash functions.
- 3 code-based KEMs in the 4th Round.

# NIST call for proposals



## Post-Quantum Cryptography standardization process

- KEM + Signature.
- 4 Rounds since 2017.
- 1 KEM + 3 Signatures selected for standardization in 2022, based on Lattices and Hash functions.
- 3 code-based KEMs in the 4th Round.

## Additional Digital Signature Schemes

- June 1, 2023. First Round ongoing.
- 40 submissions.

# Post-quantum cryptography



## Rank metric Code-based cryptography

- Various proposals : KEM, PKE, signatures.

## Interesting underlying (hard) problems

- MinRank,
- Rank Decoding RD,
- Rank Support Learning RSL.

$\Rightarrow$ Algebraic cryptanalysis of these problems? Complexity?

# Rank metric [Del78]

## General Linear code

- A linear subspace $\mathscr{C} = \{\boldsymbol{x}\boldsymbol{G} : \boldsymbol{x} \in \mathbb{F}_q^K\} \subset \mathbb{F}_q^N$, dimension $K$, $\mathbb{F}_q$ finite field.
- Generator matrix $\boldsymbol{G}$ of rank $K$ in $\mathbb{F}_q^{K\times N}$.
- Parity-check matrix $\boldsymbol{H}$ of rank $N-K$, $\boldsymbol{G}\boldsymbol{H}^\top = 0$.

# Rank metric [Del78]



## General Linear code

- A linear subspace $\mathscr{C} = \{\boldsymbol{x}\boldsymbol{G} : \boldsymbol{x} \in \mathbb{F}_q^K\} \subset \mathbb{F}_q^N$, dimension $K$, $\mathbb{F}_q$ finite field.
- Generator matrix $\boldsymbol{G}$ of rank $K$ in $\mathbb{F}_q^{K\times N}$.
- Parity-check matrix $\boldsymbol{H}$ of rank $N-K$, $\boldsymbol{G}\boldsymbol{H}^\top = 0$.
- Hamming distance $d(\boldsymbol{c},\boldsymbol{c}') = \#\{i : c_i \neq c'_i\}$.

# Rank metric [Del78]



## General Linear code

- A linear subspace $\mathscr{C} = \{\boldsymbol{x}\boldsymbol{G} : \boldsymbol{x} \in \mathbb{F}_q^K\} \subset \mathbb{F}_q^N$, dimension $K$, $\mathbb{F}_q$ finite field.
- Generator matrix $\boldsymbol{G}$ of rank $K$ in $\mathbb{F}_q^{K\times N}$.
- Parity-check matrix $\boldsymbol{H}$ of rank $N-K$, $\boldsymbol{G}\boldsymbol{H}^\top = 0$.
- Hamming distance $d(\boldsymbol{c}, \boldsymbol{c}') = \#\{i : c_i \neq c_i'\}$.

## Rank metric and Matrix codes over $\mathbb{F}_q^{mn}$ when $N = mn$

- A word $\boldsymbol{x} = (x_1, \ldots, x_{mn}) \in \mathbb{F}_q^{mn}$ is viewed as a (column) matrix

$$\boldsymbol{X} = \begin{pmatrix} x_1 & \cdots & x_{m(n-1)+1} \\ x_2 & \vdots & \vdots \\ x_m & \cdots & x_{mn} \end{pmatrix} \in \mathbb{F}_q^{m\times n}.$$

- The rank distance $d(\boldsymbol{X}, \boldsymbol{Y}) = \mathtt{Rank}(\boldsymbol{Y} - \boldsymbol{X})$.

## Example 1

- $\boldsymbol{x} = (1,0,1,0,1,1,0,0,0,1,0,1,0,0,1,1,1,0,0,1) \in \mathbb{F}_2^{20}$.
- $\mathrm{Mat}(\boldsymbol{x}) = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 5}$
- The weight of $\boldsymbol{x}$ is 3.

# Rank metric [Gab85]



## Equivalent definition for Matrix codes over $\mathbb{F}_q^{nm} \leftrightarrow \mathbb{F}_{q^m}^n$

- Finite field $\mathbb{F}_q$, extension $\mathbb{F}_{q^m}$, basis $\beta = (\beta_1, \dots, \beta_m)$ as an $\mathbb{F}_q$-vector space.
- Correspondence $\boldsymbol{x} \in \mathbb{F}_{q^m}^n \leftrightarrow \mathrm{Mat}(\boldsymbol{x}) \in \mathbb{F}_q^{m \times n}$, $\boldsymbol{x} = \beta\, \mathrm{Mat}(\boldsymbol{x})$.
- Rank weight $|\boldsymbol{x}| = \mathrm{Rank}(\mathrm{Mat}(\boldsymbol{x})) = \dim(\langle x_1, \dots, x_n \rangle_{\mathbb{F}_q})$, support.

# Rank metric [Gab85]



## Equivalent definition for Matrix codes over $\mathbb{F}_q^{nm} \leftrightarrow \mathbb{F}_{q^m}^n$

- Finite field $\mathbb{F}_q$, extension $\mathbb{F}_{q^m}$, basis $\beta = (\beta_1, \dots, \beta_m)$ as an $\mathbb{F}_q$-vector space.
- Correspondence $\boldsymbol{x} \in \mathbb{F}_{q^m}^n \leftrightarrow \mathrm{Mat}(\boldsymbol{x}) \in \mathbb{F}_q^{m \times n}$, $\boldsymbol{x} = \beta\,\mathrm{Mat}(\boldsymbol{x})$.
- Rank weight $|\boldsymbol{x}| = \mathrm{Rank}(\mathrm{Mat}(\boldsymbol{x})) = \dim(\langle x_1, \dots, x_n \rangle_{\mathbb{F}_q})$, support.

## Example

- $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$, basis $(1, \alpha, \alpha^2, \alpha^3)$.
- $\boldsymbol{x} = (1+\alpha^2, 1+\alpha, \alpha+\alpha^3, \alpha^2+\alpha^3, 1+\alpha^3) \leftrightarrow$

$$\mathrm{Mat}(\boldsymbol{x}) = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 5} \text{ and } (1, \alpha, \alpha^2, \alpha^3)\,\mathrm{Mat}(\boldsymbol{x}) = \boldsymbol{x}.$$

- $|\boldsymbol{x}| = 3$, the support of $\boldsymbol{x}$ is $\mathscr{V} = \langle 1+\alpha^2, 1+\alpha, \alpha+\alpha^3 \rangle_{\mathbb{F}_q}$.

