Decoding Interleaved Gabidulin Codes using Alekhnovich's Algorithm

Sven Puchinger[1], Sven Müelich[1], David Mödinger[2],
Johan Rosenkilde né Nielsen[3], Martin Bossert[1]

[1]Institute of Communications Engineering, Ulm University, Germany
[2]Institute of Distributed Systems, Ulm University, Germany
[3]Department of Applied Mathematics & Computer Science, Technical University of Denmark, Denmark

ACCT, June 22, 2016

Outline

Skew Polynomial Ring

$\mathbb{F}[x;\sigma]$: Polynomials of the form

$$a = \sum_{i=0}^{d} a_i x^i \;:\; a_i \in \mathbb{F}_{q^m}, d \in \mathbb{N}$$

Skew Polynomial Ring

$\mathbb{F}[x;\sigma]$: Polynomials of the form

$$a = \sum_{i=0}^{d} a_i x^i \;:\; a_i \in \mathbb{F}_{q^m}, d \in \mathbb{N}$$

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

$\mathbb{F}[x;\sigma]$: Polynomials of the form

$$a = \sum_{i=0}^{d} a_i x^i \ : \ a_i \in \mathbb{F}_{q^m}, d \in \mathbb{N}$$

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

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

Skew Polynomial Ring

$\mathbb{F}[x;\sigma]$: Polynomials of the form

$$a = \sum_{i=0}^{d} a_i x^i \; : \; a_i \in \mathbb{F}_{q^m}, d \in \mathbb{N}$$

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

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

Degree $\quad \deg a = \max\{i : a_i \neq 0\}$

Skew Polynomial Ring

$\mathbb{F}[x;\sigma]$: Polynomials of the form

$$a = \sum_{i=0}^{d} a_i x^i \ : \ a_i \in \mathbb{F}_{q^m}, d \in \mathbb{N}$$

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

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

Degree $\quad \deg a = \max\{i : a_i \neq 0\}$

Properties

- Linearized polynomials isomorphic to $\mathbb{F}_{q^m}[x; \cdot^q]$ (Frobenius automorphism)
- Evaluation is linear map

Motivation: Interleaved Gabidulin Codes

Gabidulin Codes

- Rank-metric analogues of Reed–Solomon codes
- Defined using evaluation of skew polynomials
- Interleaving of ℓ codes $\Rightarrow$ increase decoding radius to $\frac{\ell}{\ell+1}(d-1)$ (w.h.p.).

Gabidulin Codes

- Rank-metric analogues of Reed–Solomon codes
- Defined using evaluation of skew polynomials
- Interleaving of ℓ codes $\Rightarrow$ increase decoding radius to $\frac{\ell}{\ell+1}(d-1)$ (w.h.p.).

Key Equation

$n, k_1, \dots, k_\ell \in \mathbb{N}$ code parameters,
$S_1, \dots, S_\ell \in \mathbb{F}[x,\sigma]$ syndromes,
$\Lambda \in \mathbb{F}[x,\sigma]$ error span polynomial.

$$\Lambda S_i \equiv \Omega_i \mod x^{n-k_i}$$
$$\deg \Omega_i < \deg \Lambda$$
Λ minimal degree

Shift Register Synthesis Problem

Given $s_1, \dots, s_\ell, g_1, \dots, g_\ell \in \mathbb{F}[x,\sigma]$,
find $\lambda, \omega_1, \dots, \omega_\ell \in \mathbb{F}[x,\sigma]$, s.t. $\forall i$

$$\lambda s_i \equiv \omega_i \mod g_i$$
$$\deg \omega_i < \deg \lambda$$
λ minimal degree

weak Popov form (wPf)

NACHRICHTENTECHNIK Universität Ulm

Leading Position

Rightmost position of maximal degree.

$$\boldsymbol{v} = \begin{bmatrix} x^2 & 1 & x & \boxed{x^2} & x \end{bmatrix} \quad \Rightarrow \mathrm{LP}(\boldsymbol{v}) = 3$$

NACHRICHTENTECHNIK Universität Ulm

Leading Position

Rightmost position of maximal degree.

$$\boldsymbol{v} = \begin{bmatrix} x^2 & 1 & x & \boxed{x^2} & x \end{bmatrix} \quad \Rightarrow \mathrm{LP}(\boldsymbol{v}) = 3$$

weak Popov form

Matrix with all leading positions different.

$$\begin{bmatrix} x^2 & \boxed{x^2} & 1 \\ \boxed{x^3} & x & x^2 \\ 1 & x^4 & \boxed{x^4} \end{bmatrix}$$

