Gröbner bases for Tate algebras

Xavier Caruso[1] Tristan Vaccon[2] Thibaut Verron[3]

1. Université de Bordeaux, CNRS, Inria, Bordeaux, France
2. Université de Limoges, CNRS, XLIM, Limoges, France
3. Johannes Kepler University, Institute for Algebra, Linz, Austria

PolSys/SpecFun joint seminar, 12 February 2021

Algebraic geometry and analytic geometry

$$
\begin{tikzcd}
\text{Analytic geometry} \arrow[rrr, dash] \arrow[d, shift right] & & & \text{Analytic series} \\
\text{Algebraic geometry} \arrow[rrr, dash] \arrow[u, shift right, "\text{GAGA (over } \mathbb{C}\text{)}"'] & & & \text{Polynomials}
\end{tikzcd}
$$

Algebraic geometry and analytic geometry ... over p-adics?

$$\begin{array}{ccc}
\text{Analytic geometry} & \text{———————} & \text{Analytic series} \\
\big\downarrow\big\uparrow \ \text{GAGA (over } \mathbb{C}\text{)} & & \\
\text{Algebraic geometry} & \text{———————} & \text{Polynomials} \\
\big\downarrow\big\uparrow \ \text{Non archimedean case: } \mathbb{Q}_p & & \\
??? & \text{———————} & ???
\end{array}$$

Rigid geometry and Tate series

$$
\begin{tikzcd}
\text{Analytic geometry} \arrow[r, dash] \arrow[d, shift right] & \text{Analytic series} \\
\text{Algebraic geometry} \arrow[u, shift right, "\text{GAGA (over } \mathbb{C})"'] \arrow[r, dash] \arrow[d, shift right] & \text{Polynomials} \\
\text{Rigid geometry} \arrow[u, shift right, "\text{Tate's theory (over } \mathbb{Q}_p)"'] \arrow[r, dash] & \text{Tate series}
\end{tikzcd}
$$

Needed for algorithmic rigid geometry:

- ☐ Basic arithmetic for Tate series
- ☐ Ideal operations for Tate series
- ☐ “Cut and patch” rigid varieties

Rigid geometry and Tate series

$$\begin{tikzcd}
\text{Analytic geometry} \arrow[r, dash] \arrow[d, shift right] & \text{Analytic series} \\
\text{Algebraic geometry} \arrow[r, dash] \arrow[u, shift right, "\text{GAGA (over } \mathbb{C}\text{)}"'] \arrow[d, shift right] & \text{Polynomials} \\
\text{Rigid geometry} \arrow[r, dash] \arrow[u, shift right, "\text{Tate's theory (over } \mathbb{Q}_p\text{)}"'] & \text{Tate series}
\end{tikzcd}$$

Needed for algorithmic rigid geometry:

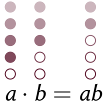
- ☐ Basic arithmetic for Tate series
- ☐ Ideal operations for Tate series
- ☐ "Cut and patch" rigid varieties

Valued fields and valuation rings: summary of basic definitions

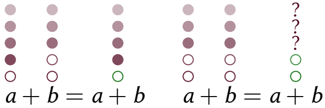
Valuation: function $\mathrm{val} : k \to \mathbb{Z} \cup \{\infty\}$ with:

- $\mathrm{val}(a) = \infty \iff a = 0$

- $\mathrm{val}(ab) = \mathrm{val}(a) + \mathrm{val}(b)$



- $\mathrm{val}(a + b) \geq \min(\mathrm{val}(a), \mathrm{val}(b))$



Examples: 1 $\quad \pi \quad$ $a = a_3\pi^3 + a_4\pi^4 + \ldots$ $\quad$ $b = b_{-3}\pi^{-3} + b_{-2}\pi^{-2} + \ldots$

$\mathrm{val}(a) = 3$

$\mathrm{val}(b) = -3$

Valued fields and valuation rings: main examples and topology

Field	$K = \mathrm{Frac}(K^\circ) = K^\circ[1/\pi]$	$\mathbb{Q}_p$	$k(\!(X)\!)$
Integer ring	$K^\circ = \{x : \mathrm{val}(x) \geq 0\}$	$\mathbb{Z}_p$	$k[\![X]\!]$
Uniformizer	π	p prime	X
Residue field	$K^\circ/\langle\pi\rangle$	$\mathbb{F}_p$	k

Valued fields and valuation rings: main examples and topology

Field	$K = \mathrm{Frac}(K^\circ) = K^\circ[1/\pi]$	$\mathbb{Q}_p$	$k(\!(X)\!)$
Integer ring	$K^\circ = \{x : \mathrm{val}(x) \geq 0\}$	$\mathbb{Z}_p$	$k[\![X]\!]$
Uniformizer	π	p prime	X
Residue field	$K^\circ/\langle\pi\rangle$	$\mathbb{F}_p$	k

- Metric and topology defined by "a is small" $\iff$ "$\mathrm{val}(a)$ is large"
- All those examples are complete for that topology
- In a complete valuation ring, a series is convergent iff its general term goes to 0:

$$\sum_{n=0}^{0} a_n = a_0$$

Valued fields and valuation rings: main examples and topology

Field	$K = \mathrm{Frac}(K^\circ) = K^\circ[1/\pi]$	$\mathbb{Q}_p$	$k((X))$
Integer ring	$K^\circ = \{x : \mathrm{val}(x) \geq 0\}$	$\mathbb{Z}_p$	$k[[X]]$
Uniformizer	π	p prime	X
Residue field	$K^\circ/\langle\pi\rangle$	$\mathbb{F}_p$	k

- Metric and topology defined by "a is small" $\iff$ "$\mathrm{val}(a)$ is large"
- All those examples are complete for that topology
- In a complete valuation ring, a series is convergent iff its general term goes to 0:

$$\sum_{n=0}^{1} a_n = a_0 + a_1$$

Valued fields and valuation rings: main examples and topology

Field	$K = \mathrm{Frac}(K^\circ) = K^\circ[1/\pi]$	$\mathbb{Q}_p$	$k((X))$
Integer ring	$K^\circ = \{x : \mathrm{val}(x) \geq 0\}$	$\mathbb{Z}_p$	$k[[X]]$
Uniformizer	π	p prime	X
Residue field	$K^\circ/\langle\pi\rangle$	$\mathbb{F}_p$	k

- Metric and topology defined by "a is small" $\iff$ "$\mathrm{val}(a)$ is large"
- All those examples are complete for that topology

