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

December 10th, 2014
What is this talk about?

Context:

Two different worlds

<table>
<thead>
<tr>
<th>Result.</th>
<th>Result.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The reduction of lattices over $\mathbb{F}[x]$ takes polynomial time.</td>
<td>The reduction of lattices over $\mathbb{Z}$ is NP-hard.</td>
</tr>
</tbody>
</table>

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 $O$-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 $\mathbb{F}[x]$?
Motivation for order bases

The following problems with matrices over a field $\mathbb{F}$ have equivalent $O$-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 $O$-complex (because of the size of the output)  

Order basis is a fundamental tool when working with polynomial matrices to reduce many problems to multiplication.
1. Polynomial matrix multiplication in time $\tilde{O}(m^{\omega}d)$

2. Order bases in $\tilde{O}(m^{\omega}d)$
   a. Definition and properties
   b. Algorithms and complexity

3. Lattice reduction in $\tilde{O}(m^{\omega}d)$
Polynomial matrix multiplication

Settings.

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

Complexity notations

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

Note:

\[ MM(n, d) = \mathcal{O}(MM(n) \ d + n^2 M(d)) \] via evaluation/interpolation on a geometric sequence
1. Polynomial matrix multiplication in time $\tilde{O}(m^\omega d)$

2. Order bases in $\tilde{O}(m^\omega d)$
   a. Definition and properties
   b. Algorithms and complexity

3. Lattice reduction in $\tilde{O}(m^\omega d)$
Order basis - Definition

Settings.

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

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

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

Remark.

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

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

Definition

An \((F, \sigma)\) order basis \(P\) is a \(\mathbb{F}[x]\)-module basis of \((F, \sigma)\) 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:
\[ \text{rdeg}((a_1, \ldots, a_n)) = \max (\deg a_i) \in \mathbb{Z} \]

2. Row degree of a matrix:
\[ \text{rdeg}\left( \begin{pmatrix} \text{row 1} \\ \vdots \\ \text{row } m \end{pmatrix} \right) = (\text{rdeg}(\text{row } i))_{i=1}^{m} \in \mathbb{Z}^m \]

Example:

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

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

\( \sim \) Notion of shifted degree
**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:**
   \[
   \text{rdeg}_\vec{s}((a_1, \ldots, a_n)) = \max (\text{deg } a_i + s_i) \in \mathbb{Z}
   \]

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

**Remark 1:** If \( x^\vec{s} = \begin{pmatrix} x^{s_1} \\ \vdots \\ x^{s_n} \end{pmatrix} \) then \( \text{rdeg}_\vec{s}(A) = \text{rdeg}(A \cdot x^\vec{s}) \).

**Example:**

If \( F = \begin{pmatrix}
1 & 0 & 1 & 1 \\
1 & \frac{1}{x} & 1+x & 0 \\
x & \frac{1}{x^2+x^3} & x & 0 \\
x^2 & 0 & x^3+x^4 & 0
\end{pmatrix} \) and \( \vec{s} := (1, 0, 0, 1) \) then

\[
\text{rdeg}_\vec{s} F = \text{rdeg}(F \cdot x^\vec{s}) = \text{rdeg}
\begin{pmatrix}
x & 0 & 1 & x \\
x^2 & \frac{1}{x} & 1+x & 0 \\
x & \frac{1}{x^2+x^3} & x & 0 \\
x^3 & 0 & x^3+x^4 & 0
\end{pmatrix} = (1, 2, 3, 4) \in \mathbb{Z}^4
\]
**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:**
   \[
   \text{rdeg}_s(P_1, \ldots, P_n) = \max (\deg P_i + s_i) \in \mathbb{Z}
   \]

2. **Row degree of a matrix:**
   \[
   \text{rdeg}_s \left( \begin{array}{c}
   \text{row 1} \\
   \vdots \\
   \text{row m}
   \end{array} \right) = (\text{rdeg}_s(\text{row } i))_{i=1 \ldots m} \in \mathbb{Z}^m
   \]

### Remark 2:

\( \text{rdeg}_s(A) \) is really related to \( x^{-\vec{v}} \cdot A \cdot x^{\vec{s}} \)!

\[
\begin{cases}
\text{rdeg}_s(A) = \vec{v} \\
\text{rdeg}_s(A) \leq \vec{v}
\end{cases}
\]

if and only if

\[
\begin{cases}
\text{rdeg}(x^{-\vec{v}} \cdot A \cdot x^{\vec{s}}) = \vec{v} \\
\text{rdeg}(x^{-\vec{v}} \cdot A \cdot x^{\vec{s}}) \leq \vec{v}
\end{cases}
\]