### General Matrix codes are $\mathbb{F}_q$-linear codes (Delsart [Del78])

They are $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^m}^n = \mathbb{F}_q^{mn} = \mathbb{F}_q^{m \times n}$, endowed with the rank metric.

# Interesting Codes in Rank metric



### General Matrix codes are $\mathbb{F}_q$-linear codes (Delsart [Del78])

They are $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^m}^n = \mathbb{F}_q^{mn} = \mathbb{F}_q^{m\times n}$, endowed with the rank metric.

### Particular Matrix codes specified as $\mathbb{F}_{q^m}$-linear codes (Gabidulin [Gab85])

They are $\mathbb{F}_{q^m}$-linear subspaces of $\mathbb{F}_{q^m}^n$, endowed with the rank metric.

- $\mathbb{F}_{q^m}$-linear codes are particular matrix codes with a structure,
- Known families of $\mathbb{F}_{q^m}$-linear codes with decoding algorithms,
- $\mathbb{F}_{q^m}$-linear codes have a much shorter description (save a factor $m$)
  $\Rightarrow$ Shorter public keys in cryptography!

# Specific family of codes

$\mathbb{F}_{q^m}$-linear codes in rank metric: $\mathscr{C} \subset \mathbb{F}_{q^m}^n$ has an additional structure

| | $\mathbb{F}_{q^m}^n$-linear code | Matrix code in $\mathbb{F}_q^{nm}$ |
|---|---|---|
| Field | $\mathbb{F}_{q^m}$ | $\mathbb{F}_q$ |
| Length | $n$ | $nm$ |
| Dimension | $k$ | $km$ |
| Codeword | $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ | matrix $\boldsymbol{X} \in \mathbb{F}_q^{m \times n}$ |
| Size of a basis | $knm \log(q)$ | $kmnm \log(q)$ |

# Application of the rank metric



Examples of $\mathbb{F}_{q^m}$-linear codes with decoding algorithms

- Gabidulin codes [Gab85] (rank-metric analogue of Reed-Solomon codes),
- Low Rank Parity Check codes [Ara+19a] (rank-metric analogue of MDPC codes)

# The Rank Decoding Problem (RD)



## Rank Decoding Problem (RD)

- `Input`: an integer $r \in \mathbb{N}$, an $\mathbb{F}_{q^m}$-basis $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ of a subspace $\mathscr{C} \subset \mathbb{F}_{q^m}^n$, and a vector $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$.
- `Output`: $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that

$$\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e} \text{ and } \mathrm{Rank}(\boldsymbol{e}) \leq r.$$

[1] $\boldsymbol{s} = \boldsymbol{y}\boldsymbol{H}^\top$, $\boldsymbol{y}$ one solution of $\boldsymbol{y}\boldsymbol{H}^\top = \boldsymbol{s}$ without constraints on the weight of $\boldsymbol{y}$.

# The Rank Decoding Problem (RD)

## Rank Decoding Problem (RD)

- Input: an integer $r \in \mathbb{N}$, an $\mathbb{F}_{q^m}$-basis $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ of a subspace $\mathscr{C} \subset \mathbb{F}_{q^m}^n$, and a vector $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$.
- Output: $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that

$$\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e} \text{ and } \mathrm{Rank}(\boldsymbol{e}) \leq r.$$

## Syndrome formulation[1]

Given $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$, find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that

$$\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\top \text{ and } \mathrm{Rank}(\boldsymbol{e}) \leq r.$$

[1] $\boldsymbol{s} = \boldsymbol{y}\boldsymbol{H}^\top$, $\boldsymbol{y}$ one solution of $\boldsymbol{y}\boldsymbol{H}^\top = \boldsymbol{s}$ without constraints on the weight of $\boldsymbol{y}$.

# The MinRank Problem



## Computational MinRank (affine)

- `Input`: integers $r, m, n \in \mathbb{N}$, and $K = k+1$ matrices $\boldsymbol{Y}, \boldsymbol{M}_1, \ldots, \boldsymbol{M}_k \in \mathbb{F}_q^{m \times n}$
- `Output`: $(x_1, \ldots, x_k) \in \mathbb{F}_q$, such that

$$\text{Rank}\left(\boldsymbol{Y} + \sum_{i=1}^{k} x_i \boldsymbol{M}_i\right) \leq r.$$

# Hardness of MinRank and RD



## Hardness of the decoding for $\mathbb{F}_q$-linear matrix codes

- MinRank is an NP-complete problem (Buss, Frandsen, Shallit 1999),
- used to cryptanalyse various multivariate and code-based cryptosystems.
- This is exactly the decoding problem for matrix codes,

# Hardness of MinRank and RD



## Hardness of the decoding for $\mathbb{F}_q$-linear matrix codes

- MinRank is an NP-complete problem (Buss, Frandsen, Shallit 1999),
- used to cryptanalyse various multivariate and code-based cryptosystems.
- This is exactly the decoding problem for matrix codes,

## Hardness of the decoding for $\mathbb{F}_{q^m}$-linear codes

- RD is not "a priori" NP-hard.
- DP (Decoding problem, Hamming metric) $\leq_{\text{randomized}}$ RD ($m > n^2$) [GZ16]
- RD $\leq$ MinRank [FLP08].

# The Rank Support Learning Problem (RSL) [Gab+16]



Generalization of RD to multiple syndromes with the same support.

## Rank Support Learning Problem (RSL)

- `Input`:
  - an integer $r \in \mathbb{N}$,
  - an $\mathbb{F}_{q^m}$-basis $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ of a subspace $\mathscr{C} \subset \mathbb{F}_{q^m}^n$,
  - a set of syndromes $\boldsymbol{s}_i = \boldsymbol{e}_i \boldsymbol{H}^\top \in \mathbb{F}_{q^m}^n$ $(1 \leq i \leq \ell)$ such that the errors $\boldsymbol{e}_i$ share the same support $\mathscr{V} = \langle e_{i,j} \rangle_{\mathbb{F}_q}$ of dimension $r$,
- `Output`: The secret subspace $\mathscr{V}$.

# The Rank Support Learning Problem (RSL) [Gab+16]



Generalization of RD to multiple syndromes with the same support.