- In a complete valuation ring, a series is convergent iff its general term goes to 0:

$$\sum_{n=0}^{2} a_n = a_0 + a_1 + a_2$$

Valued fields and valuation rings: main examples and topology

Field	$K = \mathrm{Frac}(K^\circ) = K^\circ[1/\pi]$	$\mathbb{Q}_p$	$k((X))$
Integer ring	$K^\circ = \{x : \mathrm{val}(x) \geq 0\}$	$\mathbb{Z}_p$	$k[[X]]$
Uniformizer	π	p prime	X
Residue field	$K^\circ/\langle\pi\rangle$	$\mathbb{F}_p$	k

- Metric and topology defined by "a is small" $\iff$ "$\mathrm{val}(a)$ is large"
- All those examples are complete for that topology
- In a complete valuation ring, a series is convergent iff its general term goes to 0:

$$\sum_{n=0}^{3} a_n = a_0 + a_1 + a_2 + a_3$$

Valued fields and valuation rings: main examples and topology

Field	$K = \mathrm{Frac}(K^\circ) = K^\circ[1/\pi]$	$\mathbb{Q}_p$	$k((X))$
Integer ring	$K^\circ = \{x : \mathrm{val}(x) \geq 0\}$	$\mathbb{Z}_p$	$k[\![X]\!]$
Uniformizer	π	p prime	X
Residue field	$K^\circ / \langle \pi \rangle$	$\mathbb{F}_p$	k

- Metric and topology defined by "a is small" $\iff$ "$\mathrm{val}(a)$ is large"
- All those examples are complete for that topology
- In a complete valuation ring, a series is convergent iff its general term goes to 0:

$$\sum_{n=0}^{\infty} a_n = a_0 + a_1 + a_2 + a_3 + \cdots$$

Tate Series

$\mathbf{X} = X_1, \ldots, X_n$

Definition

- $K\{\mathbf{X}\}^\circ$ = ring of series in $\mathbf{X}$ with coefficients in K° converging for all $\mathbf{x} \in K^\circ$
  = ring of power series whose general coefficients tend to 0

Examples

- Polynomials (finite sums are convergent)
- Tate series: $\displaystyle\sum_{i,j=0}^{\infty} \pi^{i+j} X^i Y^j = 1 + \pi X + \pi Y + \pi^2 X^2 + \pi^2 XY + \pi^2 Y^2 + \cdots$
- Not a Tate series: $\displaystyle\sum_{i=0}^{\infty} X^i = 1 + 1X + 1X^2 + 1X^3 + \cdots$
- $F \in \mathbb{C}[[Y]][[\mathbf{X}]]$ is a Tate series $\iff$ $F \in \mathbb{C}[\mathbf{X}][[Y]]$

Outline of the talk

1. Introduction and definitions

2. Gröbner bases

3. FGLM algorithm for zero-dimensional Tate ideals

Outline of the talk

Gröbner bases in finite precision

Gröbner bases:

- Multi-purpose tool for ideal arithmetic in polynomial algebras
- Membership testing, elimination, intersection...
- Uses successive (terminating) reductions

Main challenges with finite precision:

- Propagation of rounding errors
- Impossibility of zero-test

Gröbner bases in finite precision

Gröbner bases:

- Multi-purpose tool for ideal arithmetic in polynomial algebras
- Membership testing, elimination, intersection...
- Uses successive (terminating) reductions

Main challenges with finite precision:

- Propagation of rounding errors
  - A priori not a problem in a valuation ring
- Impossibility of zero-test
  - Consider larger coefficients first
- Non-terminating reductions

Gröbner bases in finite precision

Gröbner bases:

- Multi-purpose tool for ideal arithmetic in polynomial algebras
- Membership testing, elimination, intersection...
- Uses successive (terminating) reductions

Main challenges with finite precision:

- Propagation of rounding errors
  - A priori not a problem in a valuation ring
- Impossibility of zero-test
  - Consider larger coefficients first
- Non-terminating reductions
  - Theory: replace terminating with convergent everywhere
  - Practice: we always work with bounded precision

Term ordering for Tate algebras

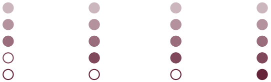
$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

- Starting from a usual monomial ordering $1 <_m \mathbf{X}^{\mathbf{i}_1} <_m \mathbf{X}^{\mathbf{i}_2} <_m \dots$
- We define a term ordering putting more weight on large coefficients

Usual term ordering:

$$\pi \cdot 1 <_m 1\,\mathbf{X}^{\mathbf{i}_1} <_m \pi\,\mathbf{X}^{\mathbf{i}_2} <_m \pi^2\,\mathbf{X}^{\mathbf{i}_3} <_m \cdots$$

Term ordering for Tate series:



$$\cdots < \pi^2\,\mathbf{X}^{\mathbf{i}_3} < \underbrace{\pi \cdot 1 < \pi\,\mathbf{X}^{\mathbf{i}_2}}_{<_m} < 1\,\mathbf{X}^{\mathbf{i}_1} < \cdots$$

Term ordering for Tate algebras

$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

- Starting from a usual monomial ordering $1 <_m \mathbf{X}^{\mathbf{i}_1} <_m \mathbf{X}^{\mathbf{i}_2} <_m \ldots$
- We define a term ordering putting more weight on large coefficients

Usual term ordering:

$$\pi \cdot 1 <_m 1\,\mathbf{X}^{\mathbf{i}_1} <_m \pi\,\mathbf{X}^{\mathbf{i}_2} <_m \pi^2\,\mathbf{X}^{\mathbf{i}_3} <_m \cdots$$

Term ordering for Tate series:

$$\cdots < \pi^2\,\mathbf{X}^{\mathbf{i}_3} < \underbrace{\pi \cdot 1 < \pi\,\mathbf{X}^{\mathbf{i}_2}}_{<_m} < 1\,\mathbf{X}^{\mathbf{i}_1} < \cdots$$

- It has infinite descending chains, but they converge to zero
- Tate series always have a leading term

$$f = \overset{\mathrm{LT}(f)}{\boxed{a_2XY}} + a_1X + a_0 \cdot 1 + a_3X^2Y^2 + \ldots$$

Term ordering for Tate algebras

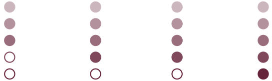
$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

- Starting from a usual monomial ordering $1 <_m \mathbf{X}^{\mathbf{i}_1} <_m \mathbf{X}^{\mathbf{i}_2} <_m \dots$
- We define a term ordering putting more weight on large coefficients

