# Interpolation-Based Decoding of Interleaved Gabidulin Codes

Antonia Wachter-Zeh[1,2] and Alexander Zeh[1,3]

[1]Institute of Communications Engineering, Ulm University, Ulm, Germany
[2]Inst. de Recherche Mathématique de Rennes, Université de Rennes 1, France
[3]Research Center INRIA Saclay - Île-de-France, École Polytechnique, France

April 19, 2013

*International Workshop on Coding and Cryptography (WCC 2013)*

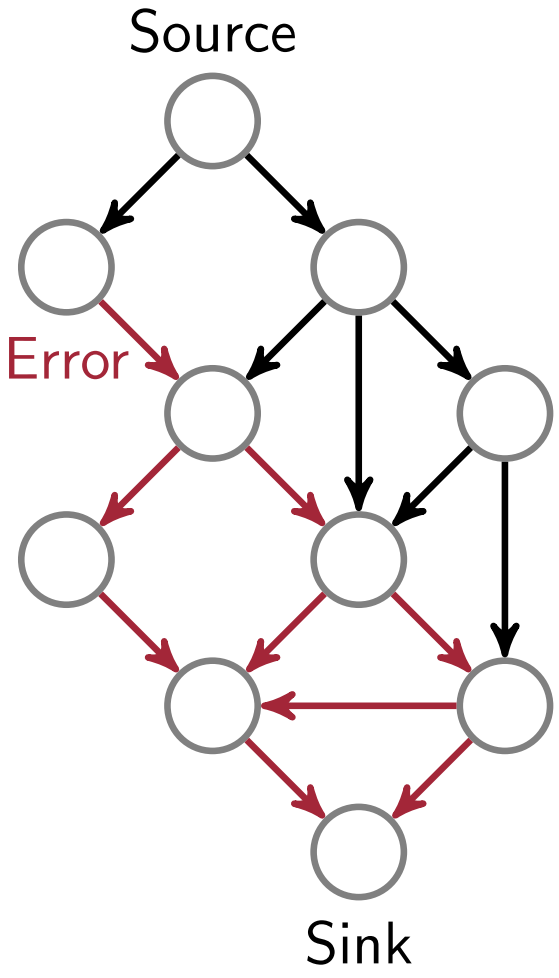
# Outline

# Outline

# Non-Coherent Random Linear Network Coding

- **Non-coherent** network coding: internal structure unknown
- Packets: vectors over finite field
- Nodes build outgoing packets as **random linear combinations** of incoming packets

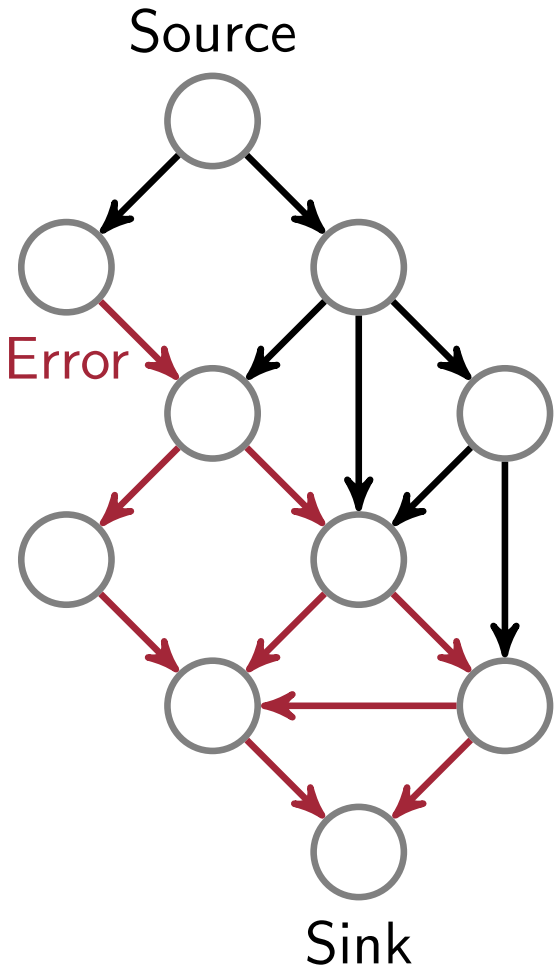
$\Longrightarrow$ Higher throughput than routing!
$\Longrightarrow$ BUT: Mixing of packets results in high error propagation



# Non-Coherent Random Linear Network Coding

- **Non-coherent** network coding: internal structure unknown
- Packets: vectors over finite field
- Nodes build outgoing packets as **random linear combinations** of incoming packets

$\Longrightarrow$ Higher throughput than routing!
$\Longrightarrow$ BUT: Mixing of packets results in high error propagation



# Lifting Construction

*Kötter & Kschischang* (2008); *Silva, Kschischang & Kötter* (2008): Error control in RLNC based on **lifted Gabidulin codes**.

