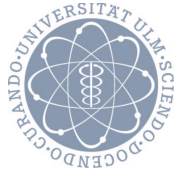


ulm university universität ulm

An Alternative Decoding Method for Gabidulin Codes in Characteristic Zero

Sven Müelich, Sven Puchinger, David Mödinger, Martin Bossert

Institute of Communications Engineering, Ulm University, Germany

IEEE International Symposium on Information Theory (ISIT)
Barcelona, July 10-15, 2016

Outline

Compressed Sensing

$$\boldsymbol{b} = \boldsymbol{A}\boldsymbol{x},$$

- $\boldsymbol{b} \in \mathbb{C}^m$ (known)
- $\boldsymbol{A} \in \mathbb{C}^{m \times n}$ (known)
- $\boldsymbol{x} \in \mathbb{C}^n$ sparse (unknown)

$(n \ll m)$

LRMR

$$\boldsymbol{b} = \mathcal{A}(\boldsymbol{X}),$$

- $\boldsymbol{b} \in \mathbb{C}^p$ (known)
- $\mathcal{A} : \mathbb{C}^{m \times n} \to \mathbb{C}^p$ linear (known)
- $\boldsymbol{X} \in \mathbb{C}^{m \times n}$ low rank (unknown)

$(p \ll n \cdot m)$

Hamming Metric Coding Problem

$$\boldsymbol{s} = \boldsymbol{H}(\boldsymbol{c} + \boldsymbol{e}) = \boldsymbol{H}\boldsymbol{e}$$

- $\boldsymbol{s} \in K^{n-k}$ syndrome (known)
- $\boldsymbol{H} \in K^{n-k \times n}$ pc matrix (known)
- $\boldsymbol{c} \in K^n$ codeword (unknown)
- $\boldsymbol{e} \in K^n$, $\mathrm{wt}_{\mathrm{H}}(\boldsymbol{e})$ small (unknown)

Rank Metric Coding Problem

$$\boldsymbol{s} = \boldsymbol{H}(\boldsymbol{c} + \boldsymbol{e}) = \boldsymbol{H}\boldsymbol{e}$$

- $\boldsymbol{s} \in L^{n-k}$ syndrome (known)
- $\boldsymbol{H} \in L^{n-k \times n}$ pc matrix (known)
- $\boldsymbol{c} \in L^n$ codeword (unknown)
- $\boldsymbol{e} \in L^n$, $\mathrm{wt}_{\mathrm{R}}(\boldsymbol{e})$ small (unknown)

$(L^n \simeq K^{m \times n})$

L/K Galois extension (i.e. normal and separable), $[L : K] =: m$

Galois group

$$\mathrm{Gal}\,(L/K) = \{\theta : L \to L \text{ automorphism s.t. } \theta(x) = x \ \forall x \in K\}$$

Assumption: $\mathrm{Gal}\,(L/K)$ is cyclic, θ generator

θ-Polynomials

L/K Galois extension, $\theta \in \mathrm{Gal}\,(L/K)$.

$$L[x;\theta] = \left\{ a = \sum_{i=0}^{d} a_i x^i \;:\; a_i \in L, d \in \mathbb{N} \right\}$$

Addition $(+)$ $\quad a + b = \sum_i (a_i + b_i) x^i$

Multiplication $(\cdot)$ $\quad a \cdot b = \sum_i \Big(\sum_{j=0}^{i} a_j \theta^j (b_{i-j}) \Big) x^i$ (non-commutative)

Generalization of Linearized Polynomials

- Isomorphic to linearized polynomials in case $\mathbb{F}_{q^m}/\mathbb{F}_q$, $\theta = \cdot^q$

Evaluation $\quad a(\cdot) := \mathrm{ev}_a : \ L \to L, \ \alpha \mapsto \sum_i a_i \theta^i(\alpha)$

Degree $\quad \deg a = \max\{i \ : \ a_i \neq 0\} \quad (\max \emptyset := -\infty)$

Properties

- $(a \cdot b)(\alpha) = a(b(\alpha))$
- $\deg(a \cdot b) = \deg a + \deg b$
- Roots of a are subspace[1] of L
- $a(\cdot) : \ L \to L$ is an K-linear map

[1] L is a K-vectorspace of dimension $[L : K]$

Theorem (Augot, Loidreau, Robert)