## Rank Support Learning Problem (RSL)

- `Input`:
  - an integer $r \in \mathbb{N}$,
  - an $\mathbb{F}_{q^m}$-basis $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ of a subspace $\mathscr{C} \subset \mathbb{F}_{q^m}^n$,
  - a set of syndromes $\boldsymbol{s}_i = \boldsymbol{e}_i \boldsymbol{H}^\top \in \mathbb{F}_{q^m}^n$ $(1 \leq i \leq \ell)$ such that the errors $\boldsymbol{e}_i$ share the same support $\mathscr{V} = \langle e_{i,j} \rangle_{\mathbb{F}_q}$ of dimension $r$,
- `Output`: The secret subspace $\mathscr{V}$.

## Hardness of RSL

- RSL $\leq$ RD.

# Code-Based cryptography



## First rank-metric code-based cryptosystem

- GPT cryptosystem based on Gabidulin codes (Eurocrypt'91, [GPT91]),
- broken by the Overbeck attack [Ove05],

## Recent proposals

- ROLLO: Analogue of the NTRU cryptosystem, secret Ideal LRPC codes ([Ara+19b], NIST ROUND-2),
- RQC: RD for Ideal codes, LWE structure, public Gabidulin code + random ideal code ([Agu+20], NIST ROUND-2)
- family of rank metric trapdoor functions: RSL, trapdoor based on secret LRPC code ([Bur+23])

# Code-Based cryptography

## Signature schemes (authentication protocoles)

- Durandal (Eurocrypt'19): RSL + Ideal structure.
- RYDE (NIST signature submission): RD.
- MIRA and MiRitH (NIST signature submission): MinRank.

# Complexity of solving RD, MinRank, RSL



## How can we solve those problems?

- **Combinatorial** approach: try "all possible solutions" efficiently;
  $\rightarrow$ the complexity is easy to estimate.
- **Algebraic** approach: solve an algebraic system.
  $\rightarrow$ how to estimate the complexity?

# Complexity of solving RD, MinRank, RSL



## How can we solve those problems?

- **Combinatorial** approach: try "all possible solutions" efficiently;
  $\rightarrow$ the complexity is easy to estimate.
- **Algebraic** approach: solve an algebraic system.
  $\rightarrow$ how to estimate the complexity?

## Hybrid approach

- Reduce the resolution of one big instance to the resolution of smaller instances.
- Works for any approach, any algorithm.
- Efficient if the small instances are easier.
- cf [BFP09; Bar+23]

# Algebraic Modeling

## Principle: write a Polynomial System

$$\begin{cases} f_1(x_1,\dots,x_n) \\ \vdots \\ f_m(x_1,\dots,x_n) \end{cases}, \quad \deg(f_i) = d_i, f_i \in \mathbb{K}[x_1,\dots,x_n].$$

such that finding the set of solutions

$$V(f_1,\dots,f_m) = \left\{(x_1,\dots,x_n) \in \overline{\mathbb{K}}^n : f_i(x_1,\dots,x_n) = 0, \forall i \in \{1..m\}\right\}$$

gives (part of) the secret.

Ideally: *any* solution is related to the secret!

# Algebraic Modeling

## Principle: write a Polynomial System

$$\begin{cases} f_1(x_1,\dots,x_n) \\ \vdots \\ f_m(x_1,\dots,x_n) \end{cases}, \quad \deg(f_i) = d_i, f_i \in \mathbb{K}[x_1,\dots,x_n].$$

such that finding the set of solutions

$$V(f_1,\dots,f_m) = \left\{(x_1,\dots,x_n) \in \overline{\mathbb{K}}^n : f_i(x_1,\dots,x_n) = 0, \forall i \in \{1..m\}\right\}$$

gives (part of) the secret.

## Ideally: *any* solution is related to the secret!

- Otherwise, we have to deal with spurious solutions.

# Algebraic Modeling

## Principle: write a Polynomial System

$$\begin{cases} f_1(x_1,\dots,x_n) \\ \vdots \\ f_m(x_1,\dots,x_n) \end{cases}, \quad \deg(f_i) = d_i, f_i \in \mathbb{K}[x_1,\dots,x_n].$$

such that finding the set of solutions

$$V(f_1,\dots,f_m) = \{(x_1,\dots,x_n) \in \overline{\mathbb{K}}^n : f_i(x_1,\dots,x_n) = 0, \forall i \in \{1..m\}\}$$

gives (part of) the secret.

## Ideally: *any* solution is related to the secret!

- Otherwise, we have to deal with spurious solutions.
- Solutions in $\mathbb{F}_q$: algebraic constraint! add the field equations $x_i^q - x_i$.

## Solving the algebraic system using Gröbner bases (object)

- A particular basis of the ideal

$$I(f_1, \ldots, f_m) = \langle f_1, \ldots, f_m \rangle$$

  that solves the ideal-membership problem.
- Depends on the choice of a monomial ordering.

## Solving the algebraic system using Gröbner bases (object)

- A particular basis of the ideal

$$I(f_1, \dots, f_m) = \langle f_1, \dots, f_m \rangle$$

that solves the ideal-membership problem.

- Depends on the choice of a monomial ordering.

## A hard problem

- Ideal Membership testing is EXPSPACE-complete,
- Existence of solutions to a system of polynomial equations over a finite field is NP-complete ([**FY79**]),

# Monomial ordering examples



## Lexicographical ordering $x_1 > \cdots > x_n$

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} > x_1^{\beta_1} \ldots x_n^{\beta_n} \text{ iff } \begin{cases} \alpha_j = \beta_j & \forall j < i, \\ \alpha_i > \beta_i. \end{cases}$$

## Graded Reverse Lexicographical ordering $x_1 > \cdots > x_n$

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} > x_1^{\beta_1} \ldots x_n^{\beta_n} \text{ iff } \begin{cases} \alpha_j = \beta_j & \forall j > i, \\ \alpha_i < \beta_i. \end{cases}$$

## Elimination Ordering $\mathrm{x} > \mathrm{y}$

$$\mathrm{x}^{\alpha}\mathrm{y}^{\beta} > \mathrm{x}^{\alpha'}\mathrm{y}^{\beta'} \text{ iff } \begin{cases} \alpha >_1 \alpha' \\ \text{or } \alpha = \alpha' \text{ and } \beta >_2 \beta'. \end{cases}$$

# Properties of monomial orderings



## Different monomial orderings have different properties

- the *lex* order (Lexicographical): in Shape Position, for a zero-dimension ideal, the lex basis is

$$\begin{cases} x_1 - g_1(x_n), \\ \vdots \\ x_{n-1} - g_{n-1}(x_n), \\ g_n(x_n), \end{cases}$$

  with $\deg(g_n) = D$ the number of solutions to the system.
- the *grevlex* order (Graded Reverse Lexicographical): usually the best one w.r.t. the complexity.
- the *elim* order (Elimination): two blocks of variables $x > y$.