## Lifted Gabidulin Code

- Transmit basis of subspace
- The matrix $\mathbf{C}$ is a codeword of Gab$[n, k]$
- Identity matrix is necessary to "identify" linear combinations of the network

$$\boxed{\mathbf{I}}\boxed{\mathbf{C}^T}$$

BUT: Additional overhead due to identity matrix.

# Lifting Construction with Interleaving

**Interleaved** Gabidulin codes relatively reduce this overhead!

## Lifted Interleaved Gabidulin Code

$$\underbrace{\mathbf{I} \quad \mathbf{C}_1^T \quad \mathbf{C}_2^T \quad \cdots \quad \mathbf{C}_s^T}_{\stackrel{\text{def}}{=} \mathbf{C}^T\text{, where } \mathbf{C} \in \mathrm{IGab}[s; n, k_1, \ldots, k_s]}$$

- Transmit basis of subspace
- $\mathbf{C}_i$ are a codewords of $\mathrm{Gab}[n, k_i]$
- $\mathbf{C}^T \stackrel{\text{def}}{=} \left(\mathbf{C}_1^T \ \mathbf{C}_2^T \ \ldots \ \mathbf{C}_s^T\right)$, where $\mathbf{C} \in \mathrm{IGab}[s; n, k_1, \ldots, k_s]$

(Relatively) less additional overhead due to identity matrix.

# Outline

# Rank Metric

## Rank Metric

- Let $\mathcal{B}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ where $q$ is a power of a prime
- One-to-one mapping between $\mathbf{x} \in \mathbb{F}_{q^m}^n$ and $\mathbf{X} \in \mathbb{F}_q^{m \times n}$
- Rank norm: $\mathrm{rk}(\mathbf{x}) \stackrel{\text{def}}{=}$ rank of $\mathbf{X}$ over $\mathbb{F}_q$

Minimum Rank Distance of a block code C with $\mathbf{c}^{(i)} \in \mathbb{F}_{q^m}^n$:

- $d \stackrel{\text{def}}{=} \min\{\mathrm{rk}(\mathbf{c}^{(1)} - \mathbf{c}^{(2)}) \mid \mathbf{c}^{(1)}, \mathbf{c}^{(2)} \in \mathsf{C}, \mathbf{c}^{(1)} \neq \mathbf{c}^{(2)}\}$
- Codes over $\mathbb{F}_{q^m}$ of cardinality $M = q^{\min\{n(m-d+1), m(n-d+1)\}}$ are called Maximum Rank Distance (MRD) codes.

For linear codes:

- $d \stackrel{\text{def}}{=} \min\{\mathrm{rk}(\mathbf{c}) \mid \mathbf{c} \in \mathsf{C}, \mathbf{c} \neq \mathbf{0}\} \leq n - k + 1$

# Rank Metric

## Rank Metric

- Let $\mathcal{B}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ where $q$ is a power of a prime
- One-to-one mapping between $\mathbf{x} \in \mathbb{F}_{q^m}^n$ and $\mathbf{X} \in \mathbb{F}_q^{m \times n}$
- Rank norm: $\mathrm{rk}(\mathbf{x}) \stackrel{\text{def}}{=}$ rank of $\mathbf{X}$ over $\mathbb{F}_q$

Minimum Rank Distance of a block code C with $\mathbf{c}^{(i)} \in \mathbb{F}_{q^m}^n$:

- $d \stackrel{\text{def}}{=} \min\{\mathrm{rk}(\mathbf{c}^{(1)} - \mathbf{c}^{(2)}) \mid \mathbf{c}^{(1)}, \mathbf{c}^{(2)} \in \mathsf{C}, \mathbf{c}^{(1)} \neq \mathbf{c}^{(2)}\}$
- Codes over $\mathbb{F}_{q^m}$ of cardinality $M = q^{\min\{n(m-d+1), m(n-d+1)\}}$ are called Maximum Rank Distance (MRD) codes.