Usual term ordering:

$$\pi \cdot 1 <_m 1\,\mathbf{X}^{\mathbf{i}_1} <_m \pi\,\mathbf{X}^{\mathbf{i}_2} <_m \pi^2\,\mathbf{X}^{\mathbf{i}_3} <_m \cdots$$

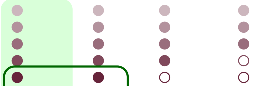
Term ordering for Tate series:



$$\cdots < \pi^2\,\mathbf{X}^{\mathbf{i}_3} < \underbrace{\pi\cdot 1 \;<\; \pi\,\mathbf{X}^{\mathbf{i}_2}}_{<_m} < 1\,\mathbf{X}^{\mathbf{i}_1} < \cdots$$

- It has infinite descending chains, but they converge to zero
- Tate series always have a leading term

$\mathrm{LT}(f)$



$$f = \boxed{a_2XY + a_1X} + a_0 \cdot 1 + a_3X^2Y^2 + \dots$$

$$\overline{f} = \overline{a_2}XY + \overline{a_1}X$$

- Isomorphism $K\{\mathbf{X}\}^\circ/\langle\pi\rangle \;\simeq\; \mathbb{F}[\mathbf{X}]$

$$f \;\mapsto\; \overline{f}$$

compatible with the term order

Gröbner bases for Tate series

- Standard definition once the term order is defined:

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

- 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

  $\exists$ sequence of reductions converging to 0

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. $\mathrm{LT}(g)$ divides $\mathrm{LT}(f)$

- Standard equivalent characterizations and a surprising one:

  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 — $\exists$ sequence of reductions converging to 0

  If I is saturated: — $\pi f \in I \implies f \in I$

  4. $\overline{G}$ is a Gröbner basis of $\overline{I}$ in the sense of $\mathbb{F}[\mathbf{X}]$

How does it work? ($4 \implies 3$)

1. Start with $f \in I$, we can assume that f has valuation 0

I is saturated

2. Separate $f = \overline{f} + f - \overline{f}$

How does it work? ($4 \implies 3$)

1. Start with $f \in I$, we can assume that f has valuation 0

   I is saturated

2. Separate $f = \overline{f} + f - \overline{f}$

3. $\overline{f} \in \overline{I}$ so we have a sequence of reductions

   $\overline{G}$ is a Gröbner basis of $\overline{I}$

$$\overline{f} - q_1\overline{g_1} - q_2\overline{g_2} - \cdots - q_r\overline{g_r} = 0$$

How does it work? ($4 \implies 3$)

1. Start with $f \in I$, we can assume that f has valuation 0

   I is saturated

2. Separate $f = \overline{f} + f - \overline{f}$

3. $\overline{f} \in \overline{I}$ so we have a sequence of reductions

   $\overline{G}$ is a Gröbner basis of $\overline{I}$

$$\overline{f} - q_1\overline{g_1} - q_2\overline{g_2} - \cdots - q_r\overline{g_r} = 0$$

4. So we have a sequence of reductions

$$f - \sum_{i=1}^{r} q_i g_i$$

How does it work? ($4 \implies 3$)

1. Start with $f \in I$, we can assume that f has valuation 0

I is saturated

2. Separate $f = \overline{f} + f - \overline{f}$

3. $\overline{f} \in \overline{I}$ so we have a sequence of reductions

$\overline{G}$ is a Gröbner basis of $\overline{I}$

$$\overline{f} - q_1\overline{g_1} - q_2\overline{g_2} - \cdots - q_r\overline{g_r} = 0$$

4. So we have a sequence of reductions

$$f - \sum_{i=1}^{r} q_i g_i = f - \sum_{i=1}^{r} q_i \overline{g_i} + \sum_{i=1}^{r} q_i \left(\overline{g_i} - g_i\right)$$

How does it work? ($4 \implies 3$)

1. Start with $f \in I$, we can assume that f has valuation 0

   I is saturated

2. Separate $f = \overline{f} + f - \overline{f}$

3. $\overline{f} \in \overline{I}$ so we have a sequence of reductions

   $\overline{G}$ is a Gröbner basis of $\overline{I}$

$$\overline{f} - q_1\overline{g_1} - q_2\overline{g_2} - \cdots - q_r\overline{g_r} = 0$$

4. So we have a sequence of reductions

$$f - \sum_{i=1}^{r} q_i g_i = f - \sum_{i=1}^{r} q_i\overline{g_i} + \sum_{i=1}^{r} q_i\left(\overline{g_i} - g_i\right)$$

$$= \quad f - \overline{f} \quad + \sum_{i=1}^{r} q_i\left(\overline{g_i} - g_i\right)$$

How does it work? ($4 \implies 3$)

1. Start with $f \in I$, we can assume that f has valuation 0 — *I is saturated*
2. Separate $f = \overline{f} + f - \overline{f}$
3. $\overline{f} \in \overline{I}$ so we have a sequence of reductions — *$\overline{G}$ is a Gröbner basis of $\overline{I}$*

$$\overline{f} - q_1\overline{g_1} - q_2\overline{g_2} - \cdots - q_r\overline{g_r} = 0$$

4. So we have a sequence of reductions

$$f - \sum_{i=1}^{r} q_i g_i = f - \sum_{i=1}^{r} q_i \overline{g_i} + \sum_{i=1}^{r} q_i \left(\overline{g_i} - g_i\right)$$

$$= \quad f - \overline{f} \quad + \sum_{i=1}^{r} q_i \left(\overline{g_i} - g_i\right) = \blacksquare = \pi \cdot f_1$$

How does it work? ($4 \implies 3$)

1. Start with $f \in I$, we can assume that f has valuation 0

I is saturated

2. Separate $f = \overline{f} + f - \overline{f}$

3. $\overline{f} \in \overline{I}$ so we have a sequence of reductions

$\overline{G}$ is a Gröbner basis of $\overline{I}$

$$\overline{f} - q_1\overline{g_1} - q_2\overline{g_2} - \cdots - q_r\overline{g_r} = 0$$

4. So we have a sequence of reductions

$$f - \sum_{i=1}^{r} q_i g_i = f - \sum_{i=1}^{r} q_i\overline{g_i} + \sum_{i=1}^{r} q_i\left(\overline{g_i} - g_i\right)$$

$$= \quad f - \overline{f} \quad + \sum_{i=1}^{r} q_i\left(\overline{g_i} - g_i\right) = \blacksquare = \pi \cdot f_1$$

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. $\mathrm{LT}(g)$ divides $\mathrm{LT}(f)$

- Standard equivalent characterizations and a surprising one:
  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 — $\exists$ sequence of reductions converging to 0

  If I is saturated: $\pi f \in I \implies f \in I$

  4. $\overline{G}$ is a Gröbner basis of $\overline{I}$ in the sense of $\mathbb{F}[\mathbf{X}]$

- Every Tate ideal has a finite Gröbner basis
- It can be computed using the usual algorithms (reduction, Buchberger, F_4)
- In practice, the algorithms run with finite precision and without loss of precision

No division by π

What about valued fields?

