On the computation of p-adic Gröbner bases

Tristan Vaccon

Université de Limoges

Branching from number theory: p-adics in the sciences, 09/02/2021

p 進数の俳句

Avi	Saiei M.	T.V.
Like a p-adic	p 進数	p 進整数
One step at a time, still trapped	一桁進めど	加法でも
In the unit ball	単位球	単位球

Overview on non-Archimedean Gröbner bases computations

p-adic precision

CRV14 Tracking p-adic precision, X.Caruso, D.Roe and T.Vaccon

Various takes on GB computations

Classical GB including joint works with G. Renault (ANSSI, France), 2014-2016

Tropical GB including joint works with Y. Ishihara (Rikkyo University and Tokyo University of Science, Japan), T. Verron (JKU Linz, Austria) and K. Yokoyama (Rikkyo University, Japan), 2015-2018

Tate algebras joint works with X. Caruso (Univ. Bordeaux, France) and T. Verron (JKU Linz, Austria), 2019-2021

Solving polynomial systems

Diversity of the methods

To solve a (zero-dimensional) polynomial system, many methods have been developped: RUR, eigenvalues, numerical homotopy, ... How they can be applied to non-archimedean settings has been seldom considered.

Reduction to shape position, over $K[x_1, \ldots, x_n]$, K a field

Solving using Gröbner bases (GB) often relies on performing a random change of variables so that a (reduced) lex GB is of the form:

$$\begin{array}{cc} x_1 - h_1(x_n) & \vdots \\ x_2 - h_2(x_n) & x_{n-1} - h_{n-1}(x_n) \\ \vdots & h_n(x_n) \end{array}$$

My personal motivation (long-term, loosely related)

Computing (some) moduli spaces of p-adic Galois representations.

Table of contents

Table of contents

Context and notations

p refers to a prime number

Context and notations

p refers to a prime number

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.
Working with a computer, we usually only can consider the beginning of this power series expansion: we only consider elements of the form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

Context and notations

p refers to a prime number

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.
Working with a computer, we usually only can consider the beginning of this power series expansion: we only consider elements of the 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 $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$ is d.

Context and notations

p refers to a prime number

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.
Working with a computer, we usually only can consider the beginning of this power series expansion: we only consider elements of the 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 $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$ is d.

Example

The order of $\ldots 654.3 = 3 * 7^{-1} + 4 * 7^0 + 5 * 7^1 + 6 * 7^2 + O(7^3)$ is 3.

But...

But... studying precision is actually not quite trivial

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 4132310 & \ldots 4020033 & \ldots 4421144 \\ \ldots 2202130 & \ldots 2220114 & \ldots 4204122 \end{pmatrix}$$

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 4132310 & \ldots 4020033 & \ldots 4421144 \\ \ldots 2202130 & \ldots 2220114 & \ldots 4204122 \end{pmatrix}$$

Answer:

(no pivoting strategy) just expand: $\ldots 4400000$

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 4132310 & \ldots 4020033 & \ldots 4421144 \\ \ldots 2202130 & \ldots 2220114 & \ldots 4204122 \end{pmatrix}$$

Answer:

(no pivoting strategy) just expand: $\ldots 4400000$

(partial choice of pivot) Hermite + expand:

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 4132310 & \ldots 4020033 & \ldots 4421144 \\ \ldots 2202130 & \ldots 2220114 & \ldots 4204122 \end{pmatrix}$$

Answer:

(no pivoting strategy) just expand: $\ldots 4400000$

(partial choice of pivot) Hermite + expand:

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 0000000 & \ldots 3414440 & \ldots 4223420 \\ \ldots 2202130 & \ldots 2220114 & \ldots 4204122 \end{pmatrix}$$

Answer:

(no pivoting strategy) just expand: $\ldots 4400000$

(partial choice of pivot) Hermite + expand:

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 0000000 & \ldots 3414440 & \ldots 4223420 \\ \ldots 0000000 & \ldots 0224020 & \ldots 2313110 \end{pmatrix}$$

Answer:

(no pivoting strategy) just expand: $\ldots 4400000$

(partial choice of pivot) Hermite + expand:

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 0000000 & \ldots 3414440 & \ldots 4223420 \\ \ldots 0000000 & \ldots 0224020 & \ldots 2313110 \end{pmatrix}$$

Answer:

(no pivoting strategy) just expand: $\ldots 4400000$

(partial choice of pivot) Hermite + expand:

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 0000000 & \ldots 3414440 & \ldots 4223420 \\ \ldots 0000000 & \ldots 0224020 & \ldots 2313110 \end{pmatrix}$$

Answer:

(no pivoting strategy) just expand: $\ldots 4400000$

(partial choice of pivot) Hermite + expand:

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 0000000 & \ldots 3414440 & \ldots 4223420 \\ \ldots 0000000 & \ldots 0000000 & \ldots 3014000 \end{pmatrix}$$

Answer:

(no pivoting strategy) just expand: $\ldots 4400000$

(partial choice of pivot) Hermite + expand:

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 0000000 & \ldots 3414440 & \ldots 4223420 \\ \ldots 0000000 & \ldots 0000000 & \ldots 3014000 \end{pmatrix}$$

Answer:

(no pivoting strategy) just expand: $\ldots 4400000$

(partial choice of pivot) Hermite + expand:

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 0000000 & \ldots 3414440 & \ldots 4223420 \\ \ldots 0000000 & \ldots 0000000 & \ldots 3014000 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 4132310 & \ldots 4020033 & \ldots 4421144 \\ \ldots 2202130 & \ldots 2220114 & \ldots 4204122 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 4324032 & \ldots 1014240 & \ldots 0101111 \\ \ldots 4020033 & \ldots 4132310 & \ldots 4421144 \\ \ldots 2220114 & \ldots 2202130 & \ldots 4204122 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 4324032 & \ldots 1014240 & \ldots 0101111 \\ \ldots 4020033 & \ldots 4132310 & \ldots 4421144 \\ \ldots 2220114 & \ldots 2202130 & \ldots 4204122 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 4324032 & \ldots 1014240 & \ldots 0101111 \\ \ldots 0000000 & \ldots 4043200 & \ldots 1221300 \\ \ldots 2220114 & \ldots 2202130 & \ldots 4204122 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 4324032 & \ldots 1014240 & \ldots 0101111 \\ \ldots 0000000 & \ldots 4043200 & \ldots 1221300 \\ \ldots 0000000 & \ldots 2223100 & \ldots 1100400 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 4324032 & \ldots 1014240 & \ldots 0101111 \\ \ldots 0000000 & \ldots 4043200 & \ldots 1221300 \\ \ldots 0000000 & \ldots 2223100 & \ldots 1100400 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 4324032 & \ldots 1014240 & \ldots 0101111 \\ \ldots 0000000 & \ldots 4043200 & \ldots 1221300 \\ \ldots 0000000 & \ldots 2223100 & \ldots 1100400 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 4324032 & \ldots 1014240 & \ldots 0101111 \\ \ldots 0000000 & \ldots 4043200 & \ldots 1221300 \\ \ldots 0000000 & \ldots 0000000 & \ldots 3014000 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 4324032 & \ldots 1014240 & \ldots 0101111 \\ \ldots 0000000 & \ldots 4043200 & \ldots 1221300 \\ \ldots 0000000 & \ldots 0000000 & \ldots 3014000 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 4324032 & \ldots 1014240 & \ldots 0101111 \\ \ldots 0000000 & \ldots 4043200 & \ldots 1221300 \\ \ldots 0000000 & \ldots 0000000 & \ldots 3014000 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	$\ldots 234400000$

But... studying precision is actually not quite trivial

Question: Compute the determinant of

$$\begin{pmatrix} \ldots 1014240 & \ldots 4324032 & \ldots 0101111 \\ \ldots 4132310 & \ldots 4020033 & \ldots 4421144 \\ \ldots 2202130 & \ldots 2220114 & \ldots 4204122 \end{pmatrix}$$

Answer:

(no pivoting strategy)	just expand:	$\ldots 4400000$
(partial choice of pivot)	Hermite + expand:	$\ldots 34400000$
(total choice of pivot)	SNF + expand:	$\ldots 234400000$

What is the optimal precision?

Table of contents

The Main lemma of p-adic differential precision

Lemma (CRV14)

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

The Main lemma of p-adic differential precision

Lemma (CRV14)

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a strictly 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 (CRV14)

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a strictly 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,

The Main lemma of p-adic differential precision

Lemma (CRV14)

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a strictly 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,

