A crash course on Order Bases : Theory and Algorithms

by Romain Lebreton

Université Montpellier 2

CLIC 2014 Seminar
Université de Versailles – Saint-Quentin en Yvelines
–
Decembre 10th, 2014

What is this talk about ?

Context:

Two different worlds

Result. The reduction of lattices over $\mathbb{F}[x]$ takes polynomial time.	versus	**Result.** The reduction of lattices over $\mathbb{Z}$ is NP-hard.

Reduction of polynomial lattices is an important tool :

- Application to the decoding of generalized Reed-Solomon codes

Today's talk :

Ideas and tools to reduce $\mathbb{F}[x]$-lattices in polynomial time with the best current exponents.

Motivation for order bases

The following problems with matrices over a field $\mathbb{F}$ have **equivalent** $\mathcal{O}$-complexity

- multiplying two matrices
- inverting a matrix
- computing the determinant of a matrix
- solving a linear system, $\ldots$

Question : What happens when working with matrices over $\mathbb{F}[x]$

Motivation for order bases

The following problems with matrices over a field $\mathbb{F}$ have **equivalent** $\mathcal{O}$-complexity

- multiplying two matrices
- inverting a matrix
- computing the determinant of a matrix
- solving a linear system, ...

Question : What happens when working with matrices over $\mathbb{F}[x]$

Answer :

- Determinant is still equivalent to multiplication

  Other operations such as order bases, column reduction are also equivalent
- Inversion is NOT (because of the size of the output)

$\rightsquigarrow$ **Order basis is a fundamental tool when working with polynomial matrices to reduce many problems to multiplication**

Outline of the talk

1. Polynomial matrix multiplication in time $\mathcal{O}(m^\omega\, d)$

2. Order bases in $\tilde{\mathcal{O}}(m^\omega\, d)$

   a. Definition and properties

   b. Algorithms and complexity

3. Lattice reduction in $\tilde{\mathcal{O}}(m^\omega\, d)$

Polynomial matrix multiplication

Settings.

- Let $\mathbb{F}$ be a field
- Let $\mathbb{F}[x]_{\leqslant d}$ be polynomials over $\mathbb{F}$ of degree $\leqslant d$
- Let $\mathbb{F}[x]^{m \times n}$ be m by n matrices with polynomial coefficients

Complexity notations

- Multiplication in $\mathbb{F}[x]_{\leqslant d}$ $\quad \mathsf{M}(d) = \mathcal{O}(d \log d \log \log d)$
- Multiplication in $\mathbb{F}^{n \times n}$ $\quad \mathsf{MM}(n) = \mathcal{O}(n^{\omega})$
- Multiplication in $(\mathbb{F}[x]_{\leqslant d})^{n \times n}$ $\quad \mathsf{MM}(n,d) = \mathcal{O}(\mathsf{MM}(n)\,\mathsf{M}(d)) = \tilde{\mathcal{O}}(n^{\omega} d)$

Note:

$\mathsf{MM}(n,d) = \mathcal{O}(\mathsf{MM}(n)\, d + n^2\, \mathsf{M}(d))$ via evaluation/interpolation on a geometric sequence

Outline of the talk

1. Polynomial matrix multiplication in time $\mathcal{O}(m^\omega\, d)$

2. Order bases in $\tilde{\mathcal{O}}(m^\omega\, d)$

   a. Definition and properties

   b. Algorithms and complexity

3. Lattice reduction in $\tilde{\mathcal{O}}(m^\omega\, d)$

Order basis - Definition

Settings.

Let $F \in \mathbb{F}[x]^{m \times n}$.

Let (F, σ) be the $\mathbb{F}[x]$-module of

$$\{v \in \mathbb{F}[x]^{1 \times m} \text{ such that } v\,F = 0 \bmod x^{\sigma}\}.$$

Remark.

$$x^{\sigma}\,\mathbb{F}[x]^{1 \times m} \subseteq (F, \sigma) \subseteq \mathbb{F}[x]^{1 \times m}$$

so (F, σ) is a $\mathbb{F}[x]$-module of dimension m.

