ulm university universität ulm

Gabidulin Codes over Fields of Characteristic Zero and Their Applications

Sven Puchinger

Institute of Communications Engineering, Ulm University, Germany

Technion Coding Theory Seminar, May 14, 2016

Outline

Outline

1978/1985/1991 Gabidulin codes over finite fields

Delsarte [Del78], Gabidulin [Gab85], Roth [Rot91]

1978/1985/1991	Gabidulin codes over finite fields
	Delsarte [Del78], Gabidulin [Gab85], Roth [Rot91]
1991	Application: Public Key Cryptography
	Gabidulin, Paramonov, Tretjakov [GPT91]
⋮	

1978/1985/1991	Gabidulin codes over finite fields
	Delsarte [Del78], Gabidulin [Gab85], Roth [Rot91]
1991	Application: Public Key Cryptography
	Gabidulin, Paramonov, Tretjakov [GPT91]
⋮	
2008	Application: Random Linear Network Coding
	Silva, Kschischang, Kötter [SKK08]
⋮	

1978/1985/1991	Gabidulin codes over finite fields Delsarte [Del78], Gabidulin [Gab85], Roth [Rot91]
1991	Application: Public Key Cryptography Gabidulin, Paramonov, Tretjakov [GPT91]
⋮	
2008	Application: Random Linear Network Coding Silva, Kschischang, Kötter [SKK08]
⋮	

1996/2013	Gabidulin codes over general fields & decoding in $O(n^3)$ Roth [Rot96], Augot, Loidreau, Robert [ALR13]

1978/1985/1991	Gabidulin codes over finite fields Delsarte [Del78], Gabidulin [Gab85], Roth [Rot91]
1991	Application: Public Key Cryptography Gabidulin, Paramonov, Tretjakov [GPT91]
⋮	
2008	Application: Random Linear Network Coding Silva, Kschischang, Kötter [SKK08]
⋮	

1996/2013	Gabidulin codes over general fields & decoding in $O(n^3)$ Roth [Rot96], Augot, Loidreau, Robert [ALR13]
2015	Application: Space–Time codes Robert [Rob15]

1978/1985/1991	Gabidulin codes over finite fields Delsarte [Del78], Gabidulin [Gab85], Roth [Rot91]
1991	Application: Public Key Cryptography Gabidulin, Paramonov, Tretjakov [GPT91]
⋮	
2008	Application: Random Linear Network Coding Silva, Kschischang, Kötter [SKK08]
⋮	

1996/2013	Gabidulin codes over general fields & decoding in $O(n^3)$ Roth [Rot96], Augot, Loidreau, Robert [ALR13]
2015	Application: Space–Time codes Robert [Rob15]
2016	Decoding in $O(n^2)$ Müelich, Puchinger, Mödinger, Bossert [MPMB16]

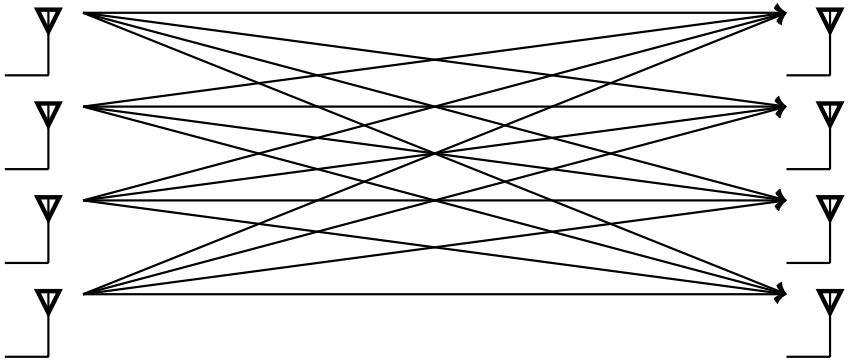
History

1978/1985/1991	Gabidulin codes over finite fields Delsarte [Del78], Gabidulin [Gab85], Roth [Rot91]
1991	Application: Public Key Cryptography Gabidulin, Paramonov, Tretjakov [GPT91]
⋮	
2008	Application: Random Linear Network Coding Silva, Kschischang, Kötter [SKK08]
⋮	

1996/2013	Gabidulin codes over general fields & decoding in $O(n^3)$ Roth [Rot96], Augot, Loidreau, Robert [ALR13]
2015	Application: Space–Time codes Robert [Rob15]
2016	Decoding in $O(n^2)$ Müelich, Puchinger, Mödinger, Bossert [MPMB16]
2016	Application: Low-Rank Matrix Recovery Müelich, Puchinger, Bossert [MPB16]

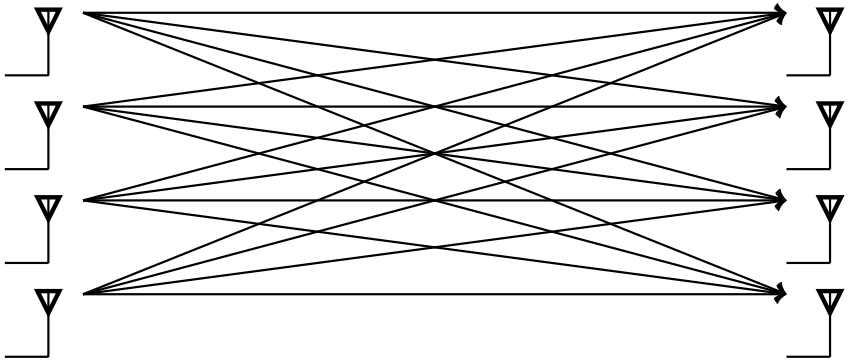
- m antennas, n time steps

- m antennas, n time steps
- MIMO with fading ($\boldsymbol{H}$) and additive noise ($\boldsymbol{N}$)



$$\boldsymbol{X} \in \mathbb{C}^{m \times n} \qquad \boldsymbol{Y} = \boldsymbol{H}\boldsymbol{X} + \boldsymbol{N} \in \mathbb{C}^{m \times n}$$

