Matrix-F5 Algorithms and Tropical Gröbner Bases Computation

ISSAC 2015

Tristan Vaccon

Université de Rennes I

July 2015

Motivations

Motivations

Motivations for finite-precision GB over p-adics

- Some varieties in arithmetic geometry are defined over p-adics.
- Better understanding of the behaviour of the computation.
- Going beyond the "luckyness" assumption. (*cf* Winckler 1988, Arnold 2003, ...)

Motivations in tropical geometry

- Tropical GB can be used to decide if a point belong to some given tropical algebraic geometry
- They are a more stable variant to classical GB.

Table of contents

Definition of the precision

Finite-precision p-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=-l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and p a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\boxed{\sum_{i=l}^{d-1} a_i p^i + O(p^d)}$, with $l \in \mathbb{Z}$.

Definition of the precision

Finite-precision p-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=-l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and p a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\boxed{\sum_{i=l}^{d-1} a_i p^i + O(p^d)}$, with $l \in \mathbb{Z}$.

Definition of the precision

Finite-precision p-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=-l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and p a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\boxed{\sum_{i=l}^{d-1} a_i p^i + O(p^d)}$, with $l \in \mathbb{Z}$.

Definition

The **order**, or the **absolute precision** of $\sum_{i=k}^{d-1} a_i p^i + O(p^d)$ is d. Its **relative precision** corresponds to the number of its significant figures, and thus, is given by $d - \min\{i \in \mathbb{Z}, a_i \neq 0\}$.

Definition of the precision

Finite-precision p-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=-l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and p a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\boxed{\sum_{i=l}^{d-1} a_i p^i + O(p^d)}$, with $l \in \mathbb{Z}$.

Definition

The **order**, or the **absolute precision** of $\sum_{i=k}^{d-1} a_i p^i + O(p^d)$ is d. Its **relative precision** corresponds to the number of its significant figures, and thus, is given by $d - \min\{i \in \mathbb{Z}, a_i \neq 0\}$.

Example

The order of $3 * 7^{-1} + 4 * 7^0 + 5 * 7^1 + 6 * 7^2 + O(7^3)$ is 3, and its relative precision is $4 = 3 - (-1)$.

Table of contents

Macaulay's matrix

Macaulay's matrix

Proposition (D. Lazard 1983)

For an homogeneous ideal $I = (f_1, \ldots, f_s) \subset R = \mathbb{Q}_p[X_1, \ldots, X_n]$ *($f_1, \ldots, f_s$ being homogeneous), $d \in \mathbb{N}$,*

$$I \cap R_d = \langle x^\alpha f_i, \ |\alpha| + deg(f_i) = d \rangle \,,$$

as $\mathbb{Q}_p$-vector spaces.

Macaulay's matrix

Definition (Macaulay's matrix)

We denote by $Mac_d(f_1, \dots, f_s)$ the matrix :

$$
\begin{array}{c}
\\
x^{\alpha_{1,1}} f_1 \\
\vdots \\
x^{\alpha_{1,\binom{n+d-d_1-1}{n-1}}} f_1 \\
x^{\alpha_{2,1}} f_2 \\
\vdots \\
x^{\alpha_{s,\binom{n+d-d_s-1}{n-1}}} f_s
\end{array}
\begin{array}{c}
x^{d_1} > \quad \dots \quad > \quad \dots \quad > x^{d_{\binom{n+d-1}{n-1}}} \\
\left[\begin{array}{cccc} & & & \\ x^{\alpha} f_i & \text{written} & \text{in the basis of the} & x^{d_i} \\ & & & \end{array} \right]
\end{array}.
$$

Its rows $x^{\alpha} f_i$ are written in the basis $x^{d_1}, \dots, x^{d_{\binom{n+d-1}{n-1}}}$, with $|\alpha| + \deg(f_i) = d$. Also, $x^{\alpha_{i,j}} < x^{\alpha_{i,j+1}}$.

An algorithm

The idea of the Matrix-F5 algorithm

The idea is to successively row-echelon the matrices $Mac_d(f_1, \ldots, f_i)$, **iteratively** with d and i.
If you know the **profile** of $Mac_d(f_1, \ldots, f_i)$, then you know what are the leading terms in $LT((f_1, \ldots, f_i)_d)$ and so, you can remove useless rows in $Mac_{d'}(f_1, \ldots, f_{i'})$ with $d' > d$ and $i' > i$.

