On Decoding of Maximum Rank Distance Codes

Chunlei Li, Wrya Kadir

University of Bergen, Norway

Boolean Functions and their Applications (BFA)

June 16-21, 2019

Overview

Representations of vectors in $\mathbb{F}_{q^m}^n$

- $\mathbb{F}_{q^m}$: the finite field of q^m elements
- $\mathcal{B} = \{\beta_1, \cdots, \beta_m\}$: a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$
- 1-to-1 correspondence (vector-matrix):

$$\begin{array}{ccc} \mathbb{F}_{q^m}^n & \rightarrow & \mathbb{F}_q^{m\times n} \\ (a_1, \cdots, a_n) & \mapsto & (\beta_1, \cdots, \beta_m) \begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & \ddots & \vdots \\ a_{1m} & \cdots & a_{nm} \end{pmatrix} \end{array}$$

- Another interesting 1-to-1 correspondence (vector-linearized poly.):

$$(a_1, \cdots, a_n) \leftrightarrow L(x) = l_0 x + l_1 x^q + \cdots + l_{n-1} x^{q^{n-1}}$$

with $l_i \in \mathbb{F}_{q^m}$ and

$$L(\beta_j) = a_j, \text{ for } j = 1, 2, \cdots, n$$

The Rank Metric

- The **rank** of a vector $a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ is defined as

$$\mathrm{Rank}(a) := \dim_{\mathbb{F}_q}(\langle a_1, \cdots, a_n \rangle)$$

- Alternatively,

$$\begin{aligned} \mathrm{Rank}(a) &= \mathrm{Rank}(\mathrm{Mat}_{\mathcal{B}}(a_1, a_2, \ldots, a_n)) \\ &= \dim_{\mathbb{F}_q}(\{L(x) \,|\, x \in \mathbb{F}_{q^m}\}) \end{aligned}$$

Given a vector $a \in \mathbb{F}_{q^m}^n$, the Hamming weight $\mathrm{WT_H}(a) \geq \mathrm{Rank}(a)$

The Rank Metric

- The **rank** of a vector $a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ is defined as

$$\mathrm{Rank}(a) := \dim_{\mathbb{F}_q}(\langle a_1, \cdots, a_n \rangle)$$

- Alternatively,

$$\begin{aligned} \mathrm{Rank}(a) &= \mathrm{Rank}(\mathrm{Mat}_{\mathcal{B}}(a_1, a_2, \ldots, a_n)) \\ &= \dim_{\mathbb{F}_q}(\{L(x) \,|\, x \in \mathbb{F}_{q^m}\}) \end{aligned}$$

Given a vector $a \in \mathbb{F}_{q^m}^n$, the Hamming weight $\mathrm{WT}_{\mathrm{H}}(a) \geq \mathrm{Rank}(a)$

The Rank Metric

- The **rank** of a vector $a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ is defined as

$$\mathrm{Rank}(a) := \dim_{\mathbb{F}_q}(\langle a_1, \cdots, a_n \rangle)$$

- Alternatively,

$$\begin{aligned} \mathrm{Rank}(a) &= \mathrm{Rank}(\mathrm{Mat}_{\mathcal{B}}(a_1, a_2, \ldots, a_n)) \\ &= \dim_{\mathbb{F}_q}(\{L(x) \,|\, x \in \mathbb{F}_{q^m}\}) \end{aligned}$$

Given a vector $a \in \mathbb{F}_{q^m}^n$, the Hamming weight $\mathrm{WT}_{\mathrm{H}}(a) \geq \mathrm{Rank}(a)$

The Rank Metric

- The **rank** of a vector $a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ is defined as

$$\mathrm{Rank}(a) := \dim_{\mathbb{F}_q}(\langle a_1, \cdots, a_n \rangle)$$

- Alternatively,

$$\begin{aligned} \mathrm{Rank}(a) &= \mathrm{Rank}(\mathrm{Mat}_{\mathcal{B}}(a_1, a_2, \ldots, a_n)) \\ &= \dim_{\mathbb{F}_q}\left(\{L(x) \,|\, x \in \mathbb{F}_{q^m}\}\right) \end{aligned}$$

Given a vector $a \in \mathbb{F}_{q^m}^n$, the Hamming weight $\mathrm{WT_H}(a) \geq \mathrm{Rank}(a)$

Rank-metric Codes

Let *rank distance* between vectors $a, b \in \mathbb{F}_{q^m}^n$ be given by

$$d_R(a, b) = \mathrm{Rank}(a - b)$$

Rank Metric Codes

A *rank metric* (n, M, d)-code $\mathcal{C}$ over $\mathbb{F}_{q^m}$:

- $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and $|\mathcal{C}| = M$
- $\min\{d_R(a, b) \mid a, b \in \mathcal{C},\ a \neq b\} = d$

Rank-metric Codes

Let *rank distance* between vectors $a, b \in \mathbb{F}_{q^m}^n$ be given by

$$d_R(a, b) = \mathrm{Rank}(a - b)$$

Rank Metric Codes

A *rank metric* (n, M, d)-code $\mathcal{C}$ over $\mathbb{F}_{q^m}$:

- $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and $|\mathcal{C}| = M$
- $\min\{d_R(a, b) \mid a, b \in \mathcal{C},\ a \neq b\} = d$

Representations of Rank-metric Codes

- Vectorial Form: a subset of $\mathbb{F}_{q^m}^n$
- Matrix Form: a subset of $\mathbb{F}_q^{n\times m}$
- Linearized Polynomial Form: a subset of

$$\mathcal{L}_n(\mathbb{F}_{q^m}) = \left\{ L(x) = \sum_{i=0}^{n-1} l_i x^{q^i} \ : \ l_i \in \mathbb{F}_{q^m} \right\}$$

with rank defined as

$$\mathrm{Rank}(L(x)) = \dim_{\mathbb{F}_q}(\mathrm{Img(L)}) = n - \dim_{\mathbb{F}_q}(\mathrm{Ker(L)})$$

$\left(\mathcal{L}_n(\mathbb{F}_{q^m}), +, \circ\right)$ is a non-commutative ring

Representations of Rank-metric Codes

- Vectorial Form: a subset of $\mathbb{F}_{q^m}^n$
- Matrix Form: a subset of $\mathbb{F}_q^{n\times m}$
- Linearized Polynomial Form: a subset of

$$\mathcal{L}_n(\mathbb{F}_{q^m}) = \left\{ L(x) = \sum_{i=0}^{n-1} l_i x^{q^i} \ : \ l_i \in \mathbb{F}_{q^m} \right\}$$

with rank defined as

$$\mathrm{Rank}(L(x)) = \dim_{\mathbb{F}_q}(\mathrm{Img(L)}) = n - \dim_{\mathbb{F}_q}(\mathrm{Ker(L)})$$