Definition

An (F, σ) order basis P is a $\mathbb{F}[x]$-module basis of (F, σ) of minimal degree.

$\rightsquigarrow$ What is the notion of degree ?

$\rightsquigarrow$ Minimality for which order ?

Row degree - Definition

Definition of row degree

1. *Row degree of a row vector:* $\mathrm{rdeg}(P_1, \ldots, P_n) = \max\,(\deg P_i) \in \mathbb{Z}$

2. *Row degree of a matrix:* $\mathrm{rdeg}\left(\begin{pmatrix} \mathrm{row}\,1 \\ \vdots \\ \mathrm{row}\,m \end{pmatrix}\right) = (\mathrm{rdeg}\,(\mathrm{row}\,i))_{i=1\ldots m} \in \mathbb{Z}^m$

Example:

$$F = \begin{pmatrix} 1 & 0 & 1 & 1 \\ x & 1 & 1+x & 0 \\ 1 & x^2+x^3 & x & 0 \\ x^2 & 0 & x^3+x^4 & 0 \end{pmatrix} \in \mathbb{F}_2[x]^{4\times 4} \quad \Rightarrow \quad \mathrm{rdeg}\,F = (0,1,3,4) \in \mathbb{Z}^4$$

Problem:

If $(c_1, \ldots, c_m) = (b_1, \ldots, b_m) \cdot A$ then $\mathrm{rdeg}(\boldsymbol{c})$ is not necessarily related to $\mathrm{rdeg}(\boldsymbol{b})$ and $\mathrm{rdeg}(A)$

$\rightsquigarrow$ Notion of shifted degree

Shifted row degree - Definition

Definition of shifted row degree

Let $\vec{s} = (s_1, \ldots, s_n) \in \mathbb{Z}^n$.

1. *Shifted row degree of a row vector:* $\operatorname{rdeg}_{\vec{s}}(P_1, \ldots, P_n) = \max\left(\deg P_i + s_i\right) \in \mathbb{Z}$

2. *Row degree of a matrix:* $\operatorname{rdeg}_{\vec{s}}\left(\begin{pmatrix} \text{row } 1 \\ \vdots \\ \text{row } m \end{pmatrix}\right) = (\operatorname{rdeg}_{\vec{s}}(\text{row } i))_{i=1\ldots m} \in \mathbb{Z}^m$

Remark 1: If $x^{\vec{s}} = \begin{pmatrix} x^{s_1} & & \\ & \ddots & \\ & & x^{s_n} \end{pmatrix}$ then $\operatorname{rdeg}_{\vec{s}}(A) = \operatorname{rdeg}(A \cdot x^{\vec{s}})$.

Example:

If $F = \begin{pmatrix} 1 & 0 & 1 & 1 \\ x & 1 & 1+x & 0 \\ 1 & x^2+x^3 & x & 0 \\ x^2 & 0 & x^3+x^4 & 0 \end{pmatrix}$ then

$$\operatorname{rdeg}_{(1,0,0,1)} F = \operatorname{rdeg}(F \cdot x^{\vec{s}}) = \operatorname{rdeg}\begin{pmatrix} x & 0 & 1 & x \\ x^2 & 1 & 1+x & 0 \\ x & x^2+x^3 & x & 0 \\ x^3 & 0 & x^3+x^4 & 0 \end{pmatrix} = (1,2,3,4) \in \mathbb{Z}^4$$

Shifted row degree - Definition

Definition of shifted row degree

Let $\vec{s} = (s_1, \ldots, s_n) \in \mathbb{Z}^n$.