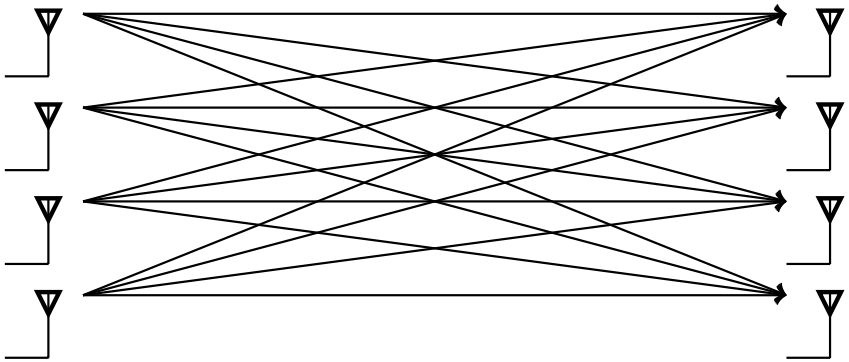
- m antennas, n time steps
- MIMO with fading ($\boldsymbol{H}$) and additive noise ($\boldsymbol{N}$)



$$\boldsymbol{X} \in \mathbb{C}^{m \times n} \qquad \boldsymbol{Y} = \boldsymbol{H}\boldsymbol{X} + \boldsymbol{N} \in \mathbb{C}^{m \times n}$$

- **Design criterion:** Find set of matrices $\mathcal{C} \subset \mathbb{C}^{m \times n}$ with pairwise rank difference as large as possible

- m antennas, n time steps
- MIMO with fading ($\boldsymbol{H}$) and additive noise ($\boldsymbol{N}$)



$$\boldsymbol{X} \in \mathbb{C}^{m \times n} \qquad \boldsymbol{Y} = \boldsymbol{H}\boldsymbol{X} + \boldsymbol{N} \in \mathbb{C}^{m \times n}$$

- **Design criterion:** Find set of matrices $\mathcal{C} \subset \mathbb{C}^{m \times n}$ with pairwise rank difference as large as possible
- Space-Times Codes based on generalized Gabidulin codes (Robert [Rob15])

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)

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)

Hamming Metric Decoding 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)
- $\boldsymbol{e} \in K^n$, $\mathrm{wt_H}(\boldsymbol{e})$ small (unknown)

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)

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)

Hamming Metric Decoding 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)
- $\boldsymbol{e} \in K^n$, $\mathrm{wt_H}(\boldsymbol{e})$ small (unknown)

Low-Rank Matrix Recovery (LRMR)

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)

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)

Hamming Metric Decoding 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 Decoding 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)

Outline

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

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

Galois group

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

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

Galois group

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

L is an m-dimensional K-vector space $\Rightarrow \exists\, \mathrm{char}_\theta(\lambda) := \det_K(\lambda \cdot \mathrm{id_L} - \theta)$

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

Galois group

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

L is an m-dimensional K-vector space $\Rightarrow \exists\, \mathrm{char}_\theta(\lambda) := \det_K(\lambda \cdot \mathrm{id_L} - \theta)$

char_θ is square-free if it does not have a square factor.

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

Galois group

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

L is an m-dimensional K-vector space $\Rightarrow \exists\, \mathrm{char}_\theta(\lambda) := \det_K(\lambda \cdot \mathrm{id_L} - \theta)$

char_θ is square-free if it does not have a square factor.

Theorem *(Augot, Loidreau, Robert [ALR13])*

char_θ is square-free
$\Leftrightarrow L^\theta = \{x : \theta(x) = x\} = K$
$\Leftrightarrow \mathrm{Gal}\,(L/K)$ is cyclic and θ is a generator

Examples

General	Finite Fields	Cyclotomic Extensions
K	$\mathbb{F}_q$	$\mathbb{Q}$
L	$\mathbb{F}_{q^m}$	$\mathbb{Q}(\zeta_n)$, $\zeta_n = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$ (n-th root of unity)
$[L:K]$	m	$\varphi(n)$
θ	$\cdot^q$ (Frobenius aut.)	i s.t. $\gcd(i,n)=1$ $\theta_i : \zeta_n^j \mapsto (\zeta_n^j)^i$

Examples

General	Finite Fields	Cyclotomic Extensions
K	$\mathbb{F}_q$	$\mathbb{Q}$
L	$\mathbb{F}_{q^m}$	$\mathbb{Q}(\zeta_n)$, $\zeta_n = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$ (n-th root of unity)
$[L:K]$	m	$\varphi(n)$
θ	$\cdot^q$ (Frobenius aut.)	i s.t. $\gcd(i,n)=1$ $\theta_i : \zeta_n^j \mapsto (\zeta_n^j)^i$

Example: $n = 4 \Rightarrow \zeta_4 = \mathrm{i}$, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\mathrm{i}) = \{a + \mathrm{i}b : a, b \in \mathbb{Q}\}$, $\varphi(4) = 2$

$$\theta_1 : 1 \mapsto 1^1 = 1, \mathrm{i} \mapsto \mathrm{i}^1 = \mathrm{i} \quad \Rightarrow a + \mathrm{i}b \mapsto a + \mathrm{i}b \ (\mathrm{char}_\theta \textbf{ not square-free})$$

$$\theta_3 : 1 \mapsto 1^3 = 1, \mathrm{i} \mapsto \mathrm{i}^3 = -\mathrm{i} \quad \Rightarrow a + \mathrm{i}b \mapsto a - \mathrm{i}b \ (\mathrm{char}_\theta \text{ square-free})$$

Examples

General	Finite Fields	Cyclotomic Extensions
K	$\mathbb{F}_q$	$\mathbb{Q}$
L	$\mathbb{F}_{q^m}$	$\mathbb{Q}(\zeta_n)$, $\zeta_n = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$ (n-th root of unity)
$[L:K]$	m	$\varphi(n)$
θ	$\cdot^q$ (Frobenius aut.)	i s.t. $\gcd(i,n)=1$ $\theta_i : \zeta_n^j \mapsto (\zeta_n^j)^i$

Example: $n = 4 \Rightarrow \zeta_4 = \mathrm{i}$, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\mathrm{i}) = \{a + \mathrm{i}b : a, b \in \mathbb{Q}\}$, $\varphi(4) = 2$

$$\theta_1 : 1 \mapsto 1^1 = 1, \mathrm{i} \mapsto \mathrm{i}^1 = \mathrm{i} \quad \Rightarrow a + \mathrm{i}b \mapsto a + \mathrm{i}b \ (\mathrm{char}_\theta \textbf{ not square-free})$$
$$\theta_3 : 1 \mapsto 1^3 = 1, \mathrm{i} \mapsto \mathrm{i}^3 = -\mathrm{i} \quad \Rightarrow a + \mathrm{i}b \mapsto a - \mathrm{i}b \ (\mathrm{char}_\theta \text{ square-free})$$

Other Field Extensions: Kummer and Artin-Schreier extensions

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

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

θ-Polynomials

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

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

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

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

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

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

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

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

Properties

- $(L[x;\theta], +, \cdot)$ is a ring
- $(L[x;\theta], +, \cdot)$ is non-commutative in general
- θ-polynomials are skew polynomials (without derivation)
- Isomorphic to linearized polynomials in case $\mathbb{F}_{q^m}/\mathbb{F}_q$, $\theta = \cdot^q$

θ-Polynomials (cont'd)

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

θ-Polynomials (cont'd)

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

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

θ-Polynomials (cont'd)

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

- $(a \cdot b)(\alpha) = a(b(\alpha))$
- $\deg(a \cdot b) = \deg a + \deg b$
- Zeros 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 $[L : K]$

θ-Polynomials (cont'd)

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

- $(a \cdot b)(\alpha) = a(b(\alpha))$
- $\deg(a \cdot b) = \deg a + \deg b$
- Zeros 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 [ALR13])

If char_θ is square-free,

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

Annihilator Polynomial

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

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

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:

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

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 [ALR13])*

If char_θ is square-free,

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

Outline

L/K field extension, $\theta \in \mathrm{Gal}\,(L/K)$ with char_θ square-free.

