p-adic precision, differentials and the example of Gröbner bases.

SpecFun Seminar

Tristan Vaccon

Université de Rennes I

23 mars 2014

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 ;

p-adic algorithms : a first example

Hensel factorization

We would like to factor $Q \in \mathbb{Z}[X]$:

p-adic algorithms : a first example

Hensel factorization

We would like to factor $Q \in \mathbb{Z}[X]$:

1. Chose a p that is well-suited to the problem ;

p-adic algorithms : a first example

Hensel factorization

We would like to factor $Q \in \mathbb{Z}[X]$:

1. Chose a p that is well-suited to the problem ;
2. Factor $\overline{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$;

p-adic algorithms : a first example

Hensel factorization

We would like to factor $Q \in \mathbb{Z}[X]$:

1. Chose a p that is well-suited to the problem ;
2. Factor $\overline{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$;
3. Lift the factors into $\mathbb{Z}/p^k\mathbb{Z}[X]$ (with *Hensel's lemma*) ;

p-adic algorithms : a first example

Hensel factorization

We would like to factor $Q \in \mathbb{Z}[X]$:

1. Chose a p that is well-suited to the problem ;
2. Factor $\overline{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$;
3. Lift the factors into $\mathbb{Z}/p^k\mathbb{Z}[X]$ (with *Hensel's lemma*) ;
4. If p^k is big enough (*Mignotte's bound*), we can obtain a factorization over Q (up to the recombination of some factors).

p-adic algorithms : another example

Idea of Kedlaya's algorithm

Let C be an hyperelliptic curve of genus g over $\mathbb{F}_p$, defined by $y^2 = P(x)$ (with $deg(P) = 2g + 1$, squarefree). We would like to determine $|Jac(C, \mathbb{F}_p)|$.

p-adic algorithms : another example

Idea of Kedlaya's algorithm

Let C be an hyperelliptic curve of genus g over $\mathbb{F}_p$, defined by $y^2 = P(x)$ (with $deg(P) = 2g + 1$, squarefree). We would like to determine $|Jac(C, \mathbb{F}_p)|$.

- Let F be the Frobenius of $\mathbb{F}_p$. Then F acts as an endomorphims on $H^1_{MW}(C, A)$, the Monsky-Washnitzer cohomology with coefficients in A.

p-adic algorithms : another example

Idea of Kedlaya's algorithm

Let C be an hyperelliptic curve of genus g over $\mathbb{F}_p$, defined by $y^2 = P(x)$ (with $deg(P) = 2g + 1$, squarefree). We would like to determine $|Jac(C, \mathbb{F}_p)|$.

- Let F be the Frobenius of $\mathbb{F}_p$. Then F acts as an endomorphims on $H^1_{MW}(C, A)$, the Monsky-Washnitzer cohomology with coefficients in A.
- Let $A = \mathbb{Z}_p^\dagger[[x, y]]/(P)$. Then $|Jac(C, \mathbb{F}_p)| = \chi_F(1)$.

p-adic algorithms : another example

Idea of Kedlaya's algorithm

Let C be an hyperelliptic curve of genus g over $\mathbb{F}_p$, defined by $y^2 = P(x)$ (with $deg(P) = 2g+1$, squarefree). We would like to determine $|Jac(C, \mathbb{F}_p)|$.

- Let F be the Frobenius of $\mathbb{F}_p$. Then F acts as an endomorphims on $H^1_{MW}(C, A)$, the Monsky-Washnitzer cohomology with coefficients in A.
- Let $A = \mathbb{Z}_p^{\dagger}[[x, y]]/(P)$. Then $|Jac(C, \mathbb{F}_p)| = \chi_F(1)$.
- We want to determine the action of F over A and $H^1_{MW}(C, A)$:

p-adic algorithms : another example

Idea of Kedlaya's algorithm

Let C be an hyperelliptic curve of genus g over $\mathbb{F}_p$, defined by $y^2 = P(x)$ (with $deg(P) = 2g+1$, squarefree). We would like to determine $|Jac(C, \mathbb{F}_p)|$.

- Let F be the Frobenius of $\mathbb{F}_p$. Then F acts as an endomorphims on $H^1_{MW}(C, A)$, the Monsky-Washnitzer cohomology with coefficients in A.
- Let $A = \mathbb{Z}_p^{\dagger}[[x, y]]/(P)$. Then $|Jac(C, \mathbb{F}_p)| = \chi_F(1)$.
- We want to determine the action of F over A and $H^1_{MW}(C, A)$:

$$F(x) = x^p \mod p \qquad\qquad F(y) = y^p \mod p$$
$$P(F(x)) = F(y)^2$$

- With Weil's conjecture, $\chi_F \in \mathbb{Z}[T]$, and $|a_i| \leqslant 2^{2g} \sqrt{q}^i$.

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 $4 = 3 - (-1)$.

Table of contents

p-adic precion *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 precion *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 precion *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 precion *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

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

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

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & m_{1,2} + O(p^k) & \cdots\cdots & m_{1,m} + O(p^k) \\ \boxed{p^{a_2} + O(p^k)} & m_{2,2} + O(p^k) & \cdots & m_{2,m} + O(p^k) \end{bmatrix} \qquad L_2 \leftarrow L_2 - \frac{M_{2,1}^{(n-1)}}{M_{1,1}^{(n-1)}} L_1$$

Proof of the theorem

Gauss' method

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & m_{1,2} + O(p^k) \cdots & \cdots & m_{1,m} + O(p^k) \\ \boxed{0} & m^{(2)}_{2,2} + O(p^{k-a_1}) & \cdots & m^{(2)}_{2,m} + O(p^{k-a_1}) \end{bmatrix} \qquad \boxed{L_2 \leftarrow L_2 - \frac{M^{(n-1)}_{2,1}}{M^{(n-1)}_{1,1}} L_1}$$

Indeed, $\boxed{M^{(n-1)}_{2,1} - \frac{M^{(n-1)}_{2,1}}{M^{(n-1)}_{1,1}} * M^{(n-1)}_{1,1} = 0}$ (formally).

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

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

Proof of the theorem

Gauss' method

$$M \simeq \begin{bmatrix} p^{a_1} + O(p^k) & m_{1,2} + O(p^k) \cdots & \cdots & m_{1,m} + O(p^k) \\ \boxed{0} & m_{2,2}^{(2)} + O(p^{k-a_1}) \cdots & \cdots & \boxed{m_{2,m}^{(2)} + O(p^{k-a_1})} \end{bmatrix} \qquad \boxed{L_2 \leftarrow L_2 + O(p^{k-a_1})L_1}$$

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

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

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

Proof of the theorem

Gauss' method

In the end, we get :

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

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

Proof of the theorem

Gauss' method

In the end, we get :

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

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

Proof of the theorem

Gauss' method

In the end, we get :

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

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

The loss in precision is upper-bounded by

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

Table of contents

The Macaulay matrix

Notations

From now on, k is a field, $n, s \in \mathbb{N}$, and $R = k[X_1, \dots, X_n]$. 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 spaces .