If $\mathrm{Gal}\,(L/K)$ is cyclic and θ generator

$$\dim \ker(a) \leq \deg a$$

Annihilator Polynomial

Subspace $\mathcal{U} \subseteq L \Rightarrow \exists$ monic $\mathcal{A}_\mathcal{U} \in L[x;\theta]$ of minimal degree:

$$\mathcal{A}_\mathcal{U}(u) = 0 \quad \forall u \in \mathcal{U}$$

Interpolation Polynomial

$x_1, \ldots, x_\ell \in L$, linearly independent over K. $y_1, \ldots, y_\ell \in L$ arbitrary.
Then, $\exists\, \mathcal{I} \in L[x;\theta]$ of minimal degree:

$$\mathcal{I}(x_i) = y_i \quad \forall i = 1, \ldots, \ell$$

Theorem *(Augot, Loidreau, Robert)*

If $\mathrm{Gal}\,(L/K)$ is cyclic and θ generator,

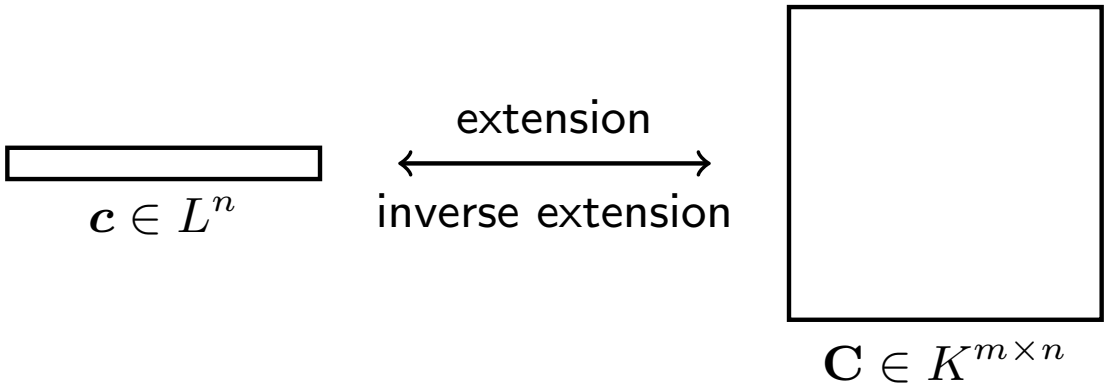
$$\deg \mathcal{A}_\mathcal{U} = \dim \mathcal{U} \quad \text{(in general: } \deg \mathcal{A}_\mathcal{U} \leq \dim \mathcal{U}\text{)}$$
$$\deg \mathcal{I} < \ell \quad \text{(and } \mathcal{I} \text{ is unique)}$$

L/K Galois extension, $\theta \in \mathrm{Gal}\,(L/K)$ generator.

Definition

$g_1, \ldots, g_n \in L$, linearly independent over K, $k \leq n \leq m = [L : K]$

$$\mathcal{C}_{\mathrm{G}}[n,k] = \left\{ \boldsymbol{c} = \left[f(g_1), \ldots, f(g_n) \right] : f \in L[x;\theta] \wedge \deg f < k \right\} \subseteq L^n$$



Rank Metric: $\mathrm{wt_R}(\boldsymbol{c}) = \mathrm{rank}(\mathbf{C}), \quad \mathrm{d_R}(\boldsymbol{c}_1, \boldsymbol{c}_2) = \mathrm{rank}(\mathbf{C}_1 - \mathbf{C}_2)$

Theorem *(Augot, Loidreau, Robert)*

Minimum rank distance $d = \min_{\boldsymbol{c}_1 \neq \boldsymbol{c}_2} \mathrm{d_R}(\boldsymbol{c}_1, \boldsymbol{c}_2) = n - k + 1$ (MRD)

Decoding: Augot, Loidreau, Robert (2013): $O(n^3)$
Müelich, Puchinger, Mödinger, Bossert (2016): $O(n^2)$

Error Model

- $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} \in L^n$, with $\mathrm{wt_R}(\boldsymbol{e}) =: \tau$

Some Polynomials

- $\Lambda := \mathcal{A}_{\langle e_1,\ldots,e_n\rangle}$ (unknown error span polynomial)
- $\hat{r}$ interpolation polynomial with $\hat{r}(g_i) = r_i \ \forall i$ (known)

Key Equation* *(Müelich, Puchinger, Mödinger, Bossert)*

$$\Lambda\hat{r} \equiv \Lambda f \mod \mathcal{A}_{\langle g_1,\ldots,g_n\rangle}$$