- Recall: K = fraction field of K°

  $\mathbb{Q}_p$ $\mathbb{Z}_p$

  $\mathbb{C}((X))$ $\mathbb{C}[[X]]$

- Elements are $\dfrac{b}{\pi^k}$ with $b \in K^\circ$, $k \in \mathbb{N}$
- The valuation can be negative but not infinite
- Same metric, same topology as K°

$a = a_{-3}\pi^{-3} + a_{-2}\pi^{-2} + \ldots$

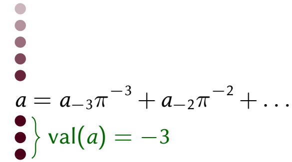
$\} \; \mathrm{val}(a) = -3$

What about valued fields?

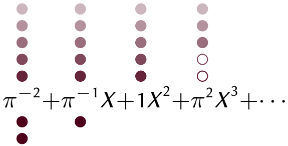
- Recall: K = fraction field of K°

  $\mathbb{Q}_p$ $\qquad$ $\mathbb{Z}_p$

  $\mathbb{C}((X))$ $\qquad$ $\mathbb{C}[[X]]$



- Elements are $\dfrac{b}{\pi^k}$ with $b \in K^\circ$, $k \in \mathbb{N}$
- The valuation can be negative but not infinite
- Same metric, same topology as K°



- Tate series can be defined as in the integer case
- Same order, same definition of Gröbner bases
- Main difference: πX now divides X

- Another surprising equivalence
  1. G is a normalized GB of I $\qquad$ $\forall g \in G, \mathrm{val}(\mathrm{LC}(g)) = 0$ (in part., $G \subset K\{\mathbf{X}\}^\circ$)
  2. $G \subset K\{\mathbf{X}\}^\circ$ is a GB of $I \cap K\{\mathbf{X}\}^\circ$

- In practice, we emulate computations in $K\{\mathbf{X}\}^\circ$ in order to avoid losses of precision (and the ideal is saturated)

Generalizing the convergence condition: log-radii in $\mathbb{Z}^n$

$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

Definition

- $K\{\mathbf{X}\}$ = ring of power series converging for all $\mathbf{x} \in K^\circ$
  = ring of power series whose general coefficients tend to 0
  = ring of power series $\sum a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$ with $\mathrm{val}(a_{\mathbf{i}}) \xrightarrow[|\mathbf{i}| \to \infty]{} +\infty$

$f \notin K\{X\}$

$$f(X) = \sum_{i=0}^{\infty} X^i = 1 + 1X + 1X^2 + \cdots \longrightarrow f(x) = 1 + x + x^2 + \cdots \text{ is divergent}$$

Generalizing the convergence condition: log-radii in $\mathbb{Z}^n$

$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

Definition

- $K\{\mathbf{X}\}$ = ring of power series converging for all $\mathbf{x}$ s.t. $\mathrm{val}(x_k) \geq 0$ ($k = 1, \ldots, n$)
  = ring of power series whose general coefficients tend to 0
  = ring of power series $\sum a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$ with $\mathrm{val}(a_{\mathbf{i}}) \xrightarrow[|\mathbf{i}| \to \infty]{} +\infty$

$f \notin K\{X\}$

$$f(X) = \sum_{i=0}^{\infty} X^i = 1 + 1X + 1X^2 + \cdots \longrightarrow f(x) = 1 + x + x^2 + \cdots \text{ is divergent}$$

Generalizing the convergence condition: log-radii in $\mathbb{Z}^n$

$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

Definition

- $K\{\mathbf{X}; \mathbf{r}\}$ = ring of power series converging for all $\mathbf{x}$ s.t. $\mathrm{val}(x_k) \geq r_k$ $(k = 1, \ldots, n)$

  = ring of power series whose general coefficients tend to 0

  = ring of power series $\sum a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$ with $\mathrm{val}(a_{\mathbf{i}}) - \mathbf{r} \cdot \mathbf{i} \xrightarrow[|\mathbf{i}| \to \infty]{} +\infty$

$f \notin K\{X\} (= K\{X; 0\})$

$$f(X) = \sum_{i=0}^{\infty} X^i = 1 + 1X + 1X^2 + \cdots \longrightarrow f(x) = 1 + x + x^2 + \cdots \text{ is divergent}$$

$f \in K\{X; 1\}$

$$\longrightarrow f(x) = 1 + x + x^2 + \cdots \text{ is convergent}$$

- Reduction to previous case by change of variables: $f(\pi X) = 1 + \pi X + \pi^2 X^2 + \cdots$

Generalizing the convergence condition: log-radii in $\mathbb{Z}^n$ and beyond

$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

Definition

- $K\{\mathbf{X}; \mathbf{r}\}$ = ring of power series converging for all $\mathbf{x}$ s.t. $\mathrm{val}(x_k) \geq r_k$ $(k = 1, \ldots, n)$

  = ring of power series whose general coefficients tend to 0

  = ring of power series $\sum a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$ with $\mathrm{val}(a_{\mathbf{i}}) - \mathbf{r} \cdot \mathbf{i} \xrightarrow[|\mathbf{i}| \to \infty]{} +\infty$
- The term order is not the same:

$$a\mathbf{X}^{\mathbf{i}} < b\mathbf{X}^{\mathbf{j}} \iff \begin{cases} \mathrm{val}(a) - \mathbf{r} \cdot \mathbf{i} < \mathrm{val}(b) - \mathbf{r} \cdot \mathbf{j} \\ \cdots = \cdots \text{ and } \mathbf{X}^{\mathbf{i}} <_m \mathbf{X}^{\mathbf{j}} \end{cases}$$

