Algebraic Decoding of Rank Metric Codes

Françoise Levy-dit-Vehel

ENSTA
Paris, France
levy@ensta.fr

joint work with Ludovic Perret (UCL Louvain)

Special Semester on Gröbner Bases - Workshop D1

Outline

- The Rank Decoding problem (RD)
  - Motivation
  - Some complexity results
  - Easy instances of RD
- Solving RD:
  - generic algorithms
  - focusing on Ourivski-Johannsson method
  - our approach
- Practical results
- Conclusion

The Rank Decoding Problem

RD

Input: $N, n, k \in \mathbb{N}^*$, $G \in \mathcal{M}_{k\times n}(\mathbb{F}_{q^N})$, $c \in \mathbb{F}_{q^N}^n$.
Question: find $m \in \mathbb{F}_{q^N}^k$, such that $e = c - mG$ has smallest rank $\mathrm{Rk}(e \,|\, \mathbb{F}_q)$?
Here, $\mathrm{Rk}(e \,|\, \mathbb{F}_q)$ is the rank of e when considered as a $(N \times n)$ matrix over $\mathbb{F}_q$.

A related problem: MR

Input: $N, n, k \in \mathbb{N}^*$, $M_0, \ldots, M_k \in \mathcal{M}_{N\times n}(\mathbb{F}_q)$.
Question: find $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$, such that $E = M_0 - \sum_{i=1}^k \lambda_i M_i$ has smallest rank ?

MR can be seen as a *Subcode Rank Decoding* problem, where m has to be searched in $\mathbb{F}_q^k$.

The Rank Decoding Problem

RD

Input: $N, n, k \in \mathbb{N}^*$, $G \in \mathcal{M}_{k\times n}(\mathbb{F}_{q^N})$, $c \in \mathbb{F}_{q^N}^n$.

Question: find $m \in \mathbb{F}_{q^N}^k$, such that $e = c - mG$ has smallest rank $\mathrm{Rk}(e \mid \mathbb{F}_q)$?

Here, $\mathrm{Rk}(e \mid \mathbb{F}_q)$ is the rank of e when considered as a $(N \times n)$ matrix over $\mathbb{F}_q$.

A related problem: **MR**

Input: $N, n, k \in \mathbb{N}^*$, $M_0, \ldots, M_k \in \mathcal{M}_{N\times n}(\mathbb{F}_q)$.

Question: find $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$, such that $E = M_0 - \sum_{i=1}^k \lambda_i M_i$ has smallest rank ?

MR can be seen as a *Subcode Rank Decoding* problem, where m has to be searched in $\mathbb{F}_q^k$.

The Rank Decoding Problem

RD

Input: $N, n, k \in \mathbb{N}^*$, $G \in \mathcal{M}_{k \times n}(\mathbb{F}_{q^N})$, $c \in \mathbb{F}_{q^N}^n$.

Question: find $m \in \mathbb{F}_{q^N}^k$, such that $e = c - mG$ has smallest rank $\mathrm{Rk}(e \mid \mathbb{F}_q)$?

Here, $\mathrm{Rk}(e \mid \mathbb{F}_q)$ is the rank of e when considered as a $(N \times n)$ matrix over $\mathbb{F}_q$.

A related problem: MR

Input: $N, n, k \in \mathbb{N}^*$, $M_0, \ldots, M_k \in \mathcal{M}_{N \times n}(\mathbb{F}_q)$.

Question: find $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$, such that $E = M_0 - \sum_{i=1}^k \lambda_i M_i$ has smallest rank ?

MR can be seen as a *Subcode Rank Decoding* problem, where m has to be searched in $\mathbb{F}_q^k$.

Motivation: cryptographic applications...

... of **MR**

- Birational permutations signature scheme [Sh 93]
- TTM cryptosystem [Mo 99]
- Courtois ZK authentication scheme [Co 01]

... of **RD**

- GPT cryptosystem [GaPaTr 91,GaOu 01]
- Chen authentication scheme [Ch 96]
- Berger-Loidreau cryptosystem [BeLo 04]

Some Complexity Results

Theorem (BuFrSh 96,Co 01)

MR *is* NP-Hard.

Proof.

