p-adic precision and Gröbner bases

ISSAC 2014

Tristan Vaccon

Université de Rennes I

24th of July 2014

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 $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, 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 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 (long-term) motivation

Computing moduli spaces of p-adic Galois representations.

1. Row-echelon form and *p*-adic precision
   - Step-by-step analysis
   - Loss in precision in the row-echelon form computation

2. Matrix-F5 algorithm and *p*-adic computations
   - On Matrix-F5 algorithm
   - Issues with finite precision
   - Which GB can be computed ?
   - Continuity and optimality

Table of contents

p-adic precision *vs* real precision

The quintessential idea of the step-by-step analysis is 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 precision *vs* real precision

The quintessential idea of the step-by-step analysis is 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 precision *vs* real precision

The quintessential idea of the step-by-step analysis is 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 precision *vs* real precision

The quintessential idea of the step-by-step analysis is 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

Let $M \in M_{n,m}(\mathbb{Z}_p)$ such that :

The result for the Gauss method

Theorem

Let $M \in M_{n,m}(\mathbb{Z}_p)$ such that :

- *its coefficients are known up to $O(p^k)$.*
- *$val(\Delta) < k$, with $\Delta = det((M_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n})$.*

The result for the Gauss method

Theorem

Let $M \in M_{n,m}(\mathbb{Z}_p)$ such that :

- *its coefficients are known up to $O(p^k)$.*
- *$val(\Delta) < k$, with $\Delta = det((M_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n})$.*

*Then the **loss of precision** to compute a row-echelon form of M is $\leq val(\Delta)$.*

Proof of the theorem

Gauss' method

$$M = \begin{bmatrix} m_{1,1} + O(p^k) & m_{1,2} + O(p^k) & \cdots & m_{1,m} + O(p^k) \\ m_{2,1} + O(p^k) & m_{2,2} + O(p^k) & \cdots & m_{2,m} + O(p^k) \end{bmatrix}$$

We assume that,

$$\det\left(\begin{bmatrix} m_{1,1} + O(p^k) & m_{1,2} + O(p^k) \\ m_{2,1} + O(p^k) & m_{2,2} + O(p^k) \end{bmatrix}\right) \neq O(p^k).$$

Proof of the theorem

Gauss' method

$$M \simeq \begin{bmatrix} p^{a1} + O(p^k) & m_{1,2} + O(p^k) & \cdots & m_{1,m} + O(p^k) \\ p^{a2} + O(p^k) & m_{2,2} + O(p^k) & \cdots & m_{2,m} + O(p^k) \end{bmatrix} \qquad L_2 \leftarrow L_2 - \frac{M_{2,1}}{M_{1,1}} L_1$$

Proof of the theorem

Gauss' method

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & m_{1,2} + O(p^k) & \cdots & m_{1,m} + O(p^k) \\ \boxed{0} & m_{2,2}^{(2)} + O(p^{k-a_1}) & \cdots & m_{2,m}^{(2)} + O(p^{k-a_1}) \end{bmatrix}$$

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

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

In addition, $\frac{M_{2,1}}{M_{1,1}} = \frac{p^{a_2} + O(p^k)}{p^{a_1} + O(p^k)} = p^{a_2 - a_1} + O(p^{k-a_1})$, therefore

$$L_2 - \frac{M_{2,1}}{M_{1,1}} L_1 = L_2 + (p^{a_2 - a_1} + O(p^{k-a_1}))L_1 \ .$$

Proof of the theorem

Gauss' method

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & m_{1,2} + O(p^k) & \cdots & m_{1,m} + O(p^k) \\ 0 & m_{2,2}^{(2)} + O(p^{k-a_1}) & \cdots & m_{2,m}^{(2)} + O(p^{k-a_1}) \end{bmatrix}$$

$$L_2 \leftarrow L_2 + O(p^{k-a_1})L_1$$

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

In addition, $\frac{M_{2,1}}{M_{1,1}} = \frac{p^{a_2}+O(p^k)}{p^{a_1}+O(p^k)} = p^{a_2-a_1} + O(p^{k-a_1})$, therefore

$$L_2 - \frac{M_{2,1}}{M_{1,1}} L_1 = L_2 + (p^{a_2-a_1} + O(p^{k-a_1}))L_1 .$$

Proof of the theorem

Gauss' method

In the end, we get :

$$M = \begin{bmatrix} p^{a_1} + O(p^k) & m_{1,2} + O(p^k) & \cdots & m_{1,m} + O(p^k) \\ 0 & p^{a_2} + O(p^{k-a_1}) & \cdots & m_{2,m} + O(p^{k-a_1}) \end{bmatrix}$$

The loss of precision on the second row is a_1 .