# Systems with 0 or 1 solution



The grevlex and lex bases are the same:

- If the system has 1 solution:

$$\begin{cases} x_1 - a_1, \\ \vdots \\ x_n - a_n, \end{cases}$$

  where $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$ is the solution.
- If the system has no solution:

$$\langle 1 \rangle.$$

# Change of ordering FGLM for zero-dimensional systems

- The FGLM ([Fau+93]) Algorithm performs a change of ordering in complexity

$$O(nD^3),$$

$n$ number of variables, $n \to \infty$, $D$ degree of the ideal (number of solutions).

# Change of ordering FGLM for zero-dimensional systems



- The FGLM ([Fau+93]) Algorithm performs a change of ordering in complexity

$$O(nD^3),$$

$n$ number of variables, $n \to \infty$, $D$ degree of the ideal (number of solutions).

- Complexity for grevlex to lex (Shape position) ([Fau+14]):

$$O(\log_2(D)(D^{\omega} + n\log_2(D)D)).$$

# Change of ordering FGLM for zero-dimensional systems



- The FGLM ([Fau+93]) Algorithm performs a change of ordering in complexity

$$O(nD^3),$$

$n$ number of variables, $n \to \infty$, $D$ degree of the ideal (number of solutions).

- Complexity for grevlex to lex (Shape position) ([Fau+14]):

$$O(\log_2(D)(D^\omega + n\log_2(D)D)).$$

- Sparse versions for generic systems grevlex to lex ([FM17]) in

$$O\left(\sqrt{\frac{6}{n\pi}}D^{2+\frac{n-1}{n}}\right).$$

# Gröbner basis algorithms

General algorithms, for any input system:

- Buchberger ([Buc65]),
- F4 ([Fau99]),
- F5 ([Fau02]).

The algorithms will always terminate and give the Gröbner basis.
But the time is hard to predict for *any* instance (goes from 1 to $d^{2^n}$ [**MM82**], simply exponential for zero-dimensional, grevlex [**G84**; Laz83]).

# Gröbner basis algorithms



General algorithms, for any input system:

- Buchberger ([Buc65]),
- F4 ([Fau99]),
- F5 ([Fau02]).

The algorithms will always terminate and give the Gröbner basis.
But the time is hard to predict for *any* instance (goes from 1 to $d^{2^n}$ [**MM82**], simply exponential for zero-dimensional, grevlex [**G84**; Laz83]).

Specific algorithms, for a particular class of systems:

The algorithms will terminate in a predictable time.
The result is not always a Gröbner basis of the system.
For random instances in the specific class, the result is a Gröbner basis.

# Generic Complexity analysis



$$\text{System}\begin{cases} f_1(x_1,\ldots,x_n) \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{cases}, \quad \deg(f_i) = d_i, f_i \in \mathbb{K}[x_1,\ldots,x_n].$$

## Tools from computer algebra

- Macaulay Matrices (1902): $\mathscr{M}_d(\{f_1,\ldots,f_m\}) = \begin{matrix} \vdots \\ (t,i) \\ \vdots \end{matrix} \overset{t'}{\begin{pmatrix} & & \\ & \text{coeff}(tf_i, t') & \\ & & \end{pmatrix}}$
- Describes the vector space $\langle tf_i : \deg(tf_i) = d \rangle_{\mathbb{K}}$.
- Lazard (1983): compute a Gb with linear algebra on the Macaulay matrices up to degree $D$.

## Complexity bounds



### Linear algebra on the Macaulay matrix of degree $D$

A Gröbner basis of a system $(f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]$ up to degree $D$ for a graded monomial ordering can be computed in, at most,

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right) \qquad n, m \to \infty.$$

operations.

# Complexity bounds



## Linear algebra on the Macaulay matrix of degree $D$

A Gröbner basis of a system $(f_1, \ldots, f_m) \in \mathbb{K}[x_1, \ldots, x_n]$ up to degree $D$ for a graded monomial ordering can be computed in, at most,

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right) \qquad n, m \to \infty.$$

operations.

## Main challenges

- Estimate $D$.
- Identify unnecessary computations to reduce the complexity, e.g. to $O\left(\binom{n+D}{D}^{\omega}\right)$.
- If there are fall degree at degree $< D$, construct a better strategy (algorithm) to take that into account, and estimate its complexity.

# Generic Complexity analysis



Known classes of particular systems (not exhaustive)

- **regular** systems [Mac94],
- **determinantal** systems [CH94],
- **semi-regular** systems [BFS04],
- solutions in $\mathbb{F}_2$: **boolean semi-regular** systems [Bar+05],
- **bi-regular bilinear** systems [FSS11].

# Difference between classes



$$O\left(mD\binom{n+D-1}{D}^{\omega}\right) \qquad\qquad n,m\to\infty.$$

## Examples of quadratic equations:

- $m=n$ regular system: : $D\leq n+1$,
- $m=n+1$ semi-regular system: $D\leq\lceil\frac{n+2}{2}\rceil$,
- $m=n$ regular bilinear system with $\lfloor\frac{n}{2}\rfloor$ variables $x$ and $\lceil\frac{n}{2}\rceil$ variables $y$: $D\leq\lceil\frac{n}{2}\rceil$.
- $m=n$ regular over $\mathbb{F}_2$: $D\simeq\frac{n}{11}$, $O(\binom{n}{D}^{\omega})$

# Algebraic attack



For each class we know

- relations between rows in the Macaulay matrices = syzygies,
- the rank of the Macaulay matrices for generic systems,
- the maximal degree $D \rightarrow$ complexity estimates,
- a specific Gb algorithm that is more efficient.

# Algebraic attack



## For each class we know

- relations between rows in the Macaulay matrices = syzygies,
- the rank of the Macaulay matrices for generic systems,
- the maximal degree $D \rightarrow$ complexity estimates,
- a specific Gb algorithm that is more efficient.

## If the system is not in a known class

- Identify a generic behavior,
- Identify a specific algorithm to compute the Gb,
- Create a new class!