An algorithm

A Matrix-F5 algorithm

Algorithm 1 Matrix-F5 algorithm

Let $F = (f_1, \dots, f_s) \in R^s$, of degree $d_1, \dots, d_s$, and $D \in \mathbb{N}$.
$G \leftarrow F$
for $d \in [\![0, D]\!]$ **do**
  for $i \in [\![1, s]\!]$ **do**
    Build $Mac_d(f_1, \dots, f_i)$;
    F5-criterion: Remove the rows $x^\alpha f_i$ such that x^α is the leading term of a row of $\widetilde{Mac_{d-d_i,i-1}}$;
    Compute the row-echelon form $\widetilde{Mac_{d,i}}$;
    Add to G the rows with a new leading monomial.
  end for
end for
Return G.

Table of contents

UNIVERSITÉ DE RENNES 1

Hypotheses

Row-echelon computation problems

$$\begin{vmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 1+O(p^k) & 1+O(p^k) & 0 & 1+O(p^k) \\ 3+O(p^k) & 3+O(p^k) & 2+O(p^k) & 1+O(p^k) \end{vmatrix}$$

Hypotheses

Row-echelon computation problems

$$\begin{vmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \\ 3+O(p^k) & 3+O(p^k) & 2+O(p^k) & 1+O(p^k) \end{vmatrix}$$

Hypotheses

Row-echelon computation problems

$$\begin{vmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \\ 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \end{vmatrix}$$

Hypotheses

Row-echelon computation problems

$$\left|\begin{array}{cccc} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \\ \hline 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \\ \hline \end{array}\right|$$

Hypotheses

Row-echelon computation problems

$$\left|\begin{array}{cccc} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \\ \hline 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \end{array}\right|$$

Injectivity problem

With the **F5**-criterion and F being a **regular sequence** (**H1** hypothesis),

Hypotheses

Row-echelon computation problems

$$\begin{array}{|cccc|}
1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\
0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \\
\hline
0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \\
\hline
\end{array}$$

Injectivity problem

With the **F5**-criterion and F being a **regular sequence** (**H1** hypothesis), no problem with injectivity (Faugère 2002, Bardet, Faugère, Salvy 2014).

Hypotheses

Row-echelon computation problems

$$\begin{vmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \end{vmatrix}$$

Injectivity problem

With the **F5**-criterion and F being a **regular sequence** (**H1** hypothesis), no problem with injectivity (Faugère 2002, Bardet, Faugère, Salvy 2014).

Hypotheses

Row-echelon computation problems

$$\begin{vmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \end{vmatrix}$$

Injectivity problem

With the **F5**-criterion and F being a **regular sequence** (**H1** hypothesis), no problem with injectivity (Faugère 2002, Bardet, Faugère, Salvy 2014).

Hypotheses

Row-echelon computation problems

$$\begin{vmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \end{vmatrix}$$

Injectivity problem

With the **F5**-criterion and F being a **regular sequence** (**H1** hypothesis), no problem with injectivity (Faugère 2002, Bardet, Faugère, Salvy 2014).

Position problem

If the $\langle f_1, \ldots, f_s \rangle$ generates **weakly-ω ideals** (**H2** hypothesis), no position problem.

Hypotheses

Row-echelon computation problems

$$\begin{vmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \end{vmatrix}$$

Injectivity problem

With the **F5**-criterion and F being a **regular sequence** (**H1** hypothesis), no problem with injectivity (Faugère 2002, Bardet, Faugère, Salvy 2014).

Position problem

If the $\langle f_1, \ldots, f_s \rangle$ generates **weakly-ω ideals** (**H2** hypothesis), no position problem. This is generic for $\omega =$ grevlex if the **Moreno-Socias conjecture** is true.

Hypotheses

Row-echelon computation problems

$$\begin{vmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \end{vmatrix}$$

Injectivity problem

With the **F5**-criterion and F being a **regular sequence** (**H1** hypothesis), no problem with injectivity (Faugère 2002, Bardet, Faugère, Salvy 2014).

Position problem

If the $\langle f_1, \ldots, f_s \rangle$ generates **weakly-ω ideals** (**H2** hypothesis), no position problem. This is generic for $\omega = \text{grevlex}$ if the **Moreno-Socias conjecture** is true.