For linear codes:

- $d \stackrel{\text{def}}{=} \min\{\mathrm{rk}(\mathbf{c}) \mid \mathbf{c} \in \mathsf{C}, \mathbf{c} \neq \mathbf{0}\} \leq n - k + 1$

# Linearized Polynomials

## Linearized Polynomial

- $f(x) \stackrel{\text{def}}{=} \sum_{i=0}^{d_f} f_i x^{[i]} = \sum_{i=0}^{d_f} f_i x^{q^i}$ with $f_i \in \mathbb{F}_{q^m}$
- If $f_{d_f} \neq 0$, define the $q$-degree: $\deg_q f(x) = d_f$

Use usual addition and non-commutative composition $f(g(x))$
$\rightsquigarrow$ Non-commutative ring of linearized polynomials $\mathbb{L}_{q^m}[x]$

## Multi-variate Linearized Polynomials

- $f(x, y_1, \ldots, y_s) \stackrel{\text{def}}{=} f^{(0)}(x) + f^{(1)}(y_1) + \cdots + f^{(s)}(y_s)$, where $f^{(i)}(x) \in \mathbb{L}_{q^m}[x]$ for all $i$
- No "mixed" terms!
- Multi-variate non-commutative ring of linearized polynomials: $\mathbb{L}_{q^m}[x, y_1, \ldots, y_s]$

# Linearized Polynomials

## Linearized Polynomial

- $f(x) \stackrel{\text{def}}{=} \sum_{i=0}^{d_f} f_i x^{[i]} = \sum_{i=0}^{d_f} f_i x^{q^i}$ with $f_i \in \mathbb{F}_{q^m}$
- If $f_{d_f} \neq 0$, define the $q$-degree: $\deg_q f(x) = d_f$

Use usual addition and non-commutative composition $f(g(x))$
$\rightsquigarrow$ Non-commutative ring of linearized polynomials $\mathbb{L}_{q^m}[x]$

## Multi-variate Linearized Polynomials

- $f(x, y_1, \ldots, y_s) \stackrel{\text{def}}{=} f^{(0)}(x) + f^{(1)}(y_1) + \cdots + f^{(s)}(y_s)$, where $f^{(i)}(x) \in \mathbb{L}_{q^m}[x]$ for all $i$
- No "mixed" terms!
- Multi-variate non-commutative ring of linearized polynomials: $\mathbb{L}_{q^m}[x, y_1, \ldots, y_s]$

# Gabidulin Codes

Introduced by *Delsarte* (1978), *Gabidulin* (1985), *Roth* (1991).

**Definition (Gabidulin Code)**

A linear Gabidulin code $\mathsf{Gab}[n,k]$ over $\mathbb{F}_{q^m}$ of length $n \leq m$ and dimension $k \leq n$ is defined by:

$$\mathsf{Gab}[n,k] \stackrel{\text{def}}{=} \big\{ (f(\alpha_0)\ f(\alpha_1)\ \ldots\ f(\alpha_{n-1})) = f(\boldsymbol{\alpha}) \mid \deg_q f(x) < k,\ f(x) \in \mathbb{L}_{q^m}[x] \big\},$$

where the fixed elements $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$.

Minimum rank distance of a Gabidulin code:

$$d = \min\{\mathrm{rank}(\mathbf{c}) \mid \mathbf{c} \in \mathsf{Gab}[n,k], \mathbf{c} \neq \mathbf{0}\} = n - k + 1.$$

$\Longrightarrow$ Gabidulin codes are MRD codes.

# Interleaved Gabidulin Codes

## Definition (Interleaved Gabidulin Code)

A linear (vertically) interleaved Gabidulin code over $\mathbb{F}_{q^m}$ of length $n \leq m$, elementary dimensions $k_1, \ldots, k_s$ and interleaving order $s$ is defined by

$$\mathrm{IGab}[s; n, k_1, \ldots, k_s] \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} \mathbf{c}^{(1)} \\ \mathbf{c}^{(2)} \\ \vdots \\ \mathbf{c}^{(s)} \end{pmatrix} = \begin{pmatrix} f^{(1)}(\boldsymbol{\alpha}) \\ f^{(2)}(\boldsymbol{\alpha}) \\ \vdots \\ f^{(s)}(\boldsymbol{\alpha}) \end{pmatrix} \right\},$$

where

- $\deg_q f^{(i)}(x) < k_i \leq n$,
- $f^{(i)}(x) \in \mathbb{L}_{q^m}[x]$ for $i = 1, \ldots, s$,
- $\mathrm{rk}(\boldsymbol{\alpha} = (\alpha_0 \ \alpha_1 \ \ldots \ \alpha_{n-1})) = n$.