Proof:

$$\begin{aligned}\big(\Lambda \cdot (\hat{r} - f)\big)(g_i) &= \Lambda(\hat{r}(g_i) - f(g_i)) \\ &= \Lambda(r_i - c_i) = \Lambda(e_i) = 0\end{aligned}$$

Thus, $\Lambda \cdot (\hat{r} - f) \equiv 0 \mod \mathcal{A}_{\langle g_1,\ldots,g_n\rangle}$ □

*characteristic zero equivalent to Gao's key equation for finite field Gabidulin codes (Wachter-Zeh)

Key Equation *(Müelich, Puchinger, Mödinger, Bossert)*

$$\Lambda\hat{r} \equiv \Lambda f \mod \mathcal{A}_{\langle g_1,\ldots,g_n\rangle}$$

Linear Shift Register (LSR) Synthesis Problem

Given $\hat{r}, \mathcal{A}_{\langle g_1,\ldots,g_n\rangle}$, find non-zero $(\lambda,\omega) \in L[x;\theta]^2$ with $\deg\lambda$ minimal and

$$\lambda\hat{r} \equiv \omega \mod \mathcal{A}_{\langle g_1,\ldots,g_n\rangle}$$

$$\deg\lambda + k > \deg\omega$$

Theorem *(Müelich, Puchinger, Mödinger, Bossert)*

If $\tau = \mathrm{wt_R}(\boldsymbol{e}) < \frac{d}{2}$, the LSR has a solution (λ,ω) and for some $\alpha \in L$,

$$(\lambda,\omega) = \alpha(\Lambda,\Lambda f)$$

Assumption that θ is generator of $\mathrm{Gal}\,(L/K)$ necessary!

Linear Shift Register (LSR) Synthesis Problem

Given $\hat{r}, \mathcal{A}_{\langle g_1,\ldots,g_n\rangle}$, find non-zero $(\lambda, \omega) \in L[x;\theta]^2$ with $\deg \lambda$ minimal and

$$\lambda \hat{r} \equiv \omega \mod \mathcal{A}_{\langle g_1,\ldots,g_n\rangle}$$

$$\deg \lambda + k > \deg \omega$$

Row reduction ($\boxed{\cdot}$ is leading position = rightmost pos. of max. degree in row)

$$\begin{bmatrix} x^k & \hat{r} \\ 0 & \mathcal{A}_{\langle g_1,\ldots,g_n\rangle} \end{bmatrix} \xrightarrow[\text{operations}]{\text{row}} \begin{bmatrix} \boxed{m_{11} \cdot x^k} & m_{12} \\ m_{21} \cdot x^k & \boxed{m_{22}} \end{bmatrix}$$

$$\overset{(*)}{\Longrightarrow} (\lambda, \omega) = (m_{11}, m_{12})$$

- Similar to the Extended Euclidean Algorithm (EEA)
- Advantage: Coefficient size reduction in intermediate computations

$(*)$ Puchinger, Nielsen, Li, Sidorenko

Decoding Summary

Algorithm: Decode Gabidulin Codes

Input: $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$

Output: f s.t. $\boldsymbol{c} = [f(g_1), \ldots, f(g_n)]$ or "decoding failure".

1 Calculate $\hat{r}$ and $\mathcal{A}_{\langle g_1,\ldots,g_n\rangle}$
2 $(\lambda, \omega) \leftarrow$ Solve LSR with input $\hat{r}$, $\mathcal{A}_{\langle g_1,\ldots,g_n\rangle}$ using row reduction
3 $(\Lambda, \Omega) \leftarrow \alpha^{-1}(\lambda, \omega)$
4 $(\chi, \varrho) \leftarrow$ Right-divide Ω by Λ
5 **if** $\varrho = 0$ **then return** χ
6 **else return** *"decoding failure"*

- If $\mathrm{wt}_{\mathrm{R}}(\boldsymbol{e}) < \frac{d}{2}$, the algorithm finds f
- Complexity/coefficient size growth tradeoff:

	Fast	**"Normal"**	**Small growth**
Operations in L	$O(n^{1.69})$	$O(n^2)$	$O(n^3)$
Row Reduction	EEA [1] or D&Q [2]	PNLS [3]	Fraction-free [4]

[1] Wachter-Zeh 2013
[2] Puchinger, Müelich, Mödinger, Bossert 2016
[3] Puchinger, Nielsen, Li, Sidorenko 2015
[4] Beckermann, Cheng, Labahn 2006

Thank you for your attention!