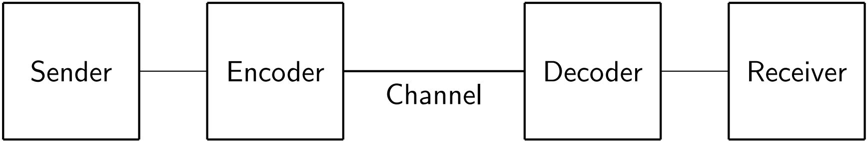
Rank Metric in Coding Theory

Sven Müelich

Institute of Communications Engineering, Ulm University, Germany

Köln, September 9-11, 2015

What is Coding Theory?



(5,2,3)	(3,0,6,5,6)	(3,0,6,1,6)	(5,2,3)
information	codeword	received word	information
$\mathbf{v}$	$\mathbf{c}$	$\mathbf{r}$	$\mathbf{v}$
length k	length n	length n	length k

What is Coding Theory?

Example: Code over $\mathbb{F}_7$

$$\begin{array}{rrl} & \mathbf{c} = & (3,0,6,5,6) \\ + & \mathbf{e} = & (0,0,0,3,0) \\ \hline & \mathbf{r} = & (3,0,6,1,6) \end{array}$$

$$\boldsymbol{\varepsilon} = \{i : e_i \neq 0\} = \{4\}$$

What is Coding Theory?

Parity Check Matrix H

$$\mathbf{H}\mathbf{r} = 0 \Leftrightarrow \mathbf{r} \in \mathcal{C}$$

$$\mathbf{H}\mathbf{r} = \mathbf{H}(\mathbf{c} + \mathbf{e}) = \mathbf{H}\mathbf{c} + \mathbf{H}\mathbf{e} = 0 + \mathbf{H}\mathbf{e} = \mathbf{H}\mathbf{e}$$

- **Coding Theory**

$$\begin{aligned} \text{minimize} \quad & ||\mathbf{e}'|| \\ \text{subject to} \quad & \mathbf{H}\mathbf{e}' = \mathbf{H}\mathbf{e} \end{aligned}$$

  - $\mathbf{H}$ Parity Check Matrix
  - $\mathbf{e}$ Error

- **Machine Learning**

$$\begin{aligned} \text{minimize} \quad & ||\mathbf{x}'|| \\ \text{subject to} \quad & \mathbf{A}\mathbf{x}' = \mathbf{A}\mathbf{x} \end{aligned}$$

  - $\mathbf{A}$ Sensing Matrix
  - $\mathbf{x}$ Unknown Signal

Outline

1. Hamming Metric
   - Reed-Solomon Codes
   - Interleaved Reed-Solomon Codes

2. Rank Metric
   - Gabidulin Codes (Finite Field Case)
   - Gabidulin Codes (Characteristic Zero Case)

Hamming Metric: Definition

Given:

- Finite alphabet $\mathbb{F}$
- $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}^n$, $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}^n$

Hamming weight:

- $wt(\mathbf{u}) = |\{i : u_i \neq 0\}|$

Hamming distance:

- $d(\mathbf{u}, \mathbf{v}) = |\{i : u_i \neq v_i\}| = wt(\mathbf{u} - \mathbf{v})$

Example:

- $\mathbf{u} = (1, 1, 1, 1)$, $wt(\mathbf{u}) = 4$
- $\mathbf{v} = (1, 0, 1, 0)$, $wt(\mathbf{v}) = 2$
- $d(\mathbf{u}, \mathbf{v}) = 2$

Hamming Metric: Definition

Given:

- Finite alphabet $\mathbb{F}$
- $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}^n$, $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}^n$

Hamming weight:

- $wt(\mathbf{u}) = |\{i : u_i \neq 0\}|$

Hamming distance:

- $d(\mathbf{u}, \mathbf{v}) = |\{i : u_i \neq v_i\}| = wt(\mathbf{u} - \mathbf{v})$

Hamming distance is metric:

- $d(\mathbf{u}, \mathbf{v}) \geq 0$ and $d(\mathbf{u}, \mathbf{v}) = 0 \Leftrightarrow \mathbf{u} = \mathbf{v}$
- $d(\mathbf{u}, \mathbf{v}) = d(\mathbf{v}, \mathbf{u})$
- $d(\mathbf{u}, \mathbf{v}) \leq d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$

Hamming Metric: Reed-Solomon Codes

Preparation:

- Finite field $\mathbb{F}$
- $\alpha_1, \ldots, \alpha_n \in \mathbb{F}, \forall i \neq j : \alpha_i \neq \alpha_j \ (\alpha_i \neq 0)$
- $\beta_1, \ldots, \beta_n \in \mathbb{F} \setminus \{0\}$

Example: $n = 5$

- $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- $\alpha_1 = 3$
- $\alpha_2 = \alpha_1^2 = 3^2 = 9 \equiv 2 \mod 7$
- $\alpha_3 = \alpha_1^3 = 3^3 = 27 \equiv 6 \mod 7$
- $\alpha_4 = \alpha_1^4 = 3^4 = 81 \equiv 4 \mod 7$
- $\alpha_5 = \alpha_1^5 = 3^5 = 243 \equiv 5 \mod 7$
- $\beta_1 = \beta_2 = \beta_3 = \beta_4 = \beta_5 = 1$

Hamming Metric: Reed-Solomon Codes

Evaluation Code:

- $f \in \mathbb{F}[x]$ with $deg(f) < k$
- $RS[n,k] = \{(\beta_1 f(\alpha_1), \ldots, \beta_n f(\alpha_n)) \in \mathbb{F}^n\}$
- $[n,k,d]$-code with $d = n - k + 1$ (MDS code)
- Error detection capability:

$$d - 1$$

- Error correction capability:

$$\left\lfloor \frac{d-1}{2} \right\rfloor$$

Hamming Metric: Reed-Solomon Codes

Encoding:

- Information $\mathbf{v} = (v_1, \ldots, v_k) \in \mathbb{F}^k$
- Associated Polynomial

$$f(x) = \sum_{i=0}^{k-1} v_{i+1} x^i = v_1 + v_2 x + v_3 x^2 + \cdots + v_k x^{k-1}$$

- Codeword $\mathbf{c} = (\beta_1 f(\alpha_1), \ldots, \beta_n f(\alpha_n))$

Example:

- Information $\mathbf{v} = (5, 2, 3) \in \mathbb{F}_7^3$
- Associated Polynomial $f(x) = 5 + 2x + 3x^2$
- Codeword $\mathbf{c} = (f(3), f(2), f(6), f(4), f(5)) = (3, 0, 6, 5, 6)$

Hamming Metric: Reed-Solomon Codes

Decoding:

3 steps:

- Interpolation
  - Find interpolation polynomial $r(x)$ with $r(\alpha_i) = r_i$
- Solve Key Equation
- Retrieve information polynomial

Hamming Metric: Reed-Solomon Codes

Decoding:

Components of the key equation:

- Error locator polynomial

$$\Lambda(x) = \prod_{i \in \varepsilon} (x - \alpha_i)$$

- Polynomial with code locators as roots

$$G(x) = \prod_{i=1}^{n} (x - \alpha_i)$$

- Interpolation polynomial $r(x)$ with $r(\alpha_i) = r_i$
- Information polynomial $f(x)$

Hamming Metric: Reed-Solomon Codes

Decoding:

Gao Key Equation

$\Lambda(x)r(x) \equiv \Omega(x) \mod G(x)$
Additional requirement: $deg(\lambda) + (k-1) \geq deg(\psi)$

- Where:
  - $\Omega(x) = \Lambda(x)f(x)$
  - λ some solution for Λ
  - ψ some solution for Ω
- Given:
  - Interpolation polynomial $r(x)$ with $r(\alpha_i) = r_i$
  - $G(x) = \prod_{i=1}^{n}(x - \alpha_i)$
- What we want:
  - $\Lambda(x) = \prod_{i\in\varepsilon}(x - \alpha_i)$

Hamming Metric: Reed-Solomon Codes

Gao Key Equation

$\Lambda(x)r(x) \equiv \Omega(x) \mod G(x)$
Additional requirement: $deg(\lambda) + (k-1) \geq deg(\psi)$