# Interleaved Gabidulin Codes

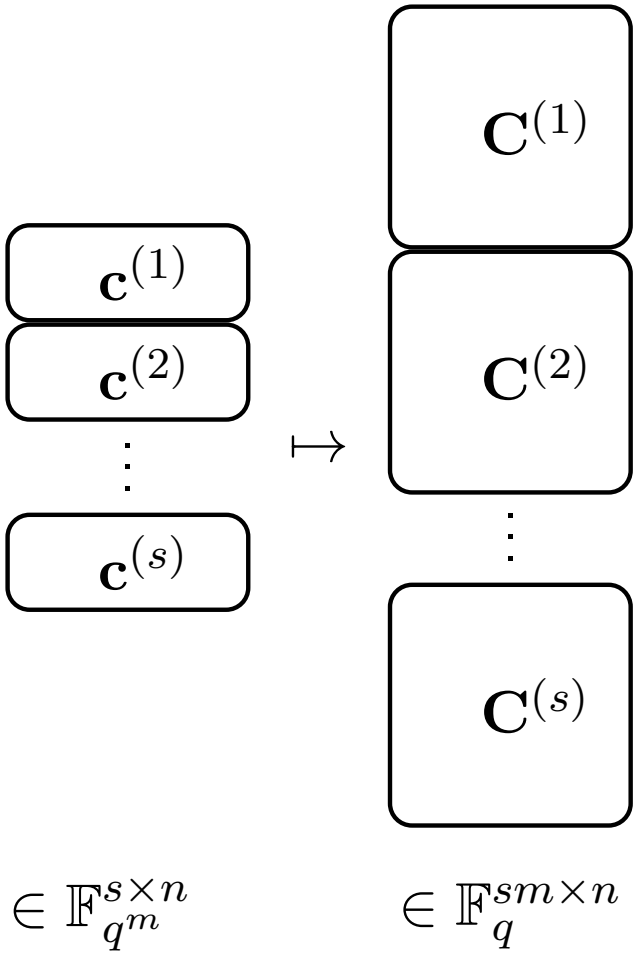
## Definition (Interleaved Gabidulin Code)

A linear (vertically) interleaved Gabidulin code over $\mathbb{F}_{q^m}$ of length $n \leq m$, elementary dimensions $k_1, \ldots, k_s$ and interleaving order $s$ is defined by

$$\mathrm{IGab}[s; n, k_1, \ldots, k_s] \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} \mathbf{c}^{(1)} \\ \mathbf{c}^{(2)} \\ \vdots \\ \mathbf{c}^{(s)} \end{pmatrix} = \begin{pmatrix} f^{(1)}(\boldsymbol{\alpha}) \\ f^{(2)}(\boldsymbol{\alpha}) \\ \vdots \\ f^{(s)}(\boldsymbol{\alpha}) \end{pmatrix} \right\},$$

where

- $\deg_q f^{(i)}(x) < k_i \leq n$,
- $f^{(i)}(x) \in \mathbb{L}_{q^m}[x]$ for $i = 1, \ldots, s$,
- $\mathrm{rk}(\boldsymbol{\alpha} = (\alpha_0 \ \alpha_1 \ \ldots \ \alpha_{n-1})) = n$.



# Error Model

"Number" of errors $t$:

$$t \stackrel{\text{def}}{=} \operatorname{rk} \begin{bmatrix} \mathbf{e}^{(1)} \\ \mathbf{e}^{(2)} \\ \vdots \\ \mathbf{e}^{(s)} \end{bmatrix} \stackrel{\text{def}}{=} \operatorname{rk} \begin{bmatrix} \mathbf{E}^{(1)} \\ \mathbf{E}^{(2)} \\ \vdots \\ \mathbf{E}^{(s)} \end{bmatrix}$$

$\in \mathbb{F}_{q^m}^{s \times n}$ $\qquad$ $\in \mathbb{F}_{q}^{sm \times n}$

- All $\mathbf{e}^{(i)}$ lie in the same rowspace!
- Corresponds to $s$ key equations with the same error span polynomial

$\Longrightarrow$ This can be used in the decoding process!