The Macaulay matrix

Definition (Macaulay's matrix)

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

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

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 $Mac_d(f_1, \dots, f_i)$ iteratively with d and i.
If you know the profile of $Mac_d(f_1, \dots, f_i)$, then you know what are the leading terms in $LT((f_1, \dots, f_i)_d)$ and so, you can remove useless rows in $Mac_{d'}(f_1, \dots, f_{i'})$ 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

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

$$\begin{bmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 1+O(p^k) & 1+O(p^k) & 0 & 1+O(p^k) \end{bmatrix} \qquad L_2 \leftarrow L_2 - \frac{M_{2,1}}{M_{1,1}} L_1$$

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

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

What is the leading term for the second row ?

Moreno-Socias conjecture

Definition (weakly-w-ideal)

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,
- 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-w-ideal)

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

Moreno-Socias conjecture

Definition (weakly-w-ideal)

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,
- 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, $s \in \mathbb{N}$, $d_1, \dots, d_s \in \mathbb{N}$, then there is a non-empty Zariski-open subset U in $R_{d_1} \times \cdots \times R_{d_s}$ such that for all $(f_1, \dots, f_s) \in U$, $I = (f_1, \dots, f_s)$ 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-w-ideal

Proposition ("weak" F5M algorithm)

We assume :

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

An algorithm suited for weakly-w-ideal

Proposition ("weak" F5M algorithm)

We assume :

- $(f_1, \dots, f_s)$ *is a regular,*
- *the* $< f_1, \dots, f_l >$ *are weakly-w-ideals,*

An algorithm suited for weakly-w-ideal

Proposition ("weak" F5M algorithm)

We assume :

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

An algorithm suited for weakly-w-ideal

Proposition ("weak" F5M algorithm)

We assume :

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

Then, we can proceed :

An algorithm suited for weakly-w-ideal

Proposition ("weak" F5M algorithm)

We assume :

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

Then, we can proceed :

- *At first, we proceed like in the normal F5M algorithm ;*

An algorithm suited for weakly-w-ideal

Proposition ("weak" F5M algorithm)

We assume :

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

Then, we can proceed :

- *At first, we proceed like in the normal F5M 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 $f_1 = x^3 + xy^2$, $f_2 = x^2 y$, and $f_3 = x^2 z$. 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 $f_1, f_2, f_1 + f_3$.

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

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

To sum up in one result

UNIVERSITÉ DE RENNES 1

To sum up in one result

Proposition

We assume :

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

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.*

To sum up in one result

Proposition

We assume :

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

Then we can compute, by an F5M 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 $< f_1, \dots, f_i >$.*
- ***Precision*** *: bigger than the valuation of the biggest principal minors.*

Then we can compute, by an F5M 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.

Table of contents

Optimality

Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_p^2 & \to & \mathbb{Q}_p^2 \\ (x, y) & \mapsto & (x + y, x - y). \end{array}$

Optimality

Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_p^2 & \rightarrow & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x,y)$ with

$(x,y) = (1 + \boxed{O(p^{10})}, 1 + O(p)).$

Optimality

Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_p^2 & \to & \mathbb{Q}_p^2 \\ (x, y) & \mapsto & (x + y, x - y). \end{array}$

We would like to compute $f \circ f(x, y)$ with

$(x, y) = (1 + \boxed{O(p^{10})}, 1 + O(p))$.

- If we apply f two times, we get :

$$f \circ f(x, y) = (2 + \boxed{O(p)}, 2 + O(p)).$$

Optimality

Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_p^2 & \rightarrow & \mathbb{Q}_p^2 \\ (x, y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x, y)$ with

$(x, y) = (1 + \boxed{O(p^{10})}, 1 + O(p))$.

- If we apply f two times, we get :

$$f \circ f(x, y) = (2 + \boxed{O(p)}, 2 + O(p)).$$

- If we remark that $f \circ f = 2Id$, we get :

$$f \circ f(x, y) = (2 + \boxed{O(p^{10})}, 2 + O(p)).$$

Optimality

Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_p^2 & \to & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x,y)$ with $(x,y) = (1 + \boxed{O(p^{10})}, 1 + O(p))$.

- If we apply f two times, we get :

$$f \circ f(x,y) = (2 + \boxed{O(p)}, 2 + O(p)).$$

- If we remark that $f \circ f = 2Id$, we get :

$$f \circ f(x,y) = (2 + \boxed{O(p^{10})}, 2 + O(p)).$$

Non intrinsic

X.Caruso (12) : Step-by-step analysis is algorithm-dependent.

Let $M \in M_d(\mathbb{Z}_p)$ be a random matrix whose all entries are known up to precision $O(p^N)$.

Non intrinsic

X.Caruso (12) : Step-by-step analysis is algorithm-dependent.

Let $M \in M_d(\mathbb{Z}_p)$ be a random matrix whose all entries are known up to precision $O(p^N)$.
We would like to compute $M = LU$ the LU factorization of M. Then :

Non intrinsic

X.Caruso (12) : Step-by-step analysis is algorithm-dependent.

Let $M \in M_d(\mathbb{Z}_p)$ be a random matrix whose all entries are known up to precision $O(p^N)$.
We would like to compute $M = LU$ the LU factorization of M. Then :

- If we apply Gaussian elimination, the average precision on L is $O(p^{n-\frac{2d}{p-1}})$.

Non intrinsic

X.Caruso (12) : Step-by-step analysis is algorithm-dependent.

Let $M \in M_d(\mathbb{Z}_p)$ be a random matrix whose all entries are known up to precision $O(p^N)$.
We would like to compute $M = LU$ the LU factorization of M. Then :

- If we apply Gaussian elimination, the average precision on L is $O(p^{n-\frac{2d}{p-1}})$.
- If we study Cramer-style formulae, the intrinsic precision determined for L is $O(p^{n-2\log_p(d)})$.

Table of contents

The Main lemma of p-adic differential precision

Lemma

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a **differentiable** mapping.*

The Main lemma of p-adic differential precision

Lemma

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*

The Main lemma of p-adic differential precision

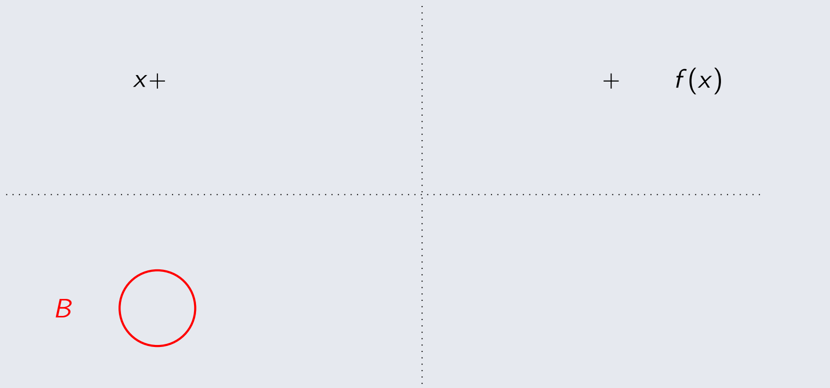
Lemma

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*
*Then for any ball $B = B(0, r)$ **small enough**,*