- $\mathbf{r} \in \mathbb{Q}^n$: similar (with special care)
- $\mathbf{r} = (\infty, \ldots, \infty)$: convergence everywhere, polynomial case

Summary and bottlenecks

What we have seen so far: (ISSAC 2019)

- Definition of Gröbner bases for Tate ideals
- Characterizations à la Buchberger
- Algorithmes to compute them (Buchberger, F4)

Complexity bottleneck: reductions

- Not unusual with Gröbner bases, but here the complexity grows badly with the precision
- Several areas of possible improvement:
  - Avoid useless reductions to zero
  - Speed-up interreductions
  - Exploit overconvergence
  - End goal: complexity of reductions quasi-linear in precision

Series converging faster, *i.e.*, living in a smaller Tate algebra
Ex: polynomials (log-radii ∞) seen as Tate series

Summary and bottlenecks

What we have seen so far: (ISSAC 2019)

- Definition of Gröbner bases for Tate ideals
- Characterizations à la Buchberger
- Algorithmes to compute them (Buchberger, F4)

Complexity bottleneck: reductions

- Not unusual with Gröbner bases, but here the complexity grows badly with the precision
- Several areas of possible improvement:
  - Avoid useless reductions to zero: signature algorithms (ISSAC 2020)
  - Speed-up interreductions
  - Exploit overconvergence
  - End goal: complexity of reductions quasi-linear in precision

Series converging faster, *i.e.*, living in a smaller Tate algebra
Ex: polynomials (log-radii ∞) seen as Tate series

Summary and bottlenecks

What we have seen so far: (ISSAC 2019)

- Definition of Gröbner bases for Tate ideals
- Characterizations à la Buchberger
- Algorithmes to compute them (Buchberger, F4)

Complexity bottleneck: reductions

- Not unusual with Gröbner bases, but here the complexity grows badly with the precision
- Several areas of possible improvement:
  - Avoid useless reductions to zero: signature algorithms (ISSAC 2020)
  - Speed-up interreductions
  - Exploit overconvergence
  - End goal: complexity of reductions quasi-linear in precision

Series converging faster, *i.e.*, living in a smaller Tate algebra
Ex: polynomials (log-radii ∞) seen as Tate series

Outline of the talk

1. Introduction and definitions

2. Gröbner bases

3. FGLM algorithm for zero-dimensional Tate ideals

Change of ordering and the FGLM algorithm

Change of ordering:

- Useful in the classical case for two-steps strategies
- For zero-dimensional ideals, can be done efficiently with the FGLM algorithm [Faugère, Gianni, Lazard, Mora 1993]

For Tate algebras:

- Change of monomial ordering
- But also change of term ordering and radius of convergence

Idea for overconvergence:

1. Compute a Gröbner basis in the smaller Tate algebra
2. Use change of ordering to restrict to the larger one

Characteristics of the FGLM algorithm

0-dimensional ideals:

- Variety = finitely many points
- Quotient $K[\mathbf{X}]/I$ has finite dimension as a vector space over K
- Given a Gröbner basis G, the staircase under G is
  $B = \{m \text{ monomial not divisible by any LT of } G\}$
- B is a K-basis of $K[\mathbf{X}]/I$

Outline of the algorithm:

In: G_1 a reduced Gröbner basis wrt an order $<_1$
$<_2$ a monomial order

Out: G_2 a reduced Gröbner basis wrt $<_2$

1. Compute the matrices of multiplication by $X_1, \ldots, X_n$ in the basis B_1 (computing B_1)
2. Convert them into the Gröbner basis G_2 (computing B_2)

Characteristics of the FGLM algorithm

0-dimensional ideals:

- Variety = finitely many points
- Quotient $K[\mathbf{X}]/I$ has finite dimension as a vector space over K
- Given a Gröbner basis G, the staircase under G is
  $B = \{m \text{ monomial not divisible by any LT of } G\}$
- B is a K-basis of $K[\mathbf{X}]/I$

Outline of the algorithm:

In: G_1 a reduced Gröbner basis wrt an order $<_1$
$<_2$ a monomial order

Out: G_2 a reduced Gröbner basis wrt $<_2$

1. Compute the matrices of multiplication by $X_1, \ldots, X_n$ in the basis B_1 (computing B_1)
2. Convert them into the Gröbner basis G_2 (computing B_2)

Complexity

- Degree δ of the ideal = size of B = number of solutions (with multiplicity)
- Complexity cubic (or subcubic) in δ

FGLM algorithm for Tate ideals

0-dimensional Tate ideals

- Same definition as in the polynomial case: $K\{\mathbf{X}\}/I$ has finite dimension
- B is a K-basis of $K\{\mathbf{X}\}/I$
- Any element of $K\{\mathbf{X}\}/I$ can be represented as a **polynomial**

FGLM algorithm for Tate ideals

0-dimensional Tate ideals

- Same definition as in the polynomial case: $K\{\mathbf{X}\}/I$ has finite dimension
- B is a K-basis of $K\{\mathbf{X}\}/I$
- Any element of $K\{\mathbf{X}\}/I$ can be represented as a **polynomial**

Outline of the algorithm

In: G_1 a reduced Gröbner basis in $K\{\mathbf{X}; \mathbf{r}\}$ wrt an order $<_1$

$<_2$ a monomial order

$\mathbf{u} \leq \mathbf{r}$ a system of log-radii

Out: G_2 a reduced Gröbner basis in $K\{\mathbf{X}; \mathbf{u}\}$ wrt $<_2$

1. Compute the matrices of multiplication by $X_1, \ldots, X_n$ in the basis $B_{1,\mathbf{r}}$
2. Convert them into matrices in the basis $B_{1,\mathbf{u}}$ (computing $B_{1,\mathbf{u}}$)
3. Convert them into the Gröbner basis G_2

FGLM algorithm for Tate ideals

0-dimensional Tate ideals

- Same definition as in the polynomial case: $K\{\mathbf{X}\}/I$ has finite dimension
- B is a K-basis of $K\{\mathbf{X}\}/I$
- Any element of $K\{\mathbf{X}\}/I$ can be represented as a **polynomial**

Outline of the algorithm

In: G_1 a reduced Gröbner basis in $K\{\mathbf{X}; \mathbf{r}\}$ wrt an order $<_1$
$<_2$ a monomial order
$\mathbf{u} \leq \mathbf{r}$ a system of log-radii