Shift Register Synthesis Problem

Given $s_1, \dots, s_\ell, g_i, \dots, g_\ell \in \mathbb{F}[x, \sigma]$, **find** $\lambda, \omega_1, \dots, \omega_\ell \in \mathbb{F}[x, \sigma]$, s.t. $\forall i$

$$\lambda s_i \equiv \omega_i \mod g_i \quad (1)$$

$$\deg \omega_i < \deg \lambda \quad (2)$$

$$\lambda \text{ minimal degree} \quad (3)$$

Shift Register Synthesis Problem

Given $s_1, \dots, s_\ell, g_i, \dots, g_\ell \in \mathbb{F}[x, \sigma]$, **find** $\lambda, \omega_1, \dots, \omega_\ell \in \mathbb{F}[x, \sigma]$, s.t. $\forall i$

$$\lambda s_i \equiv \omega_i \mod g_i \quad (1)$$

$$\deg \omega_i < \deg \lambda \quad (2)$$

$$\lambda \text{ minimal degree} \quad (3)$$

Solution of (1) in row span of

$$\mathbf{B} = \begin{bmatrix} 1 & s_1 & s_2 & \dots & s_\ell \\ & g_1 & & & \\ & & g_2 & & \\ & & & \ddots & \\ & & & & g_\ell \end{bmatrix}$$

Shift Register Synthesis Problem

Given $s_1, \dots, s_\ell, g_i, \dots, g_\ell \in \mathbb{F}[x, \sigma]$, **find** $\lambda, \omega_1, \dots, \omega_\ell \in \mathbb{F}[x, \sigma]$, s.t. $\forall i$

$$\lambda s_i \equiv \omega_i \mod g_i \quad (1)$$

$$\deg \omega_i < \deg \lambda \quad (2)$$

$$\lambda \text{ minimal degree} \quad (3)$$

Solution of (1) in row span of

$$\mathbf{B} = \begin{bmatrix} 1 & s_1 & \boxed{s_2} & \dots & s_\ell \\ & \boxed{g_1} & & & \\ & & \boxed{g_2} & & \\ & & & \ddots & \\ & & & & \boxed{g_\ell} \end{bmatrix}$$

Shift Register Synthesis Problem

Given $s_1, \dots, s_\ell, g_i, \dots, g_\ell \in \mathbb{F}[x,\sigma]$, **find** $\lambda, \omega_1, \dots, \omega_\ell \in \mathbb{F}[x,\sigma]$, s.t. $\forall i$

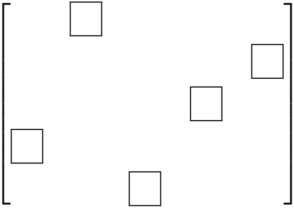
$$\lambda s_i \equiv \omega_i \mod g_i \tag{1}$$

$$\deg \omega_i < \deg \lambda \tag{2}$$

$$\lambda \text{ minimal degree} \tag{3}$$

Solution of (1) in row span of

$$\mathbf{B} = \begin{bmatrix} 1 & s_1 & \boxed{s_2} & \dots & s_\ell \\ & \boxed{g_1} & & & \\ & & \boxed{g_2} & & \\ & & & \ddots & \\ & & & & \boxed{g_\ell} \end{bmatrix} \xrightarrow[\text{row operations}]{\text{bring in wPf}}$$



Shift Register Synthesis Problem

Given $s_1, \dots, s_\ell, g_i, \dots, g_\ell \in \mathbb{F}[x, \sigma]$, **find** $\lambda, \omega_1, \dots, \omega_\ell \in \mathbb{F}[x, \sigma]$, s.t. $\forall i$

$$\lambda s_i \equiv \omega_i \mod g_i \tag{1}$$

$$\deg \omega_i < \deg \lambda \tag{2}$$

$$\lambda \text{ minimal degree} \tag{3}$$

Solution of (1) in row span of

$$\mathbf{B} = \begin{bmatrix} 1 & s_1 & \boxed{s_2} & \dots & s_\ell \\ & \boxed{g_1} & & & \\ & & \boxed{g_2} & & \\ & & & \ddots & \\ & & & & \boxed{g_\ell} \end{bmatrix} \xrightarrow[\text{row operations}]{\text{bring in wPf}} \begin{bmatrix} & \boxed{} & & & \\ & & & & \boxed{} \\ & & & \boxed{} & \\ \boxed{\lambda} & \omega_1 & \omega_2 & \dots & \omega_\ell \\ & & \boxed{} & & \end{bmatrix}$$