Proof:

- We use the following Theorem:
  - $f, h \in \mathbb{F}[x]$, $G \in \mathbb{F}[x]$
  - $(f \equiv h \mod G) \iff (G(\alpha) = 0 \Rightarrow f(\alpha) = h(\alpha))$
- We show that $\Lambda(x)r(x)$ and $\Lambda(x)f(x)$ evaluate the same for all roots of G:
  - Case 1: $e_i \neq 0$
    $\Lambda(\alpha_i) = 0 \Rightarrow \Lambda(x)r(x) = 0$ and $\Lambda(x)f(x) = 0$
  - Case 2: $e_i = 0$
    $r(\alpha_i) = f(\alpha_i) = c_i \Rightarrow \Lambda(x)c_i = \Lambda(x)c_i$

Hamming Metric: Reed-Solomon Codes

Gao Key Equation

$\Lambda(x)r(x) \equiv \Omega(x) \mod G(x)$

Additional requirement: $deg(\lambda) + (k-1) \geq deg(\psi)$

Example:

- **c** = (3,0,6,5,6), **r** = (3,0,6,1,6)
- Solve key equation with any decoding algorithm (blackbox)
- Decoding algorithm gives us:
  - $\lambda(x) = 5x + 1$
  - $\psi(x) = x^3 + 6x^2 + 6x + 5$
- Because the RHS of Gao's key equation has the structure $\psi = \lambda f$, we have:
  - $f(x) = \frac{\psi(x)}{\lambda(x)} = 5 + 2x + 3x^2$
  - $v = (5, 2, 3)$

Hamming Metric: Interleaved RS Codes

- $\mathcal{C}_1, \ldots, \mathcal{C}_s$ (not necessarily distinct) Reed-Solomon Codes of length n and dimensions $k_1, \ldots, k_s$
- $IRS[s; n, k_1, \ldots, k_s] = \left\{ \mathbf{c} = \begin{pmatrix} \mathbf{c_1} \\ \vdots \\ \mathbf{c_s} \end{pmatrix} : \mathbf{c_i} \in \mathcal{C}_i, i = 1, \ldots, s \right\}$
- Encoding: Encoding of s simple Reed-Solomon codes
- Decoding: Decode every codeword separately or use key equation for IRS-codes
- Note: RS codes are special case of IRS codes with $s = 1$

Hamming Metric: IRS Codes

Decoding:

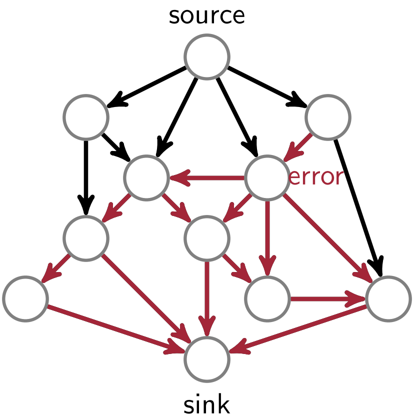
Key Equation

$\Lambda(x) r_t(x) \equiv \Lambda(x) f_t(x) \mod G(x)$
Additional requirements: $deg(\lambda) + (k_t - 1) \geq deg(\psi_i)$

- Where:
  - λ a solution for Λ
  - ψ_t a solution for Λf_t
- Given:
  - $r_t(x)$ (interpolation polynomials with $r_t(\alpha_i) = r_{t_i}$)
  - $G(x) = \prod_{i=1}^{n} (x - \alpha_i)$
- What we want:
  - $\Lambda(x) = \prod_{i \in \varepsilon} (x - \alpha_i)$

Rank Metric: Motivation

Random Linear Network Coding



Rank Metric: Preparation

Field extension: $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^m}$

$$\mathbf{A} = ext(\mathbf{a}), \quad \mathbf{a} = ext^{-1}(\mathbf{A})$$

Rank Metric: Definition

$$\mathbf{a} = (a_0, a_1 \ldots, a_{n-1}),\ \mathbf{b} = (b_0, b_1 \ldots, b_{n-1}) \in \mathbb{F}_{q^m}^n$$