# Algebraic modeling for RD

RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^{n}$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$, $\boldsymbol{H}_y$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

# Algebraic modeling for RD



RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^{n}$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$, $\boldsymbol{H}_{\boldsymbol{y}}$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

## Equivalent formulations, different algebraic modeling

- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^{n}$ , $\boldsymbol{x} \in \mathbb{F}_{q^m}^{k}$ such that $\boldsymbol{e} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{y}$ and $\text{Rank}(\boldsymbol{e}) \leq r$

# Algebraic modeling for RD



RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$, $\boldsymbol{H}_y$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

## Equivalent formulations, different algebraic modeling

- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{e}\boldsymbol{H}_y{}^\top = 0$ and $\text{Rank}(\boldsymbol{e}) \leq r$

# Algebraic modeling for RD



RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$, $\boldsymbol{H}_y$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

## Equivalent formulations, different algebraic modeling

- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{e}\boldsymbol{H}_y^\top = 0$ and $(s_1, \ldots, s_r) \in \mathbb{F}_{q^m}^r$, $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$ such that $\boldsymbol{e} = (s_1, \ldots, s_r)\boldsymbol{C}$.

# Algebraic modeling for RD



RD instance: $\mathbf{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\mathbf{y} \in \mathbb{F}_{q^m}^{n}$ such that $d(\mathbf{y}, \mathscr{C}) \leq r$, $\mathbf{H}_{\mathbf{y}}$ a parity-check matrix of the code $\mathscr{C} + \langle \mathbf{y} \rangle_{\mathbb{F}_{q^m}}$.

## Equivalent formulations, different algebraic modeling

- find $\mathbf{e} \in \mathbb{F}_{q^m}^{n}$ such that $\mathbf{e}\mathbf{H}_{\mathbf{y}}^{\top} = 0$ and $(s_1, \ldots, s_r) \in \mathbb{F}_{q^m}^{r}$, $\mathbf{C} \in \mathbb{F}_{q}^{r \times n}$ such that $\mathbf{e} = (s_1, \ldots, s_r)\mathbf{C}$.
- find $(s_1, \ldots, s_r) \in \mathbb{F}_{q^m}^{r}$ and $\mathbf{C} \in \mathbb{F}_{q}^{r \times n}$ such that $(s_1, \ldots, s_r)\mathbf{C}\mathbf{H}_{\mathbf{y}}^{\top} = 0$ [OJ02].

# Algebraic modeling for RD

RD instance: $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ public matrix, $\boldsymbol{y} \in \mathbb{F}_{q^m}^{n}$ such that $d(\boldsymbol{y}, \mathscr{C}) \leq r$, $\boldsymbol{H}_y$ a parity-check matrix of the code $\mathscr{C} + \langle \boldsymbol{y} \rangle_{\mathbb{F}_{q^m}}$.

## Equivalent formulations, different algebraic modeling

- find $\boldsymbol{e} \in \mathbb{F}_{q^m}^{n}$ such that $\boldsymbol{e}\boldsymbol{H}_y{}^{\top} = 0$ and $(s_1, \ldots, s_r) \in \mathbb{F}_{q^m}^{r}$, $\boldsymbol{C} \in \mathbb{F}_{q}^{r \times n}$ such that $\boldsymbol{e} = (s_1, \ldots, s_r)\boldsymbol{C}$.
- find $(s_1, \ldots, s_r) \in \mathbb{F}_{q^m}^{r}$ and $\boldsymbol{C} \in \mathbb{F}_{q}^{r \times n}$ such that $(s_1, \ldots, s_r)\boldsymbol{C}\boldsymbol{H}_y{}^{\top} = 0$ [OJ02].
- find $\boldsymbol{C} \in \mathbb{F}_{q}^{r \times n}$ such that $\boldsymbol{C}\boldsymbol{H}_y{}^{\top}$ has a non-trivial left kernel [Bar+20].

# MaxMinors modeling



## Algebraic Modeling [Bar+20]

$$\mathrm{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_{y}{}^{\top}) = \left\{ P_J := \left| \boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}{}^{\top} \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

- Cauchy-Binet formula: $\det(\boldsymbol{AB}) = \sum_T \det(\boldsymbol{A}_{*,T})\det(\boldsymbol{B}_{T,*})$.

# MaxMinors modeling



## Algebraic Modeling [Bar+20]

$$\mathrm{MaxMinors}(\boldsymbol{C}\boldsymbol{H_y}^\top) = \left\{ P_J := \left|\boldsymbol{C}\boldsymbol{H_y}^\top\right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

- Cauchy-Binet formula: $\det(\boldsymbol{AB}) = \sum_T \det(\boldsymbol{A}_{*,T})\det(\boldsymbol{B}_{T,*})$.
- Plücker coordinates ($N = \binom{n}{r} - 1$): injective map, easy to invert on its image.

$$p : \{\mathscr{W} \subset \mathbb{F}_q^n : \dim(\mathscr{W}) = r\} \to \mathbb{P}^N(\mathbb{F}_q)$$
$$\boldsymbol{C} \text{ generator matrix of } \mathscr{W} \mapsto (\left|\boldsymbol{C}_{*,T}\right|)_{T\subset\{1..n\},\#T=r}$$

# MaxMinors modeling



## Algebraic Modeling [Bar+20]

$$\mathrm{MaxMinors}(\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top}) = \left\{ P_J := \left|\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top}\right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

## Analysis of the system

- $\binom{n}{r}$ variables $c_T = |\boldsymbol{C}|_{*,T}$, $T \subset \{1..n\}$, $\#T = r$
- $\binom{n-k-1}{r}$ linear equations $P_J = 0$ with coefficients in $\mathbb{F}_{q^m}$,

# MaxMinors modeling



## Algebraic Modeling [Bar+20]

$$\text{MaxMinors}(\boldsymbol{C}\boldsymbol{H_y}^\top) = \left\{ P_J := \left| \boldsymbol{C}\boldsymbol{H_y}^\top \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

## Analysis of the system

- $\binom{n}{r}$ variables $c_T = |\boldsymbol{C}|_{*,T}$, $T \subset \{1..n\}$, $\#T = r$
- $\binom{n-k-1}{r}$ linear equations $P_J = 0$ with coefficients in $\mathbb{F}_{q^m}$,
- $m$ times more equations over $\mathbb{F}_q$.

# Complexity of solving the MaxMinors modeling



## Solving in the Overdetermined case

If $m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$ and the equations over $\mathbb{F}_q$ are "as linearly independent as possible" $\rightarrow$ independence assumption.