NACHRICHTENTECHNIK Universität Ulm

Shift Register Synthesis Problem

Given $s_1, \dots, s_\ell, g_i, \dots, g_\ell \in \mathbb{F}[x,\sigma]$, **find** $\lambda, \omega_1, \dots, \omega_\ell \in \mathbb{F}[x,\sigma]$, s.t. $\forall i$

$$\lambda s_i \equiv \omega_i \mod g_i \quad (1)$$

$$\deg \omega_i < \deg \lambda \quad (2)$$

$$\lambda \text{ minimal degree} \quad (3)$$

Solution of (1) in row span of

$$\mathbf{B} = \begin{bmatrix} 1 & s_1 & \boxed{s_2} & \dots & s_\ell \\ & \boxed{g_1} & & & \\ & & \boxed{g_2} & & \\ & & & \ddots & \\ & & & & \boxed{g_\ell} \end{bmatrix} \xrightarrow[\text{row operations}]{\text{bring in wPf}} \begin{bmatrix} & \square & & & \\ & & & & \square \\ & & & \square & \\ \boxed{\lambda} & \omega_1 & \omega_2 & \dots & \omega_\ell \\ & & \square & & \end{bmatrix}$$

Question: How fast can we do that?

- $O(\ell n^2)$ [Li, Nielsen, Puchinger, Sidorenko, WCC'15]
- $O(\ell^3 n^{1.69})$ [this paper] $\longleftarrow$ $\mathbb{F}[x,\sigma]$-variant of [Alekhnovich, 2005]

Outline

Degree of a Vector/Matrix

- $\deg \mathbf{m} = \max_i\{\deg m_i\}$
- $\deg \mathbf{M} = \sum_i \deg \mathbf{m}_i$

Degree of a Vector/Matrix

- $\deg \mathbf{m} = \max_i \{\deg m_i\}$
- $\deg \mathbf{M} = \sum_i \deg \mathbf{m}_i$

$$\deg \begin{bmatrix} x^2 & x \\ x^3 & x^3 \end{bmatrix} = 2 + 3 = 5$$

Degree of a Vector/Matrix

- $\deg \mathbf{m} = \max_i\{\deg m_i\}$
- $\deg \mathbf{M} = \sum_i \deg \mathbf{m}_i$

$$\deg \begin{bmatrix} x^2 & x \\ x^3 & x^3 \end{bmatrix} = 2 + 3 = 5$$

Accuracy Approximation/Length

$$a = \boxed{} \quad x^d \ldots x^0$$

Preliminaries

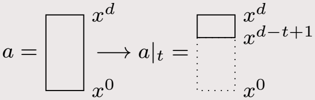
NACHRICHTENTECHNIK Universität Ulm

Degree of a Vector/Matrix

- $\deg \mathbf{m} = \max_i \{\deg m_i\}$
- $\deg \mathbf{M} = \sum_i \deg \mathbf{m}_i$

$$\deg \begin{bmatrix} x^2 & x \\ x^3 & x^3 \end{bmatrix} = 2 + 3 = 5$$

Accuracy Approximation/Length



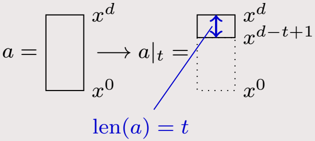
Preliminaries

Degree of a Vector/Matrix

- $\deg \mathbf{m} = \max_i \{\deg m_i\}$
- $\deg \mathbf{M} = \sum_i \deg \mathbf{m}_i$

$$\deg \begin{bmatrix} x^2 & x \\ x^3 & x^3 \end{bmatrix} = 2 + 3 = 5$$

Accuracy Approximation/Length

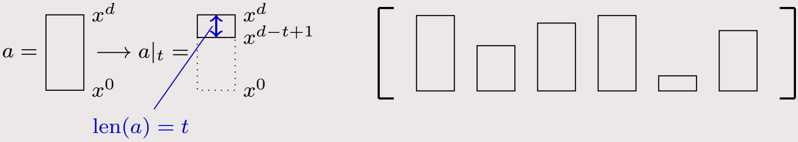


Degree of a Vector/Matrix

- $\deg \mathbf{m} = \max_i \{\deg m_i\}$
- $\deg \mathbf{M} = \sum_i \deg \mathbf{m}_i$

$$\deg \begin{bmatrix} x^2 & x \\ x^3 & x^3 \end{bmatrix} = 2 + 3 = 5$$

Accuracy Approximation/Length

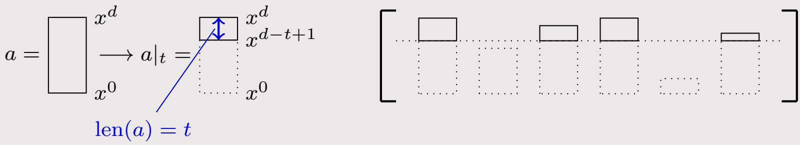


Degree of a Vector/Matrix

- $\deg \mathbf{m} = \max_i \{\deg m_i\}$
- $\deg \mathbf{M} = \sum_i \deg \mathbf{m}_i$