Definition

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

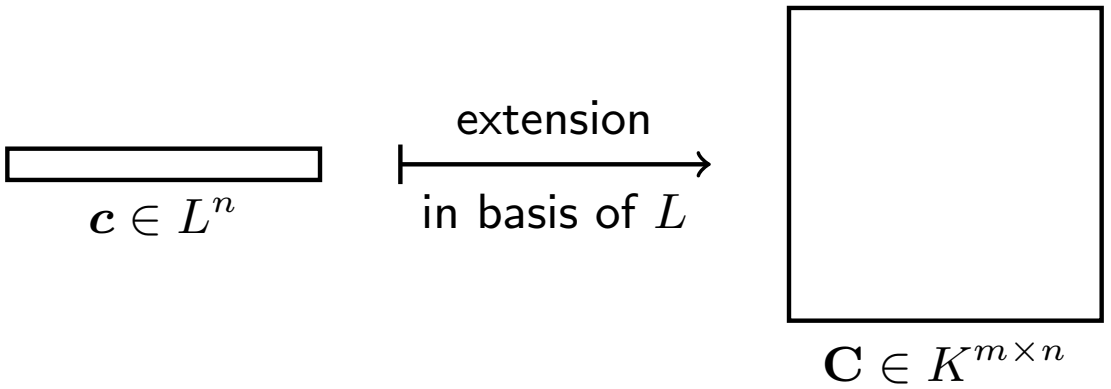
$$\mathcal{C}_{\mathrm{G}}[n,k] = \left\{ \boldsymbol{c} = \left[f(g_1), \ldots, f(g_n) \right] : f \in L[x;\theta] \wedge \deg f < k \right\} \subseteq L^n$$

L/K field extension, $\theta \in \mathrm{Gal}\,(L/K)$ with char_θ square-free.

Definition

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

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

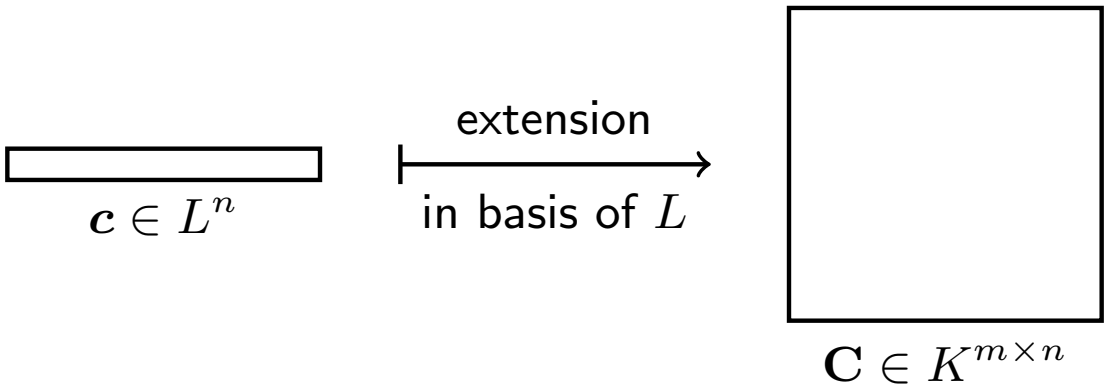


L/K field extension, $\theta \in \mathrm{Gal}\,(L/K)$ with char_θ square-free.

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[1]: $\mathrm{wt}_{\mathrm{R}}(\boldsymbol{c}) = \mathrm{rank}(\mathbf{C}), \quad \mathrm{d}_{\mathrm{R}}(\boldsymbol{c}_1, \boldsymbol{c}_2) = \mathrm{rank}(\mathbf{C}_1 - \mathbf{C}_2)$

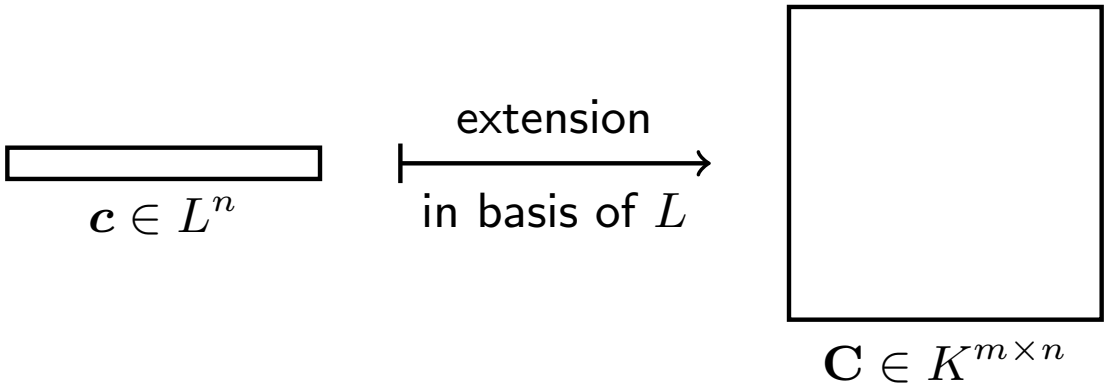
[1] Several definitions of rank metric exist. They are equivalent if char_θ is square-free, cf. [ALR13]

L/K field extension, $\theta \in \mathrm{Gal}\,(L/K)$ with char_θ square-free.

