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

Colloquium “Algorithmic Algebra”, 27 May 2020

Géométrie Algébrique, Géométrie Analytique

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

Géométrie Algébrique, Géométrie Analytique ... over *p*-adics?

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

Rigid geometry and Tate series

$$\begin{tikzcd}[row sep=huge]
\text{Analytic geometry} \arrow[r, dash] \arrow[d, shift right] & \text{Analytic series} \\
\text{Algebraic geometry} \arrow[r, dash] \arrow[u, shift right, "\text{GAGA (over } \mathbb{C})"'] \arrow[d, shift right] & \text{Polynomials} \\
\text{Rigid geometry} \arrow[r, dash] \arrow[u, shift right, "\text{Non archimedean case: } \mathbb{Q}_p"'] & \text{Tate series}
\end{tikzcd}$$

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

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

Needed for algorithmic rigid geometry:

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

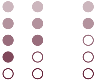
Valued fields and rings: summary of basic definitions

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

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

0

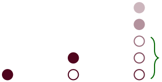
- $\mathrm{val}(ab) = \mathrm{val}(a) + \mathrm{val}(b)$



$a \cdot b = ab$

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

$a + b = a + b \qquad a + b = a + b$



Examples: $1 \qquad \pi \qquad a = a_3\pi^3 + a_4\pi^4 + \dots$ $\quad \mathrm{val}(a) = 3$

$b = b_{-3}\pi^{-3} + b_{-2}\pi^{-2} + \dots$ $\quad \mathrm{val}(b) = -3$

Examples of valued