$$\deg \begin{bmatrix} x^2 & x \\ x^3 & x^3 \end{bmatrix} = 2 + 3 = 5$$

Accuracy Approximation/Length

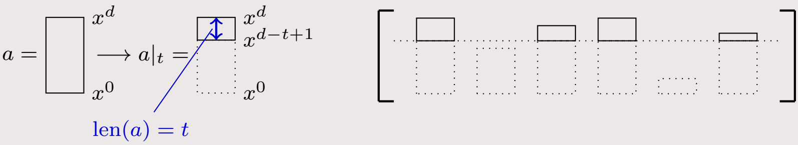


Degree of a Vector/Matrix

- $\deg \mathbf{m} = \max_i\{\deg m_i\}$
- $\deg \mathbf{M} = \sum_i \deg \mathbf{m}_i$

$$\deg \begin{bmatrix} x^2 & x \\ x^3 & x^3 \end{bmatrix} = 2+3=5$$

Accuracy Approximation/Length



Multiplication of Length-t Matrices

Multiply polynomials of length $\leq t$ (ω matrix mult. exponent):

$$\mathcal{M}(t) \in O\big(t^{\frac{\omega+1}{2}}\big) \subseteq O\big(t^{1.69}\big)$$

$(\ell+1) \times (\ell+1)$-matrices: $O\big(\ell^3 \mathcal{M}(t)\big)$

Basic Algorithm

Simple Transformation

Find two rows $\mathbf{m}_i$ and $\mathbf{m}_j$ with

$$\mathrm{LP}(\mathbf{m}_i) = \mathrm{LP}(\mathbf{m}_j) \text{ and } \deg \mathbf{m}_i \geq \deg \mathbf{m}_j.$$

Replace $\mathbf{m}_i \leftarrow \mathbf{m}_i - \alpha x^\delta \mathbf{m}_j$, s.t. leading monomial at $\mathrm{LP}(\mathbf{m}_i)$ cancels.
Remember row operation by matrix $\mathbf{U}$.

$$\mathbf{M} = \begin{bmatrix} x^2 & \boxed{x^2 + x} \\ 1 & \boxed{x} \end{bmatrix}$$

Simple Transformation

Find two rows $\mathbf{m}_i$ and $\mathbf{m}_j$ with

$$\mathrm{LP}(\mathbf{m}_i) = \mathrm{LP}(\mathbf{m}_j) \text{ and } \deg \mathbf{m}_i \geq \deg \mathbf{m}_j.$$

Replace $\mathbf{m}_i \leftarrow \mathbf{m}_i - \alpha x^{\delta} \mathbf{m}_j$, s.t. leading monomial at $\mathrm{LP}(\mathbf{m}_i)$ cancels.
Remember row operation by matrix $\mathbf{U}$.

$$\mathbf{M} = \begin{bmatrix} x^2 & \boxed{x^2 + x} \\ 1 & \boxed{x} \end{bmatrix} \xrightarrow{\mathbf{m}_1 \leftarrow \mathbf{m}_1 - x\mathbf{m}_2}$$

NACHRICHTENTECHNIK Universität Ulm

Simple Transformation

Find two rows $\mathbf{m}_i$ and $\mathbf{m}_j$ with

$$\mathrm{LP}(\mathbf{m}_i) = \mathrm{LP}(\mathbf{m}_j) \text{ and } \deg \mathbf{m}_i \geq \deg \mathbf{m}_j.$$

Replace $\mathbf{m}_i \leftarrow \mathbf{m}_i - \alpha x^{\delta} \mathbf{m}_j$, s.t. leading monomial at $\mathrm{LP}(\mathbf{m}_i)$ cancels.
Remember row operation by matrix $\mathbf{U}$.

$$\mathbf{M} = \begin{bmatrix} x^2 & \boxed{x^2 + x} \\ 1 & \boxed{x} \end{bmatrix} \xrightarrow{\mathbf{m}_1 \leftarrow \mathbf{m}_1 - x\mathbf{m}_2} \begin{bmatrix} \boxed{x^2 - x} & x \\ 1 & \boxed{x} \end{bmatrix}$$

Simple Transformation

Find two rows $\mathbf{m}_i$ and $\mathbf{m}_j$ with

$$\mathrm{LP}(\mathbf{m}_i) = \mathrm{LP}(\mathbf{m}_j) \text{ and } \deg \mathbf{m}_i \geq \deg \mathbf{m}_j.$$