$$f(x + B) = f(x) + f'(x) \cdot B.$$

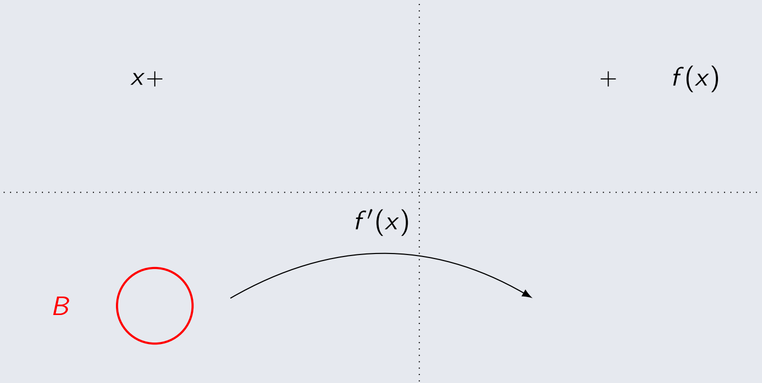
Geometrical meaning

Interpretation



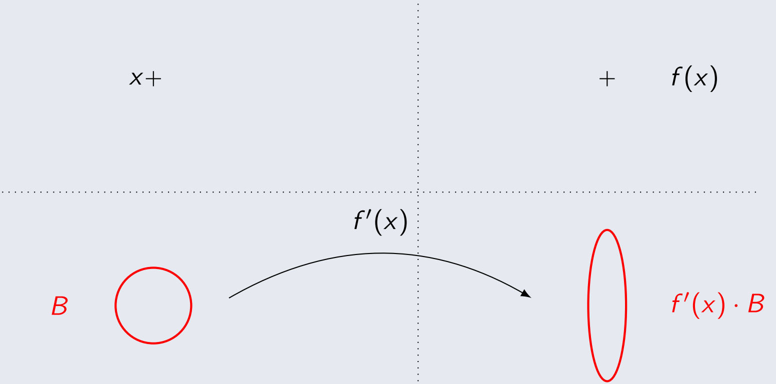
Geometrical meaning

Interpretation



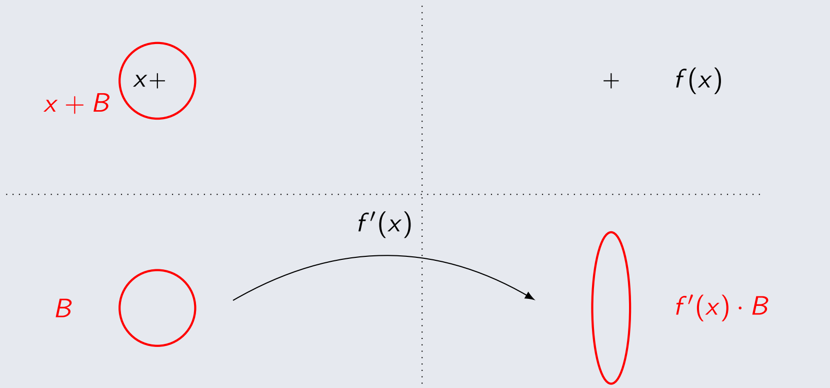
Geometrical meaning

Interpretation



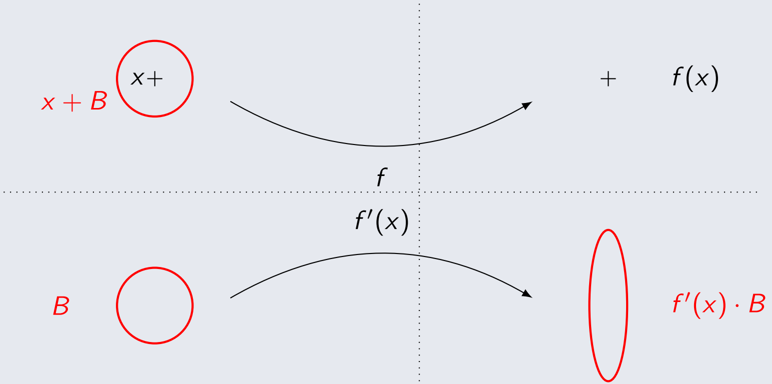
Geometrical meaning

Interpretation



Geometrical meaning

Interpretation



Geometrical meaning

Interpretation

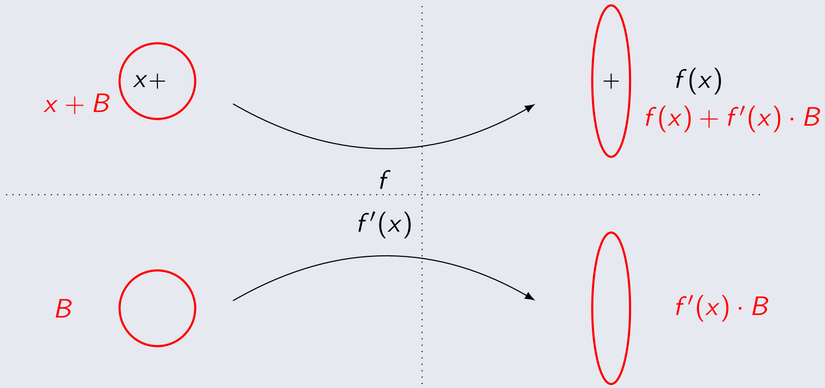


Table of contents

UNIVERSITÉ DE RENNES 1

Introduction to the Somos-4 sequence

Definition

We define the **Somos-4** sequence by recursion, with :

$$x_0, x_1, x_2, x_3 \in \mathbb{Z}_p^\times,$$

$$x_{n+4} = \frac{x_{n+1}x_{n+3} + x_{n+2}^2}{x_n}.$$

Introduction to the Somos-4 sequence

Definition

We define the **Somos-4** sequence by recursion, with :

$$x_0, x_1, x_2, x_3 \in \mathbb{Z}_p^\times,$$

$$x_{n+4} = \frac{x_{n+1}x_{n+3} + x_{n+2}^2}{x_n}.$$

Remark

This formula comes from the Z-coordinate of $[m]\,P + Q$ for some P, Q points on the **elliptic curve** $y^2 + y = x^3 + x$.

Introduction to the Somos-4 sequence

Definition

We define the **Somos-4** sequence by recursion, with :

$$x_0, x_1, x_2, x_3 \in \mathbb{Z}_p^\times,$$

$$x_{n+4} = \frac{x_{n+1}x_{n+3} + x_{n+2}^2}{x_n}.$$

Remark

This formula comes from the Z-coordinate of $[m]P + Q$ for some P, Q points on the **elliptic curve** $y^2 + y = x^3 + x$.

Proposition

For all n, $x_n \in \mathbb{Z}_p$, i.e. $v_p(x_n) \geq 0$.

The Laurent phenomenon

Remark

If x_0, x_1, x_2, x_3 are known up to $O(p^m)$, then because of the division by x_n, a naive step-by-step analysis show that x_{n+4} is known up to $O(p^{m-\sum_{k=0}^{n} v_p(x_k)})$.

The Laurent phenomenon

Remark

If x_0, x_1, x_2, x_3 are known up to $O(p^m)$, then because of the division by x_n, a naive step-by-step analysis show that x_{n+4} is known up to $O(p^{m-\sum_{k=0}^{n} v_p(x_k)})$.