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[1]: $\mathrm{wt}_{\mathrm{R}}(\boldsymbol{c}) = \mathrm{rank}(\mathbf{C}), \quad \mathrm{d}_{\mathrm{R}}(\boldsymbol{c}_1, \boldsymbol{c}_2) = \mathrm{rank}(\mathbf{C}_1 - \mathbf{C}_2)$

Theorem *(Augot, Loidreau, Robert [ALR13])*

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

[1] Several definitions of rank metric exist. They are equivalent if char_θ is square-free, cf. [ALR13]

Error Model

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

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)

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 [MPMB16])*

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

*characteristic zero equivalent to Gao's key equation for finite field Gabidulin codes (Wachter-Zeh [Wac13])

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 [MPMB16])*

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

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 [Wac13])

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 [MPMB16])*

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

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

(Also true for char_θ not square-free)

*characteristic zero equivalent to Gao's key equation for finite field Gabidulin codes (Wachter-Zeh [Wac13])

Key Equation *(Müelich, Puchinger, Mödinger, Bossert [MPMB16])*

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

Key Equation *(Müelich, Puchinger, Mödinger, Bossert [MPMB16])*

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

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

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

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

Key Equation *(Müelich, Puchinger, Mödinger, Bossert [MPMB16])*

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

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 [MPMB16])*

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

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

Key Equation *(Müelich, Puchinger, Mödinger, Bossert [MPMB16])*

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

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 [MPMB16])*

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 char_θ is square-free is 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

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

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

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)

$$\begin{bmatrix} x^k & \boxed{\hat{r}} \\ 0 & \boxed{\mathcal{A}_{\langle g_1,\ldots,g_n\rangle}} \end{bmatrix}$$

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)

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

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)

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

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

(∗) Puchinger, Nielsen, Li, Sidorenko [PNLS15]

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)

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

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

- Similar to the Extended Euclidean Algorithm (EEA)

(*) Puchinger, Nielsen, Li, Sidorenko [PNLS15]

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)

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

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

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

$(*)$ Puchinger, Nielsen, Li, Sidorenko [PNLS15]

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"*

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

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

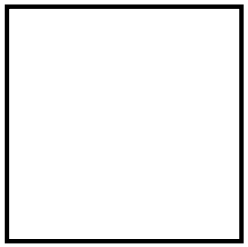
5 **if** $\varrho = 0$ **then return** χ

6 **else return** *"decoding failure"*

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

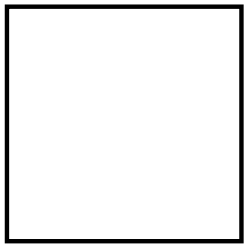
	Fast	**"Normal"**	**Small growth**
Operations in L	$O(n^{1.69})$	$O(n^2)$	$O(n^3)$
Row Reduction	EEA [Wac13] or D&Q [PMM+16]	[PNLS15]	Fraction-free [BCL06]

Back to LRMR (K-linear map $\mathcal{A}$)



$\boldsymbol{E} \in K^{m \times n}$

Back to LRMR (K-linear map $\mathcal{A}$)

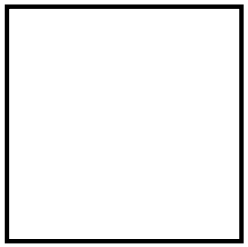


$\boldsymbol{E} \in K^{m \times n}$

Inverse extension in basis of L

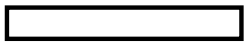
$\boldsymbol{e} \in L^n$

Back to LRMR (K-linear map $\mathcal{A}$)



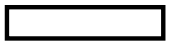
$\boldsymbol{E} \in K^{m \times n}$

Inverse extension in basis of L



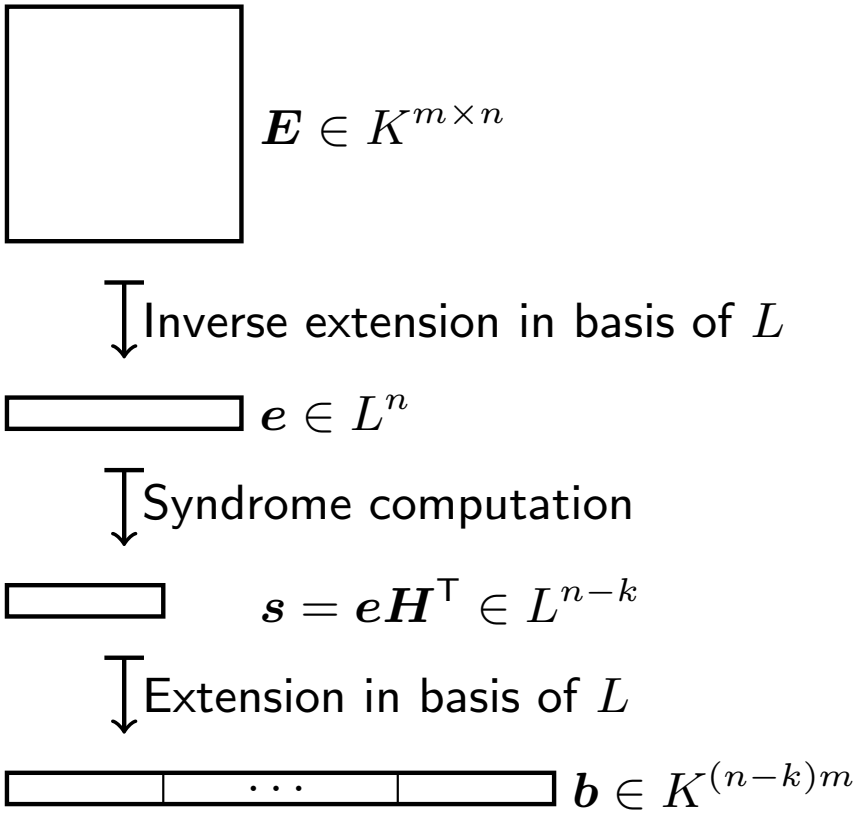
$\boldsymbol{e} \in L^n$

Syndrome computation

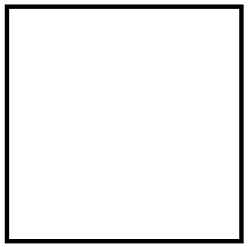


$\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^{\mathsf{T}} \in L^{n-k}$

Back to LRMR (K-linear map $\mathcal{A}$)

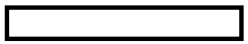


Back to LRMR (K-linear map $\mathcal{A}$)



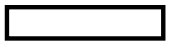
$\boldsymbol{E} \in K^{m \times n}$

(linear) Inverse extension in basis of L



$\boldsymbol{e} \in L^n$

(linear) Syndrome computation

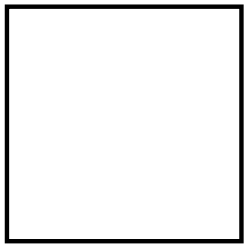


$\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^{\mathsf{T}} \in L^{n-k}$