Replace $\mathbf{m}_i \leftarrow \mathbf{m}_i - \alpha x^\delta \mathbf{m}_j$, s.t. leading monomial at $\mathrm{LP}(\mathbf{m}_i)$ cancels.
Remember row operation by matrix $\mathbf{U}$.

$$\mathbf{M} = \begin{bmatrix} x^2 & \boxed{x^2 + x} \\ 1 & \boxed{x} \end{bmatrix} \xrightarrow{\mathbf{m}_1 \leftarrow \mathbf{m}_1 - x\mathbf{m}_2} \begin{bmatrix} \boxed{x^2 - x} & x \\ 1 & \boxed{x} \end{bmatrix} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} \cdot \mathbf{M}$$

Simple Transformation

Find two rows $\mathbf{m}_i$ and $\mathbf{m}_j$ with

$$\mathrm{LP}(\mathbf{m}_i) = \mathrm{LP}(\mathbf{m}_j) \text{ and } \deg \mathbf{m}_i \geq \deg \mathbf{m}_j.$$

Replace $\mathbf{m}_i \leftarrow \mathbf{m}_i - \alpha x^\delta \mathbf{m}_j$, s.t. leading monomial at $\mathrm{LP}(\mathbf{m}_i)$ cancels.
Remember row operation by matrix $\mathbf{U}$.

$$\mathbf{M} = \begin{bmatrix} x^2 & \boxed{x^2 + x} \\ 1 & \boxed{x} \end{bmatrix} \xrightarrow{\mathbf{m}_1 \leftarrow \mathbf{m}_1 - x\mathbf{m}_2} \begin{bmatrix} \boxed{x^2 - x} & x \\ 1 & \boxed{x} \end{bmatrix} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} \cdot \mathbf{M}$$

$\mathbf{U} = \mathrm{R}(\mathbf{M})$

Apply simple transformations until $\mathbf{U} \cdot \mathbf{M}$ in wPf or $\deg(\mathbf{U} \cdot \mathbf{M}) \leq \deg \mathbf{M} - 1$.

Simple Transformation

Find two rows $\mathbf{m}_i$ and $\mathbf{m}_j$ with

$$\mathrm{LP}(\mathbf{m}_i) = \mathrm{LP}(\mathbf{m}_j) \text{ and } \deg \mathbf{m}_i \geq \deg \mathbf{m}_j.$$

Replace $\mathbf{m}_i \leftarrow \mathbf{m}_i - \alpha x^{\delta} \mathbf{m}_j$, s.t. leading monomial at $\mathrm{LP}(\mathbf{m}_i)$ cancels.
Remember row operation by matrix $\mathbf{U}$.

$$\mathbf{M} = \begin{bmatrix} x^2 & \boxed{x^2 + x} \\ 1 & \boxed{x} \end{bmatrix} \xrightarrow{\mathbf{m}_1 \leftarrow \mathbf{m}_1 - x\mathbf{m}_2} \begin{bmatrix} \boxed{x^2 - x} & x \\ 1 & \boxed{x} \end{bmatrix} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} \cdot \mathbf{M}$$

$\mathbf{U} = \mathrm{R}(\mathbf{M})$

Apply simple transformations until $\mathbf{U} \cdot \mathbf{M}$ in wPf or $\deg(\mathbf{U} \cdot \mathbf{M}) \leq \deg \mathbf{M} - 1$.

$\mathbf{U} = \mathrm{R}(\mathbf{M}, t)$

Apply $\mathrm{R}(\mathbf{M})$ t times. $\Rightarrow \deg(\mathbf{U} \cdot \mathbf{M}) \leq \deg \mathbf{M} - t$

NACHRICHTENTECHNIK Universität Ulm

Simple Transformation

Find two rows $\mathbf{m}_i$ and $\mathbf{m}_j$ with

$$\mathrm{LP}(\mathbf{m}_i) = \mathrm{LP}(\mathbf{m}_j) \text{ and } \deg \mathbf{m}_i \geq \deg \mathbf{m}_j.$$

Replace $\mathbf{m}_i \leftarrow \mathbf{m}_i - \alpha x^\delta \mathbf{m}_j$, s.t. leading monomial at $\mathrm{LP}(\mathbf{m}_i)$ cancels.
Remember row operation by matrix $\mathbf{U}$.

$$\mathbf{M} = \begin{bmatrix} x^2 & \boxed{x^2 + x} \\ 1 & \boxed{x} \end{bmatrix} \xrightarrow{\mathbf{m}_1 \leftarrow \mathbf{m}_1 - x\mathbf{m}_2} \begin{bmatrix} \boxed{x^2 - x} & x \\ 1 & \boxed{x} \end{bmatrix} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} \cdot \mathbf{M}$$

$\mathbf{U} = \mathrm{R}(\mathbf{M})$

Apply simple transformations until $\mathbf{U} \cdot \mathbf{M}$ in wPf or $\deg(\mathbf{U} \cdot \mathbf{M}) \leq \deg \mathbf{M} - 1$.