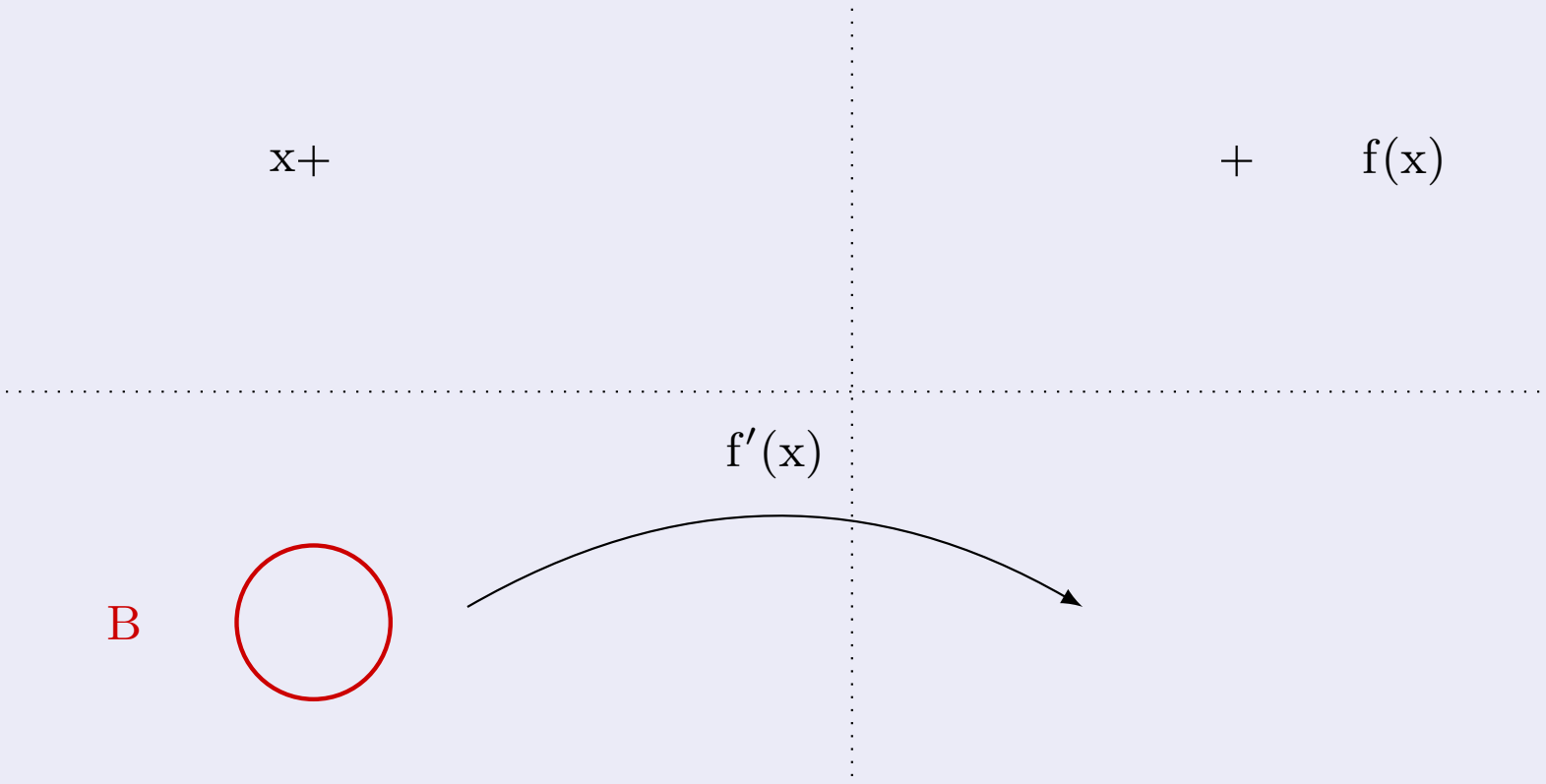
$$\boxed{f(x + B) = f(x) + f'(x) \cdot B.}$$