(linear) Extension in basis of L

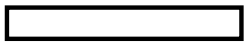
$\boldsymbol{b} \in K^{(n-k)m}$

Back to LRMR (K-linear map $\mathcal{A}$)



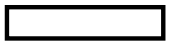
$\boldsymbol{E} \in K^{m \times n}$

(linear) ↓ Inverse extension in basis of L



$\boldsymbol{e} \in L^n$

(linear) ↓ Syndrome computation



$\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^{\mathsf{T}} \in L^{n-k}$

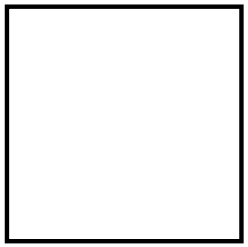
(linear) ↓ Extension in basis of L

$\boldsymbol{b} \in K^{(n-k)m}$

Theorem *Müelich, Puchinger, Bossert [MPB16]*

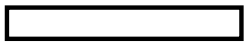
If $\operatorname{rank}(\boldsymbol{E}) \leq \frac{d-1}{2} = \frac{n-k}{2}$, $\boldsymbol{E}$ can be reconstructed from $\boldsymbol{b} = \mathcal{A}(\boldsymbol{E})$.

Back to LRMR (K-linear map $\mathcal{A}$)



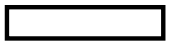
$\boldsymbol{E} \in K^{m \times n}$

(linear) ↓ Inverse extension in basis of L



$\boldsymbol{e} \in L^n$

(linear) ↓ Syndrome computation



$\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\mathsf{T} \in L^{n-k}$

(linear) ↓ Extension in basis of L

$\boldsymbol{b} \in K^{(n-k)m}$

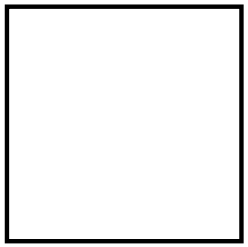
↕ Inverse extension in basis of L

$\boldsymbol{b} \in K^{(n-k)m}$

Theorem *Müelich, Puchinger, Bossert [MPB16]*

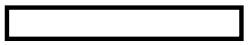
If $\operatorname{rank}(\boldsymbol{E}) \leq \frac{d-1}{2} = \frac{n-k}{2}$, $\boldsymbol{E}$ can be reconstructed from $\boldsymbol{b} = \mathcal{A}(\boldsymbol{E})$.

Back to LRMR (K-linear map $\mathcal{A}$)