# Complexity of solving the MaxMinors modeling



## Solving in the Overdetermined case

If $m\binom{n-k-1}{r} \geq \binom{n}{r} - 1$ and the equations over $\mathbb{F}_q$ are "as linearly independent as possible" $\rightarrow$ independence assumption.

## In the Underdetermined case

- Hybrid approach to reduce to the overdetermined case;
- Introduce another set of variables (e.g. $\boldsymbol{x}$ or $\boldsymbol{s}$).

# Non overdetermined cases



$$\mathbf{e} = \mathbf{x}\mathbf{G} + \mathbf{y} = \mathbf{s}\mathbf{C}$$

## Reduce to smaller problems

- if $a$ positions of $\mathbf{e}$ are zero: $a$ linear equations in $\mathbf{x}$, $a$ columns of $\mathbf{C}$ are zero $\rightarrow$ reduce to a smaller instance with parameters $(m, n-a, k-a, r)$,
- this has a chance $1/q^{ar}$ to happen.
- Deterministic version if $a + r \leq k$.
- Constraint $m\binom{n-k-1}{r} \geq \binom{n-a}{r} - 1$ will be satisfied for $a$ large enough.

Cost $q^{ar}\mathbb{C}_{RD}(m, n-a, k-a, r)$.

# Non overdetermined cases



$$\mathbf{e} = \mathbf{x}\mathbf{G} + \mathbf{y} = \mathbf{s}\mathbf{C}$$

## Support Minors modeling over $\mathbb{F}_{q^m}$ [Bar+23]

$$\left\{ Q_I \stackrel{\text{def}}{=} \left| \begin{pmatrix} \mathbf{x}\mathbf{G} + \mathbf{y} \\ \mathbf{C} \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1 \right\}$$

- $\binom{n}{r}$ variables $c_T \in \mathbb{F}_q$, $k$ variables $x_1, \dots, x_k \in \mathbb{F}_{q^m}$,
- $\binom{n}{r+1}$ equations $Q_I = 0$ for $I \subset \{1..n\}$, $\#I = r+1$, viewed as affine bilinear equations over $\mathbb{F}_{q^m}$ in the $x_i$'s and the $c_T$'s.

# Analysis of the Support Minors modeling over $\mathbb{F}_{q^m}$

$$\mathscr{Q} = \left\{ Q_I \overset{\text{def}}{=} \left| \begin{pmatrix} \mathbf{x}\mathbf{G} + \mathbf{y} \\ \mathbf{C} \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1 \right\}$$

$$\mathscr{P} = \left\{ P_J \overset{\text{def}}{=} \left| \mathbf{C}\mathbf{H}_{\mathbf{y}}{}^{\top} \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

$$\mathscr{Q}_s = \{Q_I : \#(I \cap \{1..k+1\}) = s\},$$

$$\mathscr{Q}_{\geq s} = \{Q_I : \#(I \cap \{1..k+1\}) \geq s\},$$

# Analysis of the Support Minors modeling over $\mathbb{F}_{q^m}$

$$\mathscr{Q} = \left\{ Q_I \stackrel{\text{def}}{=} \left| \begin{pmatrix} xG + y \\ C \end{pmatrix} \right|_{*,I} : I \subset \{1..n\}, \#I = r+1 \right\}$$

$$\mathscr{P} = \left\{ P_J \stackrel{\text{def}}{=} \left| C H_y{}^{\top} \right|_{*,J} : J \subset \{1..n-k-1\}, \#J = r \right\}.$$

$$\mathscr{Q}_s = \{ Q_I : \#(I \cap \{1..k+1\}) = s \},$$
$$\mathscr{Q}_{\geq s} = \{ Q_I : \#(I \cap \{1..k+1\}) \geq s \},$$

Proposition:

$$\mathscr{Q}_0 \subset \langle \mathscr{Q}_{\geq 1} \rangle_{\mathbb{F}_q}$$
$$\langle \mathscr{P}, x_i \mathscr{P} : i \in \{1..k\}, \mathscr{Q}_{\geq 2} \rangle_{\mathbb{F}_q} = \langle \mathscr{Q}_1, \mathscr{Q}_{\geq 2} \rangle_{\mathbb{F}_q}$$
$$\mathscr{P}, x_i \mathscr{P} : i \in \{1..k\}, \mathscr{Q}_{\geq 2} \text{ are linearly independent over } \mathbb{F}_q$$

# Hints of Proof



- $\left|\begin{pmatrix} \boldsymbol{x}\boldsymbol{G}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \boldsymbol{H_y}^\top\right|_{*,T} = 0$ + Cauchy-Binet formula + systematic form implies that $\mathscr{Q}_0 \subset \langle \mathscr{Q}_{\geq 1} \rangle$.
- We introduce a monomial ordering and compare leading terms.
- $\left|\begin{pmatrix} \boldsymbol{x}\boldsymbol{G}+\boldsymbol{y} \\ \boldsymbol{C} \end{pmatrix} \boldsymbol{H}^\top\right|_{*,J\cup\{n-k\}} = (-1)^r P_J$ + Cauchy-Binet formula + systematic form implies that $\mathscr{P} \subset \mathscr{Q}_1 + \langle \mathscr{Q}_{\geq 2} \rangle$.
- same idea with another matrix for $x_i P_J$.

# Solving Support Minors over $\mathbb{F}_{q^m}$: too many solutions



## With the equations $\mathscr{P} + \mathscr{Q}_{\geq 2}$

- each linear equation $P_J$ removes a variable $c_{J+k+1}$ that does not appear in $\mathscr{Q}_{\geq 2}$,
- we can describe the vector spaces generated by $\mathscr{Q}_{\geq 2}$ for each bidegree $(b, 1)$ in $(x_i, c_T)$,
- the Macaulay matrices always have a rank = # rows.

# Solving Support Minors over $\mathbb{F}_{q^m}$: too many solutions



## With the equations $\mathscr{P} + \mathscr{Q}_{\geq 2}$

- each linear equation $P_J$ removes a variable $c_{J+k+1}$ that does not appear in $\mathscr{Q}_{\geq 2}$,
- we can describe the vector spaces generated by $\mathscr{Q}_{\geq 2}$ for each bidegree $(b, 1)$ in $(x_i, c_T)$,
- the Macaulay matrices always have a rank $=$ # rows.