Geometrical meaning

Interpretation

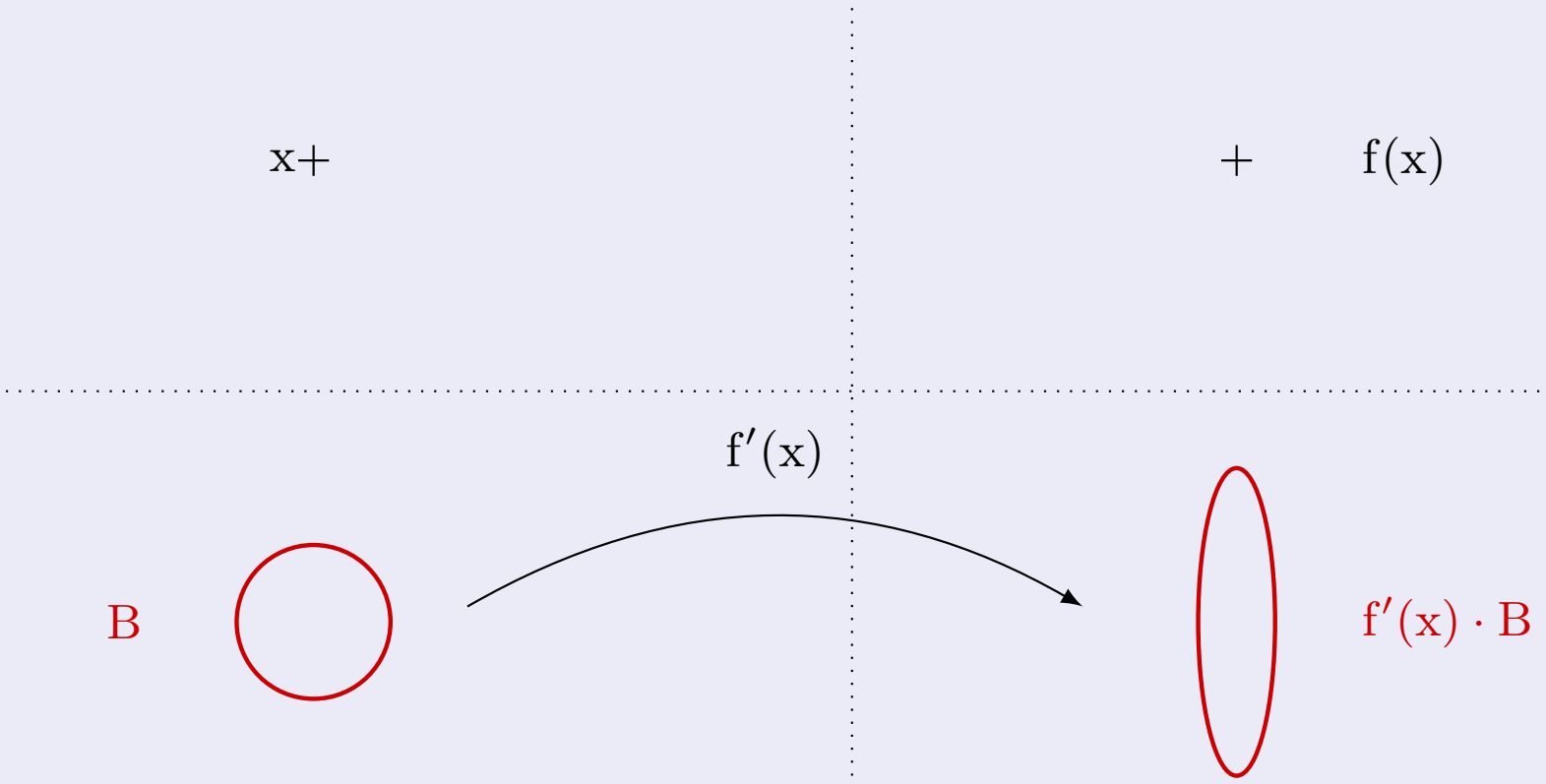
Geometrical meaning

Interpretation



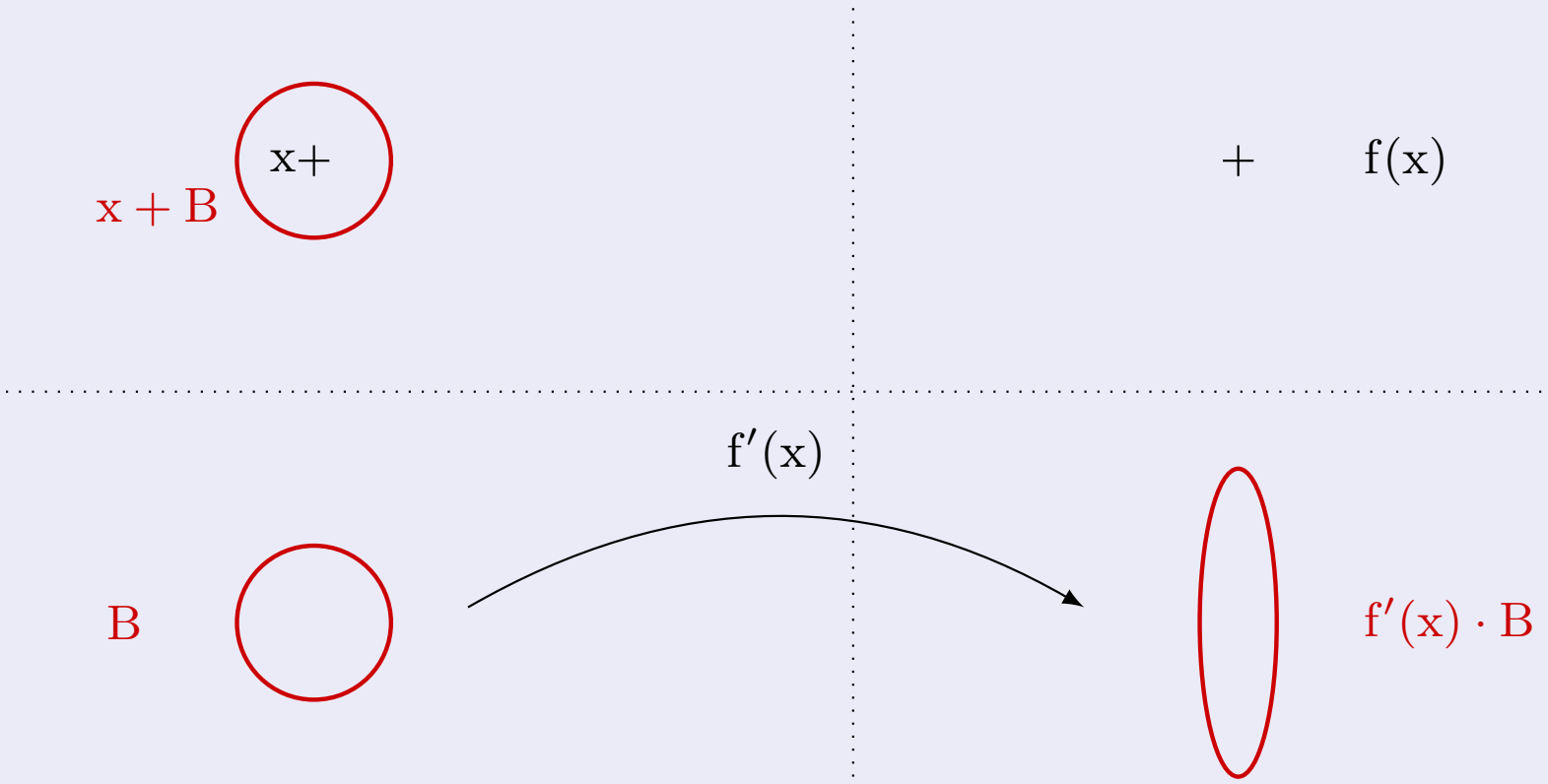
Geometrical meaning

Interpretation



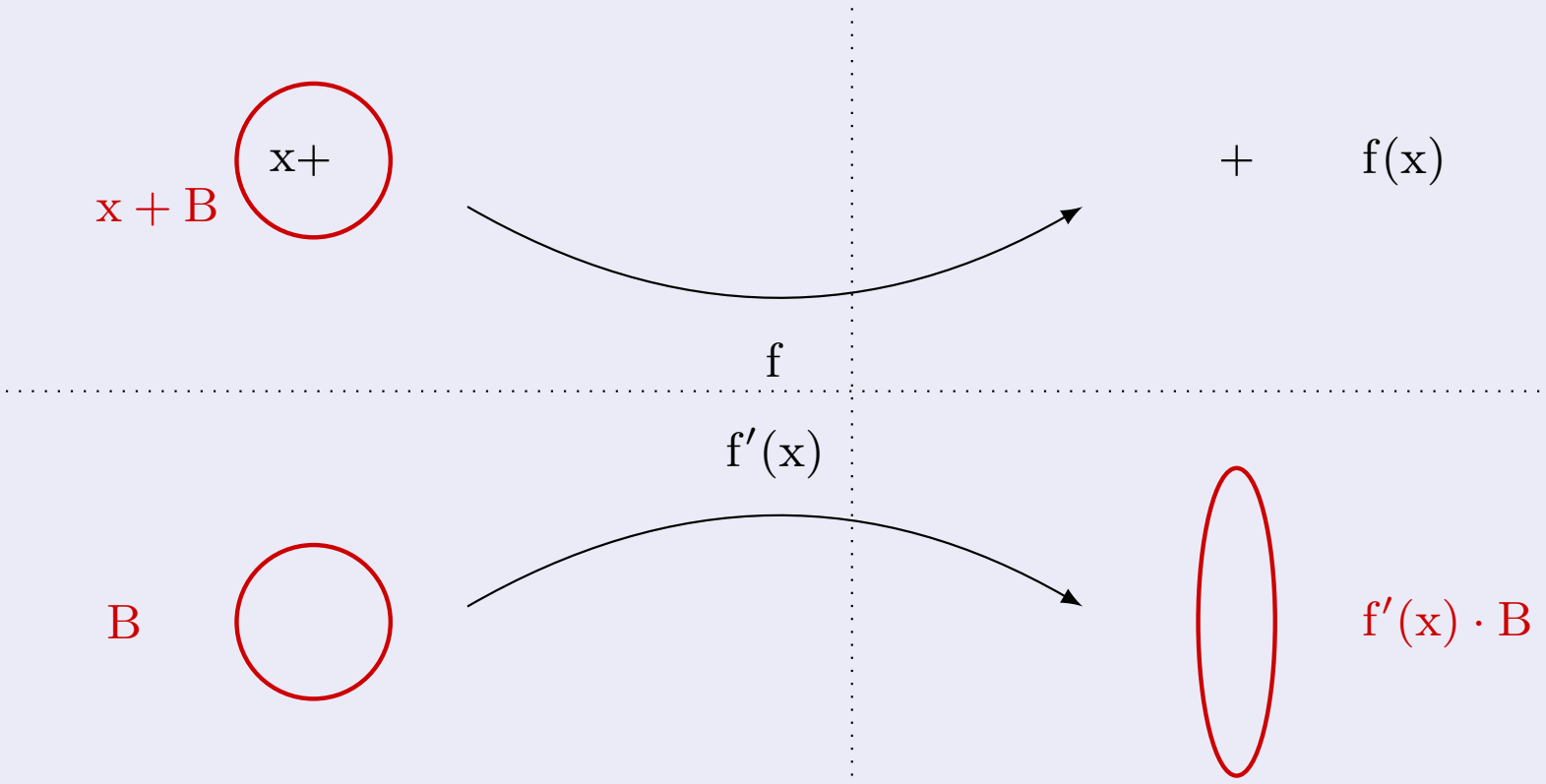
Geometrical meaning

Interpretation



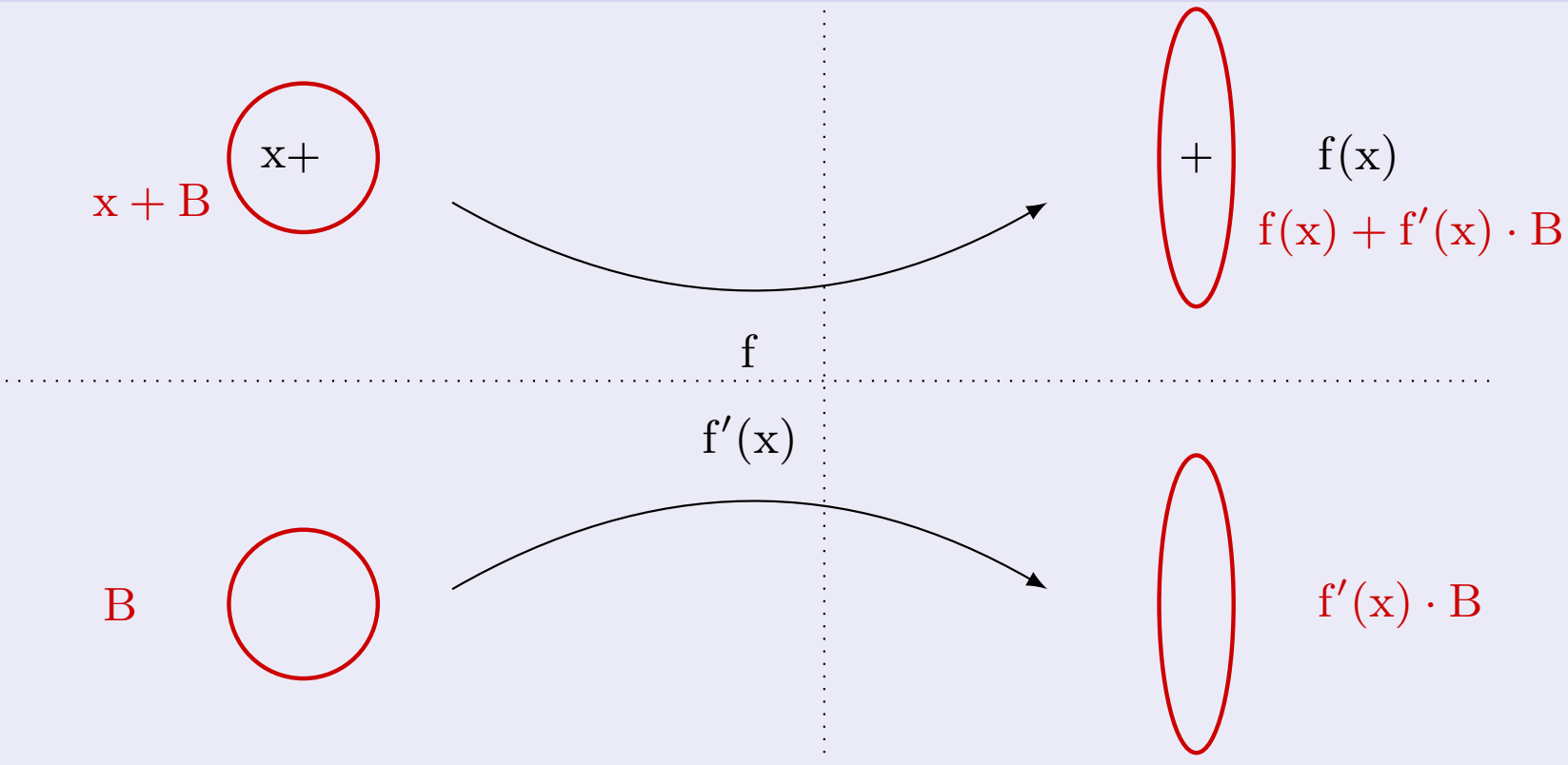
Geometrical meaning

Interpretation



Geometrical meaning

Interpretation



Looking back to the case of the determinant

Differential of the determinant

It is well known:

$$\det{}'(\mathrm{M}) : \mathrm{dM} \mapsto \mathrm{Tr}(\mathrm{Adj}(\mathrm{M}) \cdot \mathrm{dM}).$$

Looking back to the case of the determinant

Differential of the determinant

It is well known:

$$\det{}'(\mathrm{M}) : \mathrm{dM} \mapsto \mathrm{Tr}(\mathrm{Adj}(\mathrm{M}) \cdot \mathrm{dM}).$$

Consequence on precision

- Loss/gain in precision: coefficient of $\mathrm{Adj}(\mathrm{M})$ with smallest valuation.

Looking back to the case of the determinant

Differential of the determinant

It is well known:

$$\det{}'(\mathrm{M}) : \mathrm{dM} \mapsto \mathrm{Tr}(\mathrm{Adj}(\mathrm{M}) \cdot \mathrm{dM}).$$

Consequence on precision

- Loss/gain in precision: coefficient of $\mathrm{Adj}(\mathrm{M})$ with smallest valuation.
- Corresponds to the product of the first $n - 1$ invariant factors.

Looking back to the case of the determinant

Differential of the determinant

It is well known:

$$\det{}'(\mathrm{M}) : \mathrm{dM} \mapsto \mathrm{Tr}(\mathrm{Adj}(\mathrm{M}) \cdot \mathrm{dM}).$$

Consequence on precision

- Loss/gain in precision: coefficient of $\mathrm{Adj}(\mathrm{M})$ with smallest valuation.
- Corresponds to the product of the first $n - 1$ invariant factors.
- Approximate SNF is optimal.

