p-adic precision and Gröbner bases

PolSys Seminar

Tristan Vaccon

Université de Rennes I

6 december 2013

Table of contents

UNIVERSITÉ DE RENNES 1

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 $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, 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 $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, 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 $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, 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 $4 = 3 - (-1)$.

Motivation for p-adic algorithm

Why should one work with p-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;

Motivation for p-adic algorithm

Why should one work with p-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;
- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;

Motivation for p-adic algorithm

Why should one work with p-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;
- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- Some questions or algorithms are p-adic by nature.

Motivation for p-adic algorithm

Why should one work with p-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;
- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- Some questions or algorithms are p-adic by nature.

Some examples of essentially p-adic algorithms

- Polynomial factorization with Hensel lemma ;

Motivation for p-adic algorithm

Why should one work with p-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;
- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- Some questions or algorithms are p-adic by nature.

Some examples of essentially p-adic algorithms

- Polynomial factorization with Hensel lemma ;
- Kedlaya's counting-point algorithm on hyperelliptic curves with p-adic cohomology ;

Motivation for *p*-adic algorithm

Why should one work with *p*-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;
- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- Some questions or algorithms are *p*-adic by nature.

Some examples of essentially *p*-adic algorithms

- Polynomial factorization with Hensel lemma ;
- Kedlaya's counting-point algorithm on hyperelliptic curves with *p*-adic cohomology ;

My personal motivation

Computing moduli spaces of *p*-adic Galois representations.

1. Row-echelon form and *p*-adic precision
   - Powerfulness of *p*-adic precision
   - Loss in precision in the row-echelon form computation
2. The F5 algorithm and *p*-adic computation
   - The F5 algorithm
   - Issues with finite precision
   - Which GB can be computed ?
   - Conclusion regarding GB
3. Tropical computations
   - Tropical motivations
   - Tropical F5 algorithm

Table of contents

p-adic precion *vs* real precision

The quintessential idea of the first tool comes from the following :

Proposition (p-adic errors don't add)

Indeed,

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

That is to say, if a and b are known up to precision $O(p^k)$, then so is $a + b$.

p-adic precion *vs* real precision

The quintessential idea of the first tool comes from the following :

Proposition (p-adic errors don't add)

Indeed,

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

That is to say, if a and b are known up to precision $O(p^k)$, then so is $a + b$.

p-adic precion *vs* real precision

The quintessential idea of the first tool comes from the following :

Proposition (p-adic errors don't add)

Indeed,

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

That is to say, if a and b are known up to precision $O(p^k)$, then so is $a + b$.

Remark

It is quite the opposite to when dealing with real numbers, because of **Round-off error** :

$$(1 + 5 * 10^{-2}) + (2 + 6 * 10^{-2}) = 3 + 1 * 10^{-1} + 1 * 10^{-2}.$$

That is to say, if a and b are known up to precision 10^{-n}, then $a + b$ is known up to $10^{(-n+1)}$.

p-adic precion *vs* real precision

The quintessential idea of the first tool comes from the following :

Proposition (p-adic errors don't add)

Indeed,

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

That is to say, if a and b are known up to precision $O(p^k)$, then so is $a + b$.

Remark

It is quite the opposite to when dealing with real numbers, because of **Round-off error** :

$$(1 + 5 * 10^{-2}) + (2 + 6 * 10^{-2}) = 3 + 1 * 10^{-1} + 1 * 10^{-2}.$$

That is to say, if a and b are known up to precision 10^{-n}, then $a + b$ is known up to $10^{(-n+1)}$.

Precision formulae

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

Precision formulae

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

Proposition (multiplication)

$$(x_0 + O(p^{k_0})) * (x_1 + O(p^{k_1})) = x_0 * x_1 + O(p^{min(k_0+v_p(x_1),k_1+v_p(x_0))})$$

Precision formulae

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

Proposition (multiplication)

$$(x_0 + O(p^{k_0})) * (x_1 + O(p^{k_1})) = x_0 * x_1 + O(p^{min(k_0+v_p(x_1),k_1+v_p(x_0))})$$

Proposition (division)

$$\frac{xp^a + O(p^b)}{yp^c + O(p^d)} = x * y^{-1}p^{a-c} + O(p^{min(d+a-2c,b-c)})$$

In particular,

$$\frac{1}{p^c y + O(p^d)} = y^{-1}p^{-c} + O(p^{d-2c})$$

Table of contents

The result for the Gauss method

Theorem

The result for the Gauss method

Theorem

Let M be an $n \times m$ matrix with coefficients being in $\mathbb{Z}_p$ ($n \leq m$), and known with uniform absolute precision $O(p^k)$, and such that $\Delta = det((M_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n})$ is such that $val(\Delta) < k$.

The result for the Gauss method

Theorem

Let M be an $n \times m$ matrix with coefficients being in $\mathbb{Z}_p$ ($n \leq m$), and known with uniform absolute precision $O(p^k)$, and such that $\Delta = det((M_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n})$ is such that $val(\Delta) < k$.
Then, the maximal loss in precision when performing the Gauss row echelon algorithm can be upper-bounded by $val(\Delta)$ (that is to say, we can compute its coefficients with absolute precision at least $O(p^{k-val(\Delta)})$).

Proof of the theorem

Proof.

$$M = \begin{bmatrix} m_{1,1} + O(p^k) & \cdots & m_{1,n} + O(p^k) & \cdots \\ \vdots & m_{i,j} + O(p^k) & \vdots & \\ m_{n,1} + O(p^k) & \cdots & m_{n,n} + O(p^k) & m_{n,m} + O(p^k) \end{bmatrix}$$

□

Proof of the theorem

Proof.

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & \cdots & m_{1,m}^{(1)} + O(p^k) \\ O(p^k) & m_{2,2}^{(1)} + O(p^k) & \cdots & m_{2,m}^{(1)} + O(p^k) \\ \vdots & \vdots & m_{i,j}^{(1)} + O(p^k) & \\ O(p^k) & m_{n,2}^{(1)} + O(p^k) & \cdots & m_{n,m}^{(1)} + O(p^k) \end{bmatrix}$$

$$\begin{aligned} L_1 &\leftarrow c_1^{-1} L_1 \\ L_2 &\leftarrow L_2 - \frac{m_{2,1}}{m_{1,1}} L_1 \\ &\vdots \\ L_n &\leftarrow L_n - \frac{m_{n,1}}{m_{1,1}} L_1 \end{aligned}$$

We take as pivot the coefficient on the first column with **smallest valuation**, put it on the first row by swapping two rows :
$M_{1,1} = c_1 * p^{a_1} + O(p^k)$.
Furthermore, since $a_1 \leqslant val(m_{j,1})$, $\frac{m_{n,1}}{m_{1,1}}$ is in $\mathbb{Z}_p$, then everything is known up to the order k, at least. □

Proof of the theorem

Proof.

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & \cdots & & & m^{(2)}_{1,m} + O(p^k) \\ O(p^k) & p^{a_2} + O(p^k) & \cdots & & m^{(1)}_{2,m} + O(p^k) \\ \vdots & O(p^k) & & m^{(2)}_{i,j} + O(p^k) & \\ O(p^k) & O(p^k) & m^{(2)}_{n,3} + O(p^k) & \cdots & m^{(2)}_{n,m} + O(p^k) \end{bmatrix}$$

$$\begin{aligned} L_2 &\leftarrow a_2^{-1} L_2 \\ L_3 &\leftarrow L_3 - \frac{m^{(1)}_{3,2}}{m^{(1)}_{2,2}} L_2 \\ &\vdots \\ L_n &\leftarrow L_n - \frac{m^{(1)}_{n,2}}{m^{(1)}_{2,2}} L_2 \end{aligned}$$

(with $M_{2,2} = c_2 * p^{a_2} + O(p^k)$)

□

Proof of the theorem

Proof.

After performing $n-1$ steps, we have reduced our problem to that of a matrix in approximate row-echelon form, up to $O(p^k)$:

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{i,j}^{(n-1)} + O(p^k) \\ O(p^k) & p^{a_2} + O(p^k) & & \\ \vdots & \ddots & \ddots & \\ O(p^k) & \cdots & O(p^k) & p^{a_n} + O(p^k) \end{bmatrix}$$

Proof of the theorem

Proof.

Now, we can perform the "real" row-echelon form computation :

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{1,j}^{(n)} + O(p^k) \\ 0 & p^{a_2} + O(p^{k-a_1}) & & \\ \vdots & O(p^{k-a_1}) & \ddots & m_{i,j}^{(n)} + O(p^{k-a_1}) \\ 0 & O(p^{k-a_1}) & O(p^{k-a_1}) & p^{a_n} + O(p^{k-a_1}) \end{bmatrix}.$$

$$L_2 \leftarrow L_2 - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

$$L_3 \leftarrow L_3 - \frac{M_{3,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

$$\vdots$$

$$L_n \leftarrow L_n - \frac{M_{n,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

Indeed, $M_{2,1}^{(n-1)} - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} * M_{1,1}^{(n-1)} = 0$.

Moreover, $\frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} = \frac{O(p^k)}{p^{a_1}+O(p^k)} = O(p^{k-a_1})$, so $L_2 - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1 = L_2 + O(p^{k-a_1}) L_1$.

Proof of the theorem

Proof.

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{1,j}^{(n)} + O(p^k) \\ \begin{matrix}0\\ \vdots \\ 0\end{matrix} & p^{a_2} + O(p^{k-a_1}) & & \\ & O(p^{k-a_1}) & & m_{i,j}^{(n)} + O(p^{k-a_1}) \\ & O(p^{k-a_1}) \cdots O(p^{k-a_1}) & & p^{a_n} + O(p^{k-a_1}) \end{bmatrix}.$$

$$L_2 \leftarrow L_2 - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

$$L_3 \leftarrow L_3 - \frac{M_{3,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

$$\vdots$$

$$L_n \leftarrow L_n - \frac{M_{n,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

Indeed, $M_{2,1}^{(n-1)} - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} * M_{1,1}^{(n-1)} = 0$.

Moreover, $\frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} = \frac{O(p^k)}{p^{a_1}+O(p^k)} = O(p^{k-a_1})$, so $L_2 - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1 = L_2 + O(p^{k-a_1}) L_1$.

Proof of the theorem

Proof.

This can be rewritten as :

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{1,j}^{(n)} + O(p^k) \\ \begin{matrix}0\\ \vdots \\ 0\end{matrix} & p^{a_2} + O(p^{k-a_1}) & & \\ & O(p^{k-a_1}) & & m_{i,j}^{(n)} + O(p^{k-a_1}) \\ & O(p^{k-a_1}) \cdots & O(p^{k-a_1}) & p^{a_n} + O(p^{k-a_1}) \end{bmatrix}.$$

$$\begin{aligned} L_2 &\leftarrow L_2 + O(p^{k-a_1})L_1 \\ L_3 &\leftarrow L_3 + O(p^{k-a_1})L_1 \\ &\vdots \\ L_n &\leftarrow L_n + O(p^{k-a_1})L_1 \end{aligned}$$

Indeed, $M_{2,1}^{(n-1)} - \dfrac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} * M_{1,1}^{(n-1)} = 0$.

Moreover, $\dfrac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} = \dfrac{O(p^k)}{p^{a_1}+O(p^k)} = O(p^{k-a_1})$, so $L_2 - \dfrac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1 = L_2 + O(p^{k-a_1})L_1$.

Proof of the theorem

Proof.

We can do the same with the other columns :

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & & m_{1,j}^{(n+1)} + O(p^k) \\ \begin{matrix}0\\ \vdots \\ 0\end{matrix} & p^{a_2} + O(p^{k-a_1}) & & & m_{2,j}^{(n+1)} + O(p^{k-a_1}) \\ & \begin{matrix}0\\ \vdots \\ 0\end{matrix} & p^{a_3} + O(p^{k-a_1-a_2}) & & m_{3,j}^{(n+1)} + O(p^{k-a_1-a_2}) \\ & & O(p^{k-a_1-a_2}) & & \vdots \\ & & \vdots & \ddots & \vdots \\ & & O(p^{k-a_1-a_2}) & \cdots & p^{a_n} + O(p^{k-a_1-a_2}) \end{bmatrix}$$

Proof of the theorem

Proof.

In the end, we get :

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{1,j}^{(2n-2)} + O(p^k) \\ & p^{a_2} + O(p^{k-a_1}) & & \\ & \ddots & & m_{i,j}^{(2n-2)} + O(p^{k-a_1 \cdots - a_{i-1}}) \\ 0 & & \ddots & \\ & 0 & & p^{a_n} + O(p^{k-a_1 \cdots - a_{n-1}}) \end{bmatrix}$$

The loss of precision on the row i is $\sum_{j=1}^{i-1} a_i$.

□

Proof of the theorem

Proof.

In the end, we get :

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & & & m_{1,j}^{(2n-2)} + O(p^k) \\ & p^{a_2} + O(p^{k-a_1}) & & \\ & & \ddots & \\ 0 & & & m_{i,j}^{(2n-2)} + O(p^{k-a_1 \cdots - a_{i-1}}) \\ & & \ddots & \\ 0 & & 0 \; p^{a_n} + O(p^{k-a_1 \cdots - a_{n-1}}) & \end{bmatrix}$$

The loss of precision on the row i is $\sum_{j=1}^{i-1} a_i$.
Moreover, $val(det((M_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n})) = \sum_{j=1}^{n} a_i$, and the a_i are non-negative.
Therefore, the loss of precision can be upper-bounded by $val(det((M_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n}))$.

□

Table of contents

The Macaulay matrix

Notations

From now on, k is a field, $n, s \in \mathbb{N}$, and $R = k[X_1, \ldots, X_n]$. We denote by R_d the homogeneous polynomials of degree d of R.
Let ω be a monomial order on R.

The Macaulay matrix

Notations

From now on, k is a field, $n, s \in \mathbb{N}$, and $R = k[X_1, \ldots, X_n]$. We denote by R_d the homogeneous polynomials of degree d of R.
Let ω be a monomial order on R.

Proposition (D. Lazard 83)

For an homogeneous ideal $I = (f_1, \ldots, f_s) \subset R$ ($f_1, \ldots, f_s$ being homogeneous), $d \in \mathbb{N}$, $I \cap R_d =< x^\alpha f_i,\ |\alpha| + deg(f_i) = d >$, as k-vector space .

The Macaulay matrix

Definition (Macaulay's matrix)

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

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

$$\begin{matrix} x^{\alpha_{1,1}} f_1 \\ \vdots \\ x^{\alpha_{1,\binom{n-1}{n+d-d_1-1}}} f_1 \\ x^{\alpha_{2,1}} f_2 \\ \vdots \\ x^{\alpha_{s,\binom{n-1}{n+d-d_s-1}}} f_s \end{matrix} \begin{bmatrix} & & & \\ & x^{\alpha} f_i \quad \text{written} \quad \text{in the basis of the} \quad x^{d_i} & & \\ & & & \end{bmatrix}.$$

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

Gröbner basis and row-echelon form

Then, naturally, if we identify the rows vectors of $k^{\binom{n}{n+d-1}}$ with homogeneous polynomials of degree d,

Proposition

$Im(Mac_d(f_1, \ldots, f_s)) = I \cap R_d$, with Im being the left image of the matrix.

Gröbner basis and row-echelon form

We may also remark that there is a matrix characterization of Gröbner bases :

Theorem

For an homogeneous ideal $I = (f_1, \ldots, f_s)$, $f_1, \ldots, f_s$ is a Gröbner basis of I if and only if : for all $d \in \mathbb{N}$, $Mac_d(f_1, \ldots, f_s)$ contains an echelon basis of $Im(Mac_d(f_1, \ldots, f_s))$.

Gröbner basis and row-echelon form

We may also remark that there is a matrix characterization of Gröbner bases :

Theorem

For an homogeneous ideal $I = (f_1, \ldots, f_s)$, $f_1, \ldots, f_s$ is a Gröbner basis of I if and only if : for all $d \in \mathbb{N}$, $Mac_d(f_1, \ldots, f_s)$ contains an echelon basis of $Im(Mac_d(f_1, \ldots, f_s))$.

By *echelon basis*, we mean the following

Definition

Let $g_1, \ldots, g_r$ be homogeneous polynomials of degree d. Let M be the matrix whose i-th row is the row vector corresponding to g_i written in $B_{n,d}$. Then we say that $g_1, \ldots, g_r$ is an *echelon basis* of $Im(M)$ if there is a permutation matrix P such that the index function $ind_{PM} : \{1, r\} \to \mathbb{N}_{\leq 0}$, which maps i to the index of the columns of the first non-zero entry on the i-th row of PM, is increasing.

Lazard's matrix algorithm

This directly leads to Lazard's "algorithm" to compute Gröbner bases : find a row echelon basis of all the right images of the matrices $Mac_d(f_1, \ldots, f_s)$ up to some d, and if d is large enough, it will be enough to add thoses basis to the initial generating sequence of the ideal.

The criterion

Proposition

- *Let $t \in LM(I_{i-1})$, then the row tf_i of the Macaulay matrix $Mac_d(f_1, \ldots, f_i)$ can be reduced to zero with the rows above it.*

The criterion

Proposition

- *Let $t \in LM(I_{i-1})$, then the row tf_i of the Macaulay matrix $Mac_d(f_1, \ldots, f_i)$ can be reduced to zero with the rows above it.*
- *If we discard all the rows tf_i of $Mac_d(f_1, \ldots, f_i)$ such that $t \in LM(I_{i-1})$, and call the remaining matrix $\overline{Mac_d(f_1, \ldots, f_i)}$, then $Im(Mac_d(f_1, \ldots, f_i) = Im(\overline{Mac_d(f_1, \ldots, f_i)})$.*

Regular sequences and F5 criterion

Definition

A sequence $(f_1, \ldots, f_s)$ of R^s is called a regular sequence if for all $j \in [\![2, s]\!]$, f_j is not a zero-divisor in $R/(f_1, \ldots, f_{j-1})$.

Regular sequences and F5 criterion

Definition

A sequence $(f_1, \ldots, f_s)$ of R^s is called a regular sequence if for all $j \in [\![2, s]\!]$, f_j is not a zero-divisor in $R/(f_1, \ldots, f_{j-1})$.

Proposition

If $(f_1, \ldots, f_s)$ is a regular sequence, then the matrices $\overline{Mac_d(f_1, \ldots, f_i)}$ are (left) injective.

Regular sequences and F5 criterion

Definition

A sequence $(f_1, \ldots, f_s)$ of R^s is called a regular sequence if for all $j \in [\![2, s]\!]$, f_j is not a zero-divisor in $R/(f_1, \ldots, f_{j-1})$.

Proposition

If $(f_1, \ldots, f_s)$ is a regular sequence, then the matrices $\overline{Mac_d(f_1, \ldots, f_i)}$ are (left) injective. In other words, there is no reduction to zero when computing the row-echelon form of $\overline{Mac_d(f_1, \ldots, f_i)}$.

The F5 theorem

Theorem

- *To compute a Gröbner basis, it is enough to compute the row-echelon form of the* $\overline{Mac_d(f_1, \ldots, f_i)}$.

The F5 theorem

Theorem

- *To compute a Gröbner basis, it is enough to compute the row-echelon form of the* $\overline{Mac_d(f_1, \ldots, f_i)}$.
- *If* $(f_1, \ldots, f_s)$ *is a regular sequence, there is no reduction to zero when computing the row-echelon form of* $\overline{Mac_d(f_1, \ldots, f_i)}$.

An algorithm

The idea of the F5 matrix 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

The matrix F5 algorithm

Algorithm 1 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 $Mac_d f_1, \ldots, f_i$;
    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

Table of contents

The position of the leading terms ideals

Problem with testing nullity

A major issue can happen when dealing with finite-precision numbers : not being able to decide whether there is no non-zero pivot on a column or whether the precision is not enough.

Being able to compute the leading terms ideals

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

$$L_2 \leftarrow L_2 - \frac{M_{2,1}}{M_{1,1}} L_1$$

The position of the leading terms ideals

Problem with testing nullity

A major issue can happen when dealing with finite-precision numbers : not being able to decide whether there is no non-zero pivot on a column or whether the precision is not enough.

Being able to compute the leading terms ideals

$$\begin{bmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & -1+O(p^k) & 1+O(p^k) \end{bmatrix} \qquad L_2 \leftarrow L_2 - (1+O(p^k))L_1$$

The position of the leading terms ideals

Problem with testing nullity

A major issue can happen when dealing with finite-precision numbers : not being able to decide whether there is no non-zero pivot on a column or whether the precision is not enough.

Being able to compute the leading terms ideals

$$\begin{bmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & -1+O(p^k) & 1+O(p^k) \end{bmatrix} \qquad L_2 \leftarrow L_2 - (1+O(p^k))L_1$$

What is the leading term for the second row ?

Table of contents

Moreno-Socias conjecture

Definition (weakly-w-ideal)

Let I be an ideal in $R = k[X_1, \ldots, X_n]$, and w be a monomial order on R. Then I is said to be a weakly-w-ideal if, for all x^α a leading monomial according to w of the reduced Gröbner basis of I according to w, for all x^β such that $|\alpha| = |\beta|$ and $x^\beta > x^\alpha$, x^β belongs to $LM(I)$ (according to w).

Moreno-Socias conjecture

Definition (weakly-w-ideal)

Let I be an ideal in $R = k[X_1, \ldots, X_n]$, and w be a monomial order on R. Then I is said to be a weakly-w-ideal if, for all x^α a leading monomial according to w of the reduced Gröbner basis of I according to w, for all x^β such that $|\alpha| = |\beta|$ and $x^\beta > x^\alpha$, x^β belongs to $LM(I)$ (according to w).

Conjecture (Moreno-Socias)

If k is an infinite field, $s \in \mathbb{N}$, $d_1, \ldots, d_s \in \mathbb{N}$, then there is a non-empty Zariski-open subset U in $R_{d_1} \times \cdots \times R_{d_s}$ such that for all $(f_1, \ldots, f_s) \in U$, $I = (f_1, \ldots, f_s)$ is a weakly-grevlex ideal.

Moreno-Socias conjecture

Definition (weakly-w-ideal)

Let I be an ideal in $R = k[X_1, \ldots, X_n]$, and w be a monomial order on R. Then I is said to be a weakly-w-ideal if, for all x^α a leading monomial according to w of the reduced Gröbner basis of I according to w, for all x^β such that $|\alpha| = |\beta|$ and $x^\beta > x^\alpha$, x^β belongs to $LM(I)$ (according to w).

Conjecture (Moreno-Socias)

If k is an infinite field, $s \in \mathbb{N}$, $d_1, \ldots, d_s \in \mathbb{N}$, then there is a non-empty Zariski-open subset U in $R_{d_1} \times \cdots \times R_{d_s}$ such that for all $(f_1, \ldots, f_s) \in U$, $I = (f_1, \ldots, f_s)$ is a weakly-grevlex ideal.

Remark

If the conjecture holds, then regular sequence generating a weakly grevlex ideal are generic.

An algorithm suited for weakly-w-ideal

Proposition ("weak" F5 algorithm)

We can modify the F5 algorithm such that if $(f_1, \ldots, f_s)$ is a regular sequence in $\mathbb{Q}_p[X_1, \ldots, X_n]$ such that the ideals $(f_1, \ldots, f_l)$ are weakly-w-ideal I, and if the f_i are known up to large enough flat precision $O(p^k)$, then an approximation of a Gröbner base of I can be computed (and even a minimal basis) :

An algorithm suited for weakly-w-ideal

Proposition ("weak" F5 algorithm)

We can modify the F5 algorithm such that if $(f_1, \ldots, f_s)$ is a regular sequence in $\mathbb{Q}_p[X_1, \ldots, X_n]$ such that the ideals $(f_1, \ldots, f_l)$ are weakly-w-ideal I, and if the f_i are known up to large enough flat precision $O(p^k)$, then an approximation of a Gröbner base of I can be computed (and even a minimal basis) :

- *At first, we proceed like in the normal F5 algorithm ;*

An algorithm suited for weakly-w-ideal

Proposition ("weak" F5 algorithm)

We can modify the F5 algorithm such that if $(f_1, \ldots, f_s)$ is a regular sequence in $\mathbb{Q}_p[X_1, \ldots, X_n]$ such that the ideals $(f_1, \ldots, f_l)$ are weakly-w-ideal I, and if the f_i are known up to large enough flat precision $O(p^k)$, then an approximation of a Gröbner base of I can be computed (and even a minimal basis) :

- *At first, we proceed like in the normal F5 algorithm ;*
- *But, as soon as a column with no non-zero pivot is encountered, we halt the row-echelon computation. Instead, we replace the non-reduced rows by (already reduced) multiples of the rows of $\widetilde{Mac}_{d-1,i}$, so as to get a matrix under row-echelon form.*

3 quadrics in 6 variables

An example

With 3 generic quadrics in 6 variables, what we get after reducing the Macauly matrix in degree 3 is the following :

$$\left[\begin{array}{c|c} \text{a 9x9 invertible block} & \text{(loss in precision : determinant of the 9x9 matrix)} \\ \hline 0 & \text{9 rows, multiples of rows of the matrix in degree 2} \end{array}\right].$$

About strongly stable ideals

Strongly stable ideal is not enough

In $\mathbb{Q}_p[x, y, z]$,let us take $f_1 = x^3 + xy^2$, $f_2 = x^2y$, and $f_3 = x^2z$. They generate a strongly stable initial ideal regarding to grevlex.

About strongly stable ideals

Strongly stable ideal is not enough

In $\mathbb{Q}_p[x, y, z]$,let us take $f_1 = x^3 + xy^2$, $f_2 = x^2y$, and $f_3 = x^2z$. They generate a strongly stable initial ideal regarding to grevlex.
Yet, one can not recover the initial ideal from approximations of $f_1, f_2, f_1 + f_3$.

$$x^3 > x^2y > xy^2 > y^3 > x^2z > \dots$$

$$Mac_3(f_1, f_2, f_1 + f_3) \simeq \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0\dots \\ 0 & 1 & 0 & 0 & 0 & 0\dots \\ 1 & 0 & 1 & 0 & 1 & 0\dots \end{bmatrix}$$

About strongly stable ideals

Strongly stable ideal is not enough

In $\mathbb{Q}_p[x, y, z]$,let us take $f_1 = x^3 + xy^2$, $f_2 = x^2y$, and $f_3 = x^2z$. They generate a strongly stable initial ideal regarding to grevlex.
Yet, one can not recover the initial ideal from approximations of $f_1, f_2, f_1 + f_3$.

$$x^3 > x^2y > xy^2 > y^3 > x^2z > \dots$$

$$Mac_3(f_1, f_2, f_1 + f_3) \simeq \begin{bmatrix} 1 & 0 & \boxed{1} & 0 & 0 & 0\dots \\ 0 & 1 & 0 & 0 & 0 & 0\dots \\ 1 & 0 & \boxed{1} & 0 & \boxed{1} & 0\dots \end{bmatrix}$$

Table of contents

To sum up in one result

To sum up in one result

Proposition

Let $(f_1, \ldots, f_s)$ be a regular sequence in $\mathbb{Q}_p[X_1, \ldots, X_n]$ such that the $I_i = (f_1, \ldots, f_i)$ yields a weakly-ω ideal.
If the f_i are known with enough precision (i.e. bigger than the valuations of the maximal, regarding of the first columns, non-zero minor of the Macaulay matrices defined by the f_i), then we can compute, by an F5 algorithm, an approximate Gröbner basis of I for ω, with the right leading monomials.

Remark

Moreno-Socias conjecture would allow us to deduce from here that we can compute a grevlex Gröbner basis of almost any sequence $(f_1, \ldots, f_s)$ of $\mathbb{Q}_p[X_1, \ldots, X_n]$ (with $s \leqslant n$) (when precision is enough).

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 :

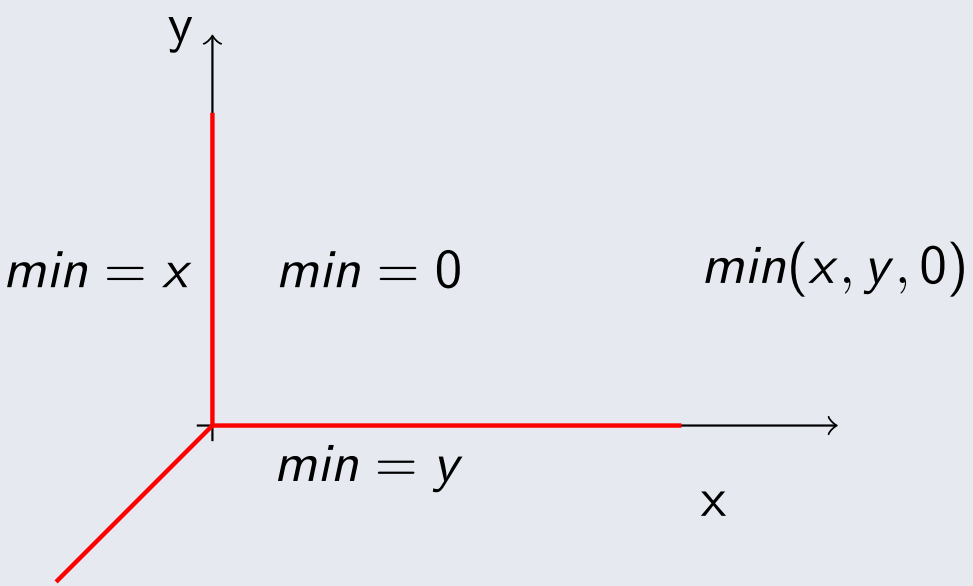
- $x \oplus y = \min(x, y)$;
- $x \otimes y = x + y$.

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 can define $V_{trop}(f) \subset \mathbb{R}^n$ to be the $(x_1, \ldots, x_n) \in \mathbb{R}^n$ such that at least two of the terms in the $\bigoplus = \min$ reach this minimum.

An exemple

The tropical line



Over fields with valuation

Definition (Tropicalization of a polynomial)

Let $f = \sum_u c_u x^u \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ 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 fields with valuation

Definition (Tropicalization of a polynomial)

Let $f = \sum_u c_u x^u \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ 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 $trop(f)(w) = \min(w_1, w_2, 0)$.

Over fields with valuation

Definition (Tropicalization of a polynomial)

Let $f = \sum_u c_u x^u \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ 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 fields with valuation

Definition (Tropicalization of a polynomial)

Let $f = \sum_u c_u x^u \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ 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 fields with valuation

Definition (Tropicalization of a polynomial)

Let $f = \sum_u c_u x^u \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ 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)

The following three sets coincides :

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

The three following subsets 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 $K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. 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)

The three following subsets coincides :

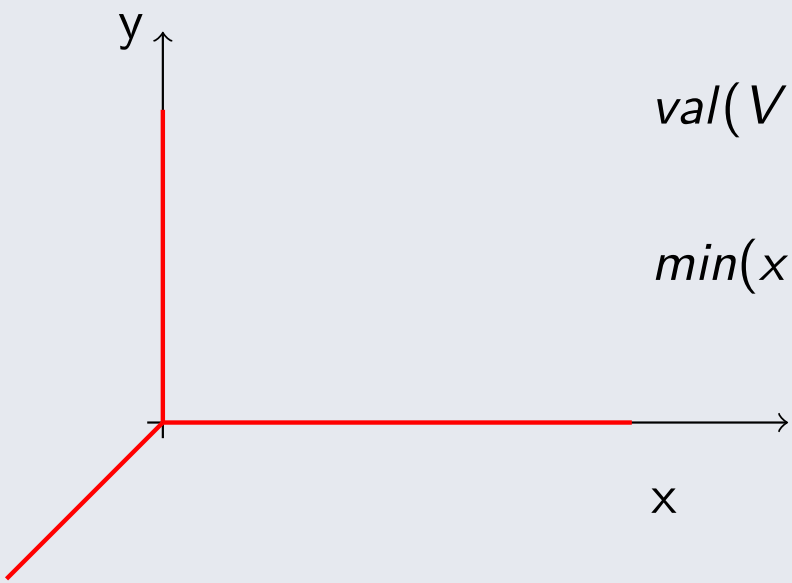
- *the tropical variety* $V_{trop}(I)$ *;*
- *the closure in* $\mathbb{R}^n$ *of the set of the vectors* $w \in \mathbb{R}^n$ *with* $in_w(I) \neq < 1 >$ *;*
- *the closure of the set* $val(V(I)) \subset \mathbb{R}^n$.

Remark

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

An exemple

Return to the tropical line



$$val(V(x = -y - 1))$$

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

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 $K[X_1, \ldots, X_n]$.

Tropical term ordering

Definition (Tropical term ordering)

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

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

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

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

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 $in_{mon}(in_w(I))$.

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 $in_{mon}(in_w(I))$.
$in_w(I)$ can then be recovered from the polynomials giving $in_{mon}(in_w(I))$.

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

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

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

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

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

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

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

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

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

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

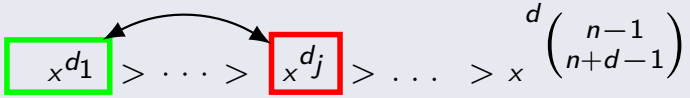
$$x^{d_1} > \cdots > x^{d_j} > \ldots > x^{d\binom{n-1}{n+d-1}}$$

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

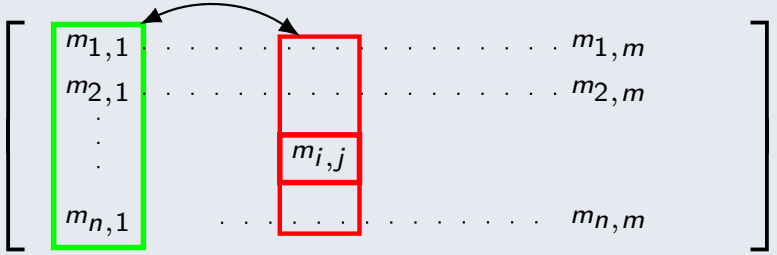
We take as pivot the coefficient $m_{i,j}$ with the **smallest** $(val(m_{i,j}) + w \cdot d_j)$, put it on the first row first column by swapping two rows and two columns.

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction



$Mac_d(f_1, \ldots, f_s) \simeq$



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

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

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

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

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

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

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

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

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

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

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

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

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

Tropical reduction of Macaulay matrices

Proposition

The tropical row-echelon form of $Mac_d(f_1, \ldots, f_s)$, result of the previous algorithm, computes $in(I) \cap K[X]_d$.

Tropical reduction of Macaulay matrices

Proposition

The tropical row-echelon form of $Mac_d(f_1, \dots, f_s)$, result of the previous algorithm, computes $in(I) \cap K[X]_d$.

Proposition (Precision issue)

- *There is no position issue.*

Tropical reduction of Macaulay matrices

Proposition

The tropical row-echelon form of $Mac_d(f_1, \dots, f_s)$, result of the previous algorithm, computes $in(I) \cap K[X]_d$.

Proposition (Precision issue)

- *There is no position issue.*
- *If the precision is enough, there is no issue in finding the coefficient with the smallest $val(m_{i,j}) + w \cdot d_j$.*

Tropical reduction of Macaulay matrices

Proposition

The tropical row-echelon form of $Mac_d(f_1, \dots, f_s)$, result of the previous algorithm, computes $in(I) \cap K[X]_d$.

Proposition (Precision issue)

- *There is no position issue.*
- *If the precision is enough, there is no issue in finding the coefficient with the smallest $val(m_{i,j}) + w \cdot d_j$.*
- *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 $Mac_d(f_1, \dots, f_s)$.*

An F5 algorithm

Proposition

The F5-criterion is compatible with tropical reduction.

An F5 algorithm

The tropical matrix F5 algorithm

Algorithm 2 Tropical 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 $Mac_d f_1, \ldots, f_i$;
    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

Conclusion

Regarding Gröbner bases

Let $(f_1, \ldots, f_s)$ be a regular sequence in $\mathbb{Q}_p[X_1, \ldots, X_n]$ such that the $I_i = (f_1, \ldots, f_i)$ yields a **weakly-ω ideal**.

Conclusion

Regarding Gröbner bases

Let $(f_1, \ldots, f_s)$ be a regular sequence in $\mathbb{Q}_p[X_1, \ldots, X_n]$ such that the $I_i = (f_1, \ldots, f_i)$ yields a **weakly-ω ideal**.
If the f_i are known with **enough precision**, then we can compute, by an F5 algorithm, an approximate Gröbner basis of I for ω, with the right leading monomials.

Conclusion

Regarding tropical Gröbner bases

Let $(f_1, \ldots, f_s)$ be a regular sequence in $\mathbb{Q}_p[X_1, \ldots, X_n]$. Let $w \in \mathbb{R}^n$. Let $<_{mon}$ be a monomial order
If the f_i are known with enough precision, then we can compute, by an F5 algorithm, an approximate Gröbner basis of I for $in_{mon}(in_w(I))$, with the right leading monomials.

Further concerns

Implementation

All the algorithms have been implemented in Sage. A patch for Sage with those algorithms will soon be available.

The three main tools of *p*-adic precision

In my opinion, these are the three main tools concerning *p*-adic precision :

Further concerns

Implementation

All the algorithms have been implemented in Sage. A patch for Sage with those algorithms will soon be available.

The three main tools of *p*-adic precision

In my opinion, these are the three main tools concerning *p*-adic precision :

- Tracking the loss in precision with formulae, operation by operation;

Further concerns

Implementation

All the algorithms have been implemented in Sage. A patch for Sage with those algorithms will soon be available.

The three main tools of *p*-adic precision

In my opinion, these are the three main tools concerning *p*-adic precision :

- Tracking the loss in precision with formulae, operation by operation;
- The study of Newton polygons;

Further concerns

Implementation

All the algorithms have been implemented in Sage. A patch for Sage with those algorithms will soon be available.

The three main tools of *p*-adic precision

In my opinion, these are the three main tools concerning *p*-adic precision :

- Tracking the loss in precision with formulae, operation by operation;
- The study of Newton polygons;
- Differential calculus.

Bardet, Magali

"Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie", thèse de doctorat, Université Paris VI, Décembre 2004.

Chan, Andrew & Maclagan, Diane

Groebner bases over fields with valuations

Faugère, Jean-Charles

A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In Proceedings of the 2002 international symposium on Symbolic and algebraic computation, ISSAC '02, pages 75-83, New York, NY, USA, 2002. ACM.

Moreno-Socias, Guillermo

Autour de la fonction de Hilbert-Samuel (escaliers d'idéaux polynomiaux), Thèse, École Polytechnique, 1991.

Pardue, Keith

Generic Sequences of Polynomials, J. Algebra 324 (2010), no. 4, 579–590

Sturmfels,B. & Maclagan,D.

Introduction to tropical geometry.