Rank weight:

$$wt_{rk}(\mathbf{a}) := rank(ext(\mathbf{a})) = rank(\mathbf{A})$$

Rank distance:

$$d_{rk}(\mathbf{a}, \mathbf{b}) := wt_{rk}(\mathbf{a}-\mathbf{b}) = rank(ext(\mathbf{a})-ext(\mathbf{b})) = rank(\mathbf{A}-\mathbf{B})$$

Rank distance is metric

- $rank(\mathbf{A}-\mathbf{B}) \geq 0$ and $rank(\mathbf{A}-\mathbf{B}) = 0 \Leftrightarrow \mathbf{A} = \mathbf{B}$
- $rank(\mathbf{A}-\mathbf{B}) = rank(\mathbf{B}-\mathbf{A})$
- $rank(\mathbf{A}-\mathbf{C}) \leq rank(\mathbf{A}-\mathbf{B}) + rank(\mathbf{B}-\mathbf{C})$

Rank Metric: Gabidulin Codes (Finite Fields)

NACHRICHTENTECHNIK Universität Ulm

Linearized Polynomials:

- $$a(x) = \sum_{i=0}^{n} a_i x^{q^i} = a_0 x^{q^0} + a_1 x^{q^1} + a_2 x^{q^2} + \cdots + a_n x^{q^n}$$
- $a_i \in \mathbb{F}_{q^m}$
- $deg_q(a(x)) = max\{i : a_i \neq 0\}$

Rank Metric: Gabidulin Codes (Finite Fields)

$$a(x) = \sum_{i=0}^{n} a_i x^{q^i} = a_0 x^{q^0} + a_1 x^{q^1} + a_2 x^{q^2} + \cdots + a_n x^{q^n}$$

Operations on linearized polynomials:

- Addition: componentwise
- Multiplication: $a(x) \otimes b(x) = a(b(x))$
- Evaluation for Element v:

$$a(v) = \sum_{i=0}^{n} a_i v^{q^i}$$

Rank Metric: Gabidulin Codes (Finite Fields)

$$a(x) = \sum_{i=0}^{n} a_i x^{q^i} = a_0 x^{q^0} + a_1 x^{q^1} + a_2 x^{q^2} + \cdots + a_n x^{q^n}$$

Properties of linearized polynomials:

- Non-commutative ring
- $deg_q(a) = log_q(deg(a))$
- $a(\lambda x + \mu y) = \lambda a(x) + \mu a(y)$ for $\lambda, \mu \in \mathbb{F}_q$, $x, y \in \mathbb{F}_{q^m}$
- Roots of linearized polynomials are subspace of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$

Rank Metric: Gabidulin Codes (Finite Fields)

Gabidulin Codes:

- Delsarte (1978), Gabidulin (1985), Roth (1991)

Definition:

- Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$, linearly independent over F_q
-

$$Gab[n,k] = \{ \ (f(g_1), \ldots, f(g_n)) \in \mathbb{F}_{q^m}^n : deg_q(f) < \ k \ \}$$

Recall Reed Solomon Codes:

- $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$, all nonzero and $\alpha_i \neq \alpha_j$
- $RS = \{(f(\alpha_1), \ldots, f(\alpha_n)) \in \mathbb{F}_q^n : deg(f) < k\}$

Rank Metric: Gabidulin Codes (Finite Fields)

Minimal Subspace Polynomial:

- $\mathcal{G} = \{g_1, \ldots, g_n\}$
-

$$M_{\mathcal{G}} = \prod_{\alpha \in \langle \mathcal{G} \rangle} (x - \alpha)$$

- Equivalence modulo Minimal Subspace Polynomial

$$(\forall u \in \mathbb{F}_{q^m} : M_{\mathcal{G}}(u) = 0 \Rightarrow f(u) = g(u)) \Rightarrow f \equiv g \mod M_{\mathcal{G}}$$

Rank Metric: Gabidulin Codes (Finite Fields)