$\left(\mathcal{L}_n(\mathbb{F}_{q^m}), +, \circ\right)$ is a non-commutative ring

Maximum Rank Distance (MRD) codes

Singleton-like bound

A rank metric (n, M, d)-code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ satisfies

$$M \leq q^{\min\{n(m-d+1), m(n-d+1)\}}$$

When $\mathcal{C}$ is linear and $m = n$, the bound is $d \leq n - k + 1$

MRD codes

A rank metric (n, M, d)-code over $\mathbb{F}_{q^m}$ is said to a **maximum rank distance (MRD) code** if it attains the Singleton-like bound

Maximum Rank Distance (MRD) codes

Singleton-like bound

A rank metric (n, M, d)-code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ satisfies

$$M \leq q^{\min\{n(m-d+1), m(n-d+1)\}}$$

When $\mathcal{C}$ is linear and $m = n$, the bound is $d \leq n - k + 1$

MRD codes

A rank metric (n, M, d)-code over $\mathbb{F}_{q^m}$ is said to a **maximum rank distance (MRD) code** if it attains the Singleton-like bound

Maximum Rank Distance (MRD) codes

Singleton-like bound

A rank metric (n, M, d)-code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ satisfies

$$M \leq q^{\min\{n(m-d+1),m(n-d+1)\}}$$

When $\mathcal{C}$ is linear and $m = n$, the bound is $d \leq n - k + 1$

MRD codes

A rank metric (n, M, d)-code over $\mathbb{F}_{q^m}$ is said to a **maximum rank distance (MRD) code** if it attains the Singleton-like bound

Properties of MRD codes

- a famous family of MRD codes: referenced as Gabidulin codes (Delsarte1978, Gabidulin1985, Roth1991)
- exist for any parameters: n, m, q, k and d
- the dual code of an MRD code is also MRD code
- the rank-distance distributions of an MRD code $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are **completely determined** by the parameters

Motivation

- Rank metric codes, especially MRD codes, have applications in space-time coding, random network coding and cryptography
- Gabidulin codes are the well-known maximum rank distance (MRD) codes and the decoding algorithms are extensively studied
- Very recently, many new MRD codes were proposed, while the decoding algorithm for them are not well-studied yet

Motivation

- Rank metric codes, especially MRD codes, have applications in space-time coding, random network coding and cryptography
- Gabidulin codes are the well-known maximum rank distance (MRD) codes and the decoding algorithms are extensively studied
- Very recently, many new MRD codes were proposed, while the decoding algorithm for them are not well-studied yet

Motivation

- Rank metric codes, especially MRD codes, have applications in space-time coding, random network coding and cryptography
- Gabidulin codes are the well-known maximum rank distance (MRD) codes and the decoding algorithms are extensively studied
- Very recently, many new MRD codes were proposed, while the decoding algorithm for them are not well-studied yet

Rank-metric Codes via Linearized Polynomials

From now on, our discussion is restricted to $m = n$

Linearized Polynomial

$$L(x) = l_0 x + l_1 x^q + \cdots + l_{n-1} x^{q^{n-1}}, \quad l_i \in \mathbb{F}_{q^n}$$

- q-degree: $deg_q(L(x)) = \max\{i \mid 0 \leq i \leq n : \ l_i \neq 0\}$.
- Kernel of L: $\mathrm{Ker}(L) = \{x \in \mathbb{F}_{q^n} | L(x) = 0\}$.
- Rank of $L(x)$:

$$Rank(L) = n - \dim_{\mathbb{F}_q}(\mathrm{Ker(L)}) \geq n - deg_q(L(x))$$

MRD Codes - Gabidulin Codes

Gabidulin Codes [**Gabidulin-1985**]

$$\mathcal{G} = \left\{ (L(\alpha_1), \cdots, L(\alpha_n)) \ : \ L(x) = \sum_{i=0}^{k-1} l_i x^{q^i}, \ l_i \in \mathbb{F}_{q^n} \right\},$$

where $\alpha_1, \cdots, \alpha_n$ in $\mathbb{F}_{q^n}$ are linearly independent over $\mathbb{F}_q$

The Gabidulin code $\mathcal{G}$ is the first and well-known MRD code

$$n - \dim_{\mathbb{F}_q}(Ker(L)) \leq d(\mathcal{G}) \leq n - k + 1$$

*For simplicity, we will express codes by linear polynomials

MRD Codes - Gabidulin Codes

Gabidulin Codes [**Gabidulin-1985**]

$$\mathcal{G} = \left\{ (L(\alpha_1), \cdots, L(\alpha_n)) \ : \ L(x) = \sum_{i=0}^{k-1} l_i x^{q^i}, \ l_i \in \mathbb{F}_{q^n} \right\},$$

where $\alpha_1, \cdots, \alpha_n$ in $\mathbb{F}_{q^n}$ are linearly independent over $\mathbb{F}_q$

The Gabidulin code $\mathcal{G}$ is the first and well-known MRD code

$$n - \dim_{\mathbb{F}_q}(Ker(L)) \leq d(\mathcal{G}) \leq n - k + 1$$

*For simplicity, we will express codes by linear polynomials

MRD Codes - Generalized Gabidulin Codes

Generalized Gabidulin Codes [**Gabidulin-2005**]

Let $\gcd(s, n) = 1$. The linear code

$$\mathcal{GG} = \left\{ \sum_{i=0}^{k-1} l_i x^{q^{si}}, \ l_i \in \mathbb{F}_{q^n} \right\}, \tag{1}$$

is an MRD code

MRD codes - Twisted Gabidulin (TG) Codes

Lemma ([Sheekey.16])

Let $0 < k < n$ and $l_k \neq 0$. If the linearized polynomial $L(x) = \sum_{i=0}^{k-1} l_i x^{q^i} + l_k x^{q^k}$ has q^k roots, then

$$Norm_{q^n/q}(l_k) = (-1)^{nk} Norm_{q^n/q}(l_0). \tag{2}$$

- when (2) doesn't hold,

$$Rank(L) = n - \dim_{\mathbb{F}_q}(\mathrm{Ker(L)}) \geq n - k + 1$$

$\Rightarrow$ We obtain MRD codes if (2) doesn't hold

MRD codes - Twisted Gabidulin (TG) Codes

Theorem ([Sheekey.16])

