# List Decoding of Lifted Gabidulin Codes via the Plücker Embedding

Anna-Lena Trautmann

Institute of Mathematics
University of Zurich

WCC in Bergen, Norway
April 19th, 2013

joint work with Natalia Silberstein and Joachim Rosenthal

# Outline

## Definition

- The *Grassmannian* $\mathcal{G}_q(k,n)$ is the set of all $k$-dimensional subspaces of $\mathbb{F}_q^n$.
- A *constant dimension code (CDC)* is a subset of $\mathcal{G}_q(k,n)$.

## Definition

- The *Grassmannian* $\mathcal{G}_q(k,n)$ is the set of all $k$-dimensional subspaces of $\mathbb{F}_q^n$.
- A *constant dimension code (CDC)* is a subset of $\mathcal{G}_q(k,n)$.

## Definition

- The *subspace distance* $d_S$ is a metric on $\mathcal{G}_q(k,n)$:

$$d_S(\mathcal{U},\mathcal{V}) := 2k - 2\dim(\mathcal{U}\cap\mathcal{V})$$

- The minimum distance of a CDC $\mathcal{C}\subseteq\mathcal{G}_q(k,n)$ is

$$d_S(\mathcal{C}) := \min\{d_S(\mathcal{U},\mathcal{V}) \mid \mathcal{U},\mathcal{V}\in\mathcal{C}, \mathcal{U}\neq\mathcal{V}\}.$$

## Definition

- The *Grassmannian* $\mathcal{G}_q(k,n)$ is the set of all $k$-dimensional subspaces of $\mathbb{F}_q^n$.
- A *constant dimension code (CDC)* is a subset of $\mathcal{G}_q(k,n)$.

## Definition

- The *subspace distance* $d_S$ is a metric on $\mathcal{G}_q(k,n)$:

$$d_S(\mathcal{U},\mathcal{V}) := 2k - 2\dim(\mathcal{U}\cap\mathcal{V})$$

- The minimum distance of a CDC $\mathcal{C}\subseteq\mathcal{G}_q(k,n)$ is

$$d_S(\mathcal{C}) := \min\{d_S(\mathcal{U},\mathcal{V}) \mid \mathcal{U},\mathcal{V}\in\mathcal{C}, \mathcal{U}\neq\mathcal{V}\}.$$

Constant dimension codes (or subspace codes in general) can be used in random network coding, distributed storage, storage of biometric data etc.

Let $\mathcal{U} \in \mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be a sent word and $\mathcal{R} = \bar{\mathcal{U}} \oplus \mathcal{E}$ be the received vector space.

## Definition

- A *minimum distance decoder* outputs the unique word of $\mathcal{C}$ that is closest to $\mathcal{R}$, if it exists:

$$MDD_{\mathcal{C}}(\mathcal{R}) := \operatorname{argmin}\{d_S(\mathcal{V},\mathcal{R}) \mid \mathcal{V} \in \mathcal{C}\}$$

Let $\mathcal{U} \in \mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be a sent word and $\mathcal{R} = \bar{\mathcal{U}} \oplus \mathcal{E}$ be the received vector space.

## Definition

- A *minimum distance decoder* outputs the unique word of $\mathcal{C}$ that is closest to $\mathcal{R}$, if it exists:

$$MDD_{\mathcal{C}}(\mathcal{R}) := \operatorname{argmin}\{d_S(\mathcal{V},\mathcal{R}) \mid \mathcal{V} \in \mathcal{C}\}$$

- A *(complete) list decoder* outputs the complete list of words of $\mathcal{C}$ that are within a given radius $t$ to $\mathcal{R}$:

$$LD_{\mathcal{C}}(\mathcal{R},t) := \{\mathcal{V} \in \mathcal{C} \mid d_S(\mathcal{V},\mathcal{R}) \leq t\}$$

Let $\mathcal{U} \in \mathcal{C} \subseteq \mathcal{G}_q(k,n)$ be a sent word and $\mathcal{R} = \bar{\mathcal{U}} \oplus \mathcal{E}$ be the received vector space.