By reduction of Maximum Likelihood Decoding over $\mathbb{F}_q$ - proven to be NP-Hard [BeMcEvT 78, Ba 94, GuVa 05] - to MR. □

Corollary

There exists a reduction from RD *to* MR.

Open Questions

- No known explicit reduction.
- Is RD NP-hard ?

Solving the RD problem (I)

Algorithms for particular codes

Gabidulin codes: the generator matrix is of the form

$$G = \begin{pmatrix} g_1 & \cdots & g_n \\ g_1^q & \cdots & g_n^q \\ \vdots & \ddots & \vdots \\ g_1^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix}, \quad (g_1, \dots, g_n) \in \mathbb{F}_{q^N}^n.$$

$\diamondsuit$ Decoding algorithms ($\mathbb{F}_{q^N}$-mult.): $r^3 + (2n + N)r$ [Ga 91], $(5/2)n^2$ [Lo 05].

Reducible rank codes: generator matrix of the form $\begin{pmatrix} G_1 & 0 \\ A & G_2 \end{pmatrix}$, where G_i, $i = 1, 2$, are matrices of Gabidulin codes.

$\diamondsuit$ Decoding complexity ($\mathbb{F}_{q^N}$-mult.): $O(kn + n^3)$ [OuGaHoAm 03].

Solving the RD problem (II)

Generic algorithms

Stern-Chabaud (96):

- Problem modeled in terms of parity-check matrix.
- Solving approach: enumerating rank r r-tuples of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$, and trying to solve a linear system.
- Improved exhaustive enumeration from q^{Nr} to $q^{(N-r)(r-1)}$.
- Complexity: $O((nr+N)^3 q^{(N-r)(r-1)})$.

Ourivski-Johansson (02):

- Problem reduced to finding a minimum rank codeword in an extended code.
- Enumeration + solving a linear system over $\mathbb{F}_q$.
- Two versions, with complexities $O((rN)^3 q^{(r-1)(k+1)+2})$ and $O((k+r)^3 r^3 q^{(N-r)(r-1)+2})$.

Ourivski-Johannsson algorithm: idea

Problem: given $G \in \mathcal{M}_{k \times n}(\mathbb{F}_{q^N})$ and $c \in \mathbb{F}^n_{q^N}$, find $m \in \mathbb{F}^k_{q^N}$, such that $e = c - mG$ has smallest rank $r = \mathrm{Rk}(e \mid \mathbb{F}_q)$.

Construct the code $\mathcal{C}_e$ with generator matrix

$$\begin{pmatrix} G \\ c \end{pmatrix} = \begin{pmatrix} I_k & 0 \\ m & 1 \end{pmatrix} \begin{pmatrix} G \\ e \end{pmatrix}$$

Provided $r \leq (d-1)/2$, the problem is then "reduced" to finding a codeword of minimum rank r in $\mathcal{C}_e$.
Indeed, all those are of the form ϵe, $\epsilon \in \mathbb{F}^*_{q^N}$.
Having found $e' = \epsilon e$, the value of ϵ is retrieved by computing cH^t and $e'H^t$, H being the parity-check matrix of C.

Modeling the problem as a set of quadratic equations

Any vector $v \in \mathbb{F}_{q^N}^n$ can be expressed in a basis $X = (x_1, \ldots, x_N)$ of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$ as

$$v = (x_1, \ldots, x_N)A,$$

where $A \in \mathcal{M}_{N \times n}(\mathbb{F}_q)$ and $\mathrm{Rk}(A) = \mathrm{Rk}(v \mid \mathbb{F}_q)$. Thus, if $\mathrm{Rk}(v \mid \mathbb{F}_q) = r$, we can write

$$v = (\tilde{x_1}, \ldots, \tilde{x_N}) \begin{pmatrix} \tilde{A} \\ 0 \end{pmatrix} = (\tilde{x_1}, \ldots, \tilde{x_r})\tilde{A}$$

with $\tilde{A} \in \mathcal{M}_{r \times n}(\mathbb{F}_q)$ of full rank r.