The linear code

$$\mathcal{TG} = \left\{ \sum_{i=0}^{k-1} l_i x^{q^i} + \eta l_0^{q^h} x^{q^k},\ l_i \in \mathbb{F}_{q^n} \right\}$$

with $Norm_{q^n/q}(\eta) \neq (-1)^{nk}$ *is an MRD code with*

- *size* q^{nk},
- *rank distance* $n - k + 1$

and is inequivalent to known ones

MRD codes - Twisted Gabidulin (TG) Codes

Theorem ([Luradon-Tronbetti-Zhou.18])

Let $\gcd(s, n) = 1$ *and* $[i] := q^{si}$. *The linear code*

$$\mathcal{GTG} = \left\{ \sum_{i=0}^{k-1} l_i x^{[i]} + \eta l_0^{q^h} x^{[k]},\ l_i \in \mathbb{F}_{q^n} \right\}$$

with $N_{q^{sn}/q^s}(\eta) \neq (-1)^{nk}$ *is an MRD code with*

- *size* q^{nk},
- *rank distance* $n - k + 1$

and is inequivalent to known ones

Additive Generalized Twisted Gabidulin Code

[Otal and Ozbudak.17]

Let $n, k, s, h \in \mathbb{Z}^+$ satisfying $(s, n) = 1$ and $k < n$.

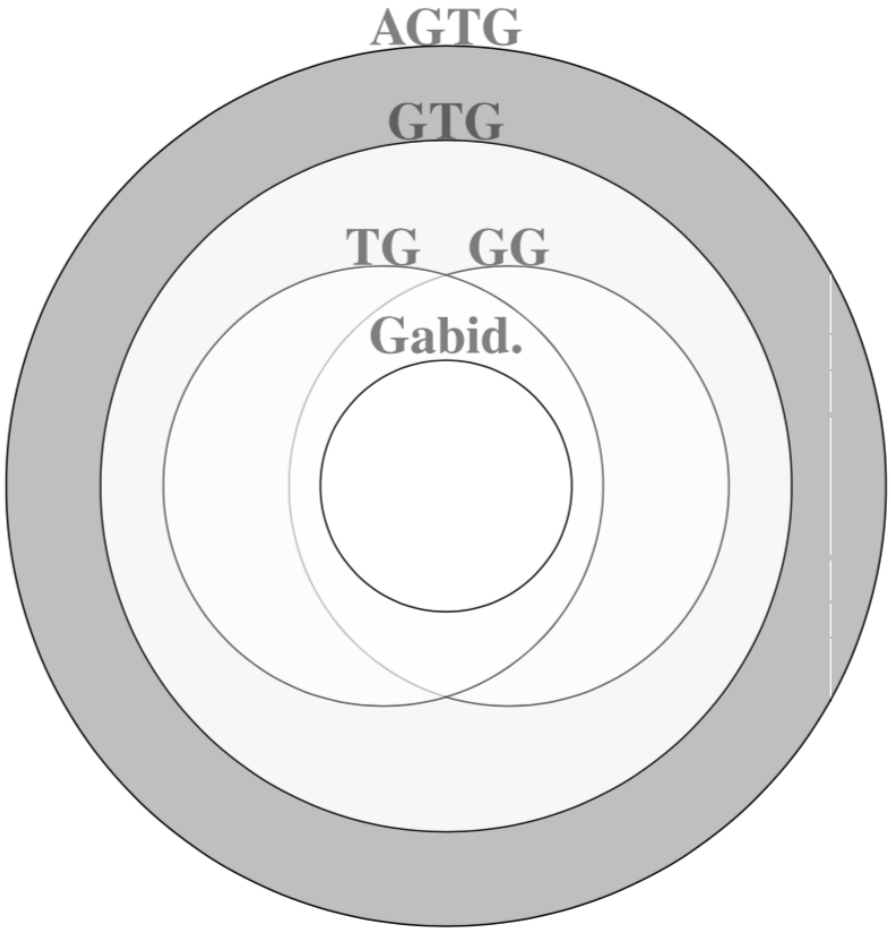
Let $q = q_0^u$ and $\eta \in \mathbb{F}_{q^n}$ such that $\eta^{\frac{q^{sn}-1}{q_0^s-1}} \neq (-1)^{nku}$. Then

$$\mathcal{AGTG} = \left\{ \sum_{i=0}^{k-1} l_i x^{[i]} + \eta l_0^{\mathbf{q_0^h}} x^{[k]} : \ l_i \in \mathbb{F}_{q^n} \right\} \tag{3}$$

is an $\mathrm{GF}(q_0)$-linear (but maybe not $\mathbb{F}_q$-linear) MRD code with

- size q^{nk},
- rank distance $n - k + 1$

Relations of these MRD codes



Encoding and Decoding of Linear Codes

Traditional encoding: $m \mapsto mG$, where G is the generator matrix

Rank Syndrome Decoding Problem

Given a parity-check matrix H over $\mathbb{F}_{q^n}$ and a vector s, find an error vector e with $\mathrm{Rank}(e) \leq t$ such that

$$eH^T = s$$

This is (approximately) NP-hard problem

So far no efficient decoding algorithm exist for random H and s

Poly.-time decoding algorithms only exist for certain instances

Encoding and Decoding of Linear Codes

Traditional encoding: $m \mapsto mG$, where G is the generator matrix

Rank Syndrome Decoding Problem

Given a parity-check matrix H over $\mathbb{F}_{q^n}$ and a vector s, find an error vector e with $\mathrm{Rank}(e) \leq t$ such that

$$eH^T = s$$

This is (approximately) NP-hard problem

So far no efficient decoding algorithm exist for random H and s

Poly.-time decoding algorithms only exist for certain instances

Decoding of Gabidulin Codes

Encoding:

$$(f_0, \cdots, f_{k-1}) \mapsto (f(a_1), \cdots, f(a_n)) = (f_0, \cdots, f_{k-1}) \cdot G$$

where G is the submatrix formed by the first k rows of

$$\mathcal{M} = \left(\alpha_{i+1}^{[j]}\right)_{n\times n} = \begin{pmatrix} \alpha_1 & \alpha_1^{[1]} & \cdots & \alpha_1^{[n-1]} \\ \alpha_2 & \alpha_2^{[1]} & \cdots & \alpha_2^{[n-1]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_n & \alpha_n^{[1]} & \cdots & \alpha_n^{[n-1]} \end{pmatrix}^T$$

The parity-check matrix $H = \left(h_{ij}\right)_{(n-k)\times n}$ has the same form as $\mathcal{M}$