**Definition**

- A *minimum distance decoder* outputs the unique word of $\mathcal{C}$ that is closest to $\mathcal{R}$, if it exists:

$$MDD_{\mathcal{C}}(\mathcal{R}) := \operatorname{argmin}\{d_S(\mathcal{V},\mathcal{R}) \mid \mathcal{V} \in \mathcal{C}\}$$

- A *(complete) list decoder* outputs the complete list of words of $\mathcal{C}$ that are within a given radius $t$ to $\mathcal{R}$:

$$LD_{\mathcal{C}}(\mathcal{R},t) := \{\mathcal{V} \in \mathcal{C} \mid d_S(\mathcal{V},\mathcal{R}) \leq t\}$$

- List decoding for classical Reed-Solomon codes: Sudan, Guruswami
- List decoding for subcodes (!) of lifted Gabidulin codes: Mahdavifar and Vardy; Guruswami and Xing; Guruswami, Narayanan and Wang

1 Constant Dimension Codes

2 The Plücker Embedding
- Balls inside $\mathcal{G}_q(k, n)$
- Lifted MRD Codes
- A First List Decoding Algorithm

3 Conclusion

The maximal minors of a matrix representation of a subspace constitute the *Plücker coordinates* of the subspace:

**Theorem**

*The map*

$$\begin{aligned} \varphi : \mathcal{G}_q(k,n) &\longrightarrow \mathbb{P}^{\binom{n}{k}-1} \\ \text{rowspace}(U) &\longmapsto [M_{1,\ldots,k}(U) : \ldots : M_{n-k+1,\ldots,n}(U)]. \end{aligned}$$

*is an embedding of the Grassmannian $\mathcal{G}_q(k,n)$. It is called the* Plücker embedding *of $\mathcal{G}_q(k,n)$.*

The maximal minors of a matrix representation of a subspace constitute the *Plücker coordinates* of the subspace:

**Theorem**

*The map*

$$\begin{aligned} \varphi : \mathcal{G}_q(k,n) &\longrightarrow \mathbb{P}^{\binom{n}{k}-1} \\ \text{rowspace}(U) &\longmapsto [M_{1,\ldots,k}(U) : \ldots : M_{n-k+1,\ldots,n}(U)]. \end{aligned}$$

*is an embedding of the Grassmannian $\mathcal{G}_q(k,n)$. It is called the* Plücker embedding *of $\mathcal{G}_q(k,n)$.*

**Plücker coordinates in $\mathcal{G}_q(2,4)$**

$$U = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{bmatrix}, \quad M_{i,j} := a_i b_j - a_j b_i$$

$$\varphi(\text{rs}(U)) = [M_{1,2} : M_{1,3} : M_{1,4} : M_{2,3} : M_{2,4} : M_{3,4}] \in \mathbb{P}^5$$

**Theorem**

*The Plücker embedded Grassmannian $\mathcal{G}_q(k,n)$ forms a variety in $\mathbb{P}^{\binom{n}{k}-1}$. The* shuffle relations *(or* straightening syzygies*) form a (minimal Gröbner) basis for this variety.*

**Theorem**

*The Plücker embedded Grassmannian $\mathcal{G}_q(k,n)$ forms a variety in $\mathbb{P}^{\binom{n}{k}-1}$. The* shuffle relations *(or* straightening syzygies*) form a (minimal Gröbner) basis for this variety.*

**Basis of $\mathcal{G}_q(2,4)$:**

$$M_{1,2}M_{3,4} - M_{1,3}M_{2,4} + M_{1,4}M_{2,3} = 0$$

$\implies$ $u = [1:0:1:0:1:0]$ fulfills this equation,

*indices* $12:13:14:23:24:34$

$$\varphi^{-1}(u) = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

**Theorem**

*The Plücker embedded Grassmannian $\mathcal{G}_q(k,n)$ forms a variety in $\mathbb{P}^{\binom{n}{k}-1}$. The* shuffle relations *(or* straightening syzygies*) form a (minimal Gröbner) basis for this variety.*

**Basis of $\mathcal{G}_q(2,4)$:**

$$M_{1,2}M_{3,4} - M_{1,3}M_{2,4} + M_{1,4}M_{2,3} = 0$$

$\implies$ $u = [1:0:1:0:1:0]$ fulfills this equation,

*indices* $12:13:14:23:24:34$

$$\varphi^{-1}(u) = \mathrm{rs}\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

$v = [1:1:1:0:1:0]$ does not fulfill this equation,
hence it is not the Plücker coordinates of some subspace.