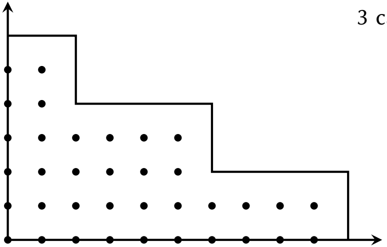
Out: G_2 a reduced Gröbner basis in $K\{\mathbf{X}; \mathbf{u}\}$ wrt $<_2$

1. Compute the matrices of multiplication by $X_1, \ldots, X_n$ in the basis $B_{1,\mathbf{r}}$
2. Convert them into matrices in the basis $B_{1,\mathbf{u}}$ (computing $B_{1,\mathbf{u}}$)
3. Convert them into the Gröbner basis G_2

Complexity

- Complexity cubic in δ
- Base complexity quasi-linear in the precision

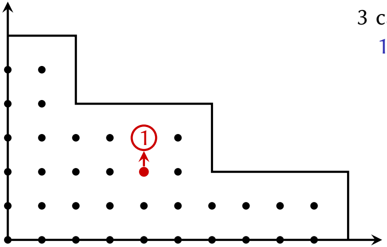
- Idea: need to compute $\mathrm{NF}(X_i m)$ for all $i \in \{1, \ldots, n\}$, $m \in B$
- Proceed in increasing order and reuse the computations



3 cases:

Iterative computation of the multiplication matrices

- Idea: need to compute $\mathrm{NF}(X_i m)$ for all $i \in \{1, \ldots, n\}$, $m \in B$
- Proceed in increasing order and reuse the computations

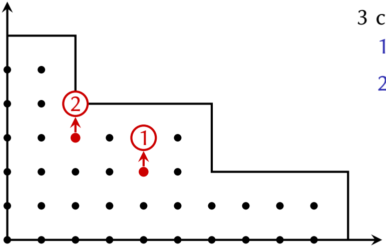


3 cases:

1. $X_i m \in B$: $\to \mathrm{NF}(X_i m) = X_i m$

Iterative computation of the multiplication matrices

- Idea: need to compute $\mathrm{NF}(X_i m)$ for all $i \in \{1, \ldots, n\}$, $m \in B$
- Proceed in increasing order and reuse the computations

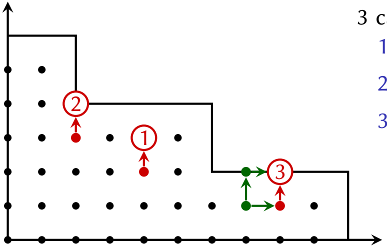


3 cases:

1. $X_i m \in B$: $\rightarrow \mathrm{NF}(X_i m) = X_i m$
2. $X_i m = \mathrm{LT}(g)$ for $g \in G \rightarrow \mathrm{NF}(X_i m) = X_i m - g$

Iterative computation of the multiplication matrices

- Idea: need to compute $\mathrm{NF}(X_i m)$ for all $i \in \{1, \ldots, n\}$, $m \in B$
- Proceed in increasing order and reuse the computations

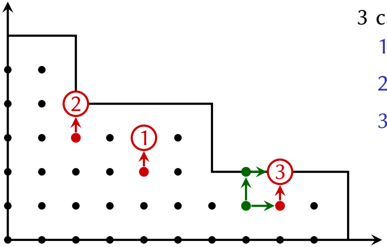


3 cases:

1. $X_i m \in B$: $\to \mathrm{NF}(X_i m) = X_i m$
2. $X_i m = \mathrm{LT}(g)$ for $g \in G \to \mathrm{NF}(X_i m) = X_i m - g$
3. Otherwise, write $m = X_j m'$ with
   $\mathrm{NF}(X_i m') = \sum a_\mu \mu$
   $\to \mathrm{NF}(X_i m) = \mathrm{NF}(X_j X_i m') = \sum a_\mu \mathrm{NF}(X_j \mu)$

Iterative computation of the multiplication matrices

- Idea: need to compute $\mathrm{NF}(X_i m)$ for all $i \in \{1, \dots, n\}$, $m \in B$
- Proceed in increasing order and reuse the computations

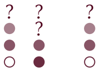


3 cases:

1. $X_i m \in B$: $\to \mathrm{NF}(X_i m) = X_i m$
2. $X_i m = \mathrm{LT}(g)$ for $g \in G \to \mathrm{NF}(X_i m) = X_i m - g$
3. Otherwise, write $m = X_j m'$ with
   $\mathrm{NF}(X_i m') = \sum a_\mu \mu$
   $\to \mathrm{NF}(X_i m) = \mathrm{NF}(X_j X_i m') = \sum a_\mu \mathrm{NF}(X_j \mu)$

Why does it work?

- Usual case: $\mathrm{NF}(m)$ only involves monomials smaller than m
- Tate case: not true, but if not their coefficient is smaller than 1 (i.e. divisible by π)
- So we can recover the value mod π, and repeating k times, the value mod π^k:



$$a \cdot b = ab$$

Two improvements on the computation of the multiplication matrices

Recursive computation:

- The previous algorithm relies on the order of the monomials
- Base complexity cubic in δ but quadratic in the precision
- Alternative: recursive algorithm, computing the coefficients mod π^k as needed
- Gives an order-agnostic algorithm which also works with non-0 log-radii
- Fast arithmetic + relaxed algorithms $\rightarrow$ base complexity quasi-linear in the precision
  [van der Hoeven 1997] [Berthomieu, van der Hoeven, Lecerf 2011] [Berthomieu, Lebreton 2012]

Two improvements on the computation of the multiplication matrices

Recursive computation:

- The previous algorithm relies on the order of the monomials
- Base complexity cubic in δ but quadratic in the precision
- Alternative: recursive algorithm, computing the coefficients mod π^k as needed
- Gives an order-agnostic algorithm which also works with non-0 log-radii
- Fast arithmetic + relaxed algorithms $\rightarrow$ base complexity quasi-linear in the precision
  [van der Hoeven 1997] [Berthomieu, van der Hoeven, Lecerf 2011] [Berthomieu, Lebreton 2012]

Non-reduced bases:

- Usual case: need bases to be reduced to ensure structure of the order
- Here, we have to consider monomials which we have not yet seen in any case
- As long as the basis is reduced mod π, the hypotheses hold
- So FGLM (with same order and log-radii as input and output)
  gives an algorithm for interreduction with complexity quasi-linear in precision
- The complexity is not only bounded in terms of δ anymore

Changing log-radii: what happens to the staircase?

Example with $K = \mathbb{Q}_p$

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

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

Changing log-radii: what happens to the staircase?