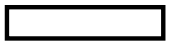
$\boldsymbol{E} \in K^{m \times n}$

(linear) Inverse extension in basis of L



$\boldsymbol{e} \in L^n$

(linear) Syndrome computation

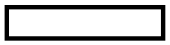


$\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\mathsf{T} \in L^{n-k}$

(linear) Extension in basis of L

$\boldsymbol{b} \in K^{(n-k)m}$

Find a solution of $\boldsymbol{r}\boldsymbol{H}^\mathsf{T} = \boldsymbol{s}$



$\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^\mathsf{T} \in L^{n-k}$

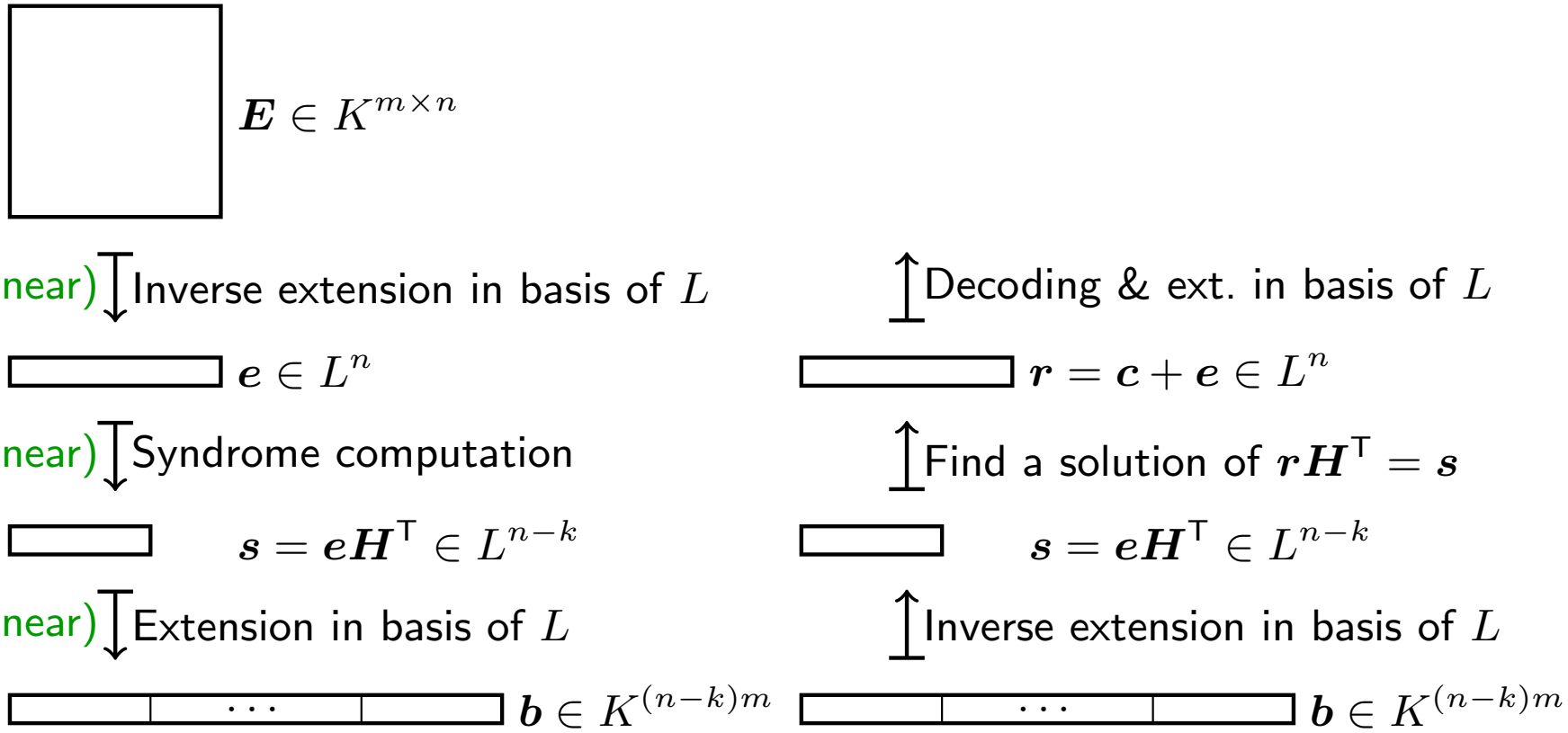
Inverse extension in basis of L

$\boldsymbol{b} \in K^{(n-k)m}$

Theorem *Müelich, Puchinger, Bossert [MPB16]*

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

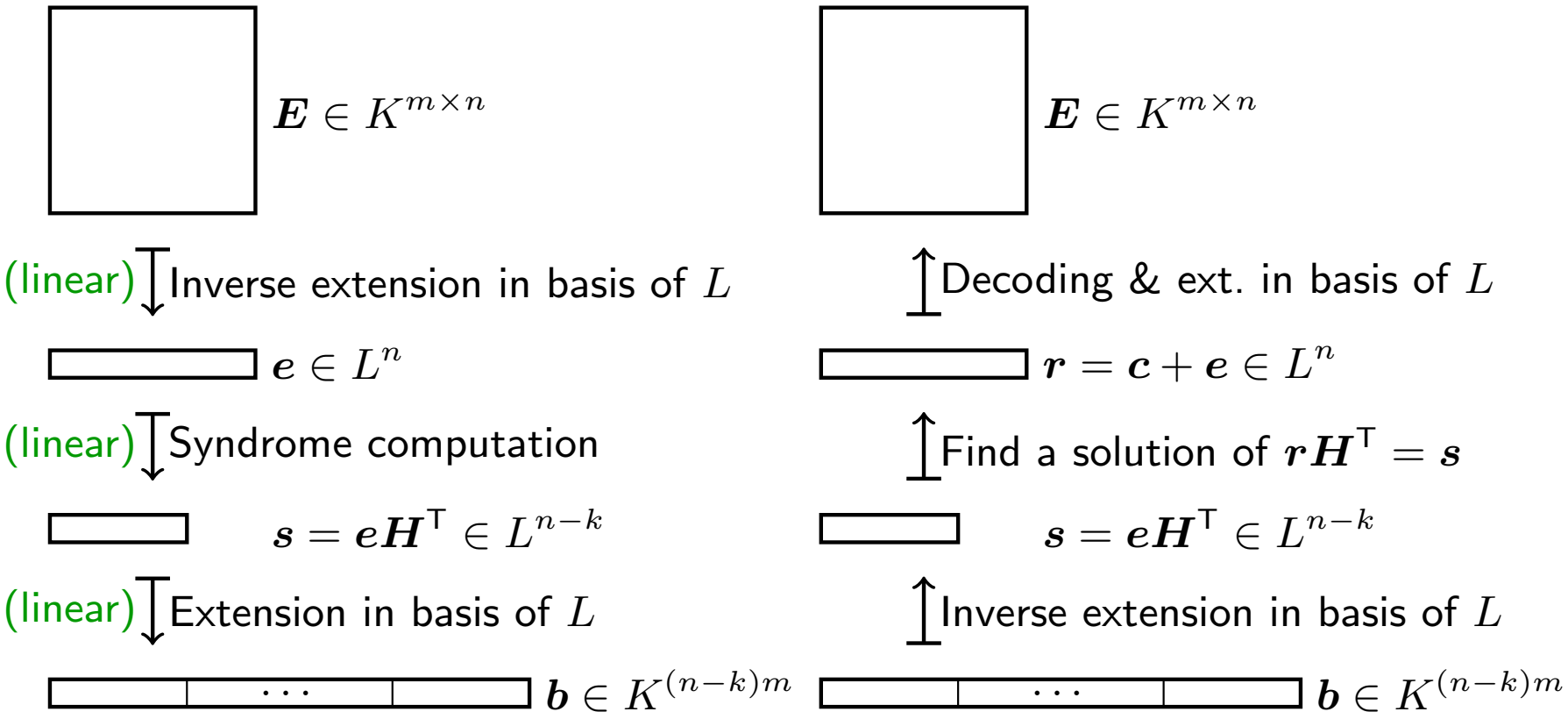
Back to LRMR (K-linear map $\mathcal{A}$)



Theorem *Müelich, Puchinger, Bossert [MPB16]*

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

Back to LRMR (K-linear map $\mathcal{A}$)

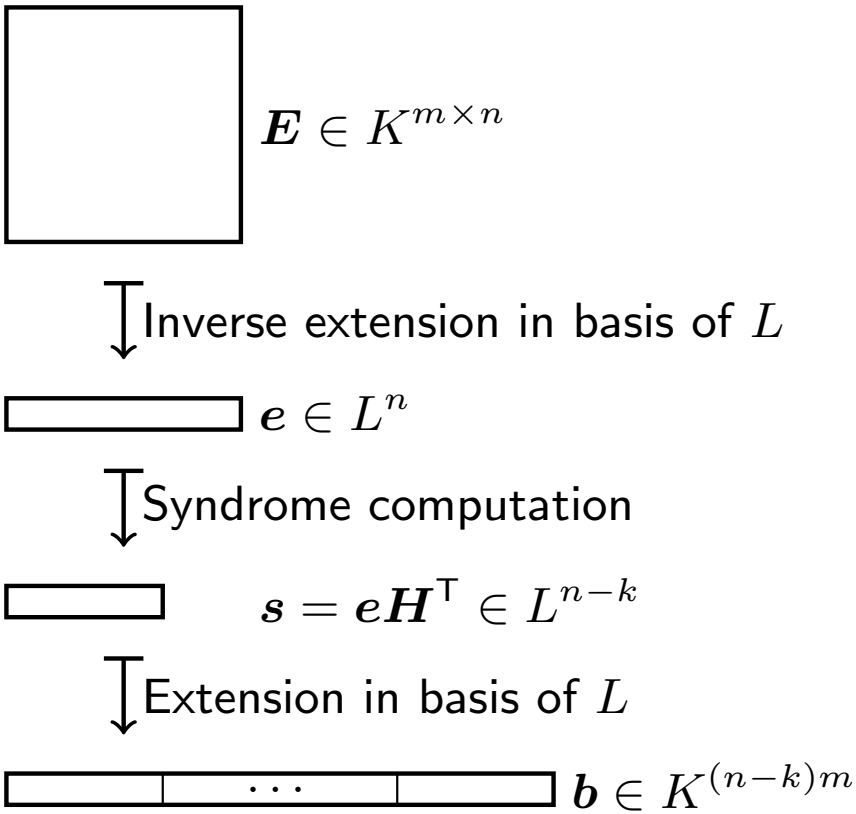


Theorem *Müelich, Puchinger, Bossert [MPB16]*

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

Back to LRMR (Choice of K and L)