Theorem (Fomin, Zelevinsky)

Let P_n be the rational fraction defined by the recursion formula defining Somos-4 :

$$x_n = P_n(x_0, x_1, x_2, x_3).$$

The Laurent phenomenon

Remark

If x_0, x_1, x_2, x_3 are known up to $O(p^m)$, then because of the division by x_n, a naive step-by-step analysis show that x_{n+4} is known up to $O(p^{m-\sum_{k=0}^{n} v_p(x_k)})$.

Theorem (Fomin, Zelevinsky)

Let P_n be the rational fraction defined by the recursion formula defining Somos-4 :

$$x_n = P_n(x_0, x_1, x_2, x_3).$$

Then $P_n \in \mathbb{Z}[x_0^{\pm 1}, x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$.

Consequence

Consequence

Theorem

$P_n \in \mathbb{Z}[x_0^{\pm 1}, x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$.

Consequence

Theorem

$P_n \in \mathbb{Z}[x_0^{\pm 1}, x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$.

Remark

If m is big enough,

$$P_n(x_0 + O(p^m), x_1 + O(p^m), x_2 + O(p^m), x_3 + O(p^m)) \\ = x_n + P_n'(x_0, x_1, x_2, x_3) \cdot (O(p^m), O(p^m), O(p^m), O(p^m))^t.$$

Consequence

Theorem

$P_n \in \mathbb{Z}[x_0^{\pm 1}, x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$.

Remark

If m is big enough,

$$P_n(x_0 + O(p^m), x_1 + O(p^m), x_2 + O(p^m), x_3 + O(p^m)) \\ = x_n + P_n'(x_0, x_1, x_2, x_3) \cdot (O(p^m), O(p^m), O(p^m), O(p^m))^t.$$

Coefficients of $P_n'(x_0, x_1, x_2, x_3)$ are in $\mathbb{Z}_p$.

Consequence

Theorem

$P_n \in \mathbb{Z}[x_0^{\pm 1}, x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$.

Remark

If m is big enough,

$$P_n(x_0 + O(p^m), x_1 + O(p^m), x_2 + O(p^m), x_3 + O(p^m))$$
$$= x_n + P_n'(x_0, x_1, x_2, x_3) \cdot (O(p^m), O(p^m), O(p^m), O(p^m))^t.$$

Coefficients of $P_n'(x_0, x_1, x_2, x_3)$ are in $\mathbb{Z}_p$.

Corollary

There is no intrinsic loss of precision : x_n is determined up to $O(p^m)$.

Table of contents

Lattices

Lattices

Lemma

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*
*Then for any ball $B = B(0, r)$ **small enough**,*

$$f(x + B) = f(x) + f'(x) \cdot B.$$

Lattices

Lemma

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*
*Then for any ball $B = B(0, r)$ **small enough**, for any open **lattice** $H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

Lattices

Lemma

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective****.*
Then for any ball $B = B(0, r)$ ***small enough****, for any open* ***lattice*** *$H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

Remark

This allows more models of precision, like

$$(x, y) = (1 + O(p^{10}), 1 + O(p)).$$

Higher differentials

Higher differentials

What is **small enough**

How can we determine when the lemma applies ?

Higher differentials

What is **small enough**

How can we determine when the lemma applies ?
When f is locally analytic, it corresponds to

$$\sum_{k=2}^{+\infty} \frac{1}{k!} f^{(k)}(x) \cdot H^k \subset f'(x) \cdot H.$$

Higher differentials

What is **small enough**

How can we determine when the lemma applies ?
When f is locally analytic, it corresponds to

$$\sum_{k=2}^{+\infty} \frac{1}{k!} f^{(k)}(x) \cdot H^k \subset f'(x) \cdot H.$$

This can be determined with **Newton-polygon** techniques.

Higher differentials

What is **small enough**

How can we determine when the lemma applies ?
When f is locally analytic, it corresponds to

$$\sum_{k=2}^{+\infty} \frac{1}{k!} f^{(k)}(x) \cdot H^k \subset f'(x) \cdot H.$$

This can be determined with **Newton-polygon** techniques.

Remark

Concerning the Somos-4 sequence, since $P_n \in \mathbb{Z}[X_0^{\pm 1}, X_1^{\pm 1}, X_2^{\pm 1}, X_3^{\pm 1}]$, all the coefficients of $\frac{1}{k!} f^{(k)}(x)$ are in $\mathbb{Z}$.

Higher differentials

What is **small enough**

How can we determine when the lemma applies ?
When f is locally analytic, it corresponds to

$$\sum_{k=2}^{+\infty} \frac{1}{k!} f^{(k)}(x) \cdot H^k \subset f'(x) \cdot H.$$

This can be determined with **Newton-polygon** techniques.

Remark

Concerning the Somos-4 sequence, since $P_n \in \mathbb{Z}[X_0^{\pm 1}, X_1^{\pm 1}, X_2^{\pm 1}, X_3^{\pm 1}]$, all the coefficients of $\frac{1}{k!} f^{(k)}(x)$ are in $\mathbb{Z}$.
As a consequence,

$$\frac{1}{k!} f^{(k)}(x) \cdot (p^m \mathbb{Z}_p)^k \subset p^m \mathbb{Z}_p.$$

Table of contents

Computation in SOMOS-4

Loss in precision in SOMOS-4 with Sage ?!

$$x_0 = 1 + O(5^{20})$$
$$x_1 = 1 + O(5^{20})$$
$$x_2 = 1 + O(5^{20})$$
$$x_3 = -1 + 5 + O(5^{20})$$

Computation in SOMOS-4

Loss in precision in SOMOS-4 with Sage ?!

$$
\begin{aligned}
x_0 &= 1 + O(5^{20}) \\
x_1 &= 1 + O(5^{20}) \\
x_2 &= 1 + O(5^{20}) \\
x_3 &= -1 + 5 + O(5^{20}) \\
x_4 &= 4 * 5 + \cdots + O(5^{20})
\end{aligned}
$$

Computation in SOMOS-4

Loss in precision in SOMOS-4 with Sage ?!

$$x_0 = 1 + O(5^{20})$$
$$x_1 = 1 + O(5^{20})$$
$$x_2 = 1 + O(5^{20})$$
$$x_3 = -1 + 5 + O(5^{20})$$
$$x_4 = 4 * 5 + \cdots + O(5^{20})$$
$$x_8 = 4 + \cdots + O(5^{19})$$

Computation in SOMOS-4

Loss in precision in SOMOS-4 with Sage ?!

$$
\begin{aligned}
x_0 &= 1 + O(5^{20}) \\
x_1 &= 1 + O(5^{20}) \\
x_2 &= 1 + O(5^{20}) \\
x_3 &= -1 + 5 + O(5^{20}) \\
x_4 &= 4 * 5 + \cdots + O(5^{20}) \\
x_8 &= 4 + \cdots + O(5^{19}) \\
x_{40} &= 4 + \cdots + O(5^{13})
\end{aligned}
$$

Computation in SOMOS-4

Loss in precision in SOMOS-4 with Sage ?!

$$
\begin{aligned}
x_0 &= 1 + O(5^{20}) \\
x_1 &= 1 + O(5^{20}) \\
x_2 &= 1 + O(5^{20}) \\
x_3 &= -1 + 5 + O(5^{20}) \\
x_4 &= 4 * 5 + \cdots + O(5^{20}) \\
x_8 &= 4 + \cdots + O(5^{19}) \\
x_{40} &= 4 + \cdots + O(5^{13})
\end{aligned}
$$

