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
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 \( \text{Rk}(e | \mathbb{F}_q) \)?

Here, \( \text{Rk}(e | \mathbb{F}_q) \) 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 \( \mathbb{F}_q^k \).

F. Levy-dit-Vehel  Algebraic Decoding of Rank Metric Codes
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 \( \text{Rk}(e|\mathbb{F}_q) \)?

Here, \( \text{Rk}(e|\mathbb{F}_q) \) 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:** \( N, n, k \in \mathbb{N}^* \), \( G \in \mathcal{M}_{k \times n}(\mathbb{F}_{q^N}) \), \( c \in \mathbb{F}_{qN}^n \).

**Question:** find \( m \in \mathbb{F}_{qN}^k \), such that \( e = c - mG \) has smallest rank \( Rk(e|\mathbb{F}_q) \)?

Here, \( Rk(e|\mathbb{F}_q) \) 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
\[
E = M_0 - \sum_{i=1}^k \lambda_i M_i \text{ has smallest rank}?
\]

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?
Algorithms for particular codes

**Gabidulin codes**: the generator matrix is of the form

$$G = \begin{pmatrix}
g_1 & \cdots & g_n \\
g_1^q & \cdots & g_n^q \\
\vdots & \ddots & \vdots \\
g_1^{q^{k-1}} & \cdots & g_n^{q^{k-1}}
ge_1 & \cdots & g_n
\end{pmatrix}, \ (g_1, \ldots, g_n) \in \mathbb{F}_{q^N}^n.$$

♦ 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.

♦ 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: $O((nr + N)^3 q^{(N-r)(r-1)})$.

**Ouivski-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 \( G \in \mathbb{M}_{k \times n}(\mathbb{F}_{q^N}) \) and \( c \in \mathbb{F}_{q^N}^n \), find \( m \in \mathbb{F}_{q^N}^k \), such that \( e = c - mG \) has smallest rank \( r = \text{Rk}(e \mid \mathbb{F}_q) \).

Construct the code \( C_e \) with generator matrix

\[
\begin{pmatrix}
G \\

c
\end{pmatrix} = \begin{pmatrix}
I_k & 0 \\
\epsilon 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 \( C_e \).

Indeed, all those are of the form \( \epsilon e \), \( \epsilon \in \mathbb{F}_{q^N}^* \).

Having found \( e' = \epsilon e \), the value of \( \epsilon \) 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 \( v \in \mathbb{F}^n_{q^N} \) 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 \( \text{Rk}(A) = \text{Rk}(v | \mathbb{F}_q) \). Thus, if \( \text{Rk}(v | \mathbb{F}_q) = r \), 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 \( C_e = \langle G_{\text{syst}} \rangle \), \( G_{\text{syst}} = (I_{k+1} R) \), \( R \in \mathcal{M}_{(k+1) \times (n-k-1)}(\mathbb{F}_q^N) \). Then, there exists \( u \in (\mathbb{F}_q^N)^{k+1} \), such that

\[
uG_{\text{syst}} = (u, uR) = e
\]
Modeling the problem as a set of quadratic equations

Any vector $v \in \mathbb{F}_q^n$ 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 $\text{Rk}(A) = \text{Rk}(v \mid \mathbb{F}_q)$. Thus, if $\text{Rk}(v \mid \mathbb{F}_q) = r$, 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 $C_e = \langle G_{\text{syst}} \rangle$, $G_{\text{syst}} = (I_{k+1} \ R)$, $R \in \mathcal{M}_{(k+1) \times (n-k-1)}(\mathbb{F}_q^n)$. Then, there exists $u \in (\mathbb{F}_q^n)^{k+1}$, such that

$$uG_{\text{syst}} = (u, uR) = e$$
Modeling the problem as a set of quadratic equations

Writing
\[ e = (e_1, e_1R) = XA, \]

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

\[ e_1 = (x_0, \ldots, x_{r-1})A_1 \text{ and } e_1R = (x_0, \ldots, x_{r-1})A_2, \]

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

We thus have to solve

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

As it suffices to retrieve \( \epsilon e \), 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 \( \mathbb{F}_{q^N} \).
Systeme (1) is equivalent to

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

\((A_2)_j\) (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 \(\Omega\),

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

Expressing this way \(X\) and each \(R_j\) w.r.t. \(\Omega\), 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 $x_i$s’ in the basis $\Omega$.
- 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.

<table>
<thead>
<tr>
<th>Strategy 1: $O(((r - 1)N + m + k + 1)^3 q^{(r-1)(m+k+1-r)+2})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Guess values of $\alpha_{i,j}$ contributing to quadratic terms.</td>
</tr>
<tr>
<td>♦ Solve the resulting <strong>linear</strong> system of $Nm$ equations in $N(r - 1) + m + k + 1$ unknowns ($m \geq r - 1 + \lceil \frac{k+1}{N-1} \rceil$).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strategy 2: $O((m + k + 1)^3 r^3 q^{(N-r)(r-1)+2})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Guess the coordinates of the $x_i$s’ in the basis $\Omega$.</td>
</tr>
<tr>
<td>♦ Solve the resulting <strong>linear</strong> system of $Nm$ equations in $r(m + k + 1)$ unknowns ($m \geq \lceil \frac{(k+1)r}{N-r} \rceil$).</td>
</tr>
<tr>
<td>♦ Similar to [ChSt 96], but there the system solved is in $rn + N$ unknowns.</td>
</tr>
</tbody>
</table>
Solving the system: our approach

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

\[
\begin{align*}
(x_0, \ldots, x_{r-1})(A_2)_{j} &= (x_0, \ldots, x_{r-1})A_1 R_j, \quad k + 2 \leq j \leq n \\
(x_0, \ldots, x_{r-1})A H^t &= cH^t. 
\end{align*}
\]  

Take a basis \( \Omega \) of \( \mathbb{F}_q^N \) over \( \mathbb{F}_q \), and express \( X \) w.r.t. \( \Omega \). 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 \((\tilde{X}, \tilde{A}) \in \mathbb{F}_q^r \times \mathcal{M}_{r \times n}(\mathbb{F}_q) \) (going from \( \mathbb{F}_q^r \) back to \( \mathbb{F}_q^N \)).
- Set \( \tilde{e} = \tilde{X}\tilde{A} \). Compute the rank of \( \tilde{e} \) and keep the one satisfying \( \text{Rk}(\tilde{e} \mid \mathbb{F}_q) = r \) and \( c - \tilde{e} \in \mathcal{C} = \langle G \rangle \).
### Results

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

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

---

F. Levy-dit-Vehel  
Algebraic Decoding of Rank Metric Codes
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, $c - e \in C$).
- Construct a system directly from RD, and compare the results.