Looking back to the case of the determinant

Differential of the determinant

It is well known:

$$\det{}'(\mathrm{M}) : \mathrm{dM} \mapsto \mathrm{Tr}(\mathrm{Adj}(\mathrm{M}) \cdot \mathrm{dM}).$$

Consequence on precision

- Loss/gain in precision: coefficient of $\mathrm{Adj}(\mathrm{M})$ with smallest valuation.
- Corresponds to the product of the first $\mathrm{n} - 1$ invariant factors.
- Approximate SNF is optimal.

Linear equations

One can easily prove that SNF is also optimal to solve linear equations.

Relation with the condition number

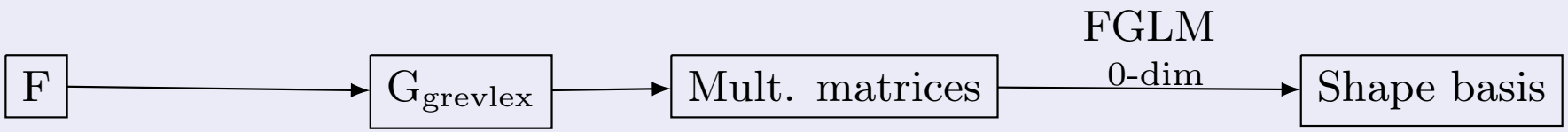
The condition number is given by the first and last invariant factors.

Table of contents

Table of contents

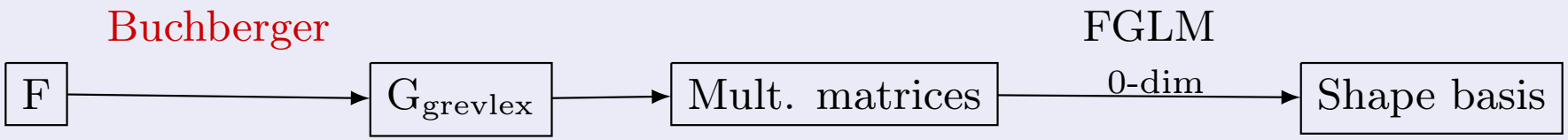
Classical strategy to compute shape position bases

Change of ordering and FGLM



Classical strategy to compute shape position bases

Change of ordering and FGLM



Buchberger's algorithm: no choice for pivot

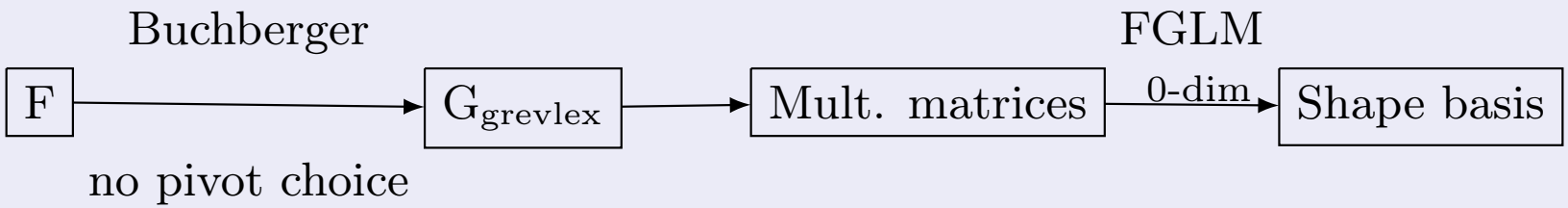
Algorithm 1: Buchberger's algorithm

input : Polynomials $f_1, \ldots, f_m$
output: a GB G of the ideal spanned by the f_i's

```
1  G ← {f_1, ..., f_m};
2  B ← {(f_i, f_j), 1 ≤ i < j ≤ m};
3  while B ≠ ∅ do
4  |   (f, g) ← element of B; B ← B ∖ {(f, g)};
5  |   h ← S-polynomial of f and g;
6  |   _, r ← division(h, G);
7  |   if r ≠ 0 then
8  |   |   B ← B ∪ {(g, r) for g ∈ G};
9  |   |   G ← G ∪ {r} ;
10 Return G;
```

Classical strategy to compute shape position bases

Change of ordering and FGLM



Macaulay's matrices

We can reduce the computations to linear algebra using so-called Macaulay matrices.

Macaulay's matrices

We can reduce the computations to linear algebra using so-called Macaulay matrices.

Definition (Macaulay matrix)

For polynomials $(h_1, \ldots, h_t)$, we denote by $\mathrm{Mac}(h_1, \ldots, h_t)$ the matrix :

$$
\begin{array}{c}
 \\
h_1 \\
\vdots \\
h_i \\
\vdots \\
h_t
\end{array}
\begin{array}{c}
\begin{array}{ccccccc} x^{\alpha_1} & > & \ldots & > & \ldots & & > x^{\alpha_l} \end{array} \\
\left[\begin{array}{ccccccc}
 & & & & & & \\
 & & & & & & \\
 & & & & & & \\
h_i & & \text{written} & & \text{in the basis of the} & & x^{\alpha_*} \\
 & & & & & & \\
 & & & & & & \\
 & & & & & &
\end{array}\right]
\end{array}
.
$$

Faugère's F4 idea: partial pivot choice

Algorithm 2: F4 algorithm

input : Polynomials $f_1, \ldots, f_m$
output: a GB G of the ideal spanned by the f_i's

```
1  G ← {f_1, ..., f_m};
2  B ← {(f_i, f_j), 1 ≤ i < j ≤ m};
3  while B ≠ ∅ do
4      d ← min_{(u,v)∈B} deg lcm(LT(u), LT(v));
5      P receives the pop of the pairs of degree d in B;
6      M is calculated as a Macaulay matrix representing the pairs in P along with
         their reducers ;
7      M ← row reduction of M (choice of pivot on every column);
8      Add to G all the polynomials obtained from M that provide new leading terms;
9      Add to B the corresponding new pairs;
10 Return G;
```

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

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

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

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

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

On signature-based GB computations

Origin and history:

- In Buchberger's algorithm, most of the time is spent reducing polynomials to zero
- Using signatures, Faugère's F5 algorithm from 2002 avoids many such reductions
- Used to be very hard to understand and is still hard to implement. Simplest (easy to prove) version of F5 is the GVW variant using the cover criterion.

On signature-based GB computations

Origin and history:

- In Buchberger's algorithm, most of the time is spent reducing polynomials to zero
- Using signatures, Faugère's F5 algorithm from 2002 avoids many such reductions
- Used to be very hard to understand and is still hard to implement. Simplest (easy to prove) version of F5 is the GVW variant using the cover criterion.

Basic idea:

- We can work with a module of $s+1$-tuples of the form:

$$(a_1, \ldots, a_s, f), \text{ s.t. } \sum_{i=1}^{s} a_i f_i = f$$

- A reduction to zero corresponds to a syzygy:

$$(b_1, \ldots, b_s, 0), \text{ meaning } \sum_{i=1}^{s} b_i f_i = 0$$

Faugère's criterion

Detecting syzygies:

- We already know well the "trivial" syzygies, with $i < j$:

$$(0, ..., 0, f_j, 0, \ldots, 0, -f_i, 0, \ldots, 0), \text{ meaning } f_j \times f_i - f_i \times f_j = 0$$

- F5 criterion: if $u = (a_1, \ldots, a_i, 0, \ldots, 0, f)$ is such that $LT(a_i) \in LT(\langle f_1, \ldots, f_{i-1} \rangle)$ then u is redundant, will be reduced to zero.

Faugère's criterion

Detecting syzygies:

- We already know well the "trivial" syzygies, with $i < j$:

$$(0, ..., 0, f_j, 0, \ldots, 0, -f_i, 0, \ldots, 0), \text{ meaning } f_j \times f_i - f_i \times f_j = 0$$

- F5 criterion: if $u = (a_1, \ldots, a_i, 0, \ldots, 0, f)$ is such that $LT(a_i) \in LT(\langle f_1, \ldots, f_{i-1} \rangle)$ then u is redundant, will be reduced to zero.

Consequences:

- With some constraints on the reductions, it is possible to work using only couples of the form:

$$(x^\alpha e_i, f)$$

- Basic F5 algorithm is: Buchberger (with some special orders on the couples) along with the F5 criterion. In advanced F5 algorithms, one uses Macaulay matrices
- In an F5 algorithm, all syzygies generated by trivial syzygies are avoided
- If $(f_1, \ldots, f_s)$ is a "regular sequence" and one uses an F5 algorithm, then no reduction to zero will happen $\rightarrow$ all matrices are injective

Row-echelon computation problems

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

Row-echelon computation problems

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

Row-echelon computation problems

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

Row-echelon computation problems

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

Row-echelon computation problems

$1+O(p^k)$	$1+O(p^k)$	$1+O(p^k)$	0
0	$O(p^k)$	$1+O(p^k)$	$1+O(p^k)$
0	$O(p^k)$	$1+O(p^k)$	$1+O(p^k)$

Injectivity problem

With the F5-criterion and F being a regular sequence,

F5 and finite precision

Row-echelon computation problems

$1+O(p^k)$	$1+O(p^k)$	$1+O(p^k)$	0
0	$O(p^k)$	$1+O(p^k)$	$1+O(p^k)$
0	$O(p^k)$	$1+O(p^k)$	$1+O(p^k)$

Injectivity problem

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

F5 and finite precision

Row-echelon computation problems

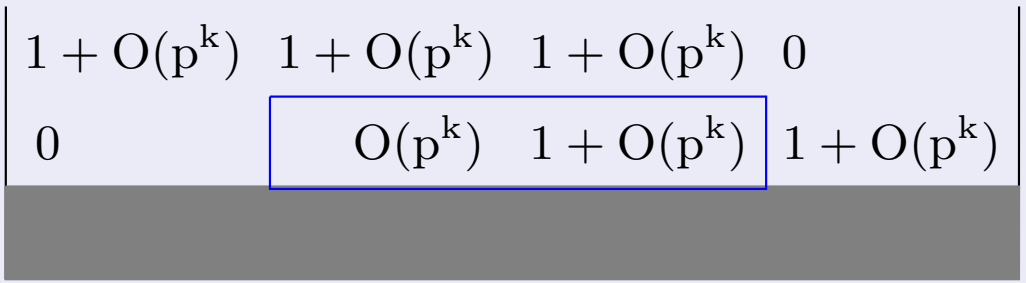
$$\begin{vmatrix} 1+O(p^k) & 1+O(p^k) & 1+O(p^k) & 0 \\ 0 & O(p^k) & 1+O(p^k) & 1+O(p^k) \end{vmatrix}$$

Injectivity problem

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

F5 and finite precision

Row-echelon computation problems



Injectivity problem

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

F5 and finite precision

Row-echelon computation problems

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

Injectivity problem

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

Position problem

If $\langle f_1, \ldots, f_s \rangle$ generates a weakly-grevlex ideals, no position problem.