A first result

Theorem

1. *If $F = (f_1, \ldots, f_s) \in \mathbb{Q}_p[X_1, \ldots, X_n]$ satisfies **H1** and **H2** and its coefficients are known at a precision $O(p^N)$ with N big enough, then it is possible to compute a (D-) GB of $\langle F \rangle$, and certify its leading terms, through an adapted Matrix-F5 algorithm.*
2. *An upper-bound on the precision required is given explicitly by minors of the Macaulay matrices.*

Table of contents

Classical tropical geometry

Definition (Tropical semi-ring)

The tropical semi-ring is $\mathbb{R} \cup \{-\infty\}$, endowed with the following operations :

- $x \oplus y = \min(x, y)$;
- $x \otimes y = x + y$.

Classical tropical geometry

Definition (Tropical semi-ring)

The tropical semi-ring is $\mathbb{R} \cup \{-\infty\}$, endowed with the following operations :

- $x \oplus y = \min(x, y)$;
- $x \otimes y = x + y$.

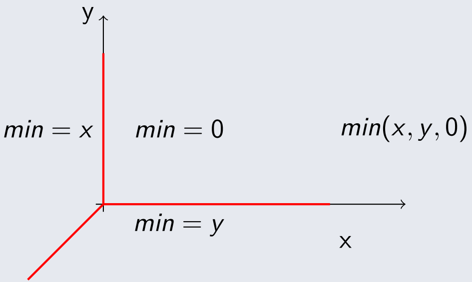
Definition (Tropical hypersurface)

Given $f = \bigoplus_u x_1^{\otimes u_1} \otimes \cdots \otimes x_n^{\otimes u_n}$ a polynomial over the tropical semi-ring, we define $V_{trop}(f) \subset \mathbb{R}^n$ as

$$\left\{ \begin{array}{r} (x_1, \ldots, x_n) \in \mathbb{R}^n, \text{ at least two of the terms in the} \\ \bigoplus = \min \ \text{ reach this minimum} \end{array} \right\}.$$

An exemple

The tropical line



Over a field K with valuation

Definition (Tropicalization of a polynomial)

Let $f = \sum_u c_u x^u \in K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be a Laurent polynomial. For any $w \in \mathbb{R}^n$, we define $trop(f)(w) = \min_u \left(val(c_u) + \sum_{i=1}^n u_i w_i \right)$.

Over a field K with valuation

Definition (Tropicalization of a polynomial)

Let $f = \sum_u c_u x^u \in K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be a Laurent polynomial. For any $w \in \mathbb{R}^n$, we define $trop(f)(w) = \min_u \left(val(c_u) + \sum_{i=1}^n u_i w_i \right)$.

Example

Let $f = x + y + 1$. Then $trop(f)(w) = \min(w_1, w_2, 0)$.

UNIVERSITÉ DE RENNES 1

Over a field K with valuation

Definition (Tropicalization of a polynomial)

Let $f = \sum_u c_u x^u \in K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be a Laurent polynomial. For any $w \in \mathbb{R}^n$, we define $trop(f)(w) = \min_u \left(val(c_u) + \sum_{i=1}^n u_i w_i \right)$.

Over a field K with valuation

Definition (Tropicalization of a polynomial)

Let $f = \sum_u c_u x^u \in K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be a Laurent polynomial. For any $w \in \mathbb{R}^n$, we define $trop(f)(w) = \min_u \left(val(c_u) + \sum_{i=1}^n u_i w_i \right)$.

Definition (Initial terms)

We define $in_w(f) = \sum_{u \,:\, val(c_u) + w \cdot u = trop(f)(w)} c_u x^u$.

Over a field K with valuation

Definition (Tropicalization of a polynomial)

Let $f = \sum_u c_u x^u \in K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be a Laurent polynomial. For any $w \in \mathbb{R}^n$, we define $trop(f)(w) = \min_u \left(val(c_u) + \sum_{i=1}^n u_i w_i \right)$.

Definition (Initial terms)

We define $in_w(f) = \sum_{u \,:\, val(c_u)+w\cdot u = trop(f)(w)} c_u x^u$.

Theorem (Kapranov)

When K is algebraically closed, the following three sets coincides :

- *the tropical hypersurface $V_{trop}(trop(f))$;*
- *the closure in $\mathbb{R}^n$ of the set $\{w \in \mathbb{R}^n,\ in_w(f)$ is not a monomial$\}$;*
- *the closure of the set $val(V(f)) \subset \mathbb{R}^n$ (with $V(f) \subset (K^*)^n$).*

Tropical Varieties

Definition

Let I be an ideal of $K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Let $X = V(I) \subset (K^*)^n$. Let us define $trop(X) = V_{trop}(I) = \cap_{f \in I} V_{trop}(f) \subset \mathbb{R}^n$.

Tropical Varieties

Definition

Let I be an ideal of $K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Let $X = V(I) \subset (K^*)^n$. Let us define $trop(X) = V_{trop}(I) = \cap_{f \in I} V_{trop}(f) \subset \mathbb{R}^n$.

Theorem (Fondamental theorem of Tropical Algebraic Geometry)

When K is algebraically closed, the following three sets coincides :

- *the tropical variety $V_{trop}(I)$;*
- *the closure in $\mathbb{R}^n$ of the set of the vectors $w \in \mathbb{R}^n$ with $in_w(I) \neq < 1 >$;*
- *the closure of the set $val(V(I)) \subset \mathbb{R}^n$.*

Tropical Varieties

Definition

Let I be an ideal of $K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$. Let $X = V(I) \subset (K^*)^n$. Let us define $trop(X) = V_{trop}(I) = \cap_{f \in I} V_{trop}(f) \subset \mathbb{R}^n$.

Theorem (Fondamental theorem of Tropical Algebraic Geometry)

When K is algebraically closed, the following three sets coincides :

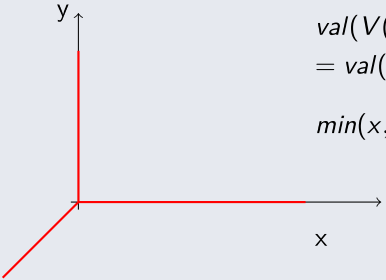
- *the tropical variety $V_{trop}(I)$;*
- *the closure in $\mathbb{R}^n$ of the set of the vectors $w \in \mathbb{R}^n$ with $in_w(I) \neq < 1 >$;*
- *the closure of the set $val(V(I)) \subset \mathbb{R}^n$.*

Remark

$in_w(I) = < 1 >$ if and only if $in_w(I)$ contains a monomial.

An exemple

Return to the tropical line



$$val(V(\langle x+y+1\rangle))$$
$$= val(\{(x,y) \in \mathbb{K}^2,\ x = -y-1\})$$

$$min(x, y, 0)$$

Computational aspect

Proposition

$Trop(V(I))$ is the closure of the set of the vectors $w \in \mathbb{R}^n$ with $in_w(I)$ not containing a monomial.

Computational aspect

Proposition

$Trop(V(I))$ is the closure of the set of the vectors $w \in \mathbb{R}^n$ with $in_w(I)$ not containing a monomial.

Tropical variety computation

When K is an exact field with trivial valuation, it is enough to compute the **Gröbner fan**.

Remark

It is implemented in the package **gfan** by Anders Jensen.

Table of contents

Tropical term ordering

Chan & Maclagan's idea to break ties

One can introduce a classical monomial order $\geq_{mon}$ in order to break the ties of $\geq_w$.

Tropical term ordering

Definition (Tropical term ordering)

Let $\Gamma = \mathbb{R}^n$, and let $w \in \Gamma$. Let $<_{mon}$ be a monomial order on $K[X_1, \dots, X_n]$.

Tropical term ordering

Definition (Tropical term ordering)

Let $\Gamma = \mathbb{R}^n$, and let $w \in \Gamma$. Let $<_{mon}$ be a monomial order on $K[X_1, \ldots, X_n]$.
Then we can define an order on the terms of $K[X_1, \ldots, X_n]$: if $a, b \in K$, x^α and x^β be two monomials of $K[X_1, \ldots, X_n]$,

Tropical term ordering

Definition (Tropical term ordering)

Let $\Gamma = \mathbb{R}^n$, and let $w \in \Gamma$. Let $<_{mon}$ be a monomial order on $K[X_1, \dots, X_n]$.
Then we can define an order on the terms of $K[X_1, \dots, X_n]$: if $a, b \in K$, x^α and x^β be two monomials of $K[X_1, \dots, X_n]$, we write $ax^\alpha > bx^\beta$ if

$$val(a) + \omega \cdot \alpha < val(b) + \omega \cdot \beta,$$

Tropical term ordering

Definition (Tropical term ordering)

Let $\Gamma = \mathbb{R}^n$, and let $w \in \Gamma$. Let $<_{mon}$ be a monomial order on $K[X_1, \dots, X_n]$.
Then we can define an order on the terms of $K[X_1, \dots, X_n]$: if $a, b \in K$, x^α and x^β be two monomials of $K[X_1, \dots, X_n]$, we write $ax^\alpha > bx^\beta$ if

$$val(a) + \omega \cdot \alpha < val(b) + \omega \cdot \beta,$$

or

$$val(a) + \omega \cdot \alpha = val(b) + \omega \cdot \beta \text{ and } x^\alpha >_{mon} x^\beta.$$

Tropical term ordering

Definition (Tropical term ordering)

Let $\Gamma = \mathbb{R}^n$, and let $w \in \Gamma$. Let $<_{mon}$ be a monomial order on $K[X_1, \ldots, X_n]$.
Then we can define an order on the terms of $K[X_1, \ldots, X_n]$: if $a, b \in K$, x^α and x^β be two monomials of $K[X_1, \ldots, X_n]$, we write $ax^\alpha > bx^\beta$ if

$$val(a) + \omega \cdot \alpha < val(b) + \omega \cdot \beta,$$

or

$$val(a) + \omega \cdot \alpha = val(b) + \omega \cdot \beta \text{ and } x^\alpha >_{mon} x^\beta.$$

We can define $in(I)$ accordingly.

A Buchberger algorithm

Proposition (Chan & Maclagan)

From a suited division algorithm, one can define a Buchberger algorithm to compute a tropical Gröbner basis of I suited to the tropical term ordering $<$.

A Buchberger algorithm

Proposition (Chan & Maclagan)

From a suited division algorithm, one can define a Buchberger algorithm to compute a tropical Gröbner basis of I suited to the tropical term ordering $<$.
As a result, it computes $in(I) = in_{mon}\left(in_w\left(I\right)\right)$.

A Buchberger algorithm

Proposition (Chan & Maclagan)

From a suited division algorithm, one can define a Buchberger algorithm to compute a tropical Gröbner basis of I suited to the tropical term ordering $<$.
As a result, it computes $in(I) = in_{mon}\left(in_w\left(I\right)\right).$
$in_w(I)$ can then be recovered from the polynomials giving $in_{mon}\left(in_w\left(I\right)\right).$

Table of contents

UNIVERSITÉ DE RENNES 1

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

$$x^{d_1} > \cdots > x^{d_j} > \ldots > x^{d_{\binom{n-1}{n+d-1}}}$$

$$Mac_d(f_1, \ldots, f_s) \simeq \begin{bmatrix} m_{1,1} & \ldots & m_{1,m} \\ m_{2,1} & \ldots & m_{2,m} \\ \vdots & m_{i,j} & \\ m_{n,1} & \ldots & m_{n,m} \end{bmatrix}$$

We take as pivot the coefficient $m_{i,j}$ with the **smallest** $(val(m_{i,j}) + w \cdot d_j)$, put it on the first row first column by swapping two rows and two columns.

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

$$x^{d_1} > \cdots > x^{d_j} > \ldots > x^{d_{\binom{n-1}{n+d-1}}}$$

$$Mac_d(f_1, \ldots, f_s) \simeq \begin{bmatrix} m_{1,1} & \ldots & m_{1,m} \\ m_{2,1} & \ldots & m_{2,m} \\ \vdots & \boxed{m_{i,j}} & \\ m_{n,1} & \ldots & m_{n,m} \end{bmatrix}$$

We take as pivot the coefficient $m_{i,j}$ with the **smallest** $(val(m_{i,j}) + w \cdot d_j)$, put it on the first row first column by swapping two rows and two columns.

UNIVERSITÉ DE RENNES 1

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

$$x^{d_1} > \cdots > \boxed{x^{d_j}} > \ldots > x^{d_{\binom{n-1}{n+d-1}}}$$

$$Mac_d(f_1, \ldots, f_s) \simeq \begin{bmatrix} m_{1,1} & \cdots & m_{1,m} \\ m_{2,1} & \cdots & m_{2,m} \\ \vdots & \boxed{m_{i,j}} & \\ m_{n,1} & \cdots & m_{n,m} \end{bmatrix}$$

We take as pivot the coefficient $m_{i,j}$ with the **smallest** $(val(m_{i,j}) + w \cdot d_j)$, put it on the first row first column by swapping two rows and two columns.

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

$$x^{d_1} > \cdots > x^{d_j} > \ldots > x^{d_{\binom{n-1}{n+d-1}}}$$

$$Mac_d(f_1, \ldots, f_s) \simeq \begin{bmatrix} m_{1,1} & \cdots & \cdots & \cdots & m_{1,m} \\ m_{2,1} & \cdots & \cdots & \cdots & m_{2,m} \\ \vdots & & m_{i,j} & & \\ m_{n,1} & & \cdots & \cdots & m_{n,m} \end{bmatrix}$$

We take as pivot the coefficient $m_{i,j}$ with the **smallest** $(val(m_{i,j}) + w \cdot d_j)$, put it on the first row first column by swapping two rows and two columns.

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

$$x^{d_1} > \cdots > x^{d_j} > \cdots > x^{d_{\binom{n-1}{n+d-1}}}$$

$$Mac_d(f_1, \ldots, f_s) \simeq \begin{bmatrix} m_{1,1} & \cdots & \cdots & \cdots & m_{1,m} \\ m_{2,1} & \cdots & \cdots & \cdots & m_{2,m} \\ \vdots & & m_{i,j} & & \\ m_{n,1} & \cdots & \cdots & \cdots & m_{n,m} \end{bmatrix}$$

We take as pivot the coefficient $m_{i,j}$ with the **smallest** $(val(m_{i,j}) + w \cdot d_j)$, put it on the first row first column by swapping two rows and two columns.

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

$$x^{d_1} > \cdots > x^{d_j} > \dots > x^{d_{\binom{n-1}{n+d-1}}}$$

$$Mac_d(f_1, \dots, f_s) \simeq \begin{bmatrix} m_{1,1} & \cdots & \cdots & m_{1,m} \\ m_{2,1} & \cdots & \cdots & m_{2,m} \\ \vdots & m_{i,j} & & \\ m_{n,1} & \cdots & \cdots & m_{n,m} \end{bmatrix}$$

We take as pivot the coefficient $m_{i,j}$ with the **smallest** $(val(m_{i,j}) + w \cdot d_j)$, put it on the first row first column by swapping two rows and two columns.

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

$$x^{d_j} > \cdots > x^{d_1} > \ldots > x^{d\binom{n-1}{n+d-1}}$$

$$Mac_d(f_1, \ldots, f_s) \simeq \begin{bmatrix} m_{i,j} & \cdots & m_{i,1} & \cdots & m_{1,m} \\ m_{2,j} & m_{2,2} & m_{2,1} & & m_{2,m} \\ m_{1,j} & & m_{1,1} & & \\ m_{n,j} & \cdots & m_{n,1} & \cdots & m_{n,m} \end{bmatrix}$$

We can pivot with $m_{i,j}$. The loss in precision is $val(m_{i,j})$.

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

$$x^{d_j} > \cdots > x^{d_1} > \ldots > x^{d\binom{n-1}{n+d-1}}$$

$$Mac_d(f_1, \ldots, f_s) \simeq \begin{bmatrix} m_{i,j} & \cdots & m_{i,1} & \cdots & m_{1,m} \\ 0 & m_{2,2} & m_{2,1} & & m_{2,m} \\ \vdots & & & & \\ 0 & & m_{1,1} & & \\ \vdots & & & & \\ 0 & \cdots & m_{n,1} & \cdots & m_{n,m} \end{bmatrix}$$

We can pivot with $m_{i,j}$. The loss in precision is $val(m_{i,j})$.

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

$$x^{d_j} > \cdots > x^{d_1} > \ldots > x^{d_{\binom{n-1}{n+d-1}}}$$

$$Mac_d(f_1, \ldots, f_s) \simeq \begin{bmatrix} m_{i,j} & \cdots & m_{i,1} & \cdots & m_{1,m} \\ 0 & m_{2,2} & m_{2,1} & & m_{2,m} \\ \vdots & & & & \\ 0 & & m_{1,1} & & \\ \vdots & & & & \\ 0 & \cdots & m_{n,1} & \cdots & m_{n,m} \end{bmatrix}$$

We can pivot with $m_{i,j}$. The loss in precision is $val(m_{i,j})$. We can proceed recursively with the remaining submatrix $(\overline{m}_{i,j})_{2 \geq i, 2 \geq j}$.

A Matrix-F5 algorithm to compute D-Tropical GB

Proposition

The F5-criterion is compatible with tropical reduction.

A Matrix-F5 algorithm to compute D-Tropical GB

The tropical Matrix F5 algorithm

Algorithm 2 Tropical Matrix-F5 algorithm

Let $F = (f_1, \ldots, f_s) \in R^s$, of degree $d_1, \ldots, d_s$, and $D \in \mathbb{N}$.
$G \leftarrow F$
for $d \in [\![0, D]\!]$ **do**
  for $i \in [\![1, s]\!]$ **do**
    Build $Mac_d(f_1, \ldots, f_i)$;
    F5-criterion: Remove the rows $x^\alpha f_i$ such that x^α is the leading term of a row of $\widetilde{Mac}_{d-d_i,i-1}$;
    Compute the **tropical** row-echelon form $\widetilde{Mac}_{d,i}$;
    Add to G the rows with a new leading monomial.
  end for
end for
Return G.

Table of contents

Tropical reduction of Macaulay matrices

Proposition (Precision issue)

- *There is **no position issue**.*

Tropical reduction of Macaulay matrices

Proposition (Precision issue)

- *There is* ***no position issue****.*
- *The* ***loss in precision*** *is upper-bounded by the sum of the valuation of the pivots : it is given by the maximal minor of the resulting matrix. It is again* ***a minor of*** $Mac_d(f_1, \dots, f_s)$*.*

Tropical reduction of Macaulay matrices

Proposition (Precision issue)

- *There is* ***no position issue****.*
- *The* ***loss in precision*** *is upper-bounded by the sum of the valuation of the pivots : it is given by the maximal minor of the resulting matrix. It is again* ***a minor of*** $Mac_d(f_1, \ldots, f_s)$.
- *When* $w = (0, \ldots, 0)$, *it corresponds to the maximal minor of the Macaulay matrix with* ***smallest valuation*** *(hence* $\simeq$ *SNF).*

Table of contents

Conclusion

Summary

- **Direct computation** of $(D-)$ GB: we need **H1** and **H2** and enough precision.

Conclusion

Summary

- **Direct computation** of $(D-)$ GB: we need **H1** and **H2** and enough precision.
- **Tropical**: **no position problem**, only **H1** and enough precision.

Conclusion

Summary

- **Direct computation** of $(D-)$ GB: we need **H1** and **H2** and enough precision.
- **Tropical**: **no position problem**, only **H1** and enough precision.
- **Tropical** $+w = (0, \dots, 0)$: (loss in precision) similar to **SNF**.

Conclusion

Summary

- **Direct computation** of $(D-)$ GB: we need **H1** and **H2** and enough precision.
- **Tropical**: **no position problem**, only **H1** and enough precision.
- **Tropical** $+w = (0, \dots, 0)$: (loss in precision) similar to **SNF**.

Future works

- **FGLM**: consider Tropical GB computation, then FGLM to obtain a classical GB (work in progress with G.Renault).
- **Tropical F5**: apply tropical Macaulay-matrix reduction in F5?

UNIVERSITE DE RENNES 1

References

On p-adic precision

- CARUSO, ROE & VACCON, "Tracking p-adic precision," 2014.

On F5 algorithms

- BARDET, FAUGÈRE & SALVY "On the Complexity of the F5 Gröbner basis Algorithm." 2014
- FAUGÈRE "A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)." 2002

On p-adic GB

- VACCON, "p-adic precision and Gröbner bases," 2014.

On tropical GB and tropical geometry

- CHAN & MACLAGAN "Gröbner bases over fields with valuations," 2013.
- MACLAGAN & STURMFELS, "Introduction to tropical geometry," 2015