Error Span Polynomial

$$\mathbf{E} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \longrightarrow \mathbf{E}^{m\times n} = \mathbf{A}^{m\times t} \cdot \mathbf{B}^{t\times n}$$

$$\operatorname{rank}(\mathbf{E}) = \operatorname{rank}(\mathbf{A}) = \operatorname{rank}(\mathbf{B}) = t$$

$$\mathbf{e} = ext^{-1}(\mathbf{AB}) = ext^{-1}(\mathbf{A})\mathbf{B} = \mathbf{aB}$$

$$\mathbf{a} = (a_1, \ldots, a_t)$$

$$\Lambda(x) = M_{\langle a \rangle} = M_{\langle a_1, \cdots, a_t \rangle} = \prod_{\alpha \in \langle a \rangle} (x - \alpha)$$

Rank Metric: Gabidulin Codes (Finite Fields)

Interpolation

- $\mathcal{G} = \{g_1, \ldots, g_n\}$
- Received word $r = (r_1, \ldots, r_n)$
- $L_i(x) = M_{\mathcal{G} \setminus g_i}$

$$\hat{r} = \sum_{i=1}^{n} r_i \frac{L_i(x)}{L_i(g_i)}$$

- $\hat{r}(g_i) = r_i$ as

$$\frac{L_i(g_j)}{L_i(g_i)} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else} \end{cases}$$

Rank Metric: Gabidulin Codes (Finite Fields)

Gao-like Key Equation

$$\Lambda(\hat{r}(x) - f(x)) \equiv 0 \mod M_{\mathcal{G}}$$

Proof: LHS and RHS evaluate the same for all roots of $M_{\mathcal{G}}$

$$\Lambda\left(\hat{r}\left(\sum_{i=1}^{n} Я_i g_i\right) - f\left(\sum_{i=1}^{n} Я_i g_i\right)\right) = \Lambda\left(\sum_{i=1}^{n} Я_i \hat{r}(g_i) - \sum_{i=1}^{n} Я_i f(g_i)\right)$$

$$= \sum_{i=1}^{n} Я_i \Lambda(\hat{r}(g_i) - f(g_i)) = \sum_{i=1}^{n} Я_i \Lambda(r_i - c_i)$$

$$= \sum_{i=1}^{n} Я_i \Lambda(e_i) = \sum_{i=1}^{n} Я_i \Lambda\left(\sum_{j=1}^{t} B_{j,i} a_j\right)$$

$$= \sum_{i=1}^{n} Я_i \Lambda(B_{1,i} a_1 + \ldots B_{t,i} a_t)$$

Rank Metric: Gabidulin Codes (Finite Fields)

Transformed Gao-like Key Equation

$\Lambda(\hat{r}(x)) \equiv \Lambda(f(x)) \mod M_{\mathcal{G}}$

Additional requirement: $deg_q(\lambda) + (k-1) \geq deg_q(\psi_i)$

Proof: LHS and RHS evaluate the same for all roots of $M_{\mathcal{G}}$

$$\Lambda\left(\hat{r}\left(\sum_{i=1}^{n} Я_i g_i\right)\right) \equiv \Lambda\left(f\left(\sum_{i=1}^{n} Я_i g_i\right)\right) \mod M_{\mathcal{G}}$$

$$\Lambda\left(\sum_{i=1}^{n} Я_i \hat{r}(g_i)\right) \equiv \Lambda\left(\sum_{i=1}^{n} Я_i f(g_i)\right) \mod M_{\mathcal{G}}$$

$$\sum_{i=1}^{n} Я_i \Lambda(\hat{r}(g_i)) \equiv \sum_{i=1}^{n} Я_i \Lambda(f(g_i)) \mod M_{\mathcal{G}}$$

Rank Metric: Gabidulin Codes (Finite Fields)

Transformed Gao-like Key Equation

$\Lambda(\hat{r}(x)) \equiv \Lambda(f(x)) \mod M_{\mathcal{G}}$

Additional requirement: $deg_q(\lambda) + (k-1) \geq deg_q(\psi_i)$

Proof (cont'd):