F5 and finite precision

Row-echelon computation problems

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

Injectivity problem

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

Position problem

If $\langle f_1, \ldots, f_s \rangle$ generates a weakly-grevlex ideals, no position problem. This is generic, if the Moreno-Socias conjecture is true.

F5 and finite precision

Row-echelon computation problems

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

Injectivity problem

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

Position problem

If $\langle f_1, \ldots, f_s \rangle$ generates a weakly-grevlex ideals, no position problem. This is generic, if the Moreno-Socias conjecture is true.

Still, we only have partial choice of pivot... (one per column)

Classical strategy to compute shape position bases

Change of ordering and FGLM: generic entries

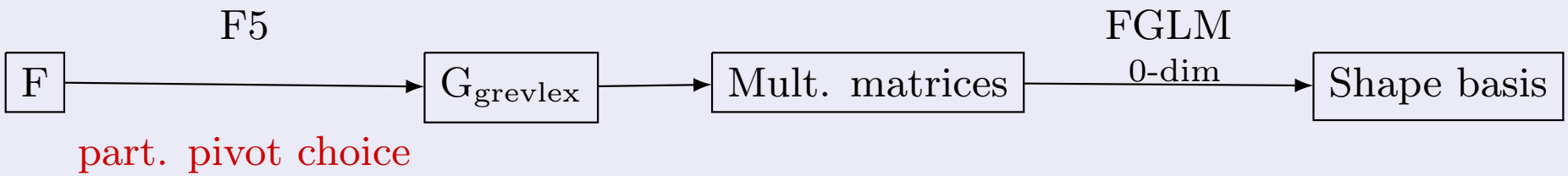
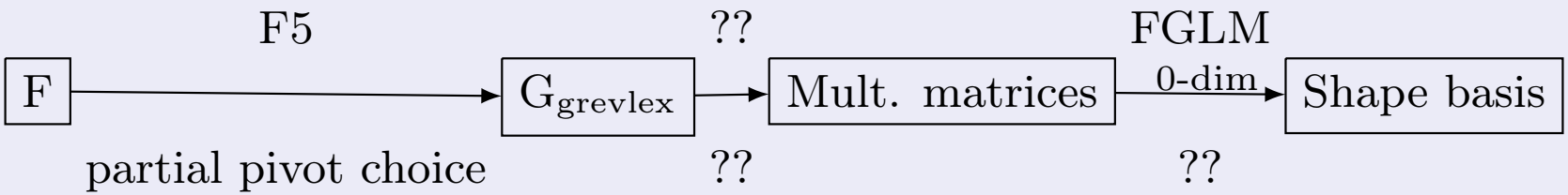


Table of contents

Classical strategy to compute shape position bases

Change of ordering and FGLM



Shape position

For an ideal in general position, the reduced lex GB of a 0-dimensional ideal is a shape position basis:

$$\begin{array}{ll} x_1 - h_1(x_n) & \vdots \\ x_2 - h_2(x_n) & x_{n-1} - h_{n-1}(x_n) \\ \vdots & h_n(x_n) \end{array}$$

Over a field of char. zero, a generic/random linear change of variable is enough for an ideal to be put in general position.

FGLM for shape position

The FGLM strategy (for grevlex to shape position)

Let $A = \mathbb{Q}_p[x_1, \ldots, x_n]$. We assume that G_1 is a GB for grevlex of an ideal I of dim. zero, in general position.

Let B be the basis of A/I given by the monomials not in LM(I), δ the dimension of A/I.

1. Compute $v_1 := x_1 \bmod G_1, \ldots, v_n := x_n \bmod G_1$ written over B
2. Compute T_n, the matrix of the multiplication by x_n in A/I, written over B
3. Iterate T_n to obtain the matrix $M := \left(x_n^{\delta-1} \bmod I, \ldots, 1 \bmod I\right)$
4. Compute M^{-1} (with SNF, total choice of pivot)
5. Read h_n from the coefficients of $-M^{-1} \cdot \left(x_n^{\delta} \bmod I\right)$
6. Read the h_i's from the coefficients of $M^{-1} \cdot v_i$

Classical strategy to compute shape position bases

Change of ordering and FGLM: generic entries

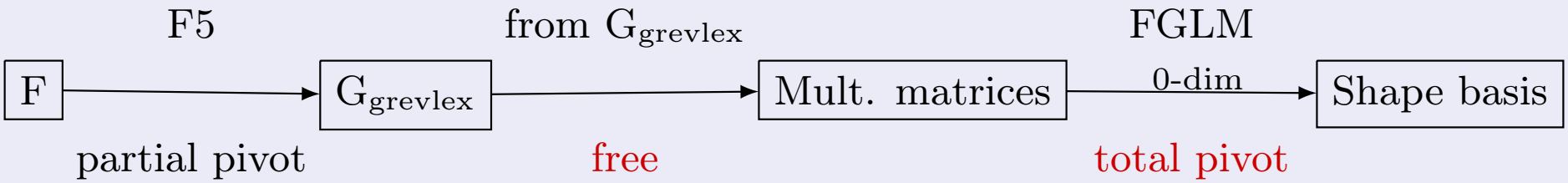


Table of contents

Back to GB

Differential of reduced GB

Let $(f_1, \ldots, f_s)$ be in "general position."

Back to GB

Differential of reduced GB

Let $(f_1, \ldots, f_s)$ be in "general position." Let $(g_1, \ldots, g_t)$ be the corresponding reduced Gröbner basis.

Back to GB

Differential of reduced GB

Let $(f_1, \ldots, f_s)$ be in "general position." Let $(g_1, \ldots, g_t)$ be the corresponding reduced Gröbner basis.
We may write

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

Back to GB

Differential of reduced GB

Let $(f_1, \ldots, f_s)$ be in "general position." Let $(g_1, \ldots, g_t)$ be the corresponding reduced Gröbner basis.
We may write

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

We can then differentiate,

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

Back to GB

Differential of reduced GB

Let $(f_1, \ldots, f_s)$ be in "general position." Let $(g_1, \ldots, g_t)$ be the corresponding reduced Gröbner basis.
We may write

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

We can then differentiate,

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

Back to GB

Differential of reduced GB

Let $(f_1, \ldots, f_s)$ be in "general position." Let $(g_1, \ldots, g_t)$ be the corresponding reduced Gröbner basis.
We may write

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

We can then differentiate,

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

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

Back to GB

Differential of reduced GB

Let $(f_1, \ldots, f_s)$ be in "general position." Let $(g_1, \ldots, g_t)$ be the corresponding reduced Gröbner basis.
We may write

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

We can then differentiate,

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

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

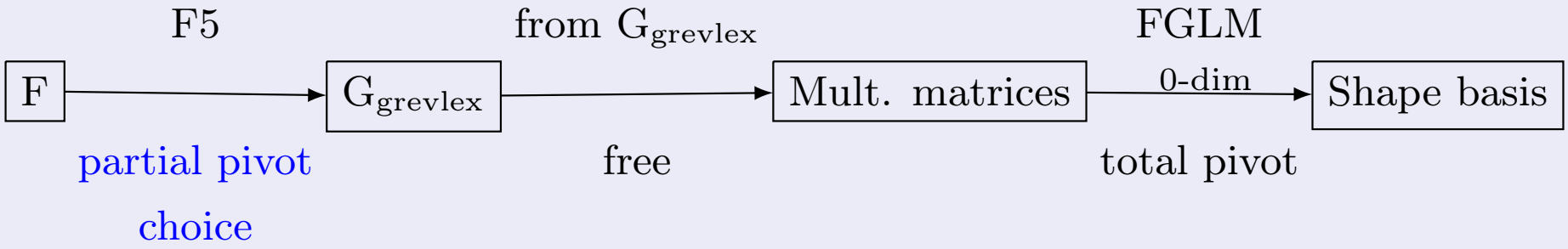
Going further

It is possible to extend further the previous formula to shape position bases, ... but the formulae are less engaging.

Table of contents

Definitions coming from tropical geometry

Change of ordering and FGLM: generic entries



Homogeneous case: total choice of pivot

For homogeneous entry polynomials, tropical geometry provides definitions allowing the best choice of pivots for Step 1.

Tropical GB

Definition (Tropical term ordering)

Let $\omega \in \mathbb{R}^n$. Let $<_{\text{mon}}$ be a monomial order on $\mathbb{Q}_p[X_1, \ldots, X_n]$.

Definition (Tropical term ordering)

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

Definition (Tropical term ordering)

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

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

Definition (Tropical term ordering)

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

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

or

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

Definition (Tropical term ordering)

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

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

or

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

We can define in(I) accordingly.

Definition (Tropical term ordering)

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

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

or

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

We can define in(I) accordingly. Then Gröbner bases are defined accordingly.

Definition (Tropical term ordering)

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

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

or

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

We can define in(I) accordingly. Then Gröbner bases are defined accordingly.
For $\omega = 0$: valuation first.

Definition (Tropical term ordering)

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

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

or

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

We can define in(I) accordingly. Then Gröbner bases are defined accordingly.
For $\omega = 0$: valuation first.

Connection with tropical geometry

This definition was first designed so that a trop. GB for weight ω can decide whether ω is in $V_{\text{trop}}(I)$.