1. *Shifted row degree of a row vector:* $\mathrm{rdeg}_{\vec{s}}(P_1, \ldots, P_n) = \max\,(\deg P_i + s_i) \in \mathbb{Z}$

2. *Row degree of a matrix:* $\mathrm{rdeg}_{\vec{s}}\left(\begin{pmatrix} \mathrm{row}\,1 \\ \vdots \\ \mathrm{row}\,m \end{pmatrix}\right) = (\mathrm{rdeg}_{\vec{s}}(\mathrm{row}\,i))_{i=1\ldots m} \in \mathbb{Z}^m$

Remark 2: $\mathrm{rdeg}_{\vec{s}}(A) = \vec{v}$ if and only if $\mathrm{rdeg}(x^{-\vec{v}} \cdot A \cdot x^{\vec{s}}) = (0, \ldots, 0)$

Example:

If $F = \begin{pmatrix} 1 & 0 & 1 & 1 \\ x & 1 & 1+x & 0 \\ 1 & x^2+x^3 & x & 0 \\ x^2 & 0 & x^3+x^4 & 0 \end{pmatrix}$, $\vec{u} := (1, 0, 0, 1)$, then $\vec{v} := \mathrm{rdeg}_{\vec{u}}(F) = (1, 2, 3, 4)$ and

$$x^{-\vec{v}} \cdot A \cdot x^{\vec{u}} = \begin{pmatrix} 1 & 0 & x^{-1} & 1 \\ 1 & x^{-2} & x^{-2}+x^{-1} & 0 \\ x^{-2} & x^{-1}+1 & x^{-2} & 0 \\ x^{-1} & 0 & x^{-1}+1 & 0 \end{pmatrix}$$

Shifted row degree - Properties

Definition of shifted row degree

Let $\vec{s} = (s_1, \ldots, s_n) \in \mathbb{Z}^n$.

1. *Shifted row degree of a row vector:* $\mathrm{rdeg}_{\vec{s}}(P_1, \ldots, P_n) = \max\,(\deg P_i + s_i) \in \mathbb{Z}$

2. *Row degree of a matrix:* $\mathrm{rdeg}_{\vec{s}}\left(\begin{pmatrix} \text{row } 1 \\ \vdots \\ \text{row } m \end{pmatrix}\right) = (\mathrm{rdeg}_{\vec{s}}(\text{row } i))_{i=1\ldots m} \in \mathbb{Z}^m$

Lemma - Transity of the shifted degree

Let $\boldsymbol{c} := \boldsymbol{b} \cdot A$, $\vec{v} = \mathrm{rdeg}_{\vec{u}}(A)$ and $w = \mathrm{rdeg}_{\vec{v}}(\boldsymbol{b})$, then

$$\mathrm{rdeg}_{\vec{u}}(\boldsymbol{c}) \leqslant w.$$

Proof.

- Reminder : $\mathrm{rdeg}_{\vec{u}}(\boldsymbol{c}) \leqslant \vec{v}$ if and only if $\mathrm{rdeg}(x^{-w} \cdot \boldsymbol{c} \cdot x^{\vec{u}}) \leqslant 0$
- Then $x^{-w} \cdot \boldsymbol{c} \cdot x^{\vec{u}} = x^{-w} \cdot (\boldsymbol{b} \cdot A) \cdot x^{\vec{u}} = \underbrace{(x^{-w} \cdot \boldsymbol{b} \cdot x^{\vec{v}})}_{\mathrm{rdeg}() \leqslant 0} \cdot \underbrace{(x^{-\vec{v}} \cdot A \cdot x^{\vec{u}})}_{\mathrm{rdeg}() \leqslant 0}$ so $\mathrm{rdeg}(x^{-w} \cdot \boldsymbol{c} \cdot x^{\vec{u}}) \leqslant 0$

$\square$

Order on row degrees

Definition

Let $\vec{u} = (u_1, \ldots, u_m), \vec{v} = (v_1, \ldots, v_m) \in \mathbb{Z}^m$ *be two row degrees.*

We say $\vec{u} \leqslant_{\mathrm{ob}} \vec{v}$ *if for all* i, $u_i \leqslant v_i$.