Example with $K = \mathbb{Q}_p$

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

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

- Why does x disappear from the staircase?

  Consider $x^4 \cdot x$

Changing log-radii: what happens to the staircase?

Example with $K = \mathbb{Q}_p$

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

- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $J = \langle y^2 - px^2, x - py^3 \rangle$
- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2!
- Why does x disappear from the staircase?

  Consider $x^4 \cdot x = \frac{1}{p} x^3 y^2$

Changing log-radii: what happens to the staircase?

Example with $K = \mathbb{Q}_p$

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

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

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

- Why does x disappear from the staircase?

  Consider $x^4 \cdot x = \dfrac{1}{p} x^3 y^2 = \dfrac{1}{p^2} xy^4$

Changing log-radii: what happens to the staircase?

Example with $K = \mathbb{Q}_p$

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

- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $J = \langle y^2 - px^2, x - py^3 \rangle$
- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2!
- Why does x disappear from the staircase?
  Consider $x^4 \cdot x = \frac{1}{p}x^3y^2 = \frac{1}{p^2}xy^4 = \frac{1}{p^3}x^2y$

Changing log-radii: what happens to the staircase?

Example with $K = \mathbb{Q}_p$

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

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

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

- Why does x disappear from the staircase?
  Consider $x^4 \cdot x = \frac{1}{p} x^3 y^2 = \frac{1}{p^2} x y^4 = \frac{1}{p^3} x^2 y = \frac{1}{p^4} y^3$

Changing log-radii: what happens to the staircase?

Example with $K = \mathbb{Q}_p$

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

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

- Why does x disappear from the staircase?
  Consider $x^4 \cdot x = \frac{1}{p} x^3 y^2 = \frac{1}{p^2} xy^4 = \frac{1}{p^3} x^2 y = \frac{1}{p^4} y^3 = \frac{1}{p^5} x$

Changing log-radii: what happens to the staircase?

Example with $K = \mathbb{Q}_p$

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

- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $J = \langle y^2 - px^2, x - py^3 \rangle$
- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2!
- Why does x disappear from the staircase?
  Consider $x^4 \cdot x = \frac{1}{p}x^3y^2 = \frac{1}{p^2}xy^4 = \frac{1}{p^3}x^2y = \frac{1}{p^4}y^3 = \frac{1}{p^5}x$

so $x = p^5x^5$

Changing log-radii: what happens to the staircase?

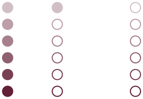
Example with $K = \mathbb{Q}_p$

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

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

- Why does x disappear from the staircase?

  Consider $x^4 \cdot x = \frac{1}{p} x^3 y^2 = \frac{1}{p^2} x y^4 = \frac{1}{p^3} x^2 y = \frac{1}{p^4} y^3 = \frac{1}{p^5} x$



  so $x = p^5 x^5 = p^{10} x^9$

Changing log-radii: what happens to the staircase?

Example with $K = \mathbb{Q}_p$

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

- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $J = \langle y^2 - px^2, x - py^3 \rangle$
- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2!
- Why does x disappear from the staircase?

  Consider $x^4 \cdot x = \frac{1}{p} x^3 y^2 = \frac{1}{p^2} xy^4 = \frac{1}{p^3} x^2 y = \frac{1}{p^4} y^3 = \frac{1}{p^5} x$

so $x = p^5 x^5 = p^{10} x^9 = \cdots = 0$

Changing log-radii: what happens to the staircase?

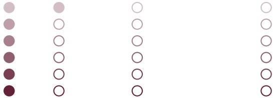
Example with $K = \mathbb{Q}_p$

- $K[x, y]$: $\mathbf{r} = (\infty, \infty)$
- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $K\{x, y\}$: $\mathbf{u} = (0, 0)$

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

- Why does x disappear from the staircase?

  Consider $x^4 \cdot x = \dfrac{1}{p} x^3 y^2 = \dfrac{1}{p^2} xy^4 = \dfrac{1}{p^3} x^2 y = \dfrac{1}{p^4} y^3 = \dfrac{1}{p^5} x$



  so $x = p^5 x^5 = p^{10} x^9 = \cdots = 0$ or equivalently $x(1 - p^5 x^4) = 0 \implies x = 0$.

Multiplication matrices and slope factorization

- Problem: how to detect this phenomenon in general?

Consider the multiplication matrix by x:

$$T_x = \begin{array}{cc} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & p^{-1} & 0 & p^{-2} & 0 & p^{-3} \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{array}{c} 1 \\ x \\ y \\ xy \\ y^2 \\ xy^2 \end{array} \\ \begin{array}{cccccc} 1 & x & y & xy & y^2 & xy^2 \end{array} & \end{array}$$

Characteristic polynomial:

$\chi_x = T^6 - p^{-5} T^2$

Multiplication matrices and slope factorization

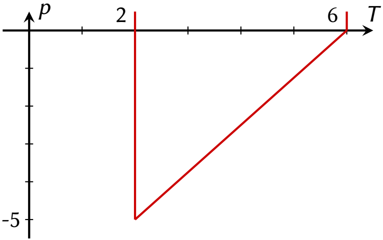
- Problem: how to detect this phenomenon in general?

Consider the multiplication matrix by x:

$$T_x = \begin{array}{cc} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & p^{-1} & 0 & p^{-2} & 0 & p^{-3} \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} 1 \\ x \\ y \\ xy \\ y^2 \\ xy^2 \end{matrix} \\ \begin{matrix} 1 & x & y & xy & y^2 & xy^2 \end{matrix} & \end{array}$$

Characteristic polynomial:

$\chi_x = T^6 - p^{-5}T^2$



Multiplication matrices and slope factorization

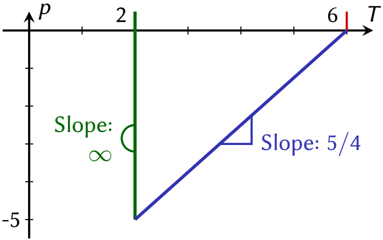
- Problem: how to detect this phenomenon in general?