Tropical Macaulay-matrix reduction

$$\mathrm{Mac}_d(f_1,\ldots,f_s) \simeq \begin{array}{c} x^{d_1} > \cdots > x^{d_j} > \ldots > x^{d\binom{n-1}{n+d-1}} \\ \left[\begin{array}{ccc} m_{1,1} & \cdots & m_{1,m} \\ m_{2,1} & \cdots & m_{2,m} \\ \vdots & & \\ & m_{i,j} & \\ & & \\ m_{n,1} & \cdots & m_{n,m} \end{array}\right] \end{array}$$

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

Tropical Macaulay-matrix reduction

$$\mathrm{Mac}_d(f_1,\ldots,f_s) \simeq \begin{array}{c} x^{d_1} \; > \cdots > \; x^{d_j} \; > \ldots \; > x^{d\binom{n-1}{n+d-1}} \\ \left[\begin{array}{ccc} m_{1,1} & \cdots & m_{1,m} \\ m_{2,1} & \cdots & m_{2,m} \\ \vdots & & \\ & \boxed{m_{i,j}} & \\ m_{n,1} & \cdots & m_{n,m} \end{array}\right] \end{array}$$

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

Tropical Macaulay-matrix reduction

$$\mathrm{Mac}_d(f_1,\ldots,f_s) \simeq \begin{array}{c} x^{d_1} \; > \cdots > \boxed{x^{d_j}} > \ldots \; > x^{d\binom{n-1}{n+d-1}} \\ \left[\begin{array}{ccc} m_{1,1} & \cdots & m_{1,m} \\ m_{2,1} & \cdots & m_{2,m} \\ \vdots & & \\ & \boxed{m_{i,j}} & \\ m_{n,1} & \cdots & m_{n,m} \end{array}\right] \end{array}$$

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

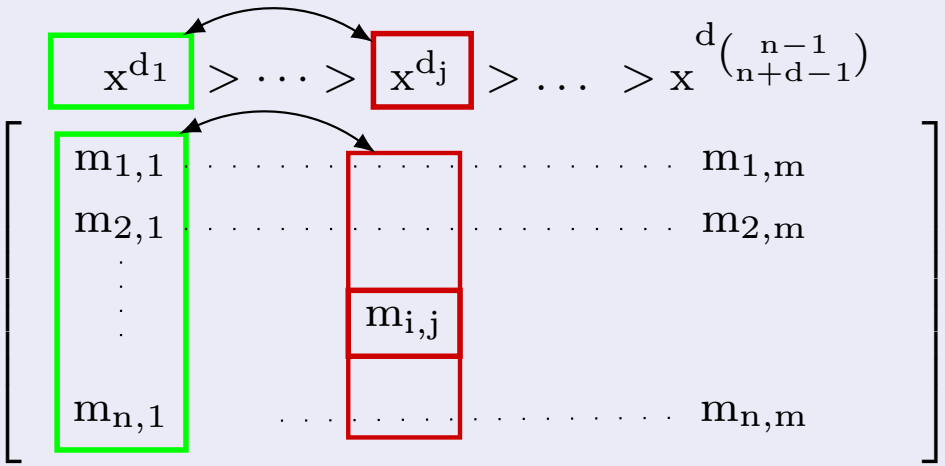
Tropical Macaulay-matrix reduction

$$\mathrm{Mac}_d(f_1,\ldots,f_s) \simeq \begin{array}{c} \boxed{x^{d_1}} > \cdots > \boxed{x^{d_j}} > \ldots > x^{d\binom{n-1}{n+d-1}} \\ \left[\begin{array}{ccccc} \boxed{m_{1,1}} & \cdots & \boxed{\phantom{m_{i,j}}} & \cdots & m_{1,m} \\ \boxed{m_{2,1}} & \cdots & \boxed{\phantom{m_{i,j}}} & \cdots & m_{2,m} \\ \boxed{\vdots} & & \boxed{m_{i,j}} & & \\ \boxed{m_{n,1}} & \cdots & \boxed{\phantom{m_{i,j}}} & \cdots & m_{n,m} \end{array}\right] \end{array}$$

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

Tropical Macaulay-matrix reduction

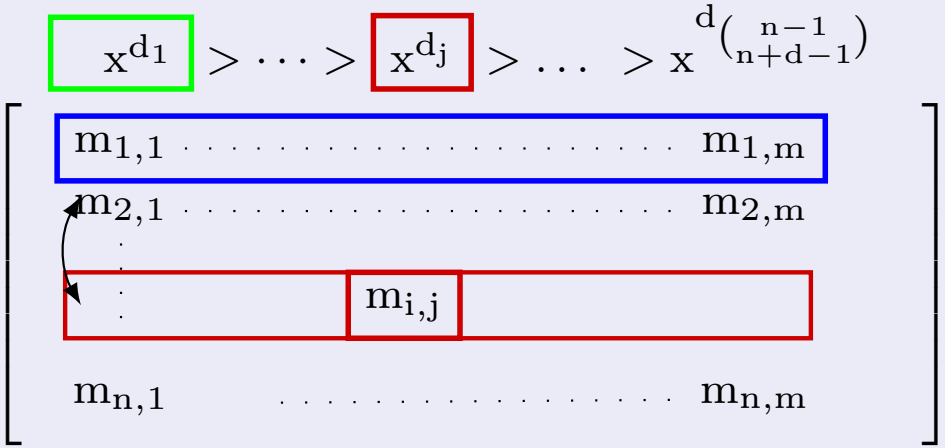
$\mathrm{Mac}_d(f_1, \ldots, f_s) \simeq$



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

Tropical Macaulay-matrix reduction

$\mathrm{Mac}_d(f_1, \ldots, f_s) \simeq$



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

Tropical reduction of Macaulay matrices

Tropical Macaulay-matrix reduction

$$\mathrm{Mac}_d(f_1,\dots,f_s) \simeq \begin{array}{c} \begin{array}{cccccc} x^{d_j} & & \dots & x^{d_1} & \dots & x^{d\binom{n-1}{n+d-1}} \end{array} \\ \left[\begin{array}{cccccc} m_{i,j} & \cdots & m_{i,1} & \cdots & m_{1,m} \\ m_{2,j} & m_{2,2} & m_{2,1} & & m_{2,m} \\ \vdots & & & & \\ m_{1,j} & & m_{1,1} & & \\ & & & & \\ m_{n,j} & \cdots & m_{n,1} & \cdots & m_{n,m} \end{array}\right] \end{array}$$

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

Tropical Macaulay-matrix reduction

$$\mathrm{Mac}_d(f_1,\dots,f_s) \simeq \begin{array}{c} \begin{array}{cccccc} x^{d_j} & & \dots & x^{d_1} & \dots & x^{d\binom{n-1}{n+d-1}} \end{array} \\ \begin{bmatrix} m_{i,j} & \cdots & m_{i,1} & \cdots & m_{1,m} \\ 0 & m_{2,2} & m_{2,1} & & m_{2,m} \\ \vdots & & & & \\ 0 & & m_{1,1} & & \\ & & & & \\ 0 & \cdots & m_{n,1} & \cdots & m_{n,m} \end{bmatrix} \end{array}$$

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

Tropical Macaulay-matrix reduction

$$\mathrm{Mac}_d(f_1,\dots,f_s) \simeq \begin{array}{c} \begin{array}{cccccc} x^{d_j} & \dots & x^{d_1} & \dots & x^{d\binom{n-1}{n+d-1}} \end{array} \\ \begin{bmatrix} m_{i,j} & \cdots & m_{i,1} & \cdots & m_{1,m} \\ 0 & m_{2,2} & m_{2,1} & & m_{2,m} \\ \vdots & & & & \\ 0 & & m_{1,1} & & \\ & & & & \\ 0 & \cdots & m_{n,1} & \cdots & m_{n,m} \end{bmatrix} \end{array}$$

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

Tropical Macaulay-matrix reduction

$$\mathrm{Mac}_d(f_1,\dots,f_s) \simeq \begin{array}{c} \begin{matrix} x^{d_j} & \dots & x^{d_1} & \dots & x^{d\binom{n-1}{n+d-1}} \end{matrix} \\ \begin{bmatrix} m_{i,j} & \cdots & m_{i,1} & \cdots & m_{1,m} \\ 0 & m_{2,2} & m_{2,1} & & m_{2,m} \\ \vdots & & & & \\ 0 & & m_{1,1} & & \\ & & & & \\ 0 & \cdots & m_{n,1} & \cdots & m_{n,m} \end{bmatrix} \end{array}$$

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

Tropical Macaulay-matrix reduction

$$\mathrm{Mac}_d(f_1,\dots,f_s) \simeq \begin{array}{c} \begin{matrix} x^{d_j} & \dots & x^{d_1} & \dots & x^{d\binom{n-1}{n+d-1}} \end{matrix} \\ \begin{bmatrix} m_{i,j} & \cdots & m_{i,1} & \cdots & m_{1,m} \\ 0 & m_{2,2} & m_{2,1} & & m_{2,m} \\ \vdots & & & & \\ 0 & & m_{1,1} & & \\ & & & & \\ 0 & \cdots & m_{n,1} & \cdots & m_{n,m} \end{bmatrix} \end{array}$$

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

When $\omega = 0$

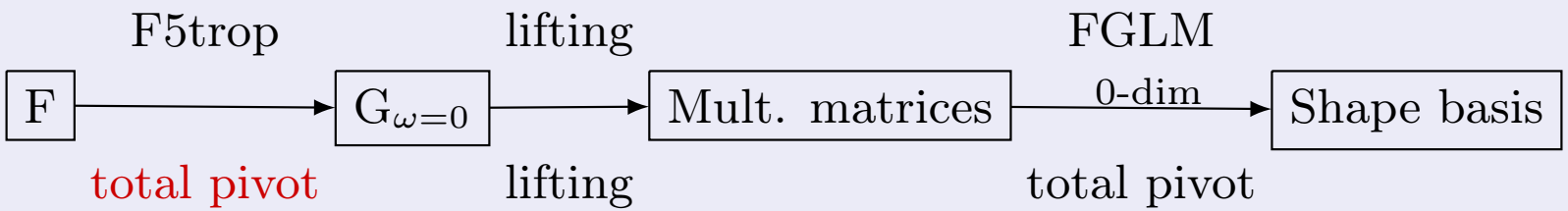
This is the SNF computation algorithm.