## Basis of $\mathcal{G}_q(2,5)$:

$$M_{1,2}M_{3,4} - M_{1,3}M_{2,4} + M_{1,4}M_{2,3} = 0$$
$$M_{1,2}M_{3,5} - M_{1,3}M_{2,5} + M_{1,5}M_{2,3} = 0$$
$$M_{1,2}M_{4,5} - M_{1,4}M_{2,5} + M_{1,5}M_{2,4} = 0$$
$$M_{1,3}M_{4,5} - M_{1,4}M_{3,5} + M_{1,5}M_{3,4} = 0$$
$$M_{2,3}M_{4,5} - M_{2,4}M_{3,5} + M_{2,5}M_{3,4} = 0$$

$$\varphi^{-1}([0:0:0:0:1:2:1:-1:-2:-3]) = \mathrm{rs}\begin{bmatrix} 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 1 \end{bmatrix}.$$

*indices* 12 : 13 : 14 : 15 : 23 : 24 : 25 : 34 : 35 : 45

**Theorem**

*The balls $B_{2t}(\mathcal{U})$ of radius $2t$ (w.r.t. the subspace distance) around some $\mathcal{U} \in \mathcal{G}_q(k,n)$ can be described by linear equations in the Plücker embedding.*

**Theorem**

*The balls $B_{2t}(\mathcal{U})$ of radius $2t$ (w.r.t. the subspace distance) around some $\mathcal{U} \in \mathcal{G}_q(k,n)$ can be described by linear equations in the Plücker embedding.*

**Example in $\mathcal{G}_2(2,4)$**

- Let $U_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ and $t = 1$. Then

$$B_2(\mathrm{rs}(U_0)) = \{\mathcal{V} \in \mathcal{G}_2(2,4) | M_{3,4}(V) = 0\}.$$

- Let $U = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. Then $B_2(\mathrm{rs}(U)) =$

$$\{\mathcal{V} \in \mathcal{G}_2(2,4) \mid M_{1,2}(V)+M_{1,4}(V)+M_{2,3}(V)+M_{3,4}(V) = 0\}.$$

We can describe the balls in the Grassmannian as varieties in the Plücker embedding.

Question: Can we describe CDCs as varieties in the Plücker embedding?

We can describe the balls in the Grassmannian as varieties in the Plücker embedding.

Question: Can we describe CDCs as varieties in the Plücker embedding?

Answer: Yes, for lifted MRD codes!

## Definition

An $[m \times n, \delta]_q$- *MRD code* is a subspace of $\mathbb{F}_q^{m \times n}$ such that $\text{rank}(A - B) \geq \delta$ for all $A, B$ in the code, of dimension $\max(m, n)(\min(m, n) - \delta + 1)$.

## Definition

An $[m \times n, \delta]_q$- *MRD code* is a subspace of $\mathbb{F}_q^{m \times n}$ such that $\text{rank}(A - B) \geq \delta$ for all $A, B$ in the code, of dimension $\max(m, n)(\min(m, n) - \delta + 1)$.

## Theorem

*If $C$ is an $[k \times (n-k), \delta]_q$-MRD code (where $k \leq n - k$), then the lifted MRD (LMRD) code*

$$\mathcal{C} = \{\text{rs}[I_k \ A] \mid A \in C\} \in \mathcal{G}_q(k, n)$$

*is a constant dimension code with minimum subspace distance $2\delta$ and cardinality $q^{(n-k)(k-\delta+1)}$.*

Gabidulin's $m \times n$ MRD construction ($n \leq m$):
Take $n$ linearly independent elements of $\mathbb{F}_{q^m} : g_1, \ldots, g_n$.
Construct a block code over $\mathbb{F}_{q^m}$ with generator matrix

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ \vdots & & & \\ g_1^{q^{n-\delta}} & g_2^{q^{n-\delta}} & \cdots & g_n^{q^{n-\delta}} \end{pmatrix}$$

and expand all coordinates as column vectors with $\mathbb{F}_{q^m} \cong \mathbb{F}_q^m$.

Gabidulin's $m \times n$ MRD construction ($n \leq m$):
Take $n$ linearly independent elements of $\mathbb{F}_{q^m}$ : $g_1, \ldots, g_n$.
Construct a block code over $\mathbb{F}_{q^m}$ with generator matrix

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ \vdots & & & \\ g_1^{q^{n-\delta}} & g_2^{q^{n-\delta}} & \cdots & g_n^{q^{n-\delta}} \end{pmatrix}$$

and expand all coordinates as column vectors with $\mathbb{F}_{q^m} \cong \mathbb{F}_q^m$.