Decoding of Gabidulin Codes

Goal of Decoding: find the unique error e such that $r - e = c$ in $\mathcal{G}$

- calculate syndrome $(s_0, \cdots, s_{n-k-1}) = rH^T = eH^T$
- express the error vector as

$$e = (e_1, \cdots, e_n) = (E_1, \cdots, E_t) \begin{pmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & \ddots & \vdots \\ X_{t1} & \cdots & X_{tn} \end{pmatrix},$$

  where $E_1, \cdots, E_t$ are linearly independent vectors in $\mathbb{F}_{q^m}$ and $X = (X_{ij}) \in \mathbb{F}_q^{t \times n}$

- then the syndrome

  $(s_0, \cdots, s_{n-k-1}) = (E_1, \cdots, E_t)XH^T = (E_1, \cdots, E_t)Y$

Decoding of Gabidulin Codes

Goal of Decoding: find the unique error e such that $r - e = c$ in $\mathcal{G}$

- calculate syndrome $(s_0, \cdots, s_{n-k-1}) = rH^T = eH^T$
- express the error vector as

$$e = (e_1, \cdots, e_n) = (E_1, \cdots, E_t) \begin{pmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & \ddots & \vdots \\ X_{t1} & \cdots & X_{tn} \end{pmatrix},$$

  where $E_1, \cdots, E_t$ are linearly independent vectors in $\mathbb{F}_{q^m}$ and $X = (X_{ij}) \in \mathbb{F}_q^{t \times n}$

- then the syndrome

$$(s_0, \cdots, s_{n-k-1}) = (E_1, \cdots, E_t)XH^T = (E_1, \cdots, E_t)Y$$

Decoding of Gabidulin Codes

Goal of Decoding: find the unique error e such that $r - e = c$ in $\mathcal{G}$

- calculate syndrome $(s_0, \cdots, s_{n-k-1}) = rH^T = eH^T$
- express the error vector as

$$e = (e_1, \cdots, e_n) = (E_1, \cdots, E_t) \begin{pmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & \ddots & \vdots \\ X_{t1} & \cdots & X_{tn} \end{pmatrix},$$

  where $E_1, \cdots, E_t$ are linearly independent vectors in $\mathbb{F}_{q^m}$ and $X = (X_{ij}) \in \mathbb{F}_q^{t \times n}$

- then the syndrome

  $(s_0, \cdots, s_{n-k-1}) = (E_1, \cdots, E_t)XH^T = (E_1, \cdots, E_t)Y$

Suppose $\Lambda(x) = \sum_{i=0}^{t} \Lambda_i x^{q^i}$ vanishes at $E_1, \cdots, E_t$, i.e.,

$$\Lambda(x) = \prod_{(a_1,\cdots,a_t)\in\mathbb{F}_q^t} \left(x - \sum_{i=1}^{t} a_i E_i\right) = \sum_{i=0}^{t} \Lambda_i x^{q^i}$$

Then it implies **the key equation**

$$\Lambda(x) \circ S(x) \mod x^{q^{n-k}} \equiv F(x)$$

where $S(x) = \sum_{i=0}^{n-k-1} s_i x^{q^i}$ and $F(x)$ has q-degree $< t$

Steps of decoding Gabidulin codes:

1. solving $\Lambda(x) \circ S(x) \mod x^{q^{n-k}} \equiv F(x)$ gives $\Lambda(x)$ and $F(x)$
2. solving $\Lambda(x) = 0$ gives linearly independent vectors $E_1, \cdots, E_t$
3. solving $s = (E_1, \cdots, E_t)Y$ gives Y
4. solving $XH^T = Y$ gives X
5. it finally determines the error vector

$$e = (E_1, \cdots, E_t)X$$

Steps of decoding Gabidulin codes:

1. solving $\Lambda(x) \circ S(x) \mod x^{q^{n-k}} \equiv F(x)$ gives $\Lambda(x)$ and $F(x)$
2. solving $\Lambda(x) = 0$ gives linearly independent vectors $E_1, \cdots, E_t$
3. solving $s = (E_1, \cdots, E_t)Y$ gives Y
4. solving $XH^T = Y$ gives X
5. it finally determines the error vector

$$e = (E_1, \cdots, E_t)X$$

Steps of decoding Gabidulin codes:

1. solving $\Lambda(x) \circ S(x) \mod x^{q^{n-k}} \equiv F(x)$ gives $\Lambda(x)$ and $F(x)$
2. solving $\Lambda(x) = 0$ gives linearly independent vectors $E_1, \cdots, E_t$
3. solving $s = (E_1, \cdots, E_t)Y$ gives Y
4. solving $XH^T = Y$ gives X
5. it finally determines the error vector

$$e = (E_1, \cdots, E_t)X$$

Steps of decoding Gabidulin codes:

1. solving $\Lambda(x) \circ S(x) \mod x^{q^{n-k}} \equiv F(x)$ gives $\Lambda(x)$ and $F(x)$
2. solving $\Lambda(x) = 0$ gives linearly independent vectors $E_1, \cdots, E_t$
3. solving $s = (E_1, \cdots, E_t)Y$ gives Y
4. solving $XH^T = Y$ gives X
5. it finally determines the error vector

$$e = (E_1, \cdots, E_t)X$$

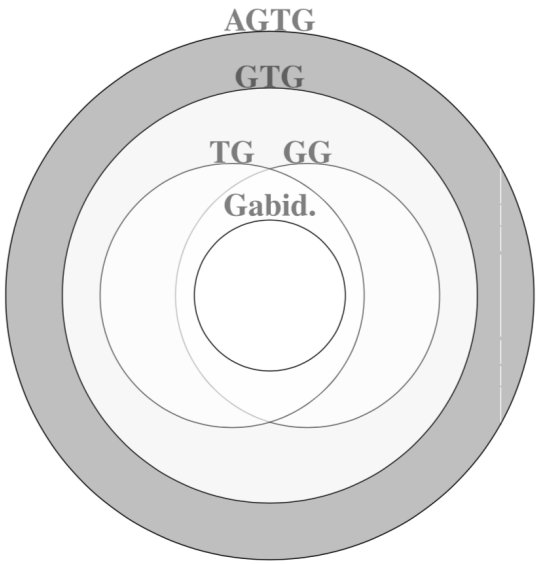
Steps of decoding Gabidulin codes:

1. solving $\Lambda(x) \circ S(x) \mod x^{q^{n-k}} \equiv F(x)$ gives $\Lambda(x)$ and $F(x)$
2. solving $\Lambda(x) = 0$ gives linearly independent vectors $E_1, \cdots, E_t$
3. solving $s = (E_1, \cdots, E_t)Y$ gives Y
4. solving $XH^T = Y$ gives X
5. it finally determines the error vector

$$e = (E_1, \cdots, E_t)X$$

1. Rank-metric Codes : Basics and Motivations
2. Recent Constructions of MRD codes
3. Decoding of Gabidulin codes
4. Decoding of New MRD Codes
   - Polynomial Reconstruction
   - Finding Coefficients λ_i
     - BM Algorithm
     - Reducing an Under-Determined System to P(x)=0
     - Solving P(x)=0
5. Conclusion

Recall of the new MRD codes



The general AGTG codes:

$$\mathcal{AGTG} = \left\{ \sum_{i=0}^{k-1} l_i x^{[i]} + \eta l_0^{\mathbf{q^h_0}} x^{[k]} : \ l_i \in \mathbb{F}_{q^n} \right\}$$

Encoding of New MRD codes

For all the previous MRD codes, denote $\tilde{f} = (f_0, \cdots, f_{k-1}, \eta f_0^{q_0^h}, 0, \cdots, 0)$.

Then the **encoding process** is given as:

$$(f_0, \cdots, f_{k-1}) \mapsto f(a_1), \cdots, f(a_n)) = \tilde{f} \cdot \mathcal{M} \tag{4}$$

where $\mathcal{M}$ is the *Moore matrix* associated to $\alpha_1, \ldots, \alpha_n$:

$$\mathcal{M} = \left(\alpha_{i+1}^{[j]}\right)_{n\times n} = \begin{pmatrix} \alpha_1 & \alpha_1^{[1]} & \cdots & \alpha_1^{[n-1]} \\ \alpha_2 & \alpha_2^{[1]} & \cdots & \alpha_2^{[n-1]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_n & \alpha_n^{[1]} & \cdots & \alpha_n^{[n-1]} \end{pmatrix}^T$$

Decoding of New MRD codes

Challenge

The parity-check matrix H of new MRD codes cannot be properly given :-(

Alternative: interpolation-based decoding

- Assume $g(x) = \sum_{i=0}^{n-1} g_i x^{[i]}$ satisfy $g(a_i) = e_i$
- find e is **equivalent to** finding $g_0, g_1, \cdots, g_{n-1}$
- Note that

$$r = c + e = (\tilde{f} + g) \cdot \mathcal{M}$$

It is equivalent to

$$\hat{r} = r \cdot (\mathcal{M})^{-1} = \begin{pmatrix} f_0 & + & g_0 \\ & \vdots & \\ f_{k-1} & + & g_{k-1} \\ \eta f_0^{q_0^{uh}} & + & g_k \\ 0 & + & g_{k+1} \\ & \vdots & \\ 0 & + & g_{n-1} \end{pmatrix}, \tag{5}$$

where $\hat{r} = (\hat{r}_0, \ldots, \hat{r}_{n-1}) = r \cdot (\mathcal{M})^{-1}$ is known

Then,

- $(g_{k+1}, \ldots, g_{n-1}) = (\hat{r}_{k+1}, \ldots, \hat{r}_{n-1})$
- $\eta f_0^{q_0^h} + g_k = \hat{r}_k$, and $f_0 + g_0 = \hat{r}_0$, implying

$$\eta g_0^{q_0^h} + g_k = \eta \hat{r}_0^{q_0^h} + \hat{r}_k \tag{6}$$

Decoding of AGTG codes

How to reconstruct $g(x)$ from the above information?

Then,

- $(g_{k+1}, \ldots, g_{n-1}) = (\hat{r}_{k+1}, \ldots, \hat{r}_{n-1})$
- $\eta f_0^{q_0^h} + g_k = \hat{r}_k$, and $f_0 + g_0 = \hat{r}_0$, implying

$$\eta g_0^{q_0^h} + g_k = \eta \hat{r}_0^{q_0^h} + \hat{r}_k \tag{6}$$

Decoding of AGTG codes

How to reconstruct $g(x)$ from the above information?

Reconstructing $g(x)$

For $g(x) = \sum_{i=0}^{n-1} g_i x^{[i]}$, define the Dickson matrix

$$G = \left(g_{i-j(\bmod n)}^{[j]}\right)_{n\times n} = \begin{pmatrix} g_0 & g_{n-1}^{[1]} & \cdots & g_1^{[n-1]} \\ g_1 & g_0^{[1]} & \cdots & g_2^{[n-1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-1} & g_{n-2}^{[1]} & \cdots & g_0^{[n-1]} \end{pmatrix}, \tag{7}$$

Property of the Dickson Matrix

Any $t \times t$ submatrix of G from consecutive rows and columns is non-singular

We consider the $(t+1) \times n$ sub-matrix

$$\left(\begin{array}{cccccccc}
[0] & [1] & \cdots & [n-(k+t)] & [n-(k+t-1)] & \cdots & [n-k] & \cdots & [n-1] \\
\hline
g_0 & g_{n-1} & \cdots & g_{k+t} & g_{k+t-1} & \cdots & g_k & \cdots & g_1 \\
g_1 & g_0 & \cdots & g_{k+t+1} & g_{k+t} & \cdots & g_{k+1} & \cdots & g_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
g_{t-1} & g_{t-2} & \cdots & g_{k+2t-1} & g_{k+2t-2} & \cdots & g_{k+t-1} & \cdots & g_t \\
g_t & g_{t-1} & \cdots & g_0 & g_{k+2t-1} & \cdots & g_{k+t} & \cdots & g_{t+1} \\
\hline
g_{t+1} & g_t & \cdots & g_1 & g_{k+2t} & \cdots & g_{k+t+1} & \cdots & g_{t+2} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
g_{n-1} & g_{n-2} & \cdots & g_{k+t-1} & g_{k+t-2} & \cdots & g_{k-1} & \cdots & g_0
\end{array}\right)$$

We can express the $(n-(k+t))$-th column as a linear combination

$$G_{n-(k+t)} = \lambda_0 G_{n-(k+t)+1} + \lambda_1 G_{n-(k+t)+2} + \cdots + \lambda_{t-1} G_{n-k}$$