# Outline

# Previous Work

- *Loidreau & Overbeck* (2006): **Unique decoding** of interleaved Gabidulin codes:
  - by solving a linear system of equations,
  - up to $\tau \leq \left\lfloor \frac{s}{s+1}(d-1) \right\rfloor$ errors w.h.p.,
  - complexity $\mathcal{O}(n^3)$,
  - upper bound on the failure probability: $P_{f,LO} \leq 4/q^m$.
- *Sidorenko & Bossert* (2010): **Unique decoding** of interleaved Gabidulin codes:
  - by linearized shift-register synthesis,
  - up to $\tau \leq \left\lfloor \frac{s}{s+1}(d-1) \right\rfloor$ errors w.h.p.,
  - complexity $\mathcal{O}(n^2)$,
  - improved upper bound on the failure probability.

# Previous Work

- *Loidreau & Overbeck* (2006): **Unique decoding** of interleaved Gabidulin codes:
  - by solving a linear system of equations,
  - up to $\tau \leq \left\lfloor \frac{s}{s+1}(d-1) \right\rfloor$ errors w.h.p.,
  - complexity $\mathcal{O}(n^3)$,
  - upper bound on the failure probability: $P_{f,LO} \leq 4/q^m$.
- *Sidorenko & Bossert* (2010): **Unique decoding** of interleaved Gabidulin codes:
  - by linearized shift-register synthesis,
  - up to $\tau \leq \left\lfloor \frac{s}{s+1}(d-1) \right\rfloor$ errors w.h.p.,
  - complexity $\mathcal{O}(n^2)$,
  - improved upper bound on the failure probability.

# Our Contribution

We use an interpolation-based decoding algorithm...

- ... for **unique decoding** of interleaved Gabidulin codes:
  - up to $\tau \leq \left\lfloor \frac{s}{s+1}(d-1) \right\rfloor$ errors w.h.p,
  - complexity $\mathcal{O}(n^2)$,
  - failure probability: $P_f \leq P_{f,LO} \leq 4/q^m$
- ... for **list decoding** of interleaved Gabidulin codes:
  - finds the list of all codewords within distance $\tau < \frac{s}{s+1} \cdot d$,
  - basis of this list can be found with complexity $\mathcal{O}(n^2)$,
  - list size can be exponential in $n$,
  - average list size: $\overline{\ell} < 1 + 4\left(q^{m\sum_{i=1}^{s} k_i} - 1\right) q^{(sm+n)\tau - \tau^2 - smn}$.

# Our Contribution

We use an interpolation-based decoding algorithm...

- ... for **unique decoding** of interleaved Gabidulin codes:
  - up to $\tau \leq \left\lfloor \frac{s}{s+1}(d-1) \right\rfloor$ errors w.h.p,
  - complexity $\mathcal{O}(n^2)$,
  - failure probability: $P_f \leq P_{f,LO} \leq 4/q^m$
- ... for **list decoding** of interleaved Gabidulin codes:
  - finds the list of all codewords within distance $\tau < \frac{s}{s+1} \cdot d$,
  - basis of this list can be found with complexity $\mathcal{O}(n^2)$,
  - list size can be exponential in $n$,
  - average list size: $\overline{\ell} < 1 + 4\left(q^{m\sum_{i=1}^{s} k_i} - 1\right) q^{(sm+n)\tau - \tau^2 - smn}$.

# Outline

# Overview and Idea of Decoder

Let $\begin{pmatrix} \mathbf{r}^{(1)}=(r_0^{(1)} & r_1^{(1)} & \dots & r_{n-1}^{(1)}) \\ & \vdots & & \\ \mathbf{r}^{(s)}=(r_0^{(s)} & r_1^{(s)} & \dots & r_{n-1}^{(s)}) \end{pmatrix} \in \mathbb{F}_{q^m}^{s\times n}$ be the received word

1. **Interpolation**:
   Find non-zero $(s+1)$-variate linearized polynomial of the form $Q(x, y_1, \dots, y_s) = Q_0(x) + Q_1(y_1) + \dots + Q_s(y_s)$ such that
   - $Q(\alpha_i, r_i^{(1)}, \dots, r_i^{(s)}) = 0$, for $i = 0, \dots, n-1$,
   - $\deg_q Q_0(x) < n - \tau$,
   - $\deg_q Q_i(y_i) < n - \tau - (k_i - 1)$, for $i = 1, \dots, s$.
2. **Root-finding**:
   Find all tuples of polynomials $f^{(1)}(x), \dots, f^{(s)}(x)$ such that $Q\left(x, f^{(1)}(x), \dots, f^{(s)}(x)\right) = 0$.

