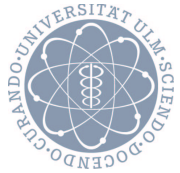


ulm university universität ulm

Low-Rank Matrix Recovery using Gabidulin Codes in Characteristic Zero

Sven Müelich, Sven Puchinger, Martin Bossert

Institute of Communications Engineering, Ulm University, Germany

15^{th} Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT)
Albena, June 18-24, 2016

Outline

Compressed Sensing (Donoho, Candes, Tao 2006)

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

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

$(n \ll m)$

LRMR (Candes, Tao, Recht 2009)

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

- $\boldsymbol{b} \in \mathbb{C}^p$ (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 field 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

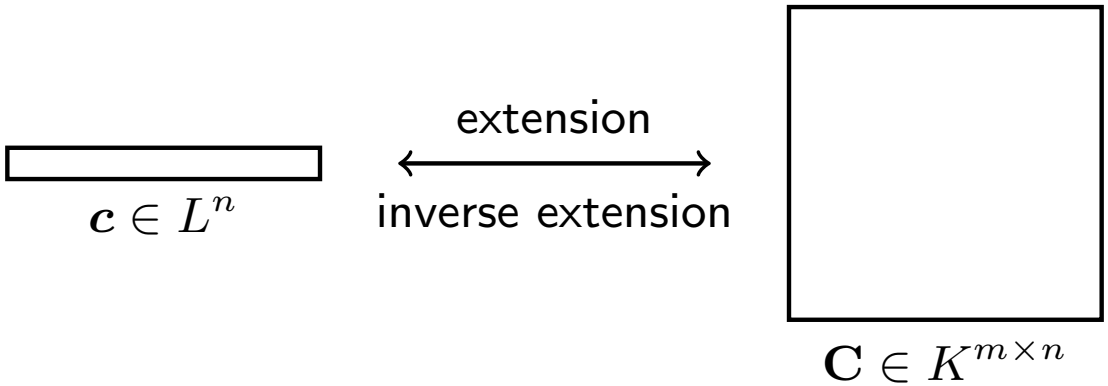
- Isomorphic to linearized polynomials in case $\mathbb{F}_{q^m}/\mathbb{F}_q$, $\theta = \cdot^q$

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

Definition

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

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



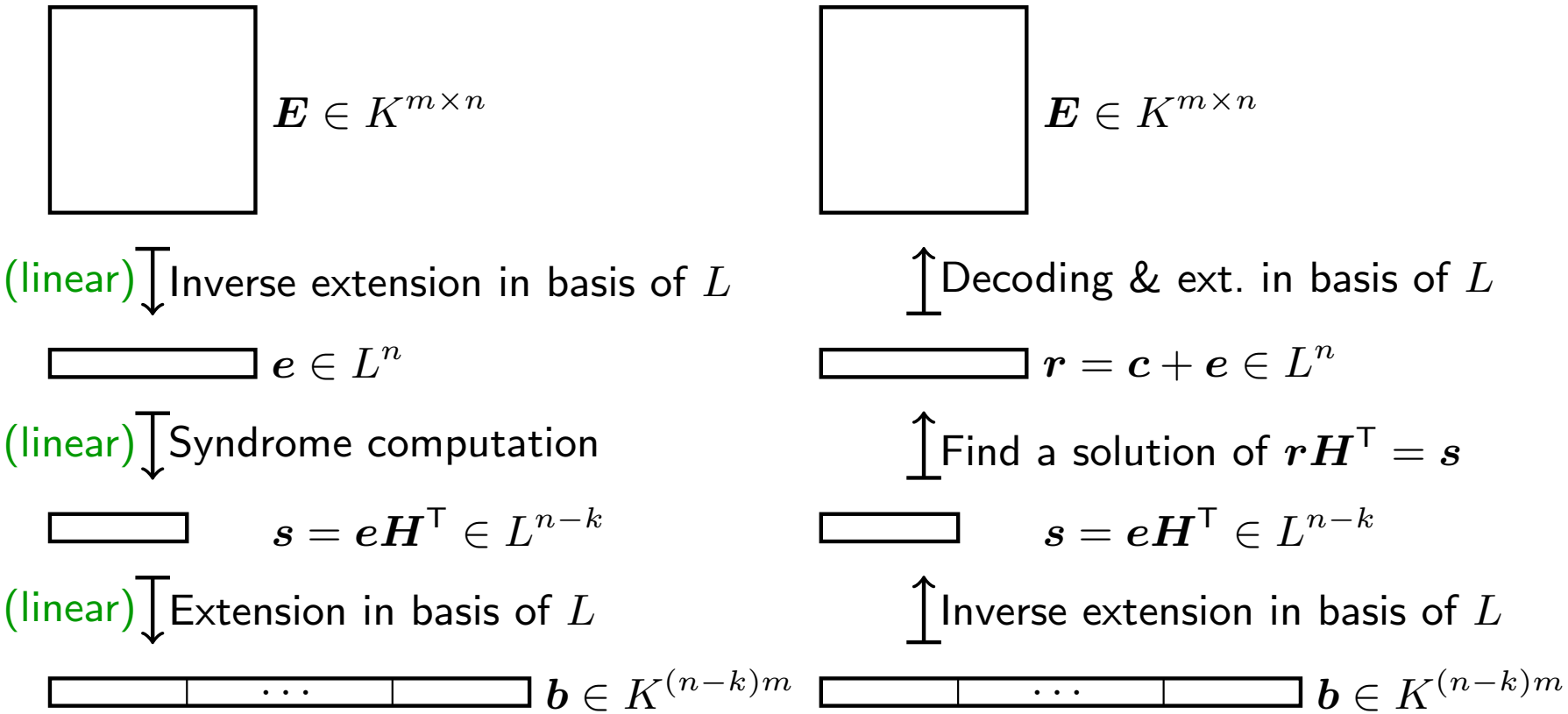
Rank Metric: $\mathrm{wt_R}(\boldsymbol{c}) = \mathrm{rank}(\mathbf{C}), \quad \mathrm{d_R}(\boldsymbol{c}_1, \boldsymbol{c}_2) = \mathrm{rank}(\mathbf{C}_1 - \mathbf{C}_2)$