We consider the $(t+1) \times n$ sub-matrix

$$\left(\begin{array}{cccccccc}
[0] & [1] & \cdots & [n-(k+t)] & [n-(k+t-1)] & \cdots & [n-k] & \cdots & [n-1] \\
\hline
g_0 & g_{n-1} & \cdots & g_{k+t} & g_{k+t-1} & \cdots & g_k & \cdots & g_1 \\
g_1 & g_0 & \cdots & g_{k+t+1} & g_{k+t} & \cdots & g_{k+1} & \cdots & g_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
g_{t-1} & g_{t-2} & \cdots & g_{k+2t-1} & g_{k+2t-2} & \cdots & g_{k+t-1} & \cdots & g_t \\
g_t & g_{t-1} & \cdots & g_0 & g_{k+2t-1} & \cdots & g_{k+t} & \cdots & g_{t+1} \\
\hline
g_{t+1} & g_t & \cdots & g_1 & g_{k+2t} & \cdots & g_{k+t+1} & \cdots & g_{t+2} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
g_{n-1} & g_{n-2} & \cdots & g_{k+t-1} & g_{k+t-2} & \cdots & g_{k-1} & \cdots & g_0
\end{array}\right)$$

We can express the $(n-(k+t))$-th column as a linear combination

$$G_{n-(k+t)} = \lambda_0 G_{n-(k+t)+1} + \lambda_1 G_{n-(k+t)+2} + \cdots + \lambda_{t-1} G_{n-k}$$

We consider the $(t+1) \times n$ sub-matrix

$$\left(\begin{array}{cccccccc}
[0] & [1] & \cdots & [n-(k+t)] & [n-(k+t-1)] & \cdots & [n-k] & \cdots & [n-1] \\
\hline
g_0 & g_{n-1} & \cdots & g_{k+t} & g_{k+t-1} & \cdots & g_k & \cdots & g_1 \\
g_1 & g_0 & \cdots & g_{k+t+1} & g_{k+t} & \cdots & g_{k+1} & \cdots & g_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
g_{t-1} & g_{t-2} & \cdots & g_{k+2t-1} & g_{k+2t-2} & \cdots & g_{k+t-1} & \cdots & g_t \\
g_t & g_{t-1} & \cdots & g_0 & g_{k+2t-1} & \cdots & g_{k+t} & \cdots & g_{t+1} \\
\hline
g_{t+1} & g_t & \cdots & g_1 & g_{k+2t} & \cdots & g_{k+t+1} & \cdots & g_{t+2} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
g_{n-1} & g_{n-2} & \cdots & g_{k+t-1} & g_{k+t-2} & \cdots & g_{k-1} & \cdots & g_0
\end{array}\right)$$

We can express the $(n-(k+t))$-th column as a linear combination

$$G_{n-(k+t)} = \lambda_0 G_{n-(k+t)+1} + \lambda_1 G_{n-(k+t)+2} + \cdots + \lambda_{t-1} G_{n-k}$$

$$\left(\begin{array}{ccccc} [n-(k+t)] & [n-(k+t-1)] & \dots & [n-k-1] & [n-k] \\ \hline g_{k+t} & g_{k+t-1} & \cdots & g_{k+1} & g_k \\ g_{k+t+1} & g_{k+t} & \cdots & g_{k+2} & g_{k+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ g_{n-1} & g_{k+2t-2} & \cdots & g_{k+t} & g_{k+2} \\ g_0 & g_{k+2t-1} & \cdots & g_{k+t+1} & g_{k+t} \end{array}\right) \cdot \begin{pmatrix} 1 \\ \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_{t-1} \end{pmatrix} = 0$$

This will give the following *key recursive equation*

$$g_{k+t+i}^{[n-(k+t)]} = \lambda_0 g_{k+t+i-1}^{[n-(k+t)+1]} + \lambda_1 g_{k+t+i-2}^{[n-(k+t)+2]} + \cdots + \lambda_{t-1} g_{k+i}^{[n-k]} \qquad (8)$$

for $i = 0, 1, \ldots, n-1$.

Now polynomial $g(x)$ can be reconstructed in two steps:

Step 1. derive the coeff. $\lambda_0, \ldots, \lambda_{t-1}$ from (6) and (8);

Step 2. use them to compute $g_{k-1}, \ldots, g_0$ recursively.

Step 2 is a simple calculation of linear combination of vectors

Our focus will be on Step 1 from now on

This will give the following *key recursive equation*

$$g_{k+t+i}^{[n-(k+t)]} = \lambda_0 g_{k+t+i-1}^{[n-(k+t)+1]} + \lambda_1 g_{k+t+i-2}^{[n-(k+t)+2]} + \cdots + \lambda_{t-1} g_{k+i}^{[n-k]} \qquad (8)$$

for $i = 0, 1, \ldots, n-1$.

Now polynomial $g(x)$ can be reconstructed in two steps:

Step 1. derive the coeff. $\lambda_0, \ldots, \lambda_{t-1}$ from (6) and (8);

Step 2. use them to compute $g_{k-1}, \ldots, g_0$ recursively.

Step 2 is a simple calculation of linear combination of vectors

Our focus will be on Step 1 from now on

Reconstructing The Error Interpolation Polynomial $g(x)$

Recall that $g_{k+1}, \ldots, g_{n-1}$ are known

We have a system of linear equations:

- $n-1-(k+t)$ linear equations
- t unknowns λ_i

As the rank of the error vector e satisfies $\mathrm{Rank}(e) = t \leq \lfloor \frac{n-k}{2} \rfloor$, we divide the discussion in two cases:

1. *Case 1:* $2t + k < n$
2. *Case 2:* $2t + k = n$

Reconstructing The Error Interpolation Polynomial $g(x)$

Recall that $g_{k+1}, \ldots, g_{n-1}$ are known

We have a system of linear equations:

- $n-1-(k+t)$ linear equations
- t unknowns λ_i

As the rank of the error vector e satisfies $\text{Rank}(e) = t \leq \lfloor \frac{n-k}{2} \rfloor$, we divide the discussion in two cases:

1. *Case 1:* $2t + k < n$
2. *Case 2:* $2t + k = n$

Solving Under-Determined System of Equations

Case 1: If $2t + k < n$, the discussion is relatively trivial

Case 2: If $2t + k = n$, we have system of $n - k - t - 1 = t - 1$ equations with $\lambda_0, \ldots, \lambda_{t-1}$ variables and (36) will be an under-determined system of linear equations. Hence

- the set of solutions $(\lambda_0, \ldots, \lambda_{t-1})$ has dimension 1 over $\mathbb{F}_{q^n}$ of the form

$$\lambda + \omega\lambda' = (\lambda_0 + \omega\lambda'_0, \ldots, \lambda_{t-1} + \omega\lambda'_{t-1}),$$

- λ, λ' are t-dimensional vectors in $\mathbb{F}_{q^n}$ and ω runs through $\mathbb{F}_{q^n}$.