### 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 \( \vec{v} := \text{rdeg}_u(F) = (1, 2, 3, 4) \)

and

\[
x^{-\vec{v}} \cdot A \cdot x^{\vec{u}} = \begin{pmatrix}
1 & 0 & x^{-1} & 1 \\
1 & x^{-2} & x^{-2} + x^{-1} & 0 \\
x^{-2} & x^{-1} + 1 & x^{-2} & 0 \\
x^{-1} & 0 & x^{-1} + 1 & 0
\end{pmatrix}
\]
Definition of shifted row degree

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

1. Shifted row degree of a row vector:
   \[
   \text{rdeg}_{\bar{s}}(P_1, \ldots, P_n) = \max (\deg P_i + s_i) \in \mathbb{Z}
   \]

2. Row degree of a matrix:
   \[
   \text{rdeg}_{\bar{s}} \begin{pmatrix} \text{row } 1 \\ \vdots \\ \text{row } m \end{pmatrix} = (\text{rdeg}_{\bar{s}}(\text{row } i))_{i=1 \ldots m} \in \mathbb{Z}^m
   \]

Lemma - Transitivity of the shifted degree

Let \( \bar{c} := b \cdot A, \bar{v} = \text{rdeg}_{\bar{u}}(A) \) and \( w = \text{rdeg}_{\bar{v}}(b) \), then
\[
\text{rdeg}_{\bar{u}}(\bar{c}) \leq w.
\]

Proof.

- Reminder: \( \text{rdeg}_{\bar{u}}(\bar{c}) \leq \bar{v} \) if and only if \( \text{rdeg}(x^{-w} \cdot c \cdot x^{\bar{u}}) \leq 0 \)
- Then \( x^{-w} \cdot c \cdot x^{\bar{u}} = x^{-w} \cdot (b \cdot A) \cdot x^{\bar{u}} = (x^{-w} \cdot b \cdot x^{\bar{v}}) \cdot (x^{-\bar{v}} \cdot A \cdot x^{\bar{u}}) \) so \( \text{rdeg}(x^{-w} \cdot c \cdot x^{\bar{u}}) \leq 0 \)
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 \( \vec{u} \leq_{ob} \vec{v} \) if for all \( i \), \( u_i \leq v_i \).

Few facts on \( \mathbb{F}[x] \)-module bases:

- \( U \in \mathbb{F}[x]^{m \times m} \) is said **unimodular** if \( \det(U) \in \mathbb{F} \setminus \{0\} \)
- \( U \) 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 \( \text{rdeg}(F) \leq_{ob} \text{rdeg}(U \cdot F) \)
Order basis - Existence

Settings (reminder).

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

Definition

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

Proposition

There exists a row-reduced basis $P$ of $(F, \sigma)$.

Example

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ x & 1 & 1+x & 0 \\ 1 & x^2 + x^3 & x & 0 \\ x^2 & 0 & x^3 + x^4 & 0 \end{pmatrix} \begin{pmatrix} x + x^2 + x^3 + x^4 + x^5 + x^6 \\ 1 + x + x^5 + x^6 + x^7 \\ 1 + x^2 + x^4 + x^5 + x^6 + x^7 \\ 1 + x + x^3 + x^7 \end{pmatrix} = 0^{4 \times 1} \text{ mod } x^8$$

$(F,8,\bar{0})$—order basis over $\mathbb{F}_2$

$F$ in $\mathbb{F}_2[x]^{4 \times 1}$
Order basis - Existence

Settings (reminder).

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

**Definition**

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

**Proposition**

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

**Remark**

Existence but no unicity (\( \rightsquigarrow \) Popov form).
Order basis - Proof of existence

Proposition

There exists a row-reduced basis $P$ of $(F, \sigma)$.

Naive proof (incorrect).

Consider the minimum of all the sorted $\text{rdeg}(P \cdot U)$ 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 $\leq_{\text{ob}}$ on basis is NOT a total order.

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

$\leadsto$ We can not guarantee the existence of a minimum (yet!).
Some properties of row reduceness

Definition

If \( \vec{v} := \text{rdeg}_u(A) \) then the leading coefficient matrix \( \text{lcoeff}(A) \in \mathbb{F}^{m \times n} \) 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 \( \vec{v} := \text{rdeg}(F) = (1, 2, 3, 4) \) and

\[
x^{-\vec{v}} \cdot A \cdot x^{\vec{s}} = \begin{pmatrix} 1 & 0 & x^{-1} & 1 \\ 1 & x^{-2} & x^{-2}+x^{-1} & 0 \\ x^{-2} & x^{-1}+1 & x^{-2} & 0 \\ x^{-1} & 0 & x^{-1}+1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} + \mathcal{O}_{x \rightarrow \infty}(x^{-1})
\]

\( \text{lcoeff}(A) \)
Some properties of row reduceness

**Definition**

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

**Lemma - Transitivity of the shifted degree (revisited)**

Let \( c := b \cdot A \), \( \vec{v} = \text{rdeg}_u(A) \) and \( w = \text{rdeg}_v(b) \).