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): $O(n^2)$

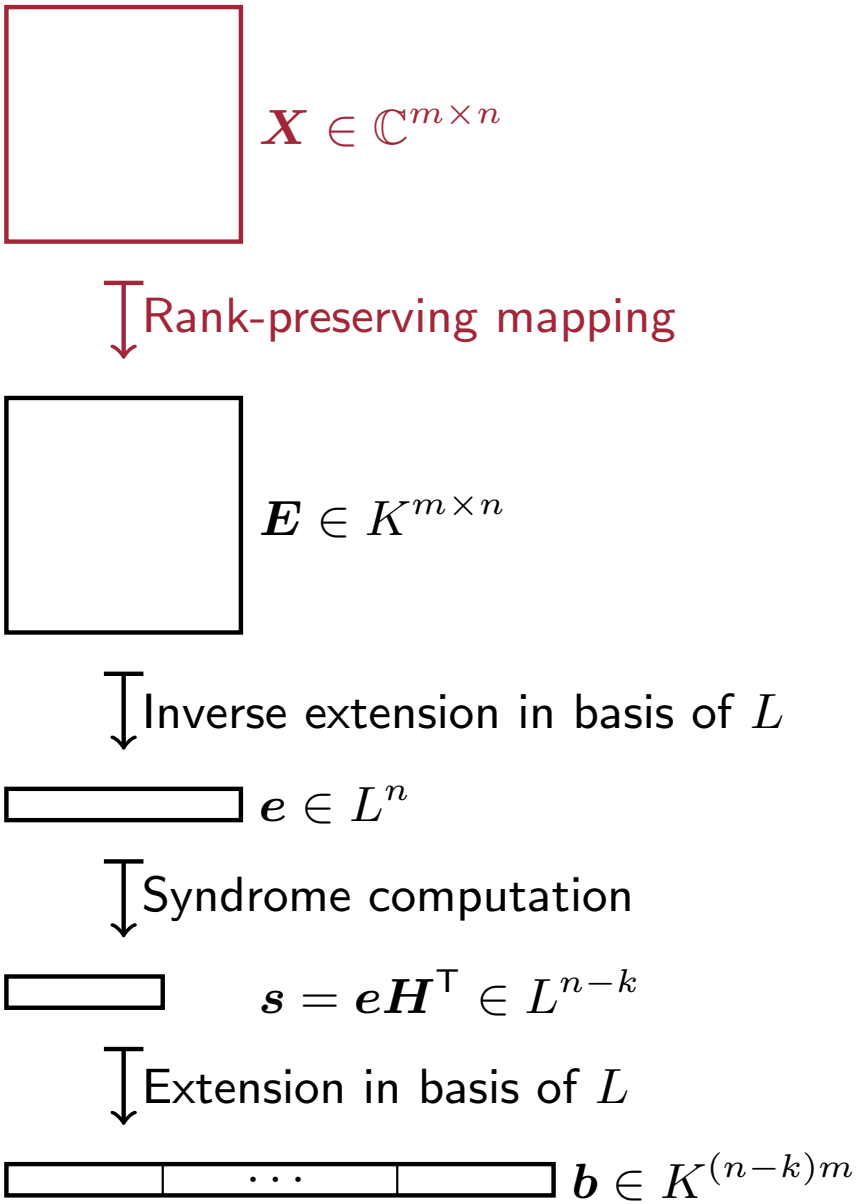
LRMR: New Approach (K-linear map $\mathcal{A} : \mathbb{C}^{m\times n} \to \mathbb{C}^{p}$)



Theorem *Müelich, Puchinger, Bossert*

If $\operatorname{rank}(\boldsymbol{E}) \leq \frac{d-1}{2} = \frac{n-k}{2}$, $\boldsymbol{E}$ can be reconstructed from $\boldsymbol{b} = \mathcal{A}(\boldsymbol{E})$.

LRMR: New Approach (Choice of K and L)



Needed: $K \in \{\mathbb{R}, \mathbb{C}\}$. Possible L:

- $K = \mathbb{R}$: $L \in \{\mathbb{R}, \mathbb{C}\}$ $(m \leq 2)$
- $K = \mathbb{C}$: $L = \mathbb{C}$ $(m = 1)$

Idea: Choose K to be a **dense** subfield of $\mathbb{R}$ or $\mathbb{C}$, e.g.,

$K \subseteq$	$\mathbb{R}$	$\mathbb{C}$
K	$\mathbb{Q}$	$\mathbb{Q}(\zeta_r)$
L	$\mathbb{Q}(\zeta_r)$	Kummer extension
m	$\varphi(r)$	r

Thank you for your attention!