Consider the multiplication matrix by x:

$$T_x = \begin{array}{c} \left(\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & p^{-1} & 0 & p^{-2} & 0 & p^{-3} \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \begin{array}{c} 1 \\ x \\ y \\ xy \\ y^2 \\ xy^2 \end{array} \\ \begin{array}{cccccc} 1 & x & y & xy & y^2 & xy^2 \end{array} \end{array}$$

Characteristic polynomial:

$$\chi_x = T^6 - p^{-5}T^2$$
$$= T^2 \cdot (T^4 - p^{-5})$$



Multiplication matrices and slope factorization

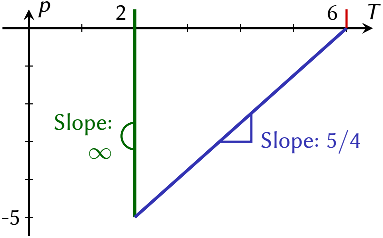
- Problem: how to detect this phenomenon in general?

Consider the multiplication matrix by x:

$$T_x = \begin{array}{cc} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & p^{-1} & 0 & p^{-2} & 0 & p^{-3} \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{array}{c} 1 \\ x \\ y \\ xy \\ y^2 \\ xy^2 \end{array} \\ \begin{array}{cccccc} 1 & x & y & xy & y^2 & xy^2 \end{array} & \end{array}$$

Characteristic polynomial:

$$\begin{aligned} \chi_x &= T^6 - p^{-5} T^2 \\ &= T^2 \cdot (T^4 - p^{-5}) \end{aligned}$$



Slope factorization:

- $\ker(T_x^4 - p^{-5})$: characteristic space with "eigenvalue" with valuation $-5/4 < 0$
  $\rightarrow$ vectors sent to 0
- $\ker(T_x^2)$: characteristic space with "eigenvalue" with valuation $\infty \geq 0$
  $\rightarrow$ vectors in the staircase

Construction

- Inclusion $K\{\mathbf{X};\mathbf{r}\} \to K\{\mathbf{X};\mathbf{u}\} \rightsquigarrow$ map $\Phi : V = K\{\mathbf{X};\mathbf{r}\}/I \to K\{\mathbf{X};\mathbf{u}\}/(I\,K\{\mathbf{X};\mathbf{u}\})$
- Φ is surjective but not injective
- Vectors sent to 0:

$$N = \bigcap \text{“Eigenspace” of } T_i \text{ with valuation} < u_i$$

Characterization and construction of the new staircase

Construction

- Inclusion $K\{\mathbf{X};\mathbf{r}\} \to K\{\mathbf{X};\mathbf{u}\} \rightsquigarrow$ map $\Phi : V = K\{\mathbf{X};\mathbf{r}\}/I \to K\{\mathbf{X};\mathbf{u}\}/(I\,K\{\mathbf{X};\mathbf{u}\})$
- Φ is surjective but not injective
- Vectors sent to 0:

$$N = \bigcap \text{“Eigenspace” of } T_i \text{ with valuation} < u_i$$

- New quotient:

$$K\{\mathbf{X};\mathbf{u}\}/(I+N) = \sum \text{“Eigenspace” of } T_i \text{ with valuation} \geq u_i$$

- Or simply compute a monomial basis of the quotient
- This linear algebra encodes a topological construction

Full FGLM algorithm for Tate algebras

In: G_1 a reduced Gröbner basis in $K\{\mathbf{X};\mathbf{r}\}$ wrt an order $<_1$
$<_2$ a monomial order
$\mathbf{u} \leq \mathbf{r}$ a system of log-radii

Out: G_2 a reduced Gröbner basis wrt $<_2$ in $K\{\mathbf{X};\mathbf{u}\}$

1. Compute the matrices of multiplication by $X_1, \ldots, X_n$ in the basis $B_{1,\mathbf{r}}$
2. Convert them into matrices of multiplication by $X_1, \ldots, X_n$ in the basis $B_{1,\mathbf{u}}$ (slope factorization)
3. Convert into the basis G_2
   - 3.1 Use the usual algorithm modulo π (in $\mathbb{F}$) to compute $B_{2,\mathbf{u}}$ and $\overline{G_2}$
   - 3.2 Lift the linear algebra operations to obtain G_2

Full FGLM algorithm for Tate algebras

In: G_1 a reduced Gröbner basis in $K\{\mathbf{X};\mathbf{r}\}$ wrt an order $<_1$
$<_2$ a monomial order
$\mathbf{u} \leq \mathbf{r}$ a system of log-radii

Out: G_2 a reduced Gröbner basis wrt $<_2$ in $K\{\mathbf{X};\mathbf{u}\}$

1. Compute the matrices of multiplication by $X_1, \ldots, X_n$ in the basis $B_{1,\mathbf{r}}$
2. Convert them into matrices of multiplication by $X_1, \ldots, X_n$ in the basis $B_{1,\mathbf{u}}$ (slope factorization)
3. Convert into the basis G_2
   3.1 Use the usual algorithm modulo π (in $\mathbb{F}$) to compute $B_{2,\mathbf{u}}$ and $\overline{G_2}$
   3.2 Lift the linear algebra operations to obtain G_2

Complexity

- Step 1 has base complexity $\tilde{O}(n\delta^3 \mathrm{prec})$
- Each other step has arithmetic complexity $\tilde{O}(n\delta^3)$
- Final base complexity: $\tilde{O}(n\delta^3 \mathrm{prec})$

Conclusion and future work

Summary

- Definition and computation of Gröbner bases for Tate ideals
- Standard algorithms (Buchberger, F4) and with signatures
- FGLM algorithm: for 0-dim ideals $\to$ interreduction and change of convergence radii

Conclusion and future work

Summary

- Definition and computation of Gröbner bases for Tate ideals
- Standard algorithms (Buchberger, F4) and with signatures
- FGLM algorithm: for 0-dim ideals $\rightarrow$ interreduction and change of convergence radii

Future work

- Integrate FGLM in the `tate_algebra` package of SageMath
- Generalizations of the interreduction in the middle of GB calculations
- Improve the complexity of reduction in positive dimension

Conclusion and future work

Summary

- Definition and computation of Gröbner bases for Tate ideals
- Standard algorithms (Buchberger, F4) and with signatures
- FGLM algorithm: for 0-dim ideals $\rightarrow$ interreduction and change of convergence radii

Future work

- Integrate FGLM in the `tate_algebra` package of SageMath
- Generalizations of the interreduction in the middle of GB calculations
- Improve the complexity of reduction in positive dimension

Thank you for your attention!

References

- *Gröbner bases over Tate algebras*, ISSAC 2019
- *Signature-based algorithms for Gröbner bases over Tate algebras*, ISSAC 2020
- *On FGLM algorithms with Tate algebras*, preprint 2021