An explanation

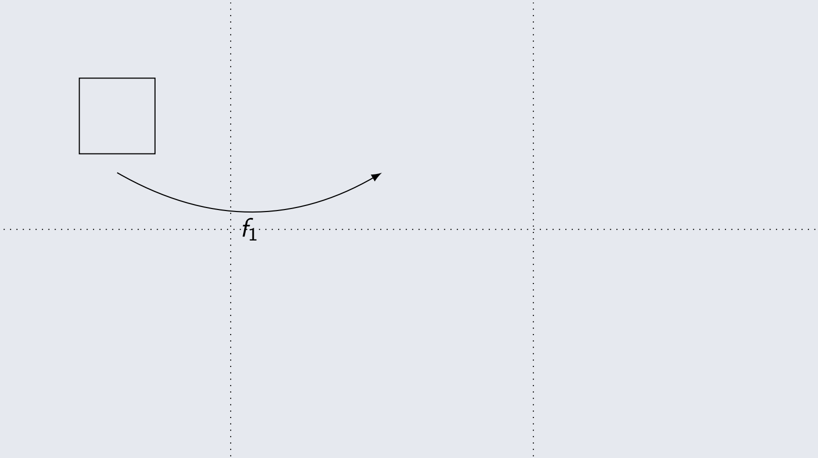
The **gain** in precision in x_8 is invisible.