Conclusion on using Tropical GB

F5

One can plug the tropical Macaulay-matrix reduction into the F4/F5 algorithms.

Change of ordering and FGLM: tropical GB for homogeneous entries?



Precision problem

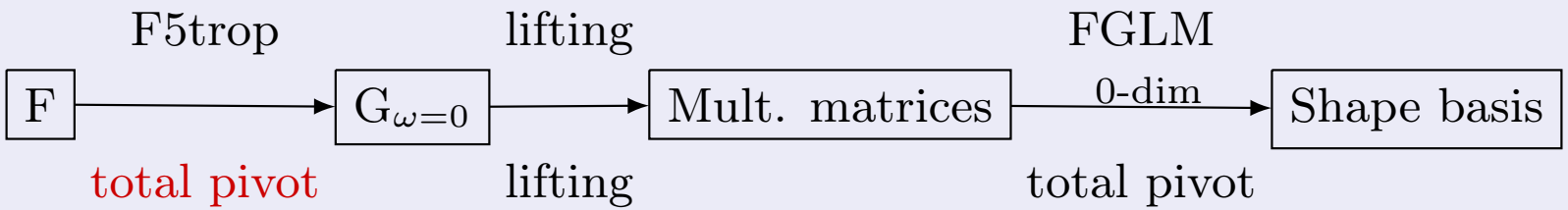
For homogeneous entry polynomials, using $\omega = 0$, we get the best choice of pivots, no position problem (when precision is enough), and no rank problem for generic entries.

Conclusion on using Tropical GB

F5

One can plug the tropical Macaulay-matrix reduction into the F4/F5 algorithms.

Change of ordering and FGLM: tropical GB for homogeneous entries?



Precision problem

For homogeneous entry polynomials, using $\omega = 0$, we get the best choice of pivots, no position problem (when precision is enough), and no rank problem for generic entries.

Problem

This strategy is flawed as the target here is an affine problem...

Table of contents

Two ways to extend to the affine case

Using polynomials

One can extend the definition of tropical term ordering using: first total degree, then a tropical term ordering.

- Benefit: F4 and F5 work well
- Problem: possibility of accumulation of loss in precision (no more always the best choice of pivot)

Another approach

Keeping "valuation first." It will lead us to Tate algebras.

Difficulty of the division

Example

We use "valuation first" to divide X by $[\underline{X} + Y, \underline{Y} + 2X]$. The steps are:

Difficulty of the division

Example

We use "valuation first" to divide X by $[\underline{X} + Y, \underline{Y} + 2X]$. The steps are:

- $f = -Y$, $r = 0$, divisor used: $\underline{X} + Y$.

Difficulty of the division

Example

We use "valuation first" to divide X by $[\underline{X} + Y, \underline{Y} + 2X]$. The steps are:

- $f = -Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 2X$, $r = 0$, divisor used: $\underline{Y} + 2X$.

Difficulty of the division

Example

We use "valuation first" to divide X by $[\underline{X} + Y, \underline{Y} + 2X]$. The steps are:

- $f = -Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 2X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- $f = -2Y$, $r = 0$, divisor used: $\underline{X} + Y$.

Difficulty of the division

Example

We use "valuation first" to divide X by $[\underline{X} + Y, \underline{Y} + 2X]$. The steps are:

- $f = -Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 2X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- $f = -2Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 4X$, $r = 0$, divisor used: $\underline{Y} + 2X$.

Difficulty of the division

Example

We use "valuation first" to divide X by $[\underline{X} + Y, \underline{Y} + 2X]$. The steps are:

- $f = -Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 2X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- $f = -2Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 4X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- $f = -4Y$, $r = 0$, divisor used: $\underline{X} + Y$.

Difficulty of the division

Example

We use "valuation first" to divide X by $[\underline{X} + Y, \underline{Y} + 2X]$. The steps are:

- $f = -Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 2X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- $f = -2Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 4X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- $f = -4Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 8X$, $r = 0$, divisor used: $\underline{Y} + 2X$.

Difficulty of the division

Example

We use "valuation first" to divide X by $[\underline{X} + Y, \underline{Y} + 2X]$. The steps are:

- $f = -Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 2X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- $f = -2Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 4X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- $f = -4Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 8X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- ...

Difficulty of the division

Example

We use "valuation first" to divide X by $[\underline{X} + Y, \underline{Y} + 2X]$. The steps are:

- $f = -Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 2X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- $f = -2Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 4X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- $f = -4Y$, $r = 0$, divisor used: $\underline{X} + Y$.
- $f = 8X$, $r = 0$, divisor used: $\underline{Y} + 2X$.
- ...

The process does not terminate, but we see here that $f \to 0$, at a rather slow rate. Hence, we need completeness.

Tate series

Definitions

$\mathbf{r} \in \mathbb{Q}^n$: convergence (log)-radii

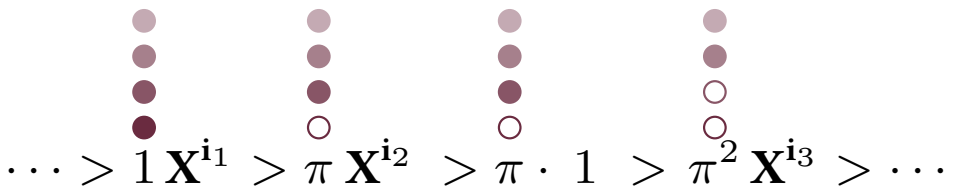
- Tate algebra $\mathbb{Q}_p\{X_1, \ldots, X_n; r_1, \ldots, r_n\} = \mathbb{Q}_p\{\mathbf{X}; \mathbf{r}\}$
- Set of series $\sum_{\alpha \in \mathbb{N}^n} a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ with $\mathrm{val}(a_\alpha) - \sum r_j \alpha_j \to \infty$
- "Convergent for substitutions by x_i's with $\mathrm{val}(x_i) \geq -r_i$"
- smaller $r_i \iff$ smaller convergence radius $\iff$ larger algebra
- Convention: $r_i = \infty$ if finitely many terms in X_i (polynomial)

Examples

- Polynomials are Tate series for all radii (finite sums)
- $f = \sum_{i,j=0}^{\infty} \pi^i X^i = 1 + \pi X + \pi^2 X^2 + \pi^3 X^3 + \cdots$
  - $f \in \mathbb{Q}_p\{X\} = \mathbb{Q}_p\{X; 0\}$
  - $f \notin \mathbb{Q}_p\{X; 1\}$: for all terms, $\mathrm{val}(\pi^\alpha) - \alpha = 0 \not\to \infty$
- $\exp(x)$, $\log(x) \in \mathbb{Q}_p\{x; -1\}$

Construction for Tate series

- Require a term ordering compatible with the topology
- First compare $\mathsf{val}(a_\alpha) - \sum r_j \alpha_j$ and break ties with a monomial order



Gröbner bases for Tate series

- Standard definition once the term order is defined:

G is a Gröbner basis of I $\iff$ for all f $\in$ I, there is g $\in$ G s.t. LT(g) divides LT(f)

- Standard equivalent characterizations:
  1. G is a Gröbner basis of I
  2. for all f $\in$ I, f is reducible modulo G
  3. for all f $\in$ I, f reduces to zero modulo G

Gröbner bases for Tate series

- Standard definition once the term order is defined:

G is a Gröbner basis of I $\iff$ for all f $\in$ I, there is g $\in$ G s.t. $\mathsf{LT}(g)$ divides $\mathsf{LT}(f)$

- Standard equivalent characterizations and a surprising one (over $\mathbb{Q}_p\{\mathbf{X}; 0\}$):
  1. G is a Gröbner basis of I
  2. for all f $\in$ I, f is reducible modulo G
  3. for all f $\in$ I, f reduces to zero modulo G
  4. (over $\mathbb{Q}_p\{\mathbf{X}; 0\}$) $\overline{G}$ is a (classical) Gröbner basis of $\bar{I}$ over $\mathbb{F}_p[\mathbf{X}]$

Gröbner bases for Tate series

- Standard definition once the term order is defined:

G is a Gröbner basis of I $\iff$ for all f $\in$ I, there is g $\in$ G s.t. $\mathsf{LT}(g)$ divides $\mathsf{LT}(f)$

- Standard equivalent characterizations and a surprising one (over $\mathbb{Q}_p\{\mathbf{X}; 0\}$):
  1. G is a Gröbner basis of I
  2. for all f $\in$ I, f is reducible modulo G
  3. for all f $\in$ I, f reduces to zero modulo G
  4. (over $\mathbb{Q}_p\{\mathbf{X}; 0\}$) $\overline{G}$ is a (classical) Gröbner basis of $\bar{I}$ over $\mathbb{F}_p[\mathbf{X}]$

- Non-terminating reductions, division algorithm
  - Theory: replace "terminating" with "convergent" everywhere
  - Practice: we always work with bounded precision

Gröbner bases for Tate series

- Standard definition once the term order is defined:

G is a Gröbner basis of I $\iff$ for all f $\in$ I, there is g $\in$ G s.t. $\mathsf{LT}(g)$ divides $\mathsf{LT}(f)$

- Standard equivalent characterizations and a surprising one (over $\mathbb{Q}_p\{\mathbf{X}; 0\}$):
  1. G is a Gröbner basis of I
  2. for all f $\in$ I, f is reducible modulo G
  3. for all f $\in$ I, f reduces to zero modulo G
  4. (over $\mathbb{Q}_p\{\mathbf{X}; 0\}$) $\overline{G}$ is a (classical) Gröbner basis of $\bar{I}$ over $\mathbb{F}_p[\mathbf{X}]$

- Non-terminating reductions, division algorithm
  - Theory: replace "terminating" with "convergent" everywhere
  - Practice: we always work with bounded precision

- Standard algorithms can be adapted: Buchberger, F4, F5, FGLM

Changing log-radii: what happens to the staircase?