Facts on $\mathbb{F}[x]$-module bases:

- $U \in \mathbb{F}[x]^{m \times m}$ is said unimodular if $\det(U) \in \mathbb{F} \backslash \{0\}$
- U is unimodular iif U is invertible in $\mathbb{F}[x]^{m \times m}$
- If P, Q are two row bases of the same $\mathbb{F}[x]$-module then $\exists U$ unimodular s.t. $P = U \cdot Q$

Definition

A matrix $F \in \mathbb{F}[x]^{m \times n}$ *is row-reduced if for any* U *unimodular* $\mathrm{rdeg}(F) \leqslant_{\mathrm{ob}} \mathrm{rdeg}(U \cdot F)$

Some properties of row reduceness

Definition

If $\vec{v} := \mathrm{rdeg}_{\vec{u}}(A)$ *then the* *leading coefficient matrix* $\mathrm{lcoeff}(A) \in \mathbb{F}^{m\times n}$ *of* A *is the constant coefficient of* $x^{-\vec{v}} \cdot A \cdot x^{\vec{s}}$.

Example:

If $F = \begin{pmatrix} 1 & 0 & 1 & 1 \\ x & 1 & 1+x & 0 \\ 1 & x^2+x^3 & x & 0 \\ x^2 & 0 & x^3+x^4 & 0 \end{pmatrix}$ then

- $\vec{v} := \mathrm{rdeg}(F) = (1, 2, 3, 4)$,
- $x^{-\vec{v}} \cdot A \cdot x^{\vec{s}} = \begin{pmatrix} 1 & 0 & x^{-1} & 1 \\ 1 & x^{-2} & x^{-2}+x^{-1} & 0 \\ x^{-2} & x^{-1}+1 & x^{-2} & 0 \\ x^{-1} & 0 & x^{-1}+1 & 0 \end{pmatrix}$,
- $\mathrm{lcoeff}(A) = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

Remark : $x^{-\vec{v}} \cdot A \cdot x^{\vec{s}} = \mathrm{lcoeff}(A) + \mathcal{O}_{x\to\infty}(x^{-1})$

Some properties of row reduceness

Definition

If $\vec{v} := \mathrm{rdeg}_{\vec{u}}(A)$ *then the* *leading coefficient matrix* $\mathrm{lcoeff}(A)$ *of* A *is the constant coefficient of* $x^{-\vec{v}} \cdot A \cdot x^{\vec{s}}$.

Lemma

If $\mathrm{lcoeff}(A)$ *is (left) injective, then* A *is row reduced.*

Proof.

Lemma - Transity of the shifted degree (revisited)

Let $\boldsymbol{c} := \boldsymbol{b} \cdot A$, $\vec{v} = \mathrm{rdeg}_{\vec{u}}(A)$ and $w = \mathrm{rdeg}_{\vec{v}}(\boldsymbol{b})$.

If $\mathrm{lcoeff}(A)$ is injective then $\mathrm{rdeg}_{\vec{u}}(\boldsymbol{c}) = w$.

Proof.

- Reminder : $\mathrm{rdeg}_{\vec{u}}(\boldsymbol{c}) = \vec{v} \Leftrightarrow \mathrm{rdeg}(x^{-w} \cdot \boldsymbol{c} \cdot x^{\vec{u}}) = 0$
- Then $x^{-w} \cdot \boldsymbol{c} \cdot x^{\vec{u}} = \underbrace{(x^{-w} \cdot \boldsymbol{b} \cdot x^{\vec{v}})}_{\substack{\mathrm{lcoeff}(\boldsymbol{b}) \text{ is} \\ a \text{ non zero vector}}} \cdot \underbrace{(x^{-\vec{v}} \cdot A \cdot x^{\vec{u}})}_{\substack{\mathrm{lcoeff}(A) \text{ is} \\ \text{an injective matrix}}}$ so $\mathrm{lcoeff}(\boldsymbol{c})$ is a non zero vector $\square$

Some properties of row reduceness

Definition

If $\vec{v} := \mathrm{rdeg}_{\vec{u}}(A)$ *then the* *leading coefficient matrix* $\mathrm{lcoeff}(A)$ *of* A *is the constant coefficient of* $x^{-\vec{v}} \cdot A \cdot x^{\vec{s}}$.

Lemma

If $\mathrm{lcoeff}(A)$ *is (left) injective, then* A *is row reduced.*

Proof.

Lemma - Transity of the shifted degree (revisited)

Let $\boldsymbol{c} := \boldsymbol{b} \cdot A$, $\vec{v} = \mathrm{rdeg}_{\vec{u}}(A)$ and $w = \mathrm{rdeg}_{\vec{v}}(\boldsymbol{b})$.