## But...

- we can eliminate $m$ times more variables $c_J$ by unfolding the $P_J$'s!
- that's SM-$\mathbb{F}_{q^m}^+ = \{Q_I : I\} + \{P_{i,J} : i, J\}$.
- we analyse the vector spaces generated by the equations in any bidegree $(b, 1)$ in $\boldsymbol{x}_i, c_T \rightarrow$ syzygies $\rightarrow$ generic complexity.

# Complexity of solving SM-$\mathbb{F}_{q^m}^+$



$$\mathcal{N}_b^{\mathbb{F}_q} = \mathcal{N}_b^{\mathbb{F}_{q^m}} - \mathcal{N}_{b,syz}^{\mathbb{F}_q},$$

$$\mathcal{N}_b^{\mathbb{F}_{q^m}} = \sum_{i=1}^{k} \binom{n-i}{r}\binom{k+b-1-i}{b-1} - \binom{n-k-1}{r}\binom{k+b-1}{b} \qquad (exact)$$

$$\mathcal{N}_{b,syz}^{\mathbb{F}_q} = (m-1)\sum_{i=1}^{b}(-1)^{i+1}\binom{k+b-i-1}{b-i}\binom{n-k-1}{r+i} \qquad (conjecture)$$

$$\mathcal{M}_b^{\mathbb{F}_q} = \binom{k+b-1}{b}\left(\binom{n}{r} - m\binom{n-k-1}{r}\right), \qquad (exact)$$

## Solving SM-$\mathbb{F}_{q^m}^+$

We can solve SM-$\mathbb{F}_{q^m}^+$ by linearization at bidegree $(b,1)$ whenever $\mathcal{N}_b^{\mathbb{F}_q} \geq \mathcal{M}_b^{\mathbb{F}_q} - 1$ with a cost $\mathcal{O}\left(m^2 \mathcal{N}_b^{\mathbb{F}_q} {\mathcal{M}_b^{\mathbb{F}_q}}^{\omega-1}\right)$ operations in $\mathbb{F}_q$.

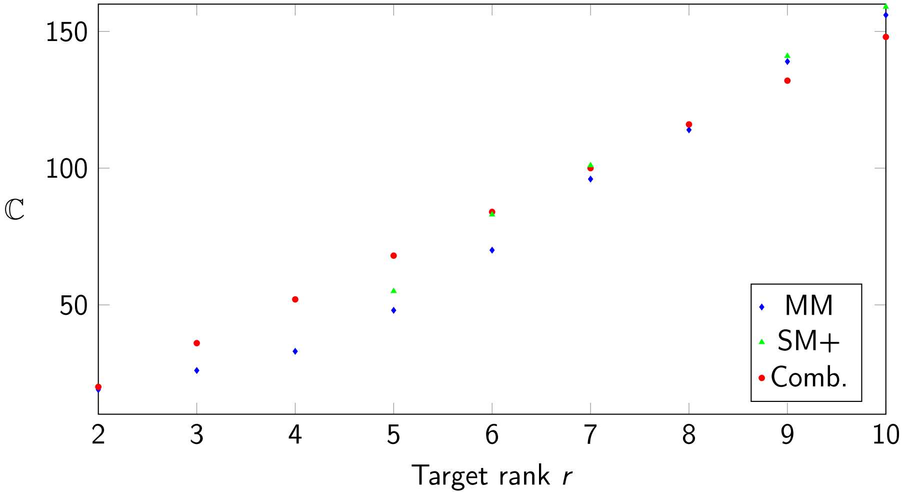


Figure: Theoretical $\log_2$ complexities $\mathbb{C}$ of MM-$\mathbb{F}_q$/SM-$\mathbb{F}_{q^m}^+$(the best one, hybrid and punctured version) and of the combinatorial attack for RD instances with fixed $(m, n, k) = (31, 33, 15)$ and various values of $r$. $d_{\mathrm{RGV}}(m, n, k, q = 2) = 10$.

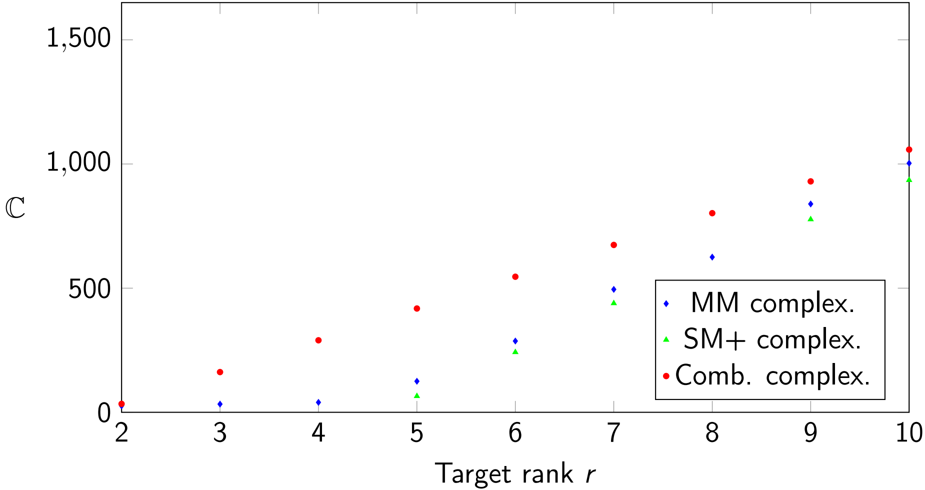


Figure: Same parameters as Fig. 1 but with $q = 2^8$.

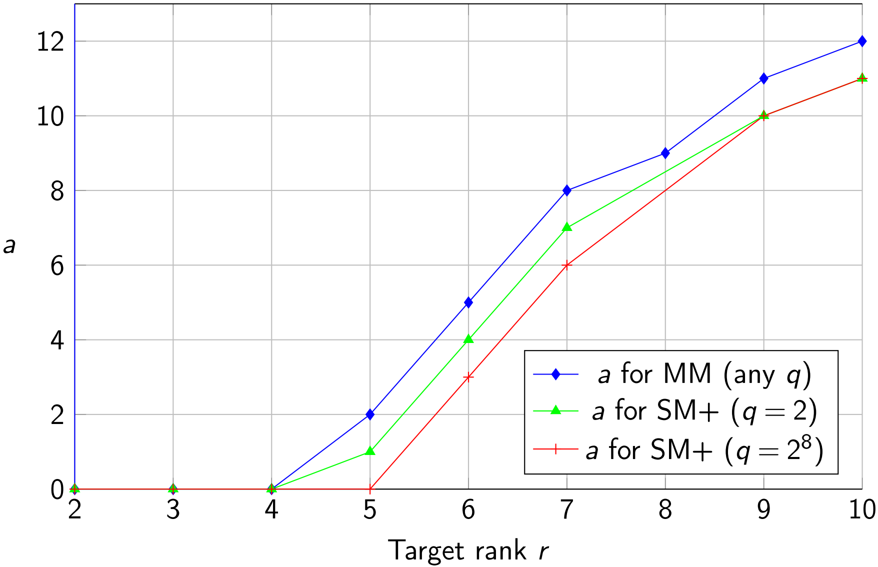


Figure: Optimal values of $a$ with $(m, n, k) = (31, 33, 15)$, for MM-$\mathbb{F}_q$ and SM-$\mathbb{F}_{q^m}^+$.