If \( \text{lcoeff}(A) \) is (left) injective then \( \text{rdeg}_u(c) = w \).

**Proof.**

- Reminder: \( \text{rdeg}_u(c) = \vec{v} \Leftrightarrow \text{rdeg}(x^{-w} \cdot x^\vec{u}) = 0 \)
- Then \( x^{-w} \cdot c \cdot x^\vec{u} = (x^{-w} \cdot b \cdot x^{\vec{v}}) \cdot (x^{-\vec{v}} \cdot A \cdot x^\vec{u}) \)
  - so \( \text{lcoeff}(c) \) is a non zero vector
  - \( \text{lcoeff}(b) \) is a non zero vector
  - \( \text{lcoeff}(A) \) is an injective matrix
Some properties of row reduceness

Definition

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

Lemma - Criteria for row reduceness

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

Proof.

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

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

So $A$ is row-reduced.

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

\[
W = \begin{pmatrix}
1 & 1 & 1 & 1 \\
2 & 1 & 1 & 1 \\
1 & 2 & 2 & 1 \\
3 & 4 & 3 & 3
\end{pmatrix}
\]
[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
   → either move a pivot to the left
   → or decrease the degree of a row
2. Stop when no more transformations are possible

**Example.**

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

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)
Proposition

There exists a row-reduced basis of $(F, \sigma)$.

Proof.

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

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

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

Notes.

1. Weak Popov $\Rightarrow$ Row reduced

2. Complexity of [Mulders, Storjohann, 2003] : $O(m^3 d^2)$

we will do better
Outline of the talk

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

2. Order bases in $\tilde{O}(m^\omega d)$
   a. Definition and properties
   b. Algorithms and complexity

3. Lattice reduction in $\tilde{O}(m^\omega d)$
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 \[ \begin{pmatrix} xS \\ K \end{pmatrix} F = \begin{pmatrix} xR \\ 0 \end{pmatrix} = 0 \mod x \]

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

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

  $\iff$ consider the row echelon form of $F$

Algorithm:

<table>
<thead>
<tr>
<th>Algorithm Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input:</strong> $F \in (\mathbb{F}[x]_{\leq 0})^{m \times n}$ and a shift vector $\vec{s}$</td>
</tr>
<tr>
<td><strong>Output:</strong> an $(F, 1, \vec{s})$ order basis and its $\vec{s}$-row degree</td>
</tr>
<tr>
<td><strong>Algorithm:</strong></td>
</tr>
<tr>
<td>1. Assume $\vec{s}$ is increasing</td>
</tr>
<tr>
<td>2. Compute a row echelon form $F = \tau \cdot L \cdot E$ with $r = \text{rank}(E)$</td>
</tr>
<tr>
<td>$\tau$ a permutation, $L = \begin{pmatrix} L_r \ G \ I_{m-r} \end{pmatrix}$ lower triangular, $E = \begin{pmatrix} E' \ 0 \end{pmatrix}$ row echelon</td>
</tr>
<tr>
<td>3. return $\begin{pmatrix} xL_r \ G \ I_{m-r} \end{pmatrix}, \tau^{-1} \vec{s} + [1_r, 0_{n-r}]$</td>
</tr>
</tbody>
</table>
Splitting the order basis problem

How can we split the order basis problem?

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

   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 $(M, \sigma_2, \bar{u})$ order basis of $\bar{u}$-row degree $\bar{v}$

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

Theorem

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

Remarks.

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

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

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

  Change of basis by $P_1 \Rightarrow$ shift the row degree by $\bar{s} := \text{rdeg}(P_1)$
Order basis algorithms

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

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

1. **Quadratic algorithm M-Basis**

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

   **Algorithm M-Basis**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>$P_0 := \text{Basis}(F \mod x)$</td>
</tr>
<tr>
<td>2.</td>
<td>for $k = 1, \ldots, \sigma - 1$ do</td>
</tr>
<tr>
<td>3.</td>
<td>$F' := x^{-k} P_{k-1} F$</td>
</tr>
<tr>
<td>4.</td>
<td>$M_k := \text{Basis}(F' \mod x)$</td>
</tr>
<tr>
<td>5.</td>
<td>$P_k := M_k P_{k-1}$</td>
</tr>
<tr>
<td>6.</td>
<td>return $P_{\sigma-1}$</td>
</tr>
</tbody>
</table>

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 $\bar{s}$ and an order $\sigma \in \mathbb{N}$