## $2 \times 2$ MRD code with $\delta = 2$

Let $\mathbb{F}_{2^2} = \mathbb{F}_2[\alpha]$ (i.e. $\alpha^2 + \alpha + 1 = 0$) and consider the generator matrix $\begin{pmatrix} 1 & \alpha \end{pmatrix}$.
block code: $\{ \quad (0,0), \quad (1,\alpha), \quad (\alpha,\alpha^2), \quad (\alpha^2,\alpha^3)\}$
MRD code: $\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\}$

Plücker coordinates of lifted MRD codes:

**Theorem**

*The restriction of the set of Plücker coordinates of a lifted MRD code $\mathcal{C} \in \mathcal{G}_q(k,n)$ with minimum distance $\delta$ to the set of the second to the $k(n-k)+1$th coordinate forms a linear code $C^p$ over $\mathbb{F}_q$ of length $k(n-k)$, dimension $(n-k)(k-\delta+1)$ and minimum distance $d_{min} \geq \delta$.*

## Example in $\mathcal{G}_2(2,4)$ with $\delta = 2$

| Gabidulin | lifting | Plücker coordinates |
|---|---|---|
| $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ | $[1:0:0:0:0:0]$ |
| $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ | $[1:1:0:0:1:1]$ |
| $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ | $[1:0:1:1:1:1]$ |
| $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ | $[1:1:1:1:0:1]$ |

## Example in $\mathcal{G}_2(2,4)$ with $\delta = 2$

| Gabidulin | lifting | Plücker coordinates |
|---|---|---|
| $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ | $[1:0:0:0:0:0]$ |
| $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ | $[1:1:0:0:1:1]$ |
| $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ | $[1:0:1:1:1:1]$ |
| $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ | $[1:1:1:1:0:1]$ |

parity-check matrix: $H^p = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$

equations that describe the lifted Gabidulin code:
$M_{1,2} = 1$, $M_{1,4} + M_{2,3} = 0$, and $M_{1,3} + M_{2,3} + M_{2,4} = 0$

# The algorithm

Input: $\mathcal{R}$, $t$

1. Find the equations defining $B_{2t}(\mathcal{R})$ in the Plücker coordinates.
2. Solve the system of equations, that arise from $\bar{M}\bar{H}^p = 0$, together with the equations of $B_{2t}(\mathcal{R})$, the shuffle relations and the equation $M_{1,\ldots,k} = 1$.

Output: The solutions $\bar{M} = [M_{1\ldots k} : \ldots : M_{n-k+1\ldots n}]$ of this system of equations.

## Example

Consider the code from the Example before. We would like to decode up to radius 2. Assume we received

$$\mathcal{R}_1 = \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Equations for the ball:

$$B_2(\mathcal{R}_1) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{1,4}(V) + M_{2,3}(V) = 0\}.$$

System of linear equations to solve:

$$\begin{aligned} M_{14} + M_{23} &= 0 \\ M_{13} + M_{14} + M_{24} &= 0 \\ M_{12} + M_{23} &= 0 \\ M_{12} &= 1 \end{aligned}$$

## Example

This system has the two solutions $(1,1,1,0)$ and $(0,1,1,1)$ for $(M_{13}, M_{14}, M_{23}, M_{24})$.

| Gabidulin | lifting | Plücker coordinates |
|---|---|---|
| $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ | $[1:0:0:0:0:0]$ |
| $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ | $[1:1:0:0:1:1]$ |
| $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ | $[1:0:1:1:1:1]$ |
| $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ | $[1:1:1:1:0:1]$ |

## Example

This system has the two solutions $(1,1,1,0)$ and $(0,1,1,1)$ for $(M_{13}, M_{14}, M_{23}, M_{24})$.

| Gabidulin | lifting | Plücker coordinates |
|---|---|---|
| $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ | $[1:0:0:0:0:0]$ |
| $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ | $[1:1:0:0:1:1]$ |
| $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ | $[1:0:1:1:1:1]$ |
| $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ | $[1:1:1:1:0:1]$ |

Verify with $\mathcal{R}_1 = \mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

## Example

Now assume we received

$$\mathcal{R}_2 = \mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

As previously, we compute $B_2(\mathcal{R}_1) = \{\mathcal{V} = \mathrm{rs}(V) \in \mathcal{G}_2(2,4) \mid M_{1,2}(V) + M_{1,3}(V) + M_{2,3}(V) + M_{2,4}(V) + M_{3,4}(V) = 0\}$. Combining with the parity check equations and the shuffle relation we obtain the following system of equations to solve:

$$\begin{aligned} M_{13} + M_{14} + M_{24} &= 0 \\ M_{14} + M_{23} &= 0 \\ M_{12} + M_{13} + M_{23} + M_{24} + M_{34} &= 0 \\ M_{12}M_{34} + M_{13}M_{24} + M_{14}M_{23} &= 0 \\ M_{12} &= 1 \end{aligned}$$

## Example

This system has three solutions $(1,0,0,1), (0,1,1,1)$, and $(1,1,1,0)$ for $(M_{13}, M_{14}, M_{23}, M_{24})$.