For simplicity, consider only $k_i = k$, for $i = 1, \dots, s$ in this talk.

# Overview and Idea of Decoder

Let $\begin{pmatrix} \mathbf{r}^{(1)}=(r_0^{(1)} & r_1^{(1)} & \dots & r_{n-1}^{(1)}) \\ & \vdots & & \\ \mathbf{r}^{(s)}=(r_0^{(s)} & r_1^{(s)} & \dots & r_{n-1}^{(s)}) \end{pmatrix} \in \mathbb{F}_{q^m}^{s\times n}$ be the received word

1. **Interpolation**:
   Find non-zero $(s+1)$-variate linearized polynomial of the form $Q(x, y_1, \dots, y_s) = Q_0(x) + Q_1(y_1) + \dots + Q_s(y_s)$ such that
   - $Q(\alpha_i, r_i^{(1)}, \dots, r_i^{(s)}) = 0$, for $i = 0, \dots, n-1$,
   - $\deg_q Q_0(x) < n - \tau$,
   - $\deg_q Q_i(y_i) < n - \tau - (k_i - 1)$, for $i = 1, \dots, s$.
2. **Root-finding**:
   Find all tuples of polynomials $f^{(1)}(x), \dots, f^{(s)}(x)$ such that $Q\left(x, f^{(1)}(x), \dots, f^{(s)}(x)\right) = 0$.

For simplicity, consider only $k_i = k$, for $i = 1, \dots, s$ in this talk.

# Overview and Idea of Decoder

Let $\begin{pmatrix} \mathbf{r}^{(1)}=(r_0^{(1)} & r_1^{(1)} & \dots & r_{n-1}^{(1)}) \\ & \vdots & & \\ \mathbf{r}^{(s)}=(r_0^{(s)} & r_1^{(s)} & \dots & r_{n-1}^{(s)}) \end{pmatrix} \in \mathbb{F}_{q^m}^{s\times n}$ be the received word

1. **Interpolation**:
   Find non-zero $(s+1)$-variate linearized polynomial of the form $Q(x, y_1, \dots, y_s) = Q_0(x) + Q_1(y_1) + \cdots + Q_s(y_s)$ such that
   - $Q(\alpha_i, r_i^{(1)}, \dots, r_i^{(s)}) = 0$, for $i = 0, \dots, n-1$,
   - $\deg_q Q_0(x) < n - \tau$,
   - $\deg_q Q_i(y_i) < n - \tau - (k_i - 1)$, for $i = 1, \dots, s$.
2. **Root-finding**:
   Find all tuples of polynomials $f^{(1)}(x), \dots, f^{(s)}(x)$ such that $Q\left(x, f^{(1)}(x), \dots, f^{(s)}(x)\right) = 0$.

For simplicity, consider only $k_i = k$, for $i = 1, \dots, s$ in this talk.

# Interpolation-Step

**Lemma (Interpolation)**

*There exists a non-zero $Q(x, y_1, \ldots, y_s)$, fulfilling the interpolation conditions if*

$$\tau < \frac{s}{s+1} \cdot (n - k + 1) = \frac{s}{s+1} \cdot d$$

- Calculating $Q(x, y_1, \ldots, y_s)$ is a linear system of equations
- Complexity:
  - with Gaussian elimination: $\mathcal{O}(sn^3)$
  - with the approach by *Xie, Yan & Suter* (2011): $\mathcal{O}(s^2 n(n - \tau))$
- We use a basis of the solution space for the root-finding step

# Interpolation-Step

**Lemma (Interpolation)**

*There exists a non-zero $Q(x, y_1, \ldots, y_s)$, fulfilling the interpolation conditions if*

$$\tau < \frac{s}{s+1} \cdot (n - k + 1) = \frac{s}{s+1} \cdot d$$

- Calculating $Q(x, y_1, \ldots, y_s)$ is a linear system of equations
- Complexity:
  - with Gaussian elimination: $\mathcal{O}(sn^3)$
  - with the approach by *Xie, Yan & Suter* (2011): $\mathcal{O}(s^2 n(n - \tau))$
- We use a basis of the solution space for the root-finding step