Solving Under-Determined System of Equations

Case 1: If $2t + k < n$, the discussion is relatively trivial

Case 2: If $2t + k = n$, we have system of $n - k - t - 1 = t - 1$ equations with $\lambda_0, \ldots, \lambda_{t-1}$ variables and (36) will be an under-determined system of linear equations. Hence

- the set of solutions $(\lambda_0, \ldots, \lambda_{t-1})$ has dimension 1 over $\mathbb{F}_{q^n}$ of the form

$$\lambda + \omega\lambda' = (\lambda_0 + \omega\lambda'_0, \ldots, \lambda_{t-1} + \omega\lambda'_{t-1}),$$

- $\lambda,\ \lambda'$ are t-dimensional vectors in $\mathbb{F}_{q^n}$ and ω runs through $\mathbb{F}_{q^n}$.

Solving Under-Determined System of Equations

Case 1: If $2t + k < n$, the discussion is relatively trivial

Case 2: If $2t + k = n$, we have system of $n - k - t - 1 = t - 1$ equations with $\lambda_0, \ldots, \lambda_{t-1}$ variables and (36) will be an under-determined system of linear equations. Hence

- the set of solutions $(\lambda_0, \ldots, \lambda_{t-1})$ has dimension 1 over $\mathbb{F}_{q^n}$ of the form

$$\lambda + \omega\lambda' = (\lambda_0 + \omega\lambda'_0, \ldots, \lambda_{t-1} + \omega\lambda'_{t-1}),$$

- $\lambda,\ \lambda'$ are t-dimensional vectors in $\mathbb{F}_{q^n}$ and ω runs through $\mathbb{F}_{q^n}$.

- Taking $i = t$ and $i = 0$ in (8) give the following two equations

$$\begin{aligned} g_0^{[t]} &= \lambda_0 g_{n-1}^{[t+1]} + \lambda_1 g_{n-2}^{[t+2]} + \cdots + \lambda_{t-1} g_{n-t}^{[2t]}, \\ g_{k+t}^{[t]} &= \lambda_0 g_{k+t-1}^{[t+1]} + \lambda_1 g_{k+t-2}^{[t+2]} + \cdots + \lambda_{t-1} g_k^{[2t]}. \end{aligned}$$

- Operations on both sides of equations to eliminate the exponents in left sides give the following equations:

$$\begin{aligned} g_0 &= \lambda_0^{[n-t]} g_{n-1}^{[1]} + \lambda_1^{[n-t]} g_{n-2}^{[2]} + \cdots + \lambda_{t-1}^{[n-t]} g_{n-t}^{[t]}, \\ g_{k+t} &= \lambda_0^{[n-t]} g_{k+t-1}^{[1]} + \lambda_1^{[n-t]} g_{k+t-2}^{[2]} + \cdots + \lambda_{t-1}^{[n-t]} g_k^{[t]}. \end{aligned}$$

- One can substitute $\lambda + \omega\lambda'$ and re-arrange the equations to get:

$$u_0\omega^{q_0^{i_1}+q_0^{i_2}} + u_1\omega^{q_0^{i_1}} + u_1\omega^{q_0^{i_2}} + u_3 = 0,$$

where $i_1 = h + us(n-t)$, $i_2 = usk$, $u_0, \ldots, u_3$ are derived from $c_0, \ldots, c_6$ and η.

- If $x = \omega^{q_0^{i_2}}$ and $v = i_1 - i_2$, then

$$u_0\omega^{q_0^{v}+1} + u_1\omega^{q_0^{v}} + u_2\omega + u_3 = 0.$$

- One can substitute $\lambda + \omega\lambda'$ and re-arrange the equations to get:

$$u_0\omega^{q_0^{i_1}+q_0^{i_2}} + u_1\omega^{q_0^{i_1}} + u_1\omega^{q_0^{i_2}} + u_3 = 0,$$

  where $i_1 = h + us(n-t)$, $i_2 = usk$, $u_0, \ldots, u_3$ are derived from $c_0, \ldots, c_6$ and η.

- If $x = \omega^{q_0^{i_2}}$ and $v = i_1 - i_2$, then

$$u_0\omega^{q_0^v+1} + u_1\omega^{q_0^v} + u_2\omega + u_3 = 0.$$

- The polynomial

$$P(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3$$

  should have unique solution, since any error vector e with $\text{Rank}(e) = t = \frac{n-k}{2}$ can be uniquely decoded.

- Unique solution of $P(x)$ gives the unique solution $\lambda_0, \lambda_1, \ldots, \lambda_{t-1}$.
- Regarding *Step 2* and using equation (8), one computes the unknown coefficients $g_0, \ldots, g_{k-1}$ of $g(x)$.

Finding the roots of $P(x) = 0$ in $\mathbb{F}_{q^n}$

$$P(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3 = 0 \tag{9}$$

Let $d = gcd(v, un)$.

- If $u_0 = 0$ then (9) becomes $u_1 x^{q_0^v} + u_2 x + u_3 = 0$
- If $u_0 \neq 0$ then (9) in equivalent to

$$Q(x) = x^{q_0^v+1} + a_1 x^{q_0^v} + a_2 x + a_3 = 0, \tag{10}$$

where $a_i = u_i/u_0$ for $i = 1, 2, 3$.

Finding the roots of $P(x) = 0$ in $\mathbb{F}_{q^n}$

$$P(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3 = 0 \tag{9}$$

Let $d = gcd(v, un)$.

- If $u_0 = 0$ then (9) becomes $u_1 x^{q_0^v} + u_2 x + u_3 = 0$
- If $u_0 \neq 0$ then (9) in equivalent to

$$Q(x) = x^{q_0^v+1} + a_1 x^{q_0^v} + a_2 x + a_3 = 0, \tag{10}$$

where $a_i = u_i/u_0$ for $i = 1, 2, 3$.

Finding the roots of $P(x) = 0$ in $\mathbb{F}_{q^n}$

$$P(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3 = 0 \tag{9}$$

Let $d = gcd(v, un)$.

- If $u_0 = 0$ then (9) becomes $u_1 x^{q_0^v} + u_2 x + u_3 = 0$
- If $u_0 \neq 0$ then (9) in equivalent to

$$Q(x) = x^{q_0^v+1} + a_1 x^{q_0^v} + a_2 x + a_3 = 0, \tag{10}$$

where $a_i = u_i/u_0$ for $i = 1, 2, 3$.

Finding the root of $Q(x) = 0$ in $\mathbb{F}_{q^n}$ for even q

- The polynomial $Q(x)$ is closely related to

$$F_a(x) = x^{2^l+1} + x + a$$

discussed in Bluher2004, Helleseth-Kholosha2008 over finite field of characteristic 2.