# Conclusion



- A powerful tool to solve problems that have an algebraic modeling,
- Design specific algorithms for specific class of systems to be efficient.
- A lot of parameters to choose, how to optimize?
- New modeling: e.g. RD over $\mathbb{F}_q$?
- Optimize the linear algebra part?

[Agu+20] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Maxime Bros, Alain Couvreur, Jean-Christophe Deneuville, Philippe Gaborit, Gilles Zémor, and Adrien Hauteville. *Rank Quasi Cyclic (RQC)*. Second Round submission to NIST Post-Quantum Cryptography call. Apr. 2020.

[Ara+19a] N. Aragon, P. Gaborit, A. Hauteville, O. Ruatta, and G. Zémor. "Low Rank Parity Check Codes: New Decoding Algorithms and Application to Cryptography". In: submitted to IEEE IT, preprint available on arXiv. 2019.

[Ara+19b] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zémor, Carlos Aguilar Melchor, Slim Bettaieb, Loïc Bidoux, Magali Bardet, and Ayoub Otmani. *ROLLO (merger of Rank-Ouroboros, LAKE and LOCKER)*. Second round submission to the NIST post-quantum cryptography call. NIST Round 2 submission for Post-Quantum Cryptography. Mar. 2019.

[Bar+05] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Bo-Yin Yang. “Asymptotic expansion of the degree of regularity for semi-regular systems of equations”. In: *MEGA’05 – Effective Methods in Algebraic Geometry*. 2005, pp. 1–14.

[Bar+20] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. “Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems”. In: *ASIACRYPT*. 2020.

[Bar+23] Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, and Jean-Pierre Tillich. “Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem”. In: *Designs, Codes and Cryptography* 91 (2023), pp. 3671–3707.

[BFP09] Luk Bettale, Jean-Charles Faugere, and Ludovic Perret. “Hybrid approach for solving multivariate systems over finite fields”. In: *Journal of Mathematical Cryptology* 3.3 (2009), pp. 177–197.

[BFS04] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. "On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations". In: *Proceedings of the International Conference on Polynomial System Solving*. 2004, pp. 71–74.

[Buc65] Bruno Buchberger. "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal". PhD thesis. Universitat Innsbruck, 1965.

[Bur+23] Étienne Burle, Philippe Gaborit, Younes Hatri, and Ayoub Otmani. *Injective Rank Metric Trapdoor Functions with Homogeneous Errors*. 2023. arXiv: 2310.08962 [cs.CR].

[CH94] Aldo Conca and Jurgen Herzog. "On the Hilbert function of determinantal rings and their canonical module". In: *Proc. Amer. Math. Soc* 122 (1994), pp. 677–681.

[Del78] Philippe Delsarte. "Bilinear Forms over a Finite Field, with Applications to Coding Theory". In: *J. Comb. Theory, Ser. A* 25.3 (1978), pp. 226–241.

[Fau+14] Jean-Charles Faugère, Pierrick Gaudry, Louise Huot, and Guénaël Renault. "Sub-Cubic Change of Ordering for GröBner Basis: A Probabilistic Approach". In: *ISSAC*. 2014.

[Fau+93] Jean-Charles Faugère, Patrizia M. Gianni, Daniel Lazard, and Teo Mora. "Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering". In: *JSC* (1993).

[Fau02] Jean-Charles Faugère. "A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero: F5". In: *Proceedings ISSAC'02*. ACM press, 2002, pp. 75–83.

[Fau99] Jean-Charles Faugère. "A New Efficient Algorithm for Computing Gröbner Bases (F4)". In: *J. Pure Appl. Algebra* 139.1-3 (1999), pp. 61–88.

[FLP08] Jean-Charles Faugère, Françoise Levy-dit-Vehel, and Ludovic Perret. "Cryptanalysis of Minrank". In: *Advances in Cryptology - CRYPTO 2008*. Ed. by David Wagner. Vol. 5157. LNCS. 2008, pp. 280–296.

[FM17] Jean-Charles Faugère and Chenqi Mou. "Sparse FGLM algorithms". In: *JSC* (2017).

[FSS11] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. "Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity". In: *J. Symbolic Comput.* 46.4 (2011), pp. 406–437.

[Gab+16] Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, and Jean-Pierre Tillich. *Identity-based Encryption from Rank Metric*. IACR Cryptology ePrint Archive, Report2017/623. `http://eprint.iacr.org/`. May 2016.

[Gab85] Ernst M. Gabidulin. "Theory of codes with maximum rank distance". In: *Problemy Peredachi Informatsii* 21.1 (1985), pp. 3–16.

[GPT91] Ernst M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. "Ideals over a non-commutative ring and their applications to cryptography". In: *Advances in Cryptology - EUROCRYPT'91*. LNCS 547. Brighton, Apr. 1991, pp. 482–489.

[GZ16] Philippe Gaborit and Gilles Zémor. "On the hardness of the decoding and the minimum distance problems for rank codes". In: *IEEE Trans. Inform. Theory* 62(12) (2016), pp. 7245–7252.

[Laz83] D. Lazard. "Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations". In: *Computer algebra*. 1983.

[Mac94] Francis Sowerby Macaulay. *The algebraic theory of modular systems*. Vol. 19. Cambridge University Press, 1994.

[OJ02] Alexei V. Ourivski and Thomas Johansson. "New Technique for Decoding Codes in the Rank Metric and Its Cryptography Applications". English. In: *Problems of Information Transmission* 38.3 (2002), pp. 237–246.

[Ove05] Raphael Overbeck. "A New Structural Attack for GPT and Variants". In: *Mycrypt*. Vol. 3715. LNCS. 2005, pp. 50–63.