$\mathbf{U} = \mathrm{R}(\mathbf{M}, t)$

Apply $\mathrm{R}(\mathbf{M})$ t times. $\Rightarrow \deg(\mathbf{U} \cdot \mathbf{M}) \leq \deg \mathbf{M} - t$

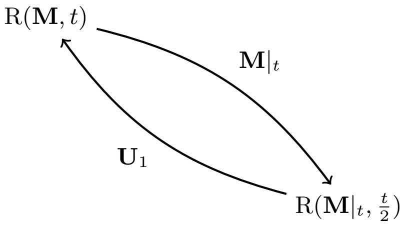
Transform $\mathbf{B}$ (from shift register) in wPf: **Only** $t \in O(n)$ **necessary!**

Divide-&-Conquer Trick

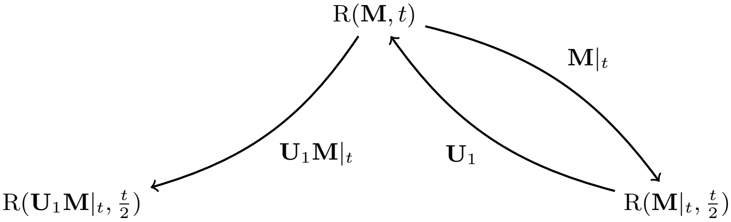
$$\mathrm{R}(\mathbf{M}, t)$$

$$\mathrm{R}(\mathbf{M}, t) \xrightarrow{\mathbf{M}|_t} \mathrm{R}(\mathbf{M}|_t, \tfrac{t}{2})$$