Lifting techniques

Methods comparison

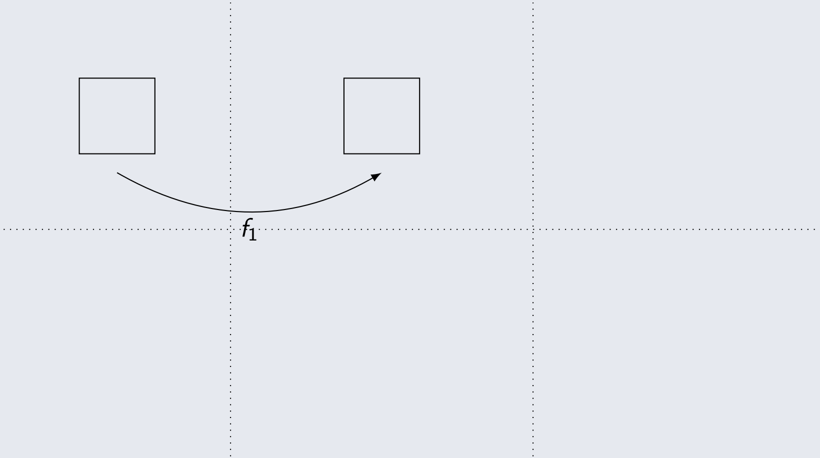
Lifting techniques

Methods comparison



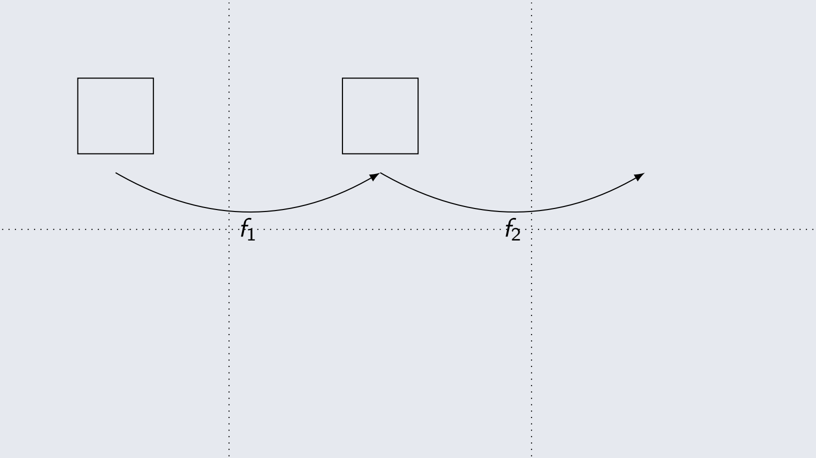
Lifting techniques

Methods comparison



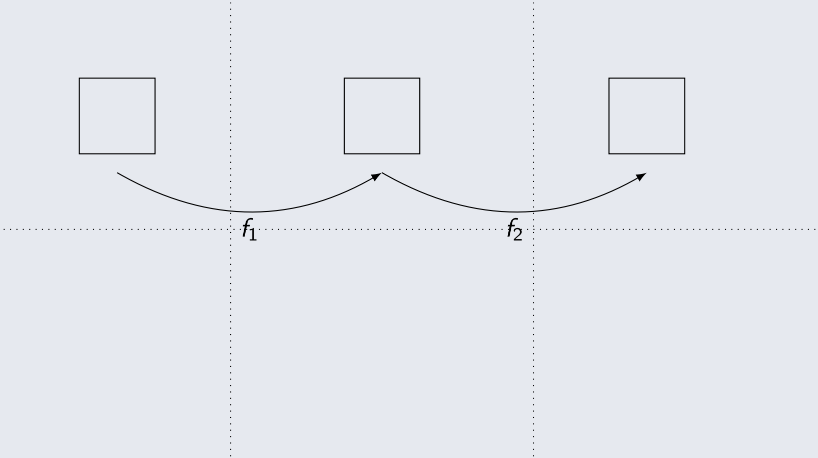
Lifting techniques

Methods comparison



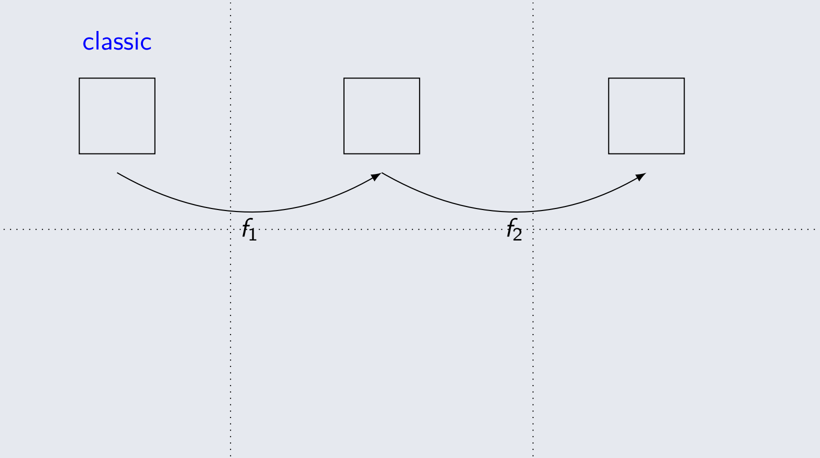
Lifting techniques

Methods comparison



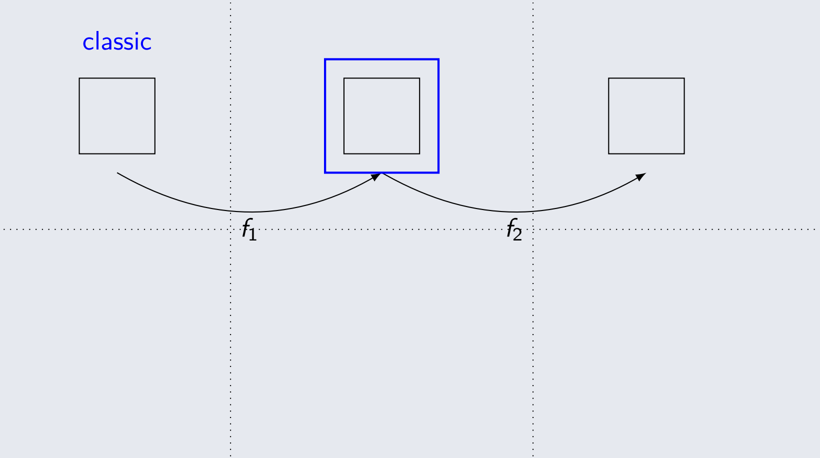
Lifting techniques

Methods comparison



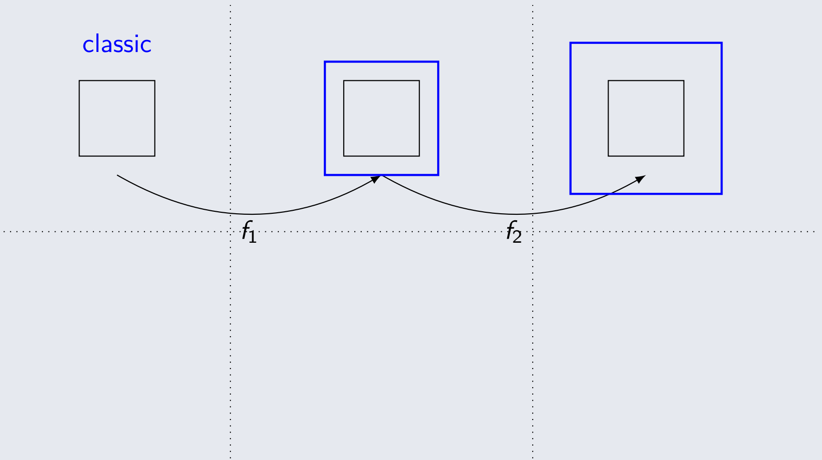
Lifting techniques

Methods comparison



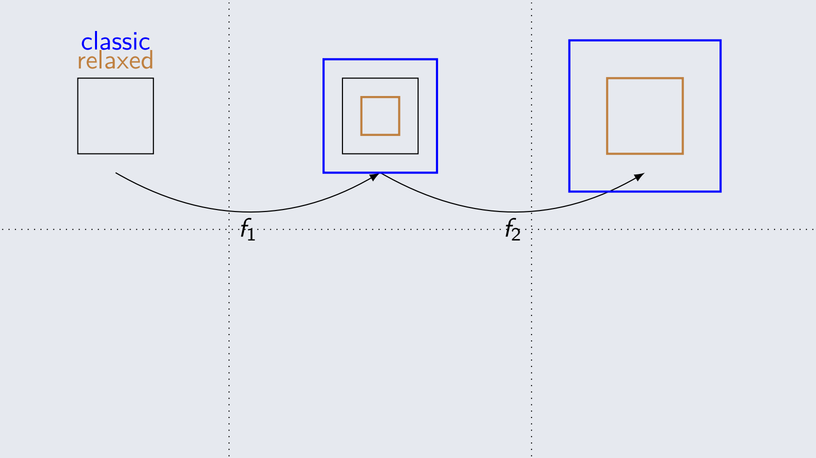
Lifting techniques

Methods comparison



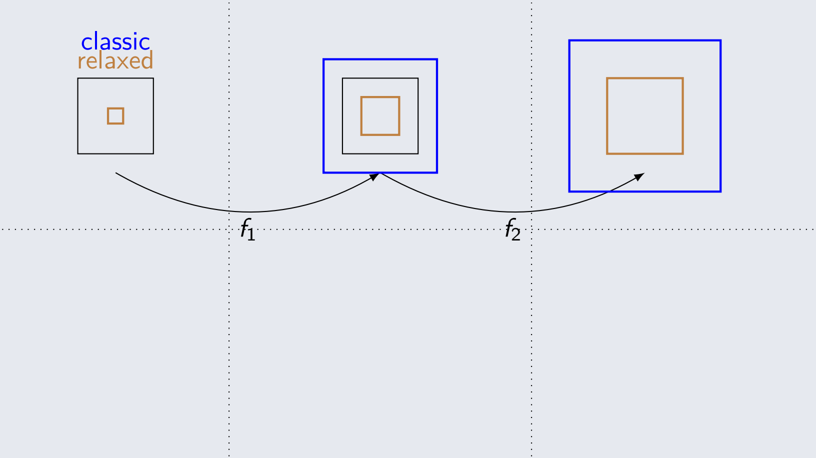
Lifting techniques

Methods comparison



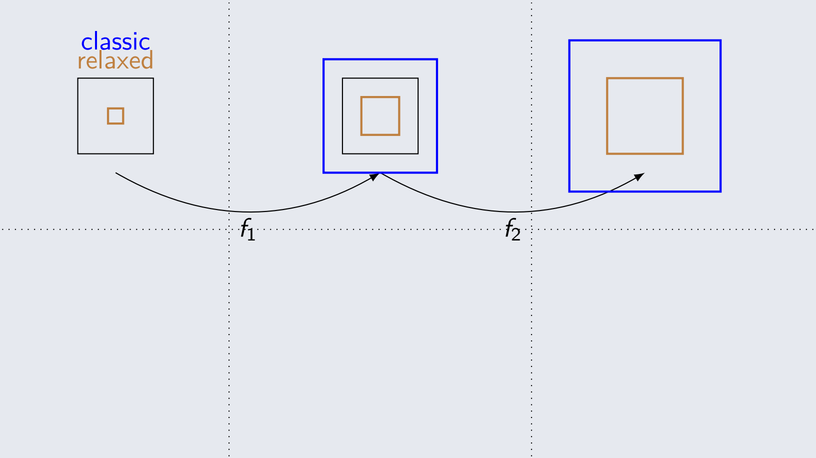
Lifting techniques

Methods comparison



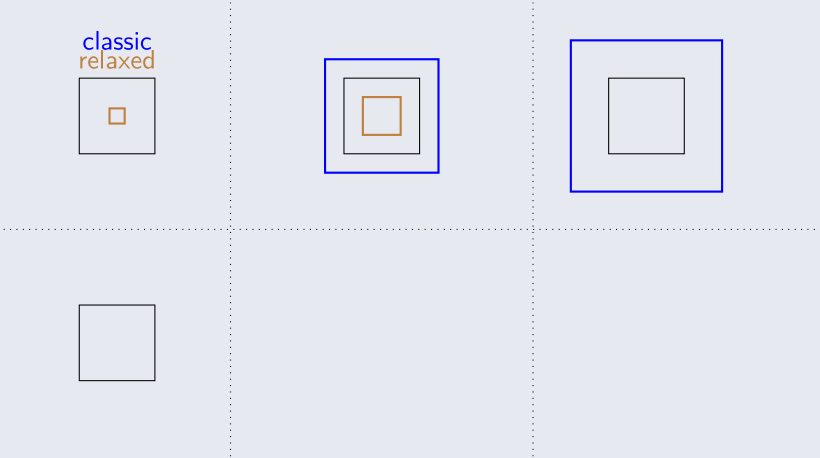
Lifting techniques