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

2. Quasi-linear algorithm PM-Basis

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

Algorithm PM-Basis

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. if $\sigma = 1$ then</td>
<td></td>
</tr>
<tr>
<td>2. return Basis($F \text{ mod } x$)</td>
<td>First subproblem</td>
</tr>
<tr>
<td>3. else</td>
<td></td>
</tr>
<tr>
<td>4. $P_{\text{low}} := \text{PM-Basis}(F, \lfloor \sigma / 2 \rfloor)$</td>
<td></td>
</tr>
<tr>
<td>5. Let $F'$ be s.t. $P_{\text{low}} \cdot F = x^{\lfloor \sigma / 2 \rfloor} \cdot F'$</td>
<td>Update problem</td>
</tr>
<tr>
<td>6. $P_{\text{high}} := \text{PM-Basis}(F', \lfloor \sigma / 2 \rfloor)$</td>
<td>Second subproblem</td>
</tr>
<tr>
<td>7. return $P_{\text{high}} \cdot P_{\text{low}}$</td>
<td>Solve original problem</td>
</tr>
</tbody>
</table>

In terms of polynomial multiplication, binary multiplication tree.

Complexity: $\mathcal{O}(\text{MM}(m, \sigma) \log(\sigma)) = \tilde{\mathcal{O}}(m^\omega \sigma)$
1. Polynomial matrix multiplication in time $\tilde{O}(m^\omega d)$

2. Order bases in $\tilde{O}(m^\omega d)$
   a. Definition and properties
   b. Algorithms and complexity

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

Problem

Let \( A \in \mathbb{F}[x]^{m \times m} \) be the matrix to reduce and \( R = U \cdot A \) its row-reduction (\( U \) unimodular)

Idea 1.

We want to express \( R \) as an order basis \( \sim R \) would be row reduced.
Lattice reduction

Problem

Let \( A \in \mathbb{F}[x]^{m \times m} \) be the matrix to reduce and \( R = U \cdot A \) its row-reduction (\( U \) unimodular).

Idea 1.

We want to express \( R \) as an order basis. \( R \) would be row reduced.

Use the relation \( (U\ R) \cdot \begin{pmatrix} A \\ -I \end{pmatrix} = 0 \Rightarrow (U\ R) \) is part of an order basis of \( F = \begin{pmatrix} A \\ -I \end{pmatrix} \).

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

\[
\begin{bmatrix}
[299] & \ldots & [300] \\
\vdots & \ddots & \vdots \\
[303] & \ldots & [304]
\end{bmatrix}
\begin{bmatrix}
\vdots & \ddots & \vdots \\
[12] & \ldots & [10]
\end{bmatrix}
= 
\begin{bmatrix}
[0] & \ldots & [0] \\
\vdots & \ddots & \vdots \\
\end{bmatrix}
\]

Remark. If \( A \) is of degree \( d \), \( U \) can have degree \( md \).
Lattice reduction

Problem

Let $A \in \mathbb{F}[x]^{m \times m}$ be the matrix to reduce and $R = U \cdot A$ its row-reduction ($U$ unimodular)

Idea 1.

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

Use the relation $(U \ R) \cdot \left( \begin{array}{c} A \\ -I \end{array} \right) = 0 \leadsto (U \ R)$ is part of an order basis of $F = \left( \begin{array}{c} A \\ -I \end{array} \right)$.

In practice:

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

$$F := \left( \begin{array}{c} A \\ -I \end{array} \right), \quad \sigma := m \cdot d + d + 1 \quad \text{and} \quad \vec{s} := (1, \ldots, 1, m \cdot d, \ldots, m \cdot d)$$

The order basis will be $\left( \begin{array}{c} U \\ \ast \end{array} \begin{array}{c} R \\ \ast \end{array} \right)$

Cost: Order basis of order $\sigma = m \cdot d \quad \Rightarrow \quad \tilde{O}(m^\omega (m \cdot d))$
Problem

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

Idea 2: Use the dual space

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

$\leadsto U$ is still of degree $m \cdot d$
Lattice reduction

Problem

Let $A \in \mathbb{F}[x]^{m \times m}$ be the matrix to reduce and $R = U \cdot A$ its row-reduction ($U$ unimodular)

Idea 3 : Use the dual space and look at an high-order component

On a scalar example

$A^{-1} = \frac{U}{R} = \frac{1 + 3x + 4x^2 + 6x^3 + x^4}{1 + x}$

$= 1 + 2x + 2x^2 + 4x^3 + 4x^4 + 3x^5 + 4x^6 + 3x^7 + 4x^8 + \cdots$

However

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

So $(R \ U') \cdot \left( A^{-1} \text{ div } x^{md} \right) = 0$ with $U'$ of degree $d$

Cost: Order basis of order $\sigma = d \implies \tilde{O}(m^\omega d)$
References

[Zhou Ph.D. 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