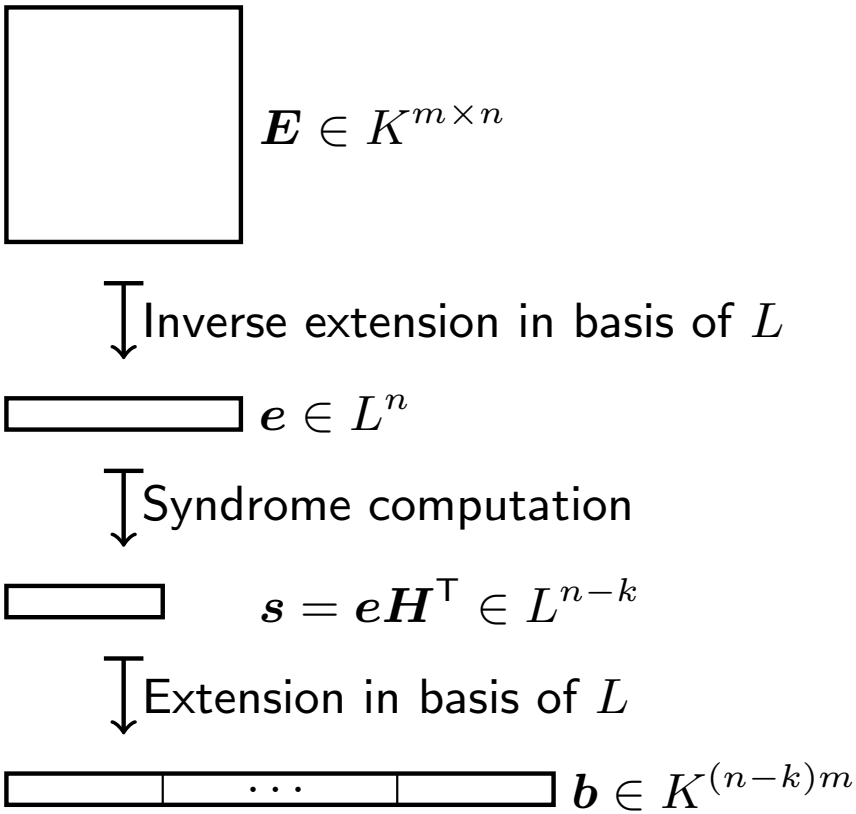
Needed: $K \in \{\mathbb{R}, \mathbb{C}\}$. Possible L:



Back to LRMR (Choice of K and L)

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

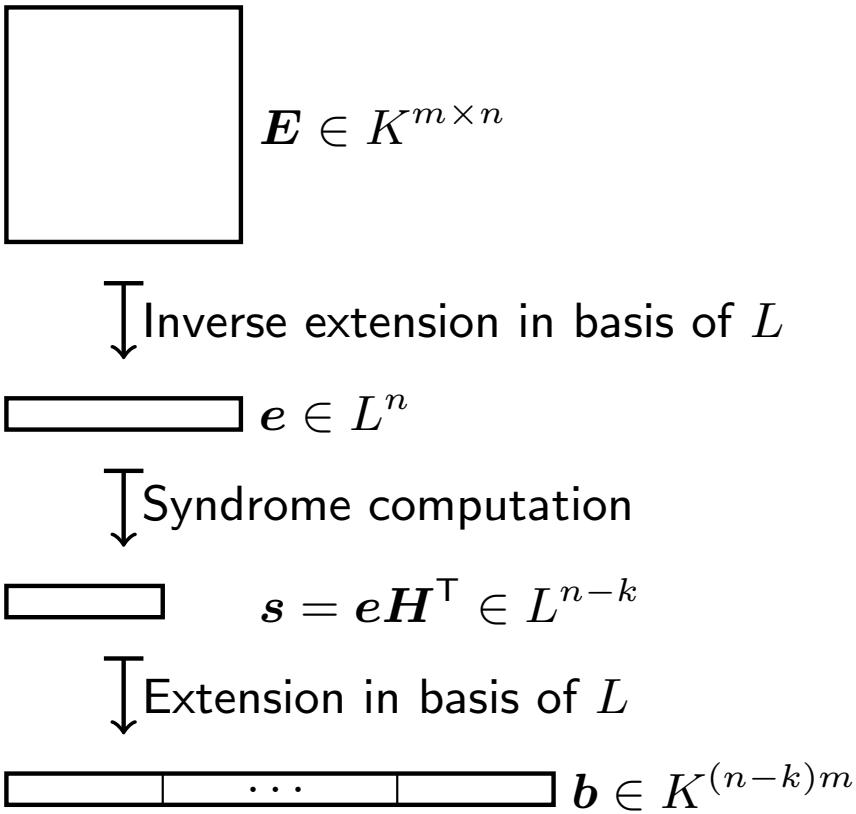
- $K = \mathbb{R}$: $L \in \{\mathbb{R}, \mathbb{C}\}$ $(m \leq 2)$



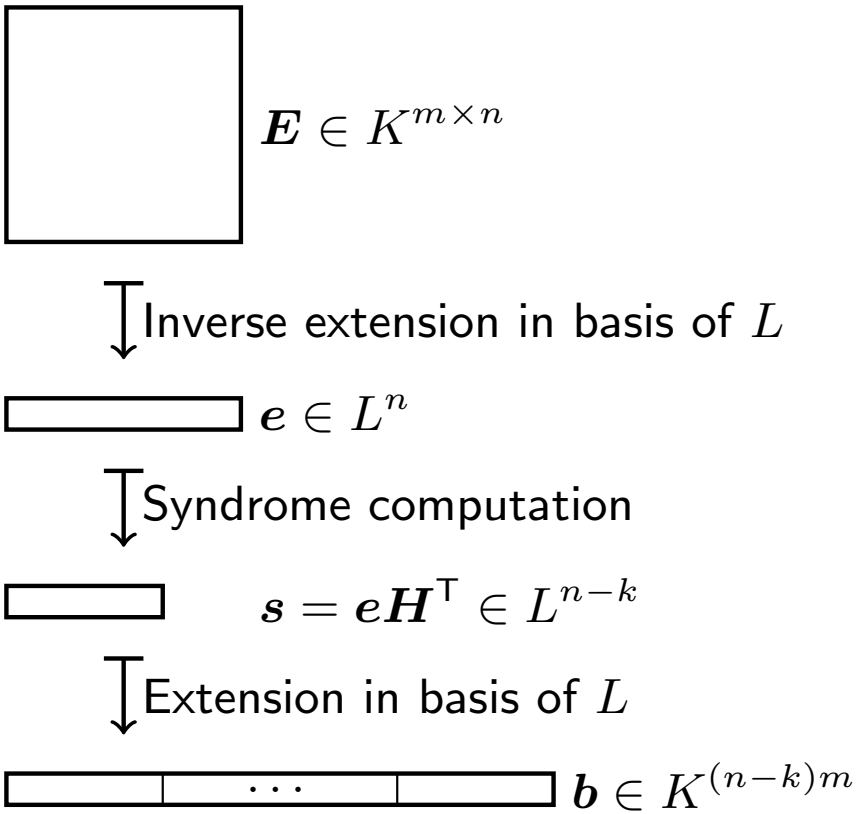
Back to LRMR (Choice of K and L)