# Root-Finding Step

**Theorem (Root-Finding)**

*Let* $\mathrm{rk}(\mathbf{E}_q) \leq \tau$*, where* $\tau < \frac{s}{s+1} \cdot d$ *and let* $Q(x, y_1, \ldots, y_s)$ *fulfill the interpolation constraints. Then,*

$$Q\left(x, f^{(1)}(x), \ldots, f^{(s)}(x)\right) = 0.$$

- This is a **linear** system of equations over $\mathbb{F}_{q^m}$ in the coefficients of $f^{(1)}(x), \ldots, f^{(s)}(x)$
- Similar to
  - *Guruswami & Wang* (2012) for folded/derivative RS codes
  - *Mahdavifar & Vardy* (2012) for folded Gabidulin codes
- Use basis for all $Q(x, y_1, \ldots, y_s)$ for the root-finding step
- Complexity (recursive calculation): $\mathcal{O}(s^3 k^2)$

# Root-Finding Step

**Theorem (Root-Finding)**

*Let* $\mathrm{rk}(\mathbf{E}_q) \leq \tau$*, where* $\tau < \frac{s}{s+1} \cdot d$ *and let* $Q(x, y_1, \ldots, y_s)$ *fulfill the interpolation constraints. Then,*

$$Q\left(x, f^{(1)}(x), \ldots, f^{(s)}(x)\right) = 0.$$

- This is a **linear** system of equations over $\mathbb{F}_{q^m}$ in the coefficients of $f^{(1)}(x), \ldots, f^{(s)}(x)$
- Similar to
  - *Guruswami & Wang* (2012) for folded/derivative RS codes
  - *Mahdavifar & Vardy* (2012) for folded Gabidulin codes
- Use basis for all $Q(x, y_1, \ldots, y_s)$ for the root-finding step
- Complexity (recursive calculation): $\mathcal{O}(s^3 k^2)$

# Interpretation as List Decoder

**Theorem (List Decoding of Interleaved Gabidulin Codes)**

- *Let* $\mathbf{c}^{(i)} = f^{(i)}(\boldsymbol{\alpha})$ *define* $\mathrm{IGab}[s; n, k_1, \ldots, k_s]$,
- $\mathbf{r}^{(i)} = \mathbf{c}^{(i)} + \mathbf{e}^{(i)}$ *for* $i = 1, \ldots, s$.

*Then, we can find a basis of the subspace containing all* $f^{(1)}(x), \ldots, f^{(s)}(x)$ *such that their evaluation is in rank distance*

$$\tau < \frac{s}{s+1} \cdot (n - k + 1) = \frac{s}{s+1} \cdot d$$

*to the received word with overall complexity at most* $\mathcal{O}(s^3 n^2)$.

- Maximum list size can be exponential: $\ell \leq q^{m(s-1)k}$
- Average list size (without transmitted codeword): $\overline{\ell} < 4\left(q^{msk} - 1\right) q^{(sm+n)\tau - \tau^2 - smn}$

# Interpretation as Unique Decoder

- Decoding failure if rank of root-finding matrix is not full.
- In the other cases there is a unique solution!

**Theorem (Unique Decoding of Interleaved Gabidulin Codes)**

- *Let* $\mathbf{c}^{(i)} = f^{(i)}(\boldsymbol{\alpha})$ *define* $\mathrm{IGab}[s; n, k_1, \ldots, k_s]$,
- $\mathbf{r}^{(i)} = \mathbf{c}^{(i)} + \mathbf{e}^{(i)}$ *for* $i = 1, \ldots, s$.

*Then, with probability at least*

$$1 - 4q^{-m(s(n-k-\tau)-t+1)} \geq 1 - P_{f,LO},$$

*we find a unique solution* $f^{(1)}(x), \ldots, f^{(s)}(x)$ *such that its evaluation is in rank distance*

$$t \leq \tau = \left\lfloor \frac{s}{s+1}(d-1) \right\rfloor$$

*to the received word with overall complexity at most* $\mathcal{O}(s^3 n^2)$.