Let $\mathcal{C}_e =< G_{syst} >$, $G_{syst} = (I_{k+1}\, R)$, $R \in \mathcal{M}_{(k+1)\times(n-k-1)}(\mathbb{F}_{q^N})$. Then, there exists $u \in (\mathbb{F}_{q^N})^{k+1}$, such that

$$uG_{syst} = (u, uR) = e$$

Modeling the problem as a set of quadratic equations

Any vector $v \in \mathbb{F}_{q^N}^n$ can be expressed in a basis $X = (x_1, \ldots, x_N)$ of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$ as

$$v = (x_1, \ldots, x_N)A,$$

where $A \in \mathcal{M}_{N \times n}(\mathbb{F}_q)$ and $\mathrm{Rk}(A) = \mathrm{Rk}(v \,|\, \mathbb{F}_q)$.
Thus, if $\mathrm{Rk}(v \,|\, \mathbb{F}_q) = r$, we can write

$$v = (\tilde{x_1}, \ldots, \tilde{x_N}) \begin{pmatrix} \tilde{A} \\ 0 \end{pmatrix} = (\tilde{x_1}, \ldots, \tilde{x_r})\tilde{A}$$

with $\tilde{A} \in \mathcal{M}_{r \times n}(\mathbb{F}_q)$ of full rank r.

Let $\mathcal{C}_e =< G_{syst} >$, $G_{syst} = (I_{k+1}\, R)$, $R \in \mathcal{M}_{(k+1)\times(n-k-1)}(\mathbb{F}_{q^N})$.
Then, there exists $u \in (\mathbb{F}_{q^N})^{k+1}$, such that

$$uG_{syst} = (u, uR) = e$$

Modeling the problem as a set of quadratic equations

Writing

$$e = (e_1, e_1 R) = XA,$$

$X = (x_0, \ldots, x_{r-1})$ being an incomplete basis of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$ and $A = (\alpha_{i,j}) \in \mathcal{M}_{r\times n}(\mathbb{F}_q)$ being of full rank r, we get

$$e_1 = (x_0, \ldots, x_{r-1})A_1 \text{ and } e_1 R = (x_0, \ldots, x_{r-1})A_2,$$

where $A = (A_1\, A_2)$, $A_1 \in \mathcal{M}_{r\times(k+1)}(\mathbb{F}_q)$, $A_2 \in \mathcal{M}_{r\times(n-k-1)}(\mathbb{F}_q)$.

We thus have to solve

$$(x_0, \ldots, x_{r-1})A_2 = (x_0, \ldots, x_{r-1})A_1 R. \tag{1}$$

As it suffices to retrieve ϵe, for any $\epsilon \in \mathbb{F}_{q^N}^*$, we can set $x_0 = 1$. System (1) is a quadratic system of $n-k-1$ equations and $nr + r - 1$ unknowns $\alpha_{i,j}$, $x_1, \ldots, x_{r-1}$ over $\mathbb{F}_{q^N}$.

Modeling the problem...

Systeme (1) is equivalent to

$$(x_0, \ldots, x_{r-1})(A_2)_j = (x_0, \ldots, x_{r-1})A_1 R_j,\ k+2 \leq j \leq n, \qquad (2)$$

$(A_2)_j$ (resp. R_j) being the j-th column of A_2 (resp. R).
Let $\Omega = (\omega_0, \ldots, \omega_{N-1})$ be a basis of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$. Over Ω,

$$x_i = \sum_{j=0}^{N-1} x_{ij}\, \omega^j,\ x_{ij} \in \mathbb{F}_q,\ 0 \leq i \leq r-1.$$

Expressing this way X and each R_j w.r.t. Ω, we can rewrite (2) as a system of $N(n-k-1)$ equations in $nr + N(r-1)$ unknowns over $\mathbb{F}_q$.

Solving the system: Ourivski-Johannsson strategy

Choose $\mathcal{J} \subseteq [k+2,\ldots,n]$, $|\mathcal{J}| = m$, yielding mN equations in $N(r-1) + r(m+k+1)$ unknowns.

Strategy 1: $O(((r-1)N + m + k + 1)^3 q^{(r-1)(m+k+1-r)+2})$

- Guess values of $\alpha_{i,j}$ contributing to quadratic terms.
- Solve the resulting linear system of Nm equations in $N(r-1) + m + k + 1$ unknowns ($m \geq r - 1 + \lceil \frac{k+1}{N-1} \rceil$).