If $\mathrm{lcoeff}(A)$ is injective then $\mathrm{rdeg}_{\vec{u}}(\boldsymbol{c}) = w$.

Let U be unimodular and $\vec{u} := \mathrm{rdeg}(A)$.

Since $\mathrm{lcoeff}(A)$ is injective, $\mathrm{rdeg}(U \cdot A) = \mathrm{rdeg}_{\vec{u}}(U) \geqslant \vec{u} = \mathrm{rdeg}(A)$.

So A is row-reduced. $\square$

Some properties of row reduceness

Definition

If $\vec{v} := \mathrm{rdeg}_{\vec{u}}(A)$ *then the leading coefficient matrix* $\mathrm{lcoeff}(A)$ *of* A *is the constant coefficient of* $x^{-\vec{v}} \cdot A \cdot x^{\vec{s}}$*.*

Lemma

If $\mathrm{lcoeff}(A)$ *is (left) injective, then* A *is row reduced.*

Note : In fact, $\mathrm{lcoeff}(A)$ injective $\Leftrightarrow$ A is row reduced.

Order basis - Existence

Settings (reminder).

- $F \in \mathbb{F}[x]^{m\times n}$,
- $(F,\sigma) := \{v \in \mathbb{F}[x]^{1\times m} \text{ such that } v\,F = 0 \bmod x^\sigma\}$.

Definition

An (F,σ) order basis P is a $\mathbb{F}[x]$-module basis of (F,σ) that is row-reduced.

Proposition

There exists a row-reduced basis P.

Example

$$\underbrace{\begin{pmatrix} 1 & 0 & 1 & 1 \\ x & 1 & 1+x & 0 \\ 1 & x^2+x^3 & x & 0 \\ x^2 & 0 & x^3+x^4 & 0 \end{pmatrix}}_{(F,8,\vec{0})-\text{order basis over } \mathbb{F}_2} \underbrace{\begin{pmatrix} x+x^2+x^3+x^4+x^5+x^6 \\ 1+x+x^5+x^6+x^7 \\ 1+x^2+x^4+x^5+x^6+x^7 \\ 1+x+x^3+x^7 \end{pmatrix}}_{F \text{ in } \mathbb{F}_2[x]^{4\times 1}} = 0^{4\times 1} \bmod x^8$$

Order basis - Existence

Settings (reminder).

- $F \in \mathbb{F}[x]^{m \times n}$,
- $(F, \sigma) := \{v \in \mathbb{F}[x]^{1 \times m} \text{ such that } v\,F = 0 \bmod x^\sigma\}$.

Definition

An (F, σ) order basis P is a $\mathbb{F}[x]$-module basis of (F, σ) that is row-reduced.

Proposition

There exists a row-reduced basis P of (F, σ).

Remark

Existence but no unicity ($\rightsquigarrow$ Popov form).

Order basis - Proof of existence

Proposition

There exists a row-reduced basis P of (F, σ).

Naive proof (incorrect).

Consider the minimum of all the sorted $\mathrm{rdeg}(P \cdot U)$ for all unimodular matrices $U \in \mathbb{F}[x]^{m \times m}$.

$\Rightarrow$ any basis $P \cdot U$ with minimal degree is an *order basis*.

Careful. The order $\leqslant_{\mathrm{ob}}$ on basis is NOT a total order.

We could have two bases whose row degrees are $(1, 2, 3)$ and $(1, 1, 4)$!

$\rightsquigarrow$ We can not guarantee the existence of a minimum (yet!).