- We show that $\Lambda(x)(\hat{r}(x))$ and $\Lambda(x)(f(x))$ evaluate the same for all g_i's:
  - Case 1: $e_i = 0$

    $$\Lambda(f(g_i)) = \Lambda(c_i) = \Lambda(r_i) = \Lambda(\hat{r}(g_i))$$

  - Case 2: $e_i \neq 0$

    $$\Lambda(\hat{r}(g_i)) = \Lambda(r_i) = \Lambda(c_i + e_i) = \Lambda\left(c_i + \sum_{j=1}^{t} B_{i,j} a_j\right)$$

    $$= \Lambda(c_i) + \Lambda\left(\sum_{j=1}^{t} B_{j,i} \Lambda(a_j)\right) = \Lambda(c_i) = \Lambda(f(g_i))$$

Rank Metric: Gabidulin Codes (Finite Fields)

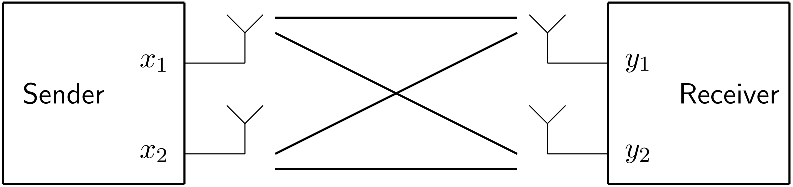
Retrieving the information polynomial

$$\lambda^{-1} \cdot \psi = \lambda^{-1} \cdot \Lambda f = \lambda^{-1} \cdot \lambda \cdot f = f$$

Rank Metric: Gabidulin Codes (Char. Zero)

Motivation: Space-Time Coding

- Improve reliability of MIMO systems



$$y_1 = h_{11}x_1 + h_{12}x_2 + n_1$$
$$y_2 = h_{21}x_1 + h_{22}x_2 + n_2$$

Rank Metric: Gabidulin Codes (Char. Zero)

Characteristic Zero Case:

- Algebraic Field extension $\mathbb{K} \hookrightarrow \mathbb{L}$ of finite degree m
- **Automorphism:** $\theta \in Gal(\mathbb{K} \hookrightarrow \mathbb{L})$ of order $n \leq Gal(\mathbb{K} \hookrightarrow \mathbb{L})$
- θ-**Polynomials:**

$$P(x) = \sum_{i=0}^{n} a_i \theta^i(x) = a_0 \theta^0(x) + a_1 \theta^1(x) + \cdots + a_n \theta^n(x)$$

- $a_i \in \mathbb{L}$
- $deg_\theta(P(x)) = max\{i : a_i \neq 0\}$

Rank Metric: Gabidulin Codes (Char. Zero)

$$P(x) = \sum_{i=0}^{n} a_i \theta^i(x) = a_0\theta^0(x) + a_1\theta^1(x) + \cdots + a_n\theta^n(x)$$

Operations on θ-polynomials:

$$A = \sum_{i=0}^{n} a_i \theta^i(x), \quad B = \sum_{j=0}^{m} b_j \theta^j(x)$$

$$A + B = \sum_{i=0}^{max\{n,m\}} (a_i + b_i)\theta^i(x)$$

$$A \cdot B = \sum_{i,j} a_i \theta^i(b_j)\theta^{i+j}(x) = A(B(X))$$

Rank Metric: Gabidulin Codes (Char. Zero)

$$P(x) = \sum_{i=0}^{n} a_i \theta^i(x) = a_0\theta^0(x) + a_1\theta^1(x) + \cdots + a_n\theta^n(x)$$

Properties of θ-Polynomials:

- non-commutative integral domain with unit $\theta^0(x) = 1$
- Also left and right euclidean ring
- Let $A, B \in L[X;\theta]$, $a, b \in L$, $\lambda, \mu \in K$
  - $A(\lambda a + b) = \lambda A(a) + A(b)$
  - $(AB)(a) = A(B(a))$
  - $\theta^i(\lambda a + \mu b) = \lambda\theta^i(a) + \mu\theta^i(b)$

Rank Metric: Gabidulin Codes (Char. Zero)

Linearized Polynomials as a special case of θ-polynomials:

- $\theta : \mathbb{L} \longrightarrow \mathbb{L}$
- $x \longmapsto x^q$
- $\theta(x) = x^q$
- $\theta^2(x) = (x^q)^q = x^{q \cdot q} = x^{q^2}$
- $\theta^3(x) = ((x^q)^q)^q = x^{q^3}$
- $\dots$
- $$\begin{aligned} P(x) &= \textstyle\sum_{i=0}^{n} a_i \theta^i(x) \\ &= a_0\theta^0(x) + a_1\theta^1(x) + a_2\theta^2(x) + \dots + a_n\theta^n(x) \\ &= a_0 x^{q^0} + a_1 x^{q^1} + a_2 x^{q^2} + \dots + a_n x^{q^n} \end{aligned}$$

Rank Metric: Gabidulin Codes (Char. Zero)

Finding a Key-Equation for the Characteristic Zero case:

- Minimal Subspace Polynomial
- Modulo Equivalence
- Interpolation Polynomial
- Error Span Polynomial Λ
- Key Equation

Rank Metric: Gabidulin Codes (Char. Zero)

Minimal Subspace Polynomial[1]:

- $V = \langle v_1 \rangle$, $dim(V) = 1$ where $v_1 \neq 0$

$$M_V(x) = \theta^1(x) - \frac{\theta(v_1)}{v_1}\theta^0(x)$$

- Create such a polynomial
  - for $V = \{v_1, \ldots, v_{i+1}\}$ of dimension $i+1$
  - assuming that we have already one for vectorspace $V' = \{v_1, \ldots, v_i\}$ of dimension i:

$$M_V(x) = \left(\theta^1(x) - \frac{\theta(M_{V'}(v_{i+1}))}{M_{V'}(v_{i+1})}\theta^0(x)\right) \cdot M_{V'}(x).$$

[1] Daniel Augot (INRIA), Pierre Loidreau, Gwezheneg Robert (Univ. Rennes)

Rank Metric: Gabidulin Codes (Char. Zero)

Modulo Equivalence:

- Let f,g, $M_{\mathcal{U}} \in \mathcal{L}[x;\theta]$ with $M_{\mathcal{U}}$ being some minimal subspace polynomial over $\mathcal{U}$.
- If ∀u $\in \mathcal{U}$ $f(u) = g(u)$ and $M_{\mathcal{U}}(u) = 0$, it holds, that $f \equiv g \mod M_{\mathcal{U}}$.

Rank Metric: Gabidulin Codes (Char. Zero)

Interpolation Polynomial[2]:

Given:

- $\mathcal{G} = \{g_1, \ldots, g_n\}$ code locators of some Gabidulin code
- $r = (r_1, \ldots, r_n) \in L^n$ the received word.

There exists a unique monic θ-polynomial $\hat{r}$ of degree $n-1$ such that $\hat{r}(g_i) = r_i$:

$$\hat{r} = \sum_{i=1}^{n} r_i \frac{M_V(x)}{M_{V'}(g_i)} \tag{1}$$

[2] Daniel Augot (INRIA), Pierre Loidreau, Gwezheneg Robert (Univ. Rennes)

Rank Metric: Gabidulin Codes (Char. Zero)

Error Span Polynomial Λ:

- Full rank decomposition of matrices holds for arbitrary fields
- We can use the error span polynomial of the finite field case directly

$$\Lambda(x) = M_{\langle a \rangle} = M_{\langle a_1, \cdots, a_t \rangle} = \prod_{\alpha \in \langle a \rangle} (x - \alpha)$$

Rank Metric: Gabidulin Codes (Char. Zero)

Key Equation:

Gao-like Key Equation (Char. Zero)

$\Lambda(\hat{r}(x) - f(x)) \equiv 0 \mod M_{\mathcal{G}}$

Transformed Gao-like Key Equation

$\Lambda(\hat{r}(x)) \equiv \Lambda(f(x)) \mod M_{\mathcal{G}}$
Additional requirement: $deg_{\theta}(\lambda) + (k-1) \geq deg_{\theta}(\psi_i)$

Proof: analogue to finite field case

Acknowledgments

- David Mödinger
- Sven Puchinger
- Martin Bossert