Theorem ([Helleseth-Kholosha 2008])

- *Take any* $a \in \mathrm{GF}(2^m)^*$. *Let* $l, m \in \mathbb{Z}^+$ *with* $l < m$ *and* $d = \gcd(l, m)$, $m_1 = m/d$. *Define two sequence of polynomials derived from the recurrence:* $C_1(x) = C_2(x) = Z_1(x) = 1$, *and for* $i = 1, 2, \cdots, m_1 - 1$

$$C_{i+2}(x) = C_{i+1}(x) + x^{2^{il}} C_i(x), \quad Z_i(x) = C_{i+1}(x) + xC_{i-1}^{2^l}(x)$$

Then the polynomial

$$F_a(x) = x^{2^l+1} + x + a$$

has exactly one zero in $\mathrm{GF}(2^m)$ *iff* $Z_{m_1}(a) = 0$ *and* $C_{m_1}(a) \neq 0$.

Moreover, this zero is equal to $(aC_{m_1}^{2^l-1}(a))^{2^m-1}$.

Theorem ([Helleseth-Kholosha 2008])

- *Take any* $a \in \mathrm{GF}(2^m)^*$. *Let* $l, m \in \mathbb{Z}^+$ *with* $l < m$ *and* $d = \gcd(l, m)$, $m_1 = m/d$. *Define two sequence of polynomials derived from the recurrence:* $C_1(x) = C_2(x) = Z_1(x) = 1$, *and for* $i = 1, 2, \cdots, m_1 - 1$

$$C_{i+2}(x) = C_{i+1}(x) + x^{2^{il}} C_i(x), \quad Z_i(x) = C_{i+1}(x) + x C_{i-1}^{2^l}(x)$$

Then the polynomial

$$F_a(x) = x^{2^l+1} + x + a$$

has exactly one zero in $\mathrm{GF}(2^m)$ *iff* $Z_{m_1}(a) = 0$ *and* $C_{m_1}(a) \neq 0$.
Moreover, this zero is equal to $(aC_{m_1}^{2^l-1}(a))^{2^m-1}$.

Finding the root of $Q(x) = 0$ in $\mathbb{F}_{q^n}$ for even q

Applying the result of Kholosha and Helleseth to a general form enables us to determine the unique solution of $Q(x) = 0$.

Theorem

The polynomial $G(x) = x^{2^l+1} + a_1 x^{2^l} + a_2 x + a_3$ has exactly one zero in $\mathrm{GF}(2^m)$ iff **one** *of the following conditions holds:*

i) $a_2 = a_1^{2^l}$ *and* $a_3 = a_1^{2^l+1}$

ii) $a_2 = a_1^{2^l}$, $a_3 \neq a_1^{2^l+1}$ *and* m_1 *is odd*

iii) $a_2 \neq a_1^{2^l}$, $Z_{m_1}(a) = 0$ *and* $C_{m_1}(a) \neq 0$ *with* $a = (a_1 a_2 + a_3)/(a_1 + a_2^{2^{m-l}})^{2^l+1}$.

Finding the root of $Q(x) = 0$ in $\mathbb{F}_{q^n}$ for even q

Applying the result of Kholosha and Helleseth to a general form enables us to determine the unique solution of $Q(x) = 0$.

Theorem

The polynomial $G(x) = x^{2^l+1} + a_1 x^{2^l} + a_2 x + a_3$ *has exactly one zero in* $\mathrm{GF}(2^m)$ *iff* **one** *of the following conditions holds:*

i) $a_2 = a_1^{2^l}$ *and* $a_3 = a_1^{2^l+1}$

ii) $a_2 = a_1^{2^l}$, $a_3 \neq a_1^{2^l+1}$ *and* m_1 *is odd*

iii) $a_2 \neq a_1^{2^l}$, $Z_{m_1}(a) = 0$ *and* $C_{m_1}(a) \neq 0$ *with* $a = (a_1 a_2 + a_3)/(a_1 + a_2^{2^{m-l}})^{2^l+1}$.

1. Rank-metric Codes : Basics and Motivations
2. Recent Constructions of MRD codes
3. Decoding of Gabidulin codes
4. Decoding of New MRD Codes
   - BM Algorithm
   - Reducing an Under-Determined System to P(x)=0
   - Solving P(x)=0
5. Conclusion

Conclusion

- We presented the first decoding algorithm for additive generalized twisted Gabidulin codes which covers most new MRD codes.
- The idea was introduced in [**Randrianarisoa.17**] and we extended the algorithm for decoding AGTG codes.
- We further investigate the zeros of the polynomial

$$P(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3$$

in the case of characteristic 2.

Conclusion

- We presented the first decoding algorithm for additive generalized twisted Gabidulin codes which covers most new MRD codes.
- The idea was introduced in [**Randrianarisoa.17**] and we extended the algorithm for decoding AGTG codes.
- We further investigate the zeros of the polynomial

$$P(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3$$

in the case of characteristic 2.

Conclusion

- We presented the first decoding algorithm for additive generalized twisted Gabidulin codes which covers most new MRD codes.
- The idea was introduced in [**Randrianarisoa.17**] and we extended the algorithm for decoding AGTG codes.
- We further investigate the zeros of the polynomial

$$P(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3$$

in the case of characteristic 2.

Further Questions

Can we develop efficient way to find the zero of

$$Q(x) = x^{q_0^v+1} + a_1 x^{q_0^v} + a_2 x + a_3$$

for general characteristics $p > 2$?

Selected References

Gabidulin, E.M. (1985)

Theory of codes with maximum rank distance

Problemy Peredachi Informatsii 21(01), 03 – 16.

Helleseth, T. & Kholosha, A. (2010)

$x^{2^l} + 1 + x + a$ and related affine polynomials over $GF(2^k)$

Cryptography and Communications 2(01), 85 – 109.

Otal, K. & Özbudak, F. (2017)

Additive Rank metric Codes

IEEE Trans. on Information Theory 63(01), 164 – 168.

Randrianarisoa, T.H. (2017)

A Decoding Algorithm for Rank Metric Codes

CoRR abs/1712.07060.

Selected References

Richter, G. & Plass, S. (2004)

Fast decoding of rank-codes with rank errors and column erasures

International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings., 398 – 404.

Sheekey, J. (2016)

A new family of linear maximum rank distance codes

Advances in Mathematics of Communications 10, 475 – 488.

Sidorenko, V ;Richter, G ; Bossert, M(2011)

Linearized Shift-Register Synthesis

IEEE Transactions on Information Theory 57 (9), 6025 - 6032.

Thanks for YOUR attention!