Order basis - Proof of existence

Weak-Popov form:

Let $[d]$ denote a polynomial of degree d

Row pivot is the rightmost element of maximal degree

A matrix W is in weak-Popov form if pivots have distinct indices

Example.

$$W = \begin{pmatrix} [1] & [1] & [1] & {\color{red}[1]} \\ {\color{red}[2]} & [1] & [1] & [1] \\ [1] & [2] & {\color{red}[2]} & [1] \\ [3] & {\color{red}[4]} & [3] & [3] \end{pmatrix}$$

Order basis - Proof of existence

[Mulders, Storjohann, 2003] Algorithm:

Algorithm - [Mulders, Storjohann, 2003]

Input : $A \in \mathbb{F}[x]^{m \times n}$
Output : its weak-Popov form $W \in \mathbb{F}[x]^{m \times n}$

Algorithm :

1. Add monomial multiples of one row to another to
   - $\longrightarrow$ either move a pivot to the left
   - $\longrightarrow$ or decrease the degree of a row
2. Stop when no more transformations are possible

Example.

$$\begin{pmatrix} [3] & [3] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{pmatrix} \xrightarrow{(1)} \begin{pmatrix} [3] & [2] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{pmatrix} \xrightarrow{(2)} \begin{pmatrix} [2] & [2] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{pmatrix}$$

(1) add $*x^2$ times second row to first row (appropriate $* \in \mathbb{F}$)

(2) add $*$ times last row to first row

- final matrix is in weak Popov form (distinct pivot locations)

Order basis - Proof of existence

Proposition

There exists a row-reduced basis P of (F,σ).

Proof.

Apply [Mulders, Storjohann, 2003] to a row basis R of (F,σ).

Transformations are unimodular so $W = U \cdot R$ with U unimodular.

W has distinct pivot locations so $\mathrm{lcoeff}(W)$ is injective $\Rightarrow$ W is row reduced.

$\square$

Notes.

1. Weak Popov $\Rightarrow$ Row reduced
2. Complexity of [Mulders, Storjohann, 2003] : $\mathcal{O}(n^3\,d^2)$

   $\rightsquigarrow$ we can do better

Outline of the talk

1. Polynomial matrix multiplication in time $\mathcal{O}(m^\omega\, d)$

2. Order bases in $\tilde{\mathcal{O}}(m^\omega\, d)$

   a. Definition and properties

   b. Algorithms and complexity

3. Lattice reduction in $\tilde{\mathcal{O}}(m^\omega\, d)$

Order basis algorithms - Base case $\sigma = 1$

Basic ideas if $\sigma = 1$ and $F \in \mathbb{F}^{m \times n}$:

- If $\begin{pmatrix} S \\ K \end{pmatrix} F = \begin{pmatrix} R \\ 0 \end{pmatrix}$ with R full rank **then** $\begin{pmatrix} x\,S \\ K \end{pmatrix} F = \begin{pmatrix} x\,R \\ 0 \end{pmatrix} = 0 \bmod x$

  $\rightsquigarrow$ $\begin{pmatrix} x\,S \\ K \end{pmatrix}$ is a basis of the module $(F, 1)$.

- Take a supplementary S of the kernel K that involves the smallest degree lines of F

  $\rightsquigarrow$ consider the row echelon form of F

Algorithm:

Algorithm Basis

Input: $F \in (\mathbb{F}[x]_{\leqslant 0})^{m \times n}$ and a shift vector $\vec{s}$
Output: an $(F, 1, \vec{s})$ order basis and its $\vec{s}$-row degree
Algorithm:

1. Assume $\vec{s}$ is increasing
2. Compute a row echelon form $F = \tau \cdot L \cdot E$ with $r = \mathrm{rank}(E)$
   τ a permutation, $L = \begin{pmatrix} L_r & 0 \\ G & I_{m-r} \end{pmatrix}$ lower triangular, $E = \begin{pmatrix} E' \\ 0 \end{pmatrix}$ row echelon
3. **return** $\begin{pmatrix} x\,L_r & 0 \\ G & I_{m-r} \end{pmatrix}$, $\tau^{-1}\vec{s} + [1_r, 0_{n-r}]$

Splitting the order basis problem

How can we split the order basis problem?