| Gabidulin | lifting | Plücker coordinates |
|---|---|---|
| $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ | $[1:0:0:0:0:0]$ |
| $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ | $[1:1:0:0:1:1]$ |
| $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ | $[1:0:1:1:1:1]$ |
| $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ | $[1:1:1:1:0:1]$ |

## Example

This system has three solutions $(1,0,0,1), (0,1,1,1)$, and $(1,1,1,0)$ for $(M_{13}, M_{14}, M_{23}, M_{24})$.

| Gabidulin | lifting | Plücker coordinates |
|---|---|---|
| $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ | $[1:0:0:0:0:0]$ |
| $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ | $[1:1:0:0:1:1]$ |
| $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ | $[1:0:1:1:1:1]$ |
| $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ | $\mathrm{rs}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ | $[1:1:1:1:0:1]$ |

Verify with $\mathcal{R}_2 = \mathrm{rs}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$.

Complexity Estimates:

- Number of variables : $\binom{n}{k}$
- Number of linear equations from the ball : $\sum_{l=0}^{k-t-1} \binom{n-k}{k-l}\binom{k}{l} = \binom{n}{k} - \sum_{l=k-e}^{k} \binom{n-k}{k-l}\binom{k}{l}$
- Number of linear equations from the LMRD code : $(\delta - 1)(n-k)$ (+1 for the identity part)
- Number of bilinear shuffle relations : $\binom{n}{2k}$

Complexity Estimates:

- Number of variables : $\binom{n}{k}$
- Number of linear equations from the ball : $\sum_{l=0}^{k-t-1} \binom{n-k}{k-l}\binom{k}{l} = \binom{n}{k} - \sum_{l=k-e}^{k} \binom{n-k}{k-l}\binom{k}{l}$
- Number of linear equations from the LMRD code : $(\delta - 1)(n-k)$ (+1 for the identity part)
- Number of bilinear shuffle relations : $\binom{n}{2k}$

Using all equations and variables $\rightarrow \mathcal{O}(n^{x \cdot k})$ $(x \geq 3)$

- We showed how to embed $\mathcal{G}_q(k,n)$ into $\mathbb{P}^{\binom{n}{k}-1}$ and that it forms a variety (with bilinear equations) in the embedding.

- We showed how to embed $\mathcal{G}_q(k,n)$ into $\mathbb{P}^{\binom{n}{k}-1}$ and that it forms a variety (with bilinear equations) in the embedding.
- The balls $B_{2t}(\mathcal{U})$ can be described by linear equations in the Plücker embedding.

- We showed how to embed $\mathcal{G}_q(k,n)$ into $\mathbb{P}^{\binom{n}{k}-1}$ and that it forms a variety (with bilinear equations) in the embedding.
- The balls $B_{2t}(\mathcal{U})$ can be described by linear equations in the Plücker embedding.
- Lifted MRD codes can be described by linear equations in the Plücker embedding.

- We showed how to embed $\mathcal{G}_q(k,n)$ into $\mathbb{P}^{\binom{n}{k}-1}$ and that it forms a variety (with bilinear equations) in the embedding.
- The balls $B_{2t}(\mathcal{U})$ can be described by linear equations in the Plücker embedding.
- Lifted MRD codes can be described by linear equations in the Plücker embedding.
- Solving all these equations describes a list decoding algorithm of lifted MRD codes (not only for subcodes of lifted Gabidulin codes).

- We showed how to embed $\mathcal{G}_q(k,n)$ into $\mathbb{P}^{\binom{n}{k}-1}$ and that it forms a variety (with bilinear equations) in the embedding.
- The balls $B_{2t}(\mathcal{U})$ can be described by linear equations in the Plücker embedding.
- Lifted MRD codes can be described by linear equations in the Plücker embedding.
- Solving all these equations describes a list decoding algorithm of lifted MRD codes (not only for subcodes of lifted Gabidulin codes).
- Algorithm can be extended to multi-component lifted MRD codes, and to received spaces of different dimension.

- We showed how to embed $\mathcal{G}_q(k,n)$ into $\mathbb{P}^{\binom{n}{k}-1}$ and that it forms a variety (with bilinear equations) in the embedding.
- The balls $B_{2t}(\mathcal{U})$ can be described by linear equations in the Plücker embedding.
- Lifted MRD codes can be described by linear equations in the Plücker embedding.
- Solving all these equations describes a list decoding algorithm of lifted MRD codes (not only for subcodes of lifted Gabidulin codes).
- Algorithm can be extended to multi-component lifted MRD codes, and to received spaces of different dimension.
- Work in progress:
  - Reduce the number of equations and variables needed for the algorithm.
  - Similar algorithm for other families of codes.

Thank you for your attention!

Takk!