Strategy 2: $O((m+k+1)^3 r^3 q^{(N-r)(r-1)+2})$

- Guess the coordinates of the x_is' in the basis Ω.
- Solve the resulting linear system of Nm equations in $r(m+k+1)$ unknowns ($m \geq \lceil \frac{(k+1)r}{N-r} \rceil$).
- Similar to [ChSt 96], but there the system solved is in $rn + N$ unknowns.

Solving the system: Ourivski-Johannsson strategy

Choose $\mathcal{J} \subseteq [k+2, \ldots, n]$, $|\mathcal{J}| = m$, yielding mN equations in $N(r-1) + r(m+k+1)$ unknowns.

Strategy 1: $O(((r-1)N + m + k + 1)^3 q^{(r-1)(m+k+1-r)+2})$

- Guess values of $\alpha_{i,j}$ contributing to quadratic terms.
- Solve the resulting linear system of Nm equations in $N(r-1) + m + k + 1$ unknowns ($m \geq r - 1 + \lceil \frac{k+1}{N-1} \rceil$).

Strategy 2: $O((m+k+1)^3 r^3 q^{(N-r)(r-1)+2})$

- Guess the coordinates of the x_is' in the basis Ω.
- Solve the resulting linear system of Nm equations in $r(m+k+1)$ unknowns ($m \geq \lceil \frac{(k+1)r}{N-r} \rceil$).
- Similar to [ChSt 96], but there the system solved is in $rn + N$ unknowns.

Solving the system: our approach

Add to system (2) the $n-k$ syndrome equations:

$$\begin{cases} (x_0,\ldots,x_{r-1})(A_2)_j = (x_0,\ldots,x_{r-1})A_1R_j, \; k+2 \le j \le n \\ (x_0,\ldots,x_{r-1})AH^t = cH^t. \end{cases} \tag{3}$$

Take a basis Ω of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$, and express X w.r.t. Ω. Rewrite (3) as a system of $N(2(n-k)-1)$ equations in $nr + N(r-1)$ unknowns over $\mathbb{F}_q$.

- ◇ Run a Gröbner basis algorithm (F_4) on this system, to obtain the associated variety $\mathcal{V}$ over $\mathbb{F}_q$.
- ◇ Express each element of $\mathcal{V}$ as $(\tilde{X},\tilde{A}) \in \mathbb{F}_{q^N}^r \times \mathcal{M}_{r\times n}(\mathbb{F}_q)$ (going from $\mathbb{F}_q^{rN}$ back to $\mathbb{F}_{q^N}^r$).
- ◇ Set $\tilde{e} = \tilde{X}\tilde{A}$. Compute the rank of $\tilde{e}$ and keep the one satisfying $\mathrm{Rk}(\tilde{e} \mid \mathbb{F}_q) = r$ and $c - \tilde{e} \in \mathcal{C} =< G >$.

Results

N	n	k	r	OuJo−1	OuJo−2	ChSt	LePe
25	30	15	2	2^{32}	2^{39}	2^{42}	31s.
30	30	16	2	2^{37}	2^{46}	2^{47}	28s.
30	50	20	2	2^{41}	2^{45}	2^{49}	83s.(5min. 30s.*)
50	50	26	2	2^{49}	2^{67}	2^{70}	1h. 5min.
15	15	7	3	2^{35}	2^{37}	2^{38}	30min. 20s.
15	15	8	3	2^{36}	2^{40}	2^{38}	13h. 30min.
20	20	10	3	2^{42}	2^{52}	2^{52}	8h.

* Running time of the algorithm on the system over $\mathbb{F}_{q^N}$.

Conclusion

Our contribution

- Consider a slightly modified system.
- Use a different solving approach.
- For $r = 2$, our algorithm performs very well even for N, n large.
- Good results for $r = 3$ when $k \leq n/2$.

Further research...

- Exploit information obtained for $r = 2, 3$ to attack $r = 4$.
- Include all the constraints in system (specially, $c - e \in \mathcal{C}$).
- Construct a system directly from RD, and compare the results.