1. Let P_1 be a $(F, \sigma_1, \vec{s})$ order basis of $\vec{s}$-row degree $\vec{u}$

   Let $M \in \mathbb{F}[x]^{m \times n}$ be s.t. $P_1 F = x^{\sigma_1} M$

2. Let P_2 be a $(M, \sigma_2, \vec{u})$ order basis of $\vec{u}$-row degree $\vec{v}$

3. Remark: $P_2 P_1 F = P_2 (x^{\sigma_1} M) = x^{\sigma_1} (P_2 M) = 0 \bmod x^{\sigma_1 + \sigma_2}$

Theorem

$P_2 P_1$ is a $(F, \sigma_1 + \sigma_2, \vec{s})$ order basis of $\vec{s}$-row degree $\vec{v}$.

Remarks.

- The module $(F, \sigma_1 + \sigma_2, \vec{s})$ is a subset of $(F, \sigma_1, \vec{s})$ of basis P_1

  $\rightsquigarrow$ Express the module $(F, \sigma_1 + \sigma_2, \vec{s})$ on the basis $P_1 \longrightarrow$ reduce the problem

- Need of $\vec{s}$-row degree:

  Change of basis by $P_1 \Rightarrow$ shift the row degree by $\vec{s} := \mathrm{rdeg}(P_1)$ $\square$

Order basis algorithms

Input: $F \in (\mathbb{F}[x]_{<\sigma})^{m \times n}$, a shift vector $\vec{s}$ and an order $\sigma \in \mathbb{N}$

Output: an $(F, \sigma, \vec{s})$ order basis and its $\vec{s}$-row degree

1. Quadratic algorithm M-Basis

Iterative : $(F, 1) \to (F, 2) \to (F, 3) \to \cdots \to (F, \sigma)$

Algorithm M-Basis

1. $P_0 := \text{Basis}(F \bmod x)$
2. **for** $k = 1, \ldots, \sigma - 1$ **do**
3. $\quad F' := x^{-k} P_{k-1} F$
4. $\quad M_k := \text{Basis}(F' \bmod x)$
5. $\quad P_k := M_k P_{k-1}$
6. **return** $P_{\sigma-1}$

In terms of polynomial multiplication, naive multiplication $P_{\sigma-1} = M_{\sigma-1} (\cdots M_3 (M_2 M_1))$ where each M_i is of degree one.

Complexity: $\mathcal{O}(m^\omega \sigma^2)$

Existing order basis algorithms

Input: $F \in (\mathbb{F}[x]_{<\sigma})^{m \times n}$, a shift vector $\vec{s}$ and an order $\sigma \in \mathbb{N}$

Output: an $(F, \sigma, \vec{s})$ order basis and its $\vec{s}$-row degree

2. Quasi-linear algorithm PM-Basis

Divide-and-conquer : $(F,1) \to (F,2) \to (F,4) \to \cdots \to (F,\sigma/2) \to (F,\sigma)$

Algorithm PM-Basis

1. **if** $\sigma = 1$ **then**
2.   **return** Basis$(F \bmod x)$
3. **else**
4. $P_{\text{low}} :=$ PM-Basis$(F, \lfloor \sigma/2 \rfloor)$ — First subproblem
5.   Let F' be s.t. $P_{\text{low}} \cdot F = x^{\lfloor \sigma/2 \rfloor} \cdot F'$ — Update problem
6. $P_{\text{high}} :=$ PM-Basis$(F', \lceil \sigma/2 \rceil)$ — Second subproblem
7. **return** $P_{\text{high}} \cdot P_{\text{low}}$ — Solve original problem

In terms of polynomial multiplication, binary multiplication tree.

Complexity: $\mathcal{O}(\mathsf{MM}(m,\sigma)\log(\sigma))$

Outline of the talk

1. Polynomial matrix multiplication in time $\mathcal{O}(m^\omega\, d)$

2. Order bases in $\tilde{\mathcal{O}}(m^\omega\, d)$

    a. Definition and properties

    b. Algorithms and complexity

3. Lattice reduction in $\tilde{\mathcal{O}}(m^\omega\, d)$

Lattice reduction

How can we compute the row reduction of a matrix :

- [Mulders, Storjohann, 2003] complexity is $\mathcal{O}(n^3\, d^2)$
- Let's sketch the ideas to get to $\tilde{\mathcal{O}}(n^\omega\, d)$

Let $A \in \mathbb{F}[x]^{m \times m}$ be the matrix to reduce and R its row-reduction.