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

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



Back to LRMR (Choice of K and L)



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

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

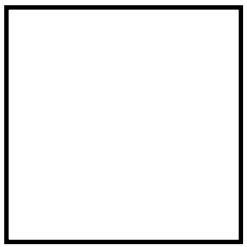
Idea: Choose K to be a **dense** subfield of $\mathbb{R}$ or $\mathbb{C}$, e.g.,

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

Back to LRMR (Choice of K and L)

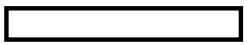
$\boldsymbol{X} \in \mathbb{C}^{m \times n}$

Rank-preserving mapping



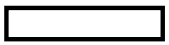
$\boldsymbol{E} \in K^{m \times n}$

Inverse extension in basis of L



$\boldsymbol{e} \in L^n$

Syndrome computation



$\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}^{\mathsf{T}} \in L^{n-k}$

Extension in basis of L

$\boldsymbol{b} \in K^{(n-k)m}$

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

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

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

Outline

If we replace

$$\begin{aligned} \mathbb{F}_{q^m}/\mathbb{F}_q &\longleftrightarrow L/K \\ \cdot^q &\longleftrightarrow \theta \in \mathrm{Gal}\left(L/K\right), \mathrm{char}_\theta \text{ square-free,} \end{aligned}$$

If we replace

$$\begin{aligned} \mathbb{F}_{q^m}/\mathbb{F}_q \quad &\longleftrightarrow \quad L/K \\ .^q \quad &\longleftrightarrow \quad \theta \in \mathrm{Gal}\left(L/K\right), \mathrm{char}_\theta \text{ square-free,} \end{aligned}$$

then the

- Definition of Rank Metric
- Definition of Gabidulin codes
- Decoding of Gabidulin codes

immediately generalize.

If we replace

$$\begin{aligned} \mathbb{F}_{q^m}/\mathbb{F}_q &\longleftrightarrow L/K \\ \cdot^q &\longleftrightarrow \theta \in \mathrm{Gal}\left(L/K\right), \mathrm{char}_\theta \text{ square-free,} \end{aligned}$$

then the

- Definition of Rank Metric
- Definition of Gabidulin codes
- Decoding of Gabidulin codes

immediately generalize.

Applications

- Space–Time codes
- Low-Rank Matrix Recovery

Bibliography I

[ALR13] Daniel Augot, Pierre Loidreau, and Gwezheneg Robert.
Rank Metric and Gabidulin Codes in Characteristic Zero.
In *IEEE International Symposium on Information Theory*, 2013.

[BCL06] Bernhard Beckermann, Howard Cheng, and George Labahn.
Fraction-Free Row Reduction of Matrices of Ore Polynomials.
Journal of Symbolic Computation, 41(5):513–543, 2006.

[Del78] P. Delsarte.
Bilinear Forms over a Finite Field, with Applications to Coding Theory.
Journal of Combinatorial Theory, Series A, 25(3):226–241, 1978.

[Gab85] Ernest M. Gabidulin.
Theory of Codes with Maximum Rank Distance.
Problemy Peredachi Informatsii, 21(1):3–16, 1985.

[GPT91] Ernst M. Gabidulin, AV Paramonov, and OV Tretjakov.
Ideals Over a Non-Commutative Ring and Their Application in Cryptology.
In *Advances in Cryptology*, pages 482–489. Springer, 1991.

[LMK14] Siyu Liu, Felice Manganiello, and Frank R Kschischang.
Kötter interpolation in skew polynomial rings.
Designs, codes and cryptography, 72(3):593–608, 2014.

[MPB16] Sven Müelich, Sven Puchinger, and Martin Bossert.
Low-Rank Matrix Recovery using Gabidulin Codes in Characteristic Zero.
In *International Workshop on Algebraic and Combinatorial Coding Theory (arXiv:1604.04397)*, 2016.

[MPMB16] Sven Müelich, Sven Puchinger, David Mödinger, and Martin Bossert.
An Alternative Decoding Method for Gabidulin Codes in Characteristic Zero.
In *IEEE International Symposium on Information Theory (arXiv:1601.05205)*, 2016.

[PMM+16] Sven Puchinger, Sven Müelich, David Mödinger, Johan S. R. Nielsen, and Martin Bossert.
Decoding Interleaved Gabidulin Codes using Alekhnovich's Algorithm.
In *International Workshop on Algebraic and Combinatorial Coding Theory (arXiv:1604.04397)*, 2016.

[PNLS15] Sven Puchinger, Johan S. R. Nielsen, Wenhui Li, and Vladimir Sidorenko.
Row Reduction Applied to Rank Metric and Subspace Codes.
Submitted to Designs, Codes and Cryptography (arXiv:1510.04728), 2015.

[PW16] Sven Puchinger and Antonia Wachter-Zeh.
Fast Operations on Linearized Polynomials and their Applications in Coding Theory.
Submitted to: Journal of Symbolic Computation, 2016.
arXiv preprint `http://arxiv.org/abs/1512.06520`.

[Rob15] Gwezheneg Robert.
A New Constellation for Space-Time Coding.
In *International Workshop on Coding and Cryptography*, 2015.

[Rot91] Ron M. Roth.
Maximum-Rank Array Codes and Their Application to Crisscross Error Correction.
IEEE Transactions on Information Theory, 37(2):328–336, 1991.

[Rot96] Ron M Roth.
Tensor Codes for the Rank Metric.
IEEE Transactions on Information Theory, 42(6):2146–2157, 1996.

[SKK08] Danilo Silva, Frank R Kschischang, and Ralf Koetter.
A Rank-Metric Approach to Error Control in Random Network Coding.
IEEE Transactions on Information Theory, 54(9):3951–3967, 2008.

[Wac13] Antonia Wachter-Zeh.
Decoding of Block and Convolutional Codes in Rank Metric.
PhD thesis, Ulm University and Université Rennes 1, 2013.