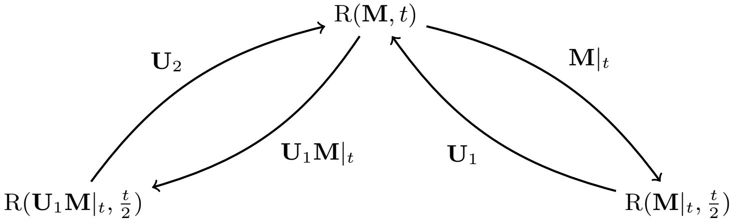
Divide-&-Conquer Trick

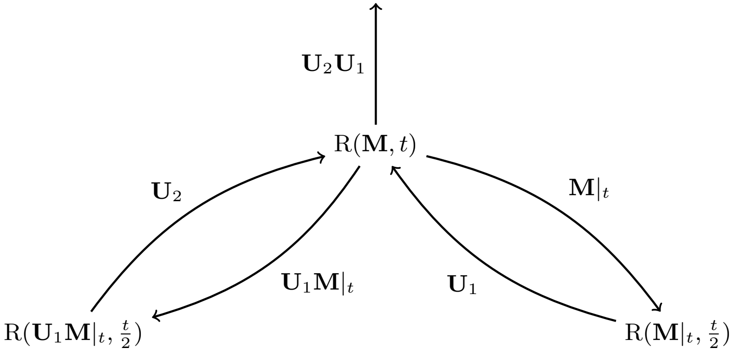


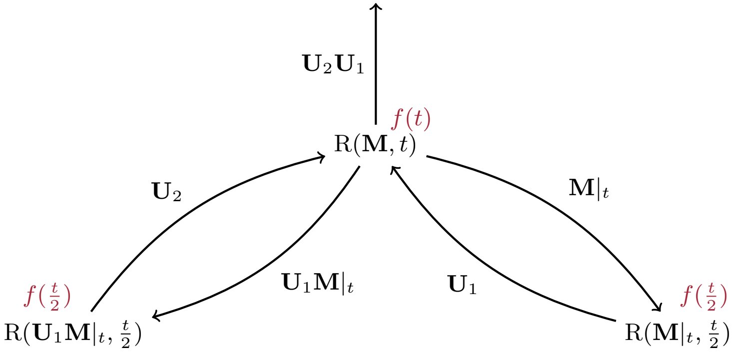
Divide-&-Conquer Trick



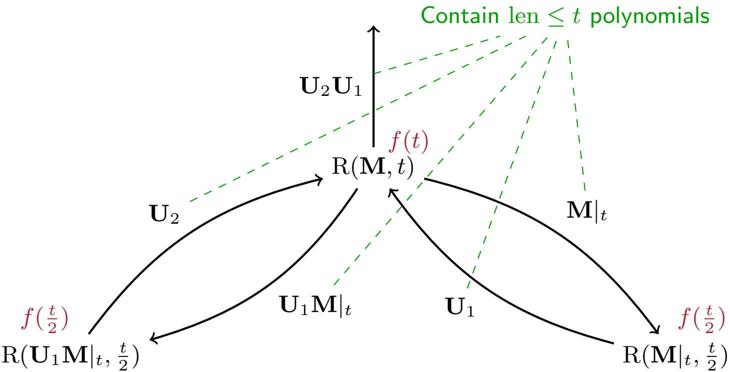
Divide-&-Conquer Trick



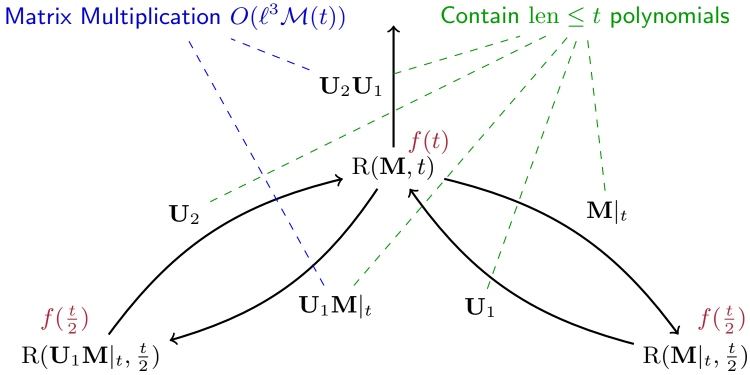

$\mathbf{U}_2\mathbf{U}_1$
$\mathrm{R}(\mathbf{M}, t)$
$\mathbf{U}_2$
$\mathbf{M}|_t$
$\mathbf{U}_1\mathbf{M}|_t$
$\mathbf{U}_1$
$\mathrm{R}(\mathbf{U}_1\mathbf{M}|_t, \frac{t}{2})$
$\mathrm{R}(\mathbf{M}|_t, \frac{t}{2})$



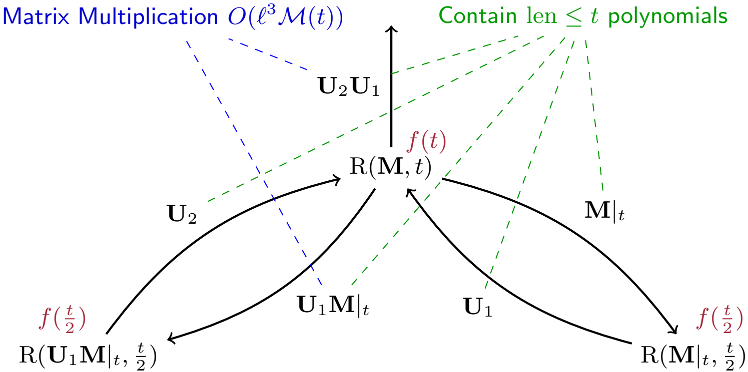
$$f(t) = 2 \cdot f(\tfrac{t}{2}) +$$



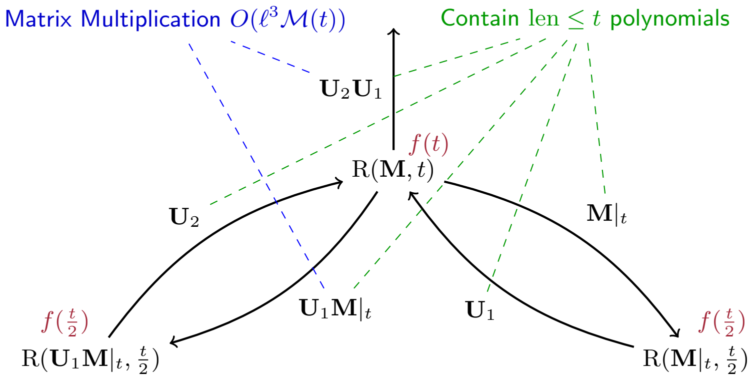
$f(t) = 2 \cdot f(\frac{t}{2}) +$



$$f(t) = 2 \cdot f(\tfrac{t}{2}) + O(\ell^3 \mathcal{M}(t))$$



$$f(t) = 2 \cdot f(\tfrac{t}{2}) + O(\ell^3 \mathcal{M}(t)) \overset{\text{master theorem}}{\Longrightarrow} f(t) \in O(\ell^3 \mathcal{M}(t))$$



$$f(t) = 2 \cdot f(\tfrac{t}{2}) + O(\ell^3\mathcal{M}(t)) \quad \overset{\text{master theorem}}{\Longrightarrow} \quad f(t) \in O(\ell^3\mathcal{M}(t))$$