We want to express R as an order basis $\rightsquigarrow$ R would be row reduced.

Let U be unimodular such that $U \cdot A = R$.

Example of an $A \in \mathbb{F}[x]^{30 \times 30}$ with degree 12

$$\overset{U}{\begin{bmatrix} [299] & \ldots & [300] \\ \vdots & \ddots & \vdots \\ [303] & \ldots & [304] \end{bmatrix}} \cdot \overset{A}{\begin{bmatrix} [12] & \ldots & [11] \\ \vdots & \ddots & \vdots \\ [12] & \ldots & [10] \end{bmatrix}} = \overset{R}{\begin{bmatrix} [0] & \ldots & [0] \\ \vdots & \ddots & \vdots \\ [1] & \ldots & [4] \end{bmatrix}}$$

Remark. If A is of degree d, U can have degree $m\, d$

Lattice reduction

Let $A \in \mathbb{F}[x]^{m \times m}$ be the matrix to reduce and R its row-reduction.

We want to express R as an order basis $\rightsquigarrow$ R would be row reduced.

Let U be unimodular such that $U \cdot A = R$.

Then $\begin{pmatrix} U & R \end{pmatrix} \cdot \begin{pmatrix} A \\ -I \end{pmatrix} = 0$

Idea 1:

Compute an $(F, \sigma, \vec{s})$ order basis with

$$F := \begin{pmatrix} A \\ -I \end{pmatrix}, \ \sigma := m\,d + d + 1 \text{ and } \vec{s} := (1, \ldots, 1, m\,d, \ldots, m\,d)$$

The order basis will be $\begin{pmatrix} U & R \\ * & * \end{pmatrix}$

Cost: $\tilde{\mathcal{O}}(m^{\omega}\,(m\,d))$

Lattice reduction

Let $A \in \mathbb{F}[x]^{m\times m}$ be the matrix to reduce and R its row-reduction.

We want to express R as an order basis $\rightsquigarrow$ R would be row reduced.

Let U be unimodular such that $U \cdot A = R$.

Then $\begin{pmatrix} U & R \end{pmatrix} \cdot \begin{pmatrix} A \\ -I \end{pmatrix} = 0$

Idea 2 : Use the dual space

$\begin{pmatrix} R & U \end{pmatrix} \cdot \begin{pmatrix} A^{-1} \\ -I \end{pmatrix} = 0$

$\rightsquigarrow$ U is still of degree $m \cdot d$

Lattice reduction

Idea 2 : Use the dual space

$$\begin{pmatrix} R & U \end{pmatrix} \cdot \begin{pmatrix} A^{-1} \\ -I \end{pmatrix} = 0$$

Idea 3 : Look at an high-order component

On a scalar example

$$\begin{aligned} A^{-1} = \frac{U}{R} &= \frac{1+3\,x+4\,x^2+6\,x^3+x^4}{1+x} \\ &= 1+2\,x+2\,x^2+4\,x^3+4\,x^4+3\,x^5+4\,x^6+3\,x^7+4\,x^8+\cdots \end{aligned}$$

but $(A^{-1}\operatorname{div} x^5)\,x^5 = 3\,x^5+4\,x^6+3\,x^7+4\,x^8+\cdots = \frac{3}{1+x}\,x^5$

So $\begin{pmatrix} R & U' \end{pmatrix} \cdot \begin{pmatrix} A^{-1} \\ -I \end{pmatrix} = 0$ with U' of degree d

Cost : $\tilde{\mathcal{O}}(m^\omega\, d)$

References

[Zhou PhD 2012]

Fast Order Basis and Kernel Basis Computation and Related Problems

[Giorgi, Jeannerod, Villard, 2003]

On the complexity of polynomial matrix computations

[Giorgi, Lebreton, 2014]

Online order basis algorithm and its impact on the block Wiedemann algorithm

[Slides of Storjohann]

Lattice reduction of polynomial matrices

[Beckermann, Labahn, 1994]

A uniform approach for the fast computation of Matrix-type Pade approximants