Example (over $\mathbb{Q}_p$)

- $K[x, y]$: $\mathbf{r} = (\infty, \infty)$
- $I = \langle p\underline{x^2} - y^2, p\underline{y^3} - x \rangle$
- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6

- $K\{x, y\}$: $\mathbf{u} = (0, 0)$

- $J = \langle \underline{y^2} - px^2, \underline{x} - py^3 \rangle$
- $B_2 = \{1, y\}$, degree 2!

Changing log-radii: what happens to the staircase?

Example (over $\mathbb{Q}_p$)

- $K[x,y]$: $\mathbf{r} = (\infty, \infty)$
- $K\{x,y\}$: $\mathbf{u} = (0,0)$

- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $J = \langle y^2 - px^2, x - py^3 \rangle$
- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2!

- Why does x disappear from the staircase?
  We have in the old quotient $x - p^5x^5 = 0$ so $x(1 - p^5x^4) = 0$ and $1 - p^5x^4$ is invertible in the new quotient, and then $x = 0$ in the new quotient
- In general, we have to be careful with the new invertibles.

Changing log-radii: what happens to the staircase?

Example (over $\mathbb{Q}_p$)

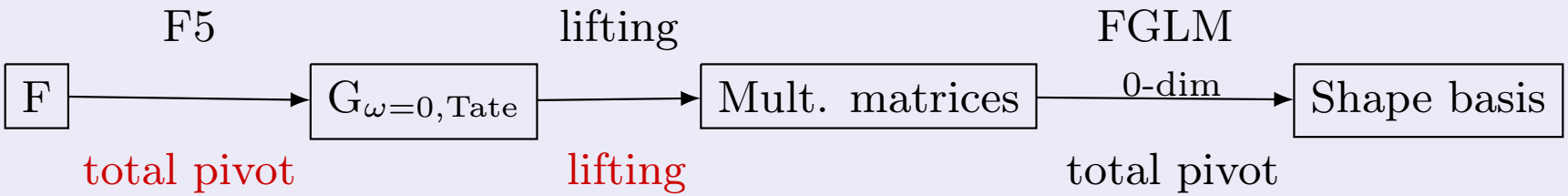
- $K[x,y]$: $\mathbf{r} = (\infty, \infty)$
- $K\{x,y\}$: $\mathbf{u} = (0,0)$

- $I = \langle p\underline{x^2} - y^2, p\underline{y^3} - x \rangle$
- $J = \langle \underline{y^2} - px^2, \underline{x} - py^3 \rangle$
- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2!

- Why does x disappear from the staircase?
  We have in the old quotient $x - p^5x^5 = 0$ so $x(1 - p^5x^4) = 0$ and $1 - p^5x^4$ is invertible in the new quotient, and then $x = 0$ in the new quotient
- In general, we have to be careful with the new invertibles.
  The solutions of big norms / small valuations are erased.

Tate algebra strategy to compute shape position bases

Change of ordering and FGLM using Tate algebra



Pros

- Best pivot strategy everywhere.

Cons

- Computing GB over Tate algebras is very, very, very slow.
- Solutions of big norms / small valuations are lost.

Conclusion

Summary

- Classical GB, Tropical GB and Tate algebra GB strategies to compute shape position bases

Conclusion

Summary

- Classical GB, Tropical GB and Tate algebra GB strategies to compute shape position bases
- Trade-off between speed and precision

Conclusion

Summary

- Classical GB, Tropical GB and Tate algebra GB strategies to compute shape position bases
- Trade-off between speed and precision
- Note: loss in precision for the shape basis can be enormous

Conclusion

Summary

- Classical GB, Tropical GB and Tate algebra GB strategies to compute shape position bases
- Trade-off between speed and precision
- Note: loss in precision for the shape basis can be enormous

Future works

- Complete implementation in SageMath

Conclusion

Summary

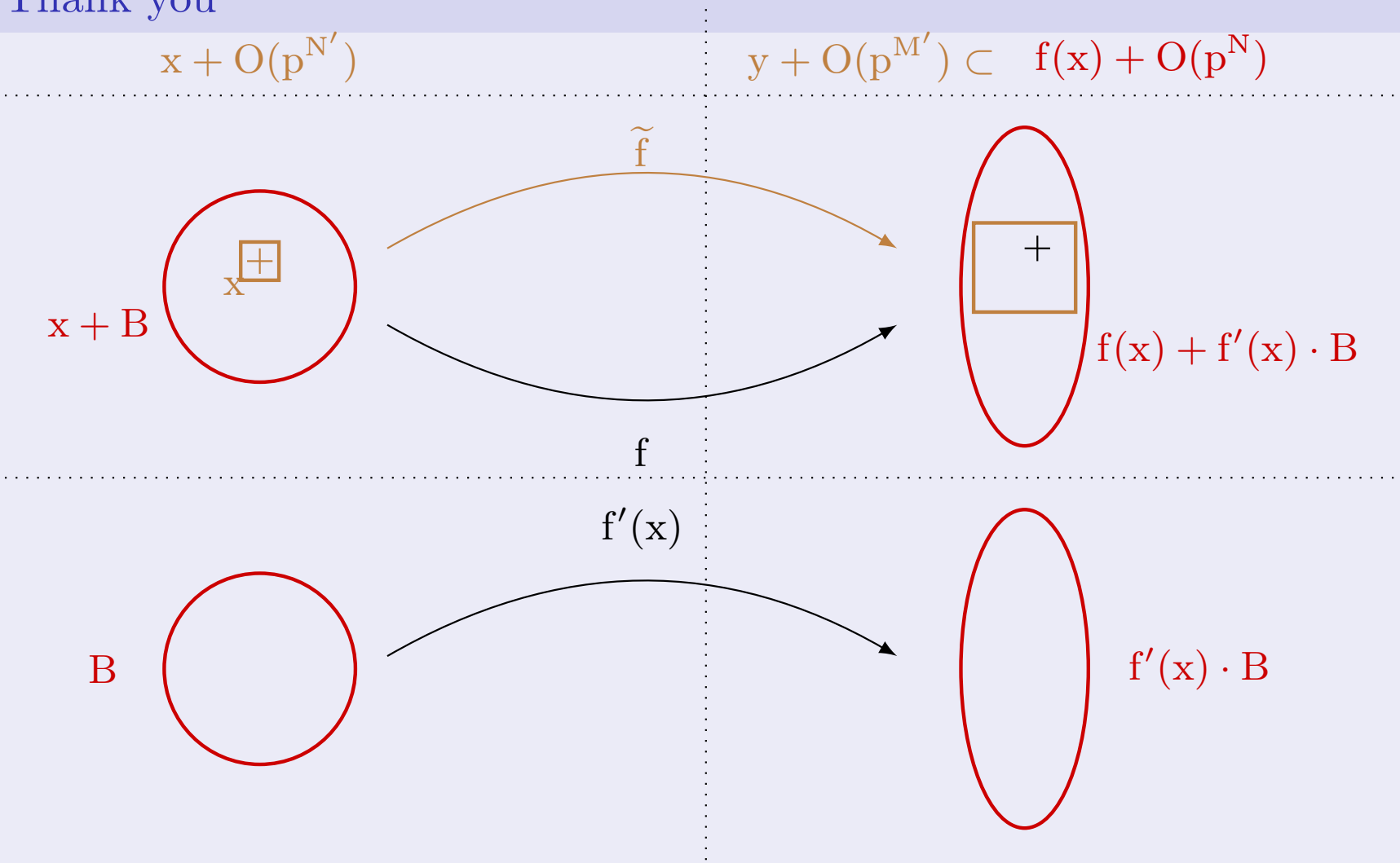
- Classical GB, Tropical GB and Tate algebra GB strategies to compute shape position bases
- Trade-off between speed and precision
- Note: loss in precision for the shape basis can be enormous

Future works

- Complete implementation in SageMath
- Implementation of rigid varieties

Thank you for your attention

Thank you



References

Differential precision

- Tracking p-adic precision, X.Caruso, D.Roe and T.Vaccon, 2014.

Solving over p-adics

- Solving p-adic polynomial systems via iterative eigenvector algorithms, A.Kulkarni, 2020.

Classical Gröbner bases

- Matrix-F5 algorithms over Finite-Precision Complete Discrete Valuation Fields, T.Vaccon, 2014, and extended version in 2016.
- On the p-adic stability of the FGLM algorithm, G.Renault and T.Vaccon, preprint.

References 2

Tropical GB

- Matrix-F5 Algorithms and Tropical Gröbner Bases Computation, T.Vaccon, 2015 and extended version in 2016.
- A Tropical F5 algorithm, T.Vaccon and K.Yokoyama, 2017.
- On Affine Tropical F5 algorithms, T.Vaccon, T.Verron and K.Yokoyama, 2018 and extended version in 2021.
- On FGLM Algorithms with Tropical Gröbner bases, Y.Ishihara, T.Vaccon, and K.Yokoyama, 2020.

Tate algebra Gröbner bases

- Gröbner bases over Tate algebras, X.Caruso, T.Vaccon and T.Verron, 2019.
- Signature-based algorithms for Gröbner bases over Tate algebras, X.Caruso, T.Vaccon and T.Verron, 2020.
- On FGLM Algorithms With Tate Algebras, X.Caruso, T.Vaccon and T.Verron, 2021.

Additional References

Classical Gröbner bases

- A new efficient algorithm for computing Gröbner bases (F4), J.C. Faugère, 1999.
- A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), J.C. Faugère, 2002.
- The F5 Criterion revised, A.Arri and J.Perry, 2011.
- A new framework for computing Gröbner bases, S.Gao, F.Volny IV, and M.Wang, 2016

Tropical Gröbner bases

- Gröbner bases over fields with valuations, A.Chan and D.Maclagan, 2013.
- Introduction to Tropical Geometry, D.Maclagan and B.Sturmfels, 2015.