Overall Complexity (ℓ interleaving degree, n codelength)

$$t \in O(n) \quad \Longrightarrow \quad O(\ell^3\mathcal{M}(n))$$

Outline

NACHRICHTENTECHNIK
Universität Ulm

Conclusion

Decoding Algorithm	Complexity
Skew Berlekamp–Massey [SJB11]	$O(\ell n^2)$
Skew Berlekamp–Massey (D&C) [SB14]	$O(\ell^3 \mathcal{M}(n) \log(n))$
Skew Demand-Driven [LNPS15]	$O(\ell n^2)$
Skew Alekhnovich [this paper]	$O(\ell^3 \mathcal{M}(n)) \subseteq O(\ell^3 n^{1.69})$*

*If $\ell^2 \in o(\log(n))$, additional $\log(n)$ (ℓ divisions of $O(n^{1.69} \log(n))$ [PW16])

[SJB11] Sidorenko, Jiang, Bossert, "Skew-Feedback Shift-Register Synthesis and Decoding Interleaved Gabidulin Codes," *IEEE Trans. Inf. Theory*, 2011.

[SB14] Sidorenko, Bossert, "Fast Skew-Feedback Shift-Register Synthesis," *Designs, Codes & Cryptography*, 2014.

[LNPS15] Li, Nielsen, Puchinger, and Sidorenko, "Solving Shift Register Problems over Skew Polynomial Rings using Module Minimisation," *WCC*, 2015.

[PW16] Puchinger, Wachter-Zeh, "Sub-Quadratic Decoding of Gabidulin Codes," *ISIT*, 2016.

NACHRICHTENTECHNIK Universität Ulm

Decoding Algorithm	Complexity
Skew Berlekamp–Massey [SJB11]	$O(\ell n^2)$
Skew Berlekamp–Massey (D&C) [SB14]	$O(\ell^3 \mathcal{M}(n) \log(n))$
Skew Demand-Driven [LNPS15]	$O(\ell n^2)$
Skew Alekhnovich [this paper]	$O(\ell^3 \mathcal{M}(n)) \subseteq O(\ell^3 n^{1.69})^*$

Usually $\ell \ll n$

*If $\ell^2 \in o(\log(n))$, additional $\log(n)$ (ℓ divisions of $O(n^{1.69} \log(n))$ [PW16])

[SJB11] Sidorenko, Jiang, Bossert, "Skew-Feedback Shift-Register Synthesis and Decoding Interleaved Gabidulin Codes," *IEEE Trans. Inf. Theory*, 2011.

[SB14] Sidorenko, Bossert, "Fast Skew-Feedback Shift-Register Synthesis," *Designs, Codes & Cryptography*, 2014.

[LNPS15] Li, Nielsen, Puchinger, and Sidorenko, "Solving Shift Register Problems over Skew Polynomial Rings using Module Minimisation," *WCC*, 2015.

[PW16] Puchinger, Wachter-Zeh, "Sub-Quadratic Decoding of Gabidulin Codes," *ISIT*, 2016.

Conclusion

Decoding Algorithm	Complexity
Skew Berlekamp–Massey [SJB11]	$O(\ell n^2)$
Skew Berlekamp–Massey (D&C) [SB14]	$O(\ell^3 \mathcal{M}(n) \log(n))$
Skew Demand-Driven [LNPS15]	$O(\ell n^2)$
Skew Alekhnovich [this paper]	$O(\ell^3 \mathcal{M}(n)) \subseteq O(\ell^3 n^{1.69})^*$

Usually $\ell \ll n \quad \Longrightarrow \quad$ BM D&C and Alekhnovich are fastest

*If $\ell^2 \in o(\log(n))$, additional $\log(n)$ (ℓ divisions of $O(n^{1.69} \log(n))$ [PW16])

[SJB11] Sidorenko, Jiang, Bossert, "Skew-Feedback Shift-Register Synthesis and Decoding Interleaved Gabidulin Codes," *IEEE Trans. Inf. Theory*, 2011.

[SB14] Sidorenko, Bossert, "Fast Skew-Feedback Shift-Register Synthesis," *Designs, Codes & Cryptography*, 2014.

[LNPS15] Li, Nielsen, Puchinger, and Sidorenko, "Solving Shift Register Problems over Skew Polynomial Rings using Module Minimisation," *WCC*, 2015.

[PW16] Puchinger, Wachter-Zeh, "Sub-Quadratic Decoding of Gabidulin Codes," *ISIT*, 2016.