# Example — Failure Probability and List Size

- Consider $\mathrm{IGab}[s=2; n=7, k_1=2, k_2=2]$ code over $\mathbb{F}_{2^7}$.
  $\Longrightarrow$ BMD decoding: $\tau = \left\lfloor \frac{d-1}{2} \right\rfloor = 2$
  $\Longrightarrow$ Interleaved decoding (for unique & list decoding): $\tau = 3$

- Simulated failure probability for $10^7$ transmissions (any error matrix $\mathbf{E}_q \in \mathbb{F}_q^{sm \times n}$ of rank $\tau = 3$ is equal probable):

$$P\big(\mathrm{rk}(\mathbf{Q}) < sk\big) = P_f = P_{f,LO} = P_{f,SB} = 6.12 \cdot 10^{-5}.$$

- Upper bound on average list size:

$$\bar{\ell} < 1 + 6.104 \cdot 10^{-5}$$

- Upper bound on failure probability:

$$P_f \leq 4q^{-m(s(n-k-\tau)-\tau+1)} = 2.44 \cdot 10^{-4}$$

# Example — Failure Probability and List Size

- Consider $\mathrm{IGab}[s=2; n=7, k_1=2, k_2=2]$ code over $\mathbb{F}_{2^7}$.
  $\Longrightarrow$ BMD decoding: $\tau = \left\lfloor \frac{d-1}{2} \right\rfloor = 2$
  $\Longrightarrow$ Interleaved decoding (for unique & list decoding): $\tau = 3$

- Simulated failure probability for $10^7$ transmissions (any error matrix $\mathbf{E}_q \in \mathbb{F}_q^{sm \times n}$ of rank $\tau = 3$ is equal probable):

$$P\big(\mathrm{rk}(\mathbf{Q}) < sk\big) = P_f = P_{f,LO} = P_{f,SB} = 6.12 \cdot 10^{-5}.$$

- Upper bound on average list size:

$$\bar{\ell} < 1 + 6.104 \cdot 10^{-5}$$

- Upper bound on failure probability:

$$P_f \leq 4q^{-m(s(n-k-\tau)-\tau+1)} = 2.44 \cdot 10^{-4}$$

# Outline

# Conclusion and Outlook

## Conclusion

Interpolation based decoding of interleaved Gabidulin codes:

- ... can be used as unique decoder
  - correcting up to $\left\lfloor \frac{s}{s+1}(d-1) \right\rfloor$ errors,
  - with probability at least $1 - P_{f,LO} \geq 1 - {}^{4}/_{q^m}$,
  - with complexity $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^m}$.
- ... or as a list decoder
  - finding all words within distance $\tau < \frac{s}{s+1} \cdot d$,
  - with worst-case exponential complexity, but complexity $\mathcal{O}(n^2)$ for finding the basis for all solutions.

## Outlook

- Use re-encoding to decrease complexity.
- Decoding usual Gabidulin code beyond half the minimum distance by virtual extension to an interleaved Gabidulin code.

# Conclusion and Outlook

## Conclusion

Interpolation based decoding of interleaved Gabidulin codes:

- ... can be used as unique decoder
  - correcting up to $\left\lfloor \frac{s}{s+1}(d-1) \right\rfloor$ errors,
  - with probability at least $1 - P_{f,LO} \geq 1 - {}^{4}/_{q^m}$,
  - with complexity $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^m}$.
- ... or as a list decoder
  - finding all words within distance $\tau < \frac{s}{s+1} \cdot d$,
  - with worst-case exponential complexity, but complexity $\mathcal{O}(n^2)$ for finding the basis for all solutions.

## Outlook

- Use re-encoding to decrease complexity.
- Decoding usual Gabidulin code beyond half the minimum distance by virtual extension to an interleaved Gabidulin code.

# Conclusion and Outlook

## Conclusion

Interpolation based decoding of interleaved Gabidulin codes:

- ... can be used as unique decoder
  - correcting up to $\left\lfloor \frac{s}{s+1}(d-1) \right\rfloor$ errors,
  - with probability at least $1 - P_{f,LO} \geq 1 - {}^{4}/_{q^m}$,
  - with complexity $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^m}$.
- ... or as a list decoder
  - finding all words within distance $\tau < \frac{s}{s+1} \cdot d$,
  - with worst-case exponential complexity, but complexity $\mathcal{O}(n^2)$ for finding the basis for all solutions.

## Outlook

- Use re-encoding to decrease complexity.
- Decoding usual Gabidulin code beyond half the minimum distance by virtual extension to an interleaved Gabidulin code.

# Thank you...

...for your attention!