Methods comparison



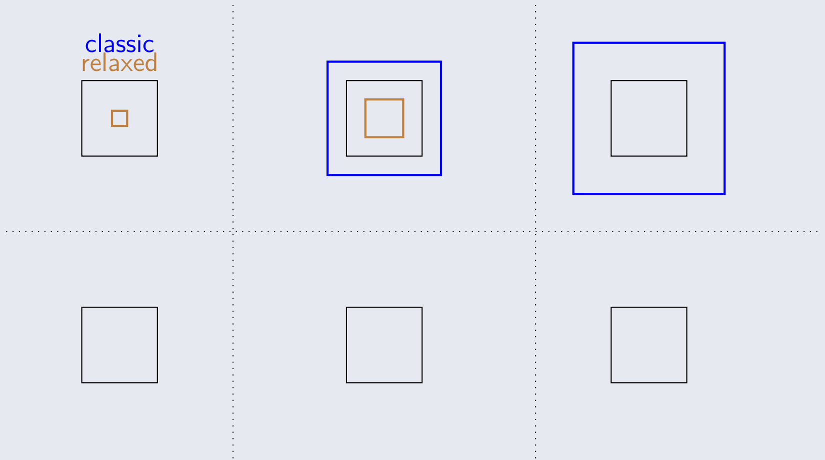
Lifting techniques

Methods comparison



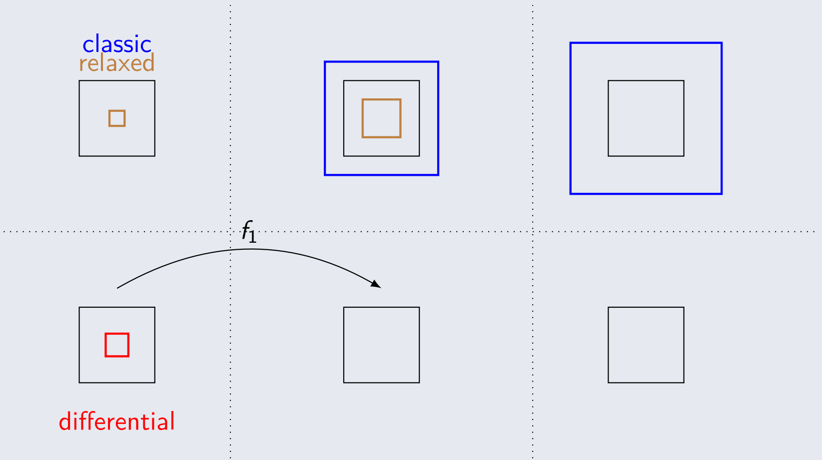
Lifting techniques

Methods comparison



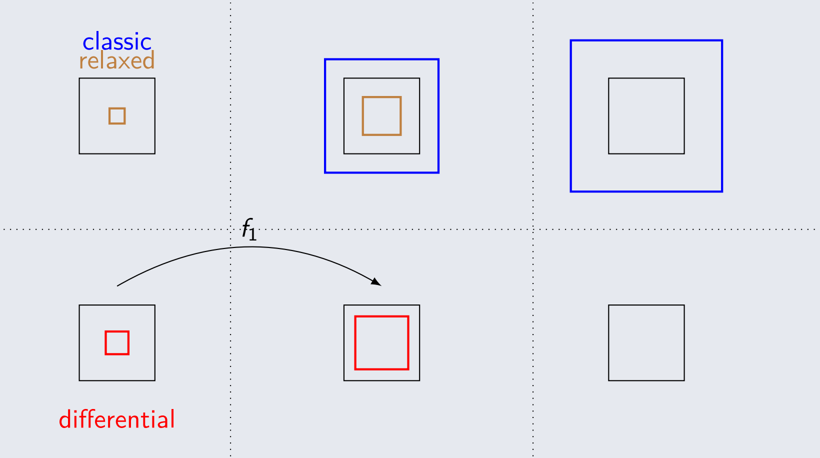
Lifting techniques

Methods comparison



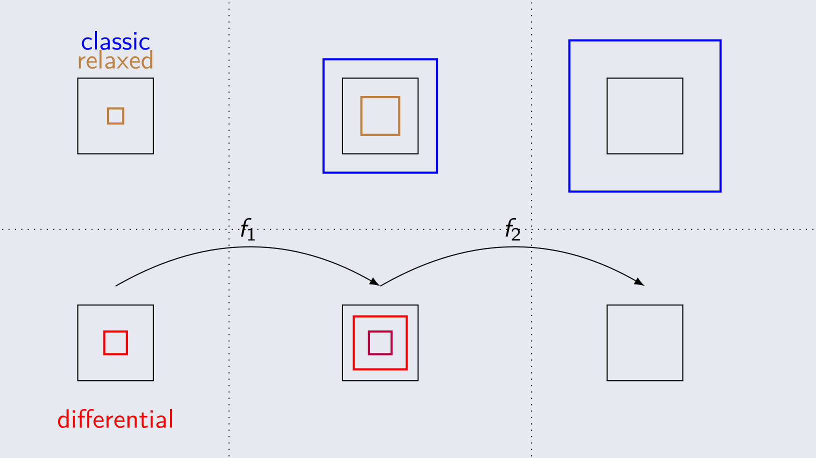
Lifting techniques

Methods comparison



Lifting techniques

Methods comparison



Lifting techniques

Methods comparison

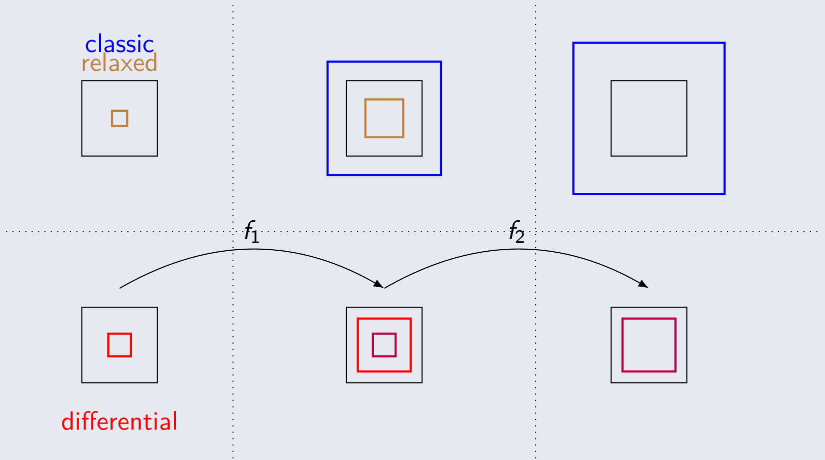


Table of contents

Some calculus

Differential of the euclidean division

Let $A, B \in \mathbb{Q}_p[X]$. We would like to differentiate $A = BQ + R$.

Some calculus

Differential of the euclidean division

Let $A, B \in \mathbb{Q}_p[X]$. We would like to differentiate $A = BQ + R$.
We can write $A + \delta A = (B + \delta B)(Q + \delta Q) + R + \delta R$.