Proof of the theorem

Gauss' method

In the end, we get :

$$M = \begin{bmatrix} p^{a_1} + O(p^k) & m_{1,2} + O(p^k) & \cdots & m_{1,m} + O(p^k) \\ \boxed{0} & p^{a_2} + O(p^{k-a_1}) & \cdots & \boxed{m_{2,m} + O(p^{k-a_1})} \end{bmatrix}$$

The loss of precision on the second row is $\boxed{a_1}$.

Proof of the theorem

Gauss' method

In the end, we get :

$$M = \begin{bmatrix} p^{a_1} + O(p^k) & m_{1,2} + O(p^k) & \cdots & m_{1,m} + O(p^k) \\ \boxed{0} & p^{a_2} + O(p^{k-a_1}) & \cdots & m_{2,m} + O(p^{k-a_1}) \end{bmatrix}$$

$$val(\det\left(\begin{bmatrix} m_{1,1} + O(p^k) & m_{1,2} + O(p^k) \\ m_{2,1} + O(p^k) & m_{2,2} + O(p^k) \end{bmatrix}\right)) = a_1 + a_2, \text{ with } a_i > 0.$$

The loss in precision is upper-bounded by

$$val(det((M_{i,j})_{1 \leqslant i \leqslant 2, 1 \leqslant j \leqslant 2}))$$

Table of contents

The Macaulay matrix

Notations

For k 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

For k 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), $d \in \mathbb{N}$,

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

as k-vector spaces .

The Macaulay matrix

Definition (Macaulay's matrix)

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

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

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

Its rows $x^{\alpha} f_i$ are written in the basis $x^{d_1}, \ldots, x^{d\binom{n+d-1}{n-1}}$, 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 $F = (f_1, \ldots, f_s) \in R^s$, 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-ω ideal)

I is said to be a weakly-ω ideal if :

- for all x^α a leading monomial according to ω of the reduced Gröbner basis of I,
- for all x^β such that $|\alpha| = |\beta|$ and $x^\beta > x^\alpha$,

we have $x^\beta \in LM(I)$.

Moreno-Socias conjecture

Definition (weakly-ω ideal)

I is said to be a weakly-ω ideal if :

- for all x^α a leading monomial according to ω of the reduced Gröbner basis of I,
- for all x^β such that $|\alpha| = |\beta|$ and $x^\beta > x^\alpha$,

we have $x^\beta \in LM(I)$.

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-ω ideal)

I is said to be a weakly-ω ideal if :

- for all x^α a leading monomial according to ω of the reduced Gröbner basis of I,
- for all x^β such that $|\alpha| = |\beta|$ and $x^\beta > x^\alpha$,

we have $x^\beta \in LM(I)$.

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 sequences generating a weakly-grevlex ideal are generic.

An algorithm suited for weakly-ω ideal

Proposition ("weak" Matrix-F5 algorithm)

We assume :

- $(f_1, \ldots, f_s)$ *is a regular,* ***(H1)***

An algorithm suited for weakly-ω ideal

Proposition ("weak" Matrix-F5 algorithm)

We assume :

- $(f_1, \ldots, f_s)$ *is a regular,* ***(H1)***
- *the* $< f_1, \ldots, f_l >$ *are weakly-*ω *ideals,* ***(H2)***

An algorithm suited for weakly-ω ideal

Proposition ("weak" Matrix-F5 algorithm)

We assume :

- $(f_1, \ldots, f_s)$ *is a regular,* ***(H1)***
- *the* $< f_1, \ldots, f_l >$ *are weakly-*ω *ideals,* ***(H2)***
- *precision on the* f_i*'s is enough.*

An algorithm suited for weakly-ω ideal

Proposition ("weak" Matrix-F5 algorithm)

We assume :

- $(f_1, \ldots, f_s)$ *is a regular,* ***(H1)***
- *the* $< f_1, \ldots, f_l >$ *are weakly-*ω *ideals,* ***(H2)***
- *precision on the* f_i*'s is enough.*

Then, we can proceed :

An algorithm suited for weakly-ω ideal

Proposition ("weak" Matrix-F5 algorithm)

We assume :

- $(f_1, \ldots, f_s)$ *is a regular,* ***(H1)***
- *the* $< f_1, \ldots, f_l >$ *are weakly-*ω *ideals,* ***(H2)***
- *precision on the* f_i*'s is enough.*

Then, we can proceed :

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

An algorithm suited for weakly-ω ideal

Proposition ("weak" Matrix-F5 algorithm)

We assume :

- $(f_1, \ldots, f_s)$ *is a regular,* ***(H1)***
- *the* $< f_1, \ldots, f_l >$ *are weakly-*ω *ideals,* ***(H2)***
- *precision on the* f_i*'s is enough.*

Then, we can proceed :

- *At first, we proceed like in the normal Matrix-F5 algorithm ;*
- *But, as soon as a column with no non-zero pivot is encountered,* ***we halt*** *the row-echelon computation. Instead, we* ***can 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 Macaulay matrix in degree 3 is the following :

$$\left[\begin{array}{c|c} \text{a 9x9 invertible block} & \text{(loss in precision : determinant of the 9x9 matrix)} \\ \hline 0 & \text{9 rows, } \in \langle x_k L,\ L \text{ row of of the matrix with } d = 2\rangle \end{array}\right].$$

Table of contents

On regularity

Proposition

*Let $F = (f_1, \ldots, f_s)$ satisfying **H1** and **H2**. Then:*

- $(h_1, \ldots, h_s) \mapsto LM(\langle f_1, \ldots, f_s \rangle)$ *is **constant** around F.*

On regularity

Proposition

*Let $F = (f_1, \ldots, f_s)$ satisfying **H1** and **H2**. Then:*

- $(h_1, \ldots, h_s) \mapsto LM(\langle f_1, \ldots, f_s \rangle)$ *is **constant** around F.*
- $(h_1, \ldots, h_s) \mapsto GBR(\langle f_1, \ldots, f_s \rangle)$ *is **rational** around F.*

On regularity

Proposition

*Let $F = (f_1, \ldots, f_s)$ satisfying **H1** and **H2**. Then:*

- $(h_1, \ldots, h_s) \mapsto LM(\langle f_1, \ldots, f_s \rangle)$ *is **constant** around F.*
- $(h_1, \ldots, h_s) \mapsto GBR(\langle f_1, \ldots, f_s \rangle)$ *is **rational** around F.*
- *We can give **explicit neighbourhood** of F with the Macaulay matrices.*

On optimality

Proposition

On optimality

Proposition

*Around $F = (f_1, \ldots, f_s)$ that does not satisfy **H1** or **H2**:*

On optimality

Proposition

*Around $F = (f_1, \ldots, f_s)$ that does not satisfy **H1** or **H2**:*

- $(h_1, \ldots, h_s) \mapsto LM(\langle f_1, \ldots, f_s \rangle)$ *may **not be constant** around F.*

On optimality

Proposition

*Around $F = (f_1, \ldots, f_s)$ that does not satisfy **H1** or **H2**:*

- $(h_1, \ldots, h_s) \mapsto LM(\langle f_1, \ldots, f_s \rangle)$ *may **not be constant** around F.*
- $(h_1, \ldots, h_s) \mapsto GBR(\langle f_1, \ldots, f_s \rangle)$ *may **not be stable** at F.*

To sum up in one result

To sum up in one result

Proposition

We assume :

- ***Structure*** *: regular sequence, and weakly-*ω *ideals* $< f_1, \ldots, f_i >$.

To sum up in one result

Proposition

We assume :

- ***Structure*** *: regular sequence, and weakly-ω ideals $< f_1, \ldots, f_i >$.*
- ***Precision*** *: bigger than the valuation of the biggest principal minors of the Macaulay matrices*

To sum up in one result

Proposition

We assume :

- ***Structure*** *: regular sequence, and weakly-ω ideals $< f_1, \ldots, f_i >$.*
- ***Precision*** *: bigger than the valuation of the biggest principal minors of the Macaulay matrices*

Then we can compute, by a Matrix-F5 algorithm, an approximate Gröbner basis of I for ω, with the right leading monomials.

To sum up in one result

Proposition

We assume :

- ***Structure*** *: regular sequence, and weakly-ω ideals $< f_1, \ldots, f_i >$.*
- ***Precision*** *: bigger than the valuation of the biggest principal minors of the Macaulay matrices*

Then we can compute, by a Matrix-F5 algorithm, an approximate Gröbner basis of I for ω, with the right leading monomials.

Remark

Moreno-Socias conjecture implies that **Structure** is generic for grevlex.

Further concerns

Implementation

All the algorithms have been implemented in Sage. A patch for Sage with those algorithms will soon be available. I maintain a toy version on my website.

Further concerns

Implementation

All the algorithms have been implemented in Sage. A patch for Sage with those algorithms will soon be available. I maintain a toy version on my website.

Future works

Further concerns

Implementation

All the algorithms have been implemented in Sage. A patch for Sage with those algorithms will soon be available. I maintain a toy version on my website.

Future works

- Differential calculs to study 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. I maintain a toy version on my website.

Future works

- Differential calculs to study p-adic precision
- F5 algorithm for tropical Gröbner bases;

Further concerns

Implementation

All the algorithms have been implemented in Sage. A patch for Sage with those algorithms will soon be available. I maintain a toy version on my website.

Future works

- Differential calculs to study *p*-adic precision
- F5 algorithm for tropical Gröbner bases;
- Border bases.

Bibliography

On *p*-adic precision

- Caruso,Roe & Vaccon, Tracking *p*-adic precision, ANTS XI.

On F5 algorithms

- Bardet "Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie" 2004.
- Faugère A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). ISSAC 2002

On weakly-ω ideals

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

On numerical Gröbner bases

- Sasaki & Kako, Term cancellations in computing floating-point Gröbner bases. CASC 2010