Some calculus

Differential of the euclidean division

Let $A, B \in \mathbb{Q}_p[X]$. We would like to differentiate $A = BQ + R$.
We can write $A + \delta A = (B + \delta B)(Q + \delta Q) + R + \delta R$.
Then,

$$\delta A - Q\delta B = B\delta Q + \delta R.$$

Some calculus

Differential of the euclidean division

Let $A, B \in \mathbb{Q}_p[X]$. We would like to differentiate $A = BQ + R$.
We can write $A + \delta A = (B + \delta B)(Q + \delta Q) + R + \delta R$.
Then,

$$\delta A - Q\delta B = B\delta Q + \delta R.$$

Therefore, δQ and δR are determined by the division of $\delta A - Q\delta B$ by B.

About matrices

Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

About matrices

Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$M = LU$$

About matrices

Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$M = LU$$
$$M + \delta M = (L + \delta L)(U + \delta U)$$

About matrices

Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$
\begin{aligned}
M &= LU \\
M + \delta M &= (L + \delta L)(U + \delta U) \\
M + \delta M &= LU + \delta L \times U + L \times \delta U
\end{aligned}
$$

About matrices

Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$
\begin{aligned}
M &= LU \\
M + \delta M &= (L + \delta L)(U + \delta U) \\
M + \delta M &= LU + \delta L \times U + L \times \delta U \\
\delta M &= \delta L \times U + L \times \delta U
\end{aligned}
$$

About matrices

Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$
\begin{aligned}
M &= LU \\
M + \delta M &= (L + \delta L)(U + \delta U) \\
M + \delta M &= LU + \delta L \times U + L \times \delta U \\
\delta M &= \delta L \times U + L \times \delta U \\
L^{-1} \times \delta M \times U^{-1} &= L^{-1} \times \delta L + \delta U \times U^{-1}
\end{aligned}
$$

About matrices

Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$\begin{aligned} M &= LU \\ M + \delta M &= (L + \delta L)(U + \delta U) \\ M + \delta M &= LU + \delta L \times U + L \times \delta U \\ \delta M &= \delta L \times U + L \times \delta U \\ L^{-1} \times \delta M \times U^{-1} &= L^{-1} \times \delta L + \delta U \times U^{-1} \end{aligned}$$

Therefore, $\begin{aligned} \delta L &= L \times \left(L^{-1} \times \delta M \times U^{-1}\right)_{\mathrm{Low}} \\ \delta U &= \left(L^{-1} \times \delta M \times U^{-1}\right)_{\mathrm{Up}} \times U \end{aligned}$

Table of contents

Multivariate polynomials

Differential of polynomial division

Like for euclidean division, it is possible to differentiate the division of f by a Gröbner basis $(f_1, \dots, , f_s)$.

Multivariate polynomials

Differential of polynomial division

Like for euclidean division, it is possible to differentiate the division of f by a Gröbner basis $(f_1, \dots, , f_s)$. If we write

$$f = q_1 f_1 + \dots q_s f_s + r,$$

Multivariate polynomials

Differential of polynomial division

Like for euclidean division, it is possible to differentiate the division of f by a Gröbner basis $(f_1, \dots, , f_s)$. If we write

$$f = q_1 f_1 + \dots q_s f_s + r,$$

then δr is the remainder of the division of $f - (\delta q_1 \times f_1 + \dots \delta q_s \times f_s)$ by $(f_1, \dots, f_s)$.

Back to GB

Differential of reduced GB

Let $(f_1, \dots, f_s)$ satisfying **Structure**.

Back to GB

Differential of reduced GB

Let $(f_1, \dots, f_s)$ satisfying **Structure**. Let $(g_1, \dots, g_t)$ be the corresponding reduced Gröbner bases.

Back to GB

Differential of reduced GB

Let $(f_1, \ldots, f_s)$ satisfying **Structure**. Let $(g_1, \ldots, g_t)$ be the corresponding reduced Gröbner bases.
We may write

$$(g_1, \ldots, g_t) = (f_1, \ldots, f_s) \times A.$$

UNIVERSITÉ DE RENNES 1

Back to GB

Differential of reduced GB

Let $(f_1, \ldots, f_s)$ satisfying **Structure**. Let $(g_1, \ldots, g_t)$ be the corresponding reduced Gröbner bases.
We may write

$$(g_1, \ldots, g_t) = (f_1, \ldots, f_s) \times A.$$

We can diffentiate,

$$(\delta g_1, \ldots, \delta g_t) = (f_1, \ldots, f_s) \times \delta A + (\delta f_1, \ldots, \delta f_s) \times A.$$

Back to GB

Differential of reduced GB

Let $(f_1, \dots, f_s)$ satisfying **Structure**. Let $(g_1, \dots, g_t)$ be the corresponding reduced Gröbner bases.
We may write

$$(g_1, \dots, g_t) = (f_1, \dots, f_s) \times A.$$

We can diffentiate,

$$(\delta g_1, \dots, \delta g_t) = (\delta f_1, \dots, \delta f_s) \times A \mod (g_1, \dots, g_t).$$

Back to GB

Differential of reduced GB

Let $(f_1, \dots, f_s)$ satisfying **Structure**. Let $(g_1, \dots, g_t)$ be the corresponding reduced Gröbner bases.
We may write

$$(g_1, \dots, g_t) = (f_1, \dots, f_s) \times A.$$

We can diffentiate,

$$(\delta g_1, \dots, \delta g_t) = (\delta f_1, \dots, \delta f_s) \times A \mod (g_1, \dots, g_t).$$

$(\delta g_1, \dots, \delta g_t)$ is the remainder of the divisions of $(\delta f_1, \dots, \delta f_s) \times A$ by $(g_1, \dots, g_t)$.

On Gröbner bases

On Gröbner bases

- With **Structure**, can be computed over $\mathbb{Q}_p$.

On Gröbner bases

- With **Structure**, can be computed over $\mathbb{Q}_p$.
- The step-by-step analysis show the differentiability.

On Gröbner bases

- With **Structure**, can be computed over $\mathbb{Q}_p$.
- The step-by-step analysis show the differentiability.

On p-adic precision

On Gröbner bases

- With **Structure**, can be computed over $\mathbb{Q}_p$.
- The step-by-step analysis show the differentiability.

On p-adic precision

- Step-by-step analysis : as a first step.

On Gröbner bases

- With **Structure**, can be computed over $\mathbb{Q}_p$.
- The step-by-step analysis show the differentiability.

On p-adic precision

- Step-by-step analysis : as a first step.
- Differential calculus : **intrinsic** and can handle both **gain** and **loss**.

On Gröbner bases

- With **Structure**, can be computed over $\mathbb{Q}_p$.
- The step-by-step analysis show the differentiability.

On p-adic precision

- Step-by-step analysis : as a first step.
- Differential calculus : **intrinsic** and can handle both **gain** and **loss**.
- New framework : differentials and lattices.

References

Over *p*-adic precision

- Xavier Caruso Random matrix over a DVR and LU factorization, preprint.
- Xavier Caruso, David Roe and Tristan Vaccon Tracking *p*-adic precision, preprint.

Over Gröbner bases

- Tristan Vaccon Matrix-F5 algorithm over finite-precision complete discrete-valuation fields, preprint.
- Tristan Vaccon Matrix-F5 algorithms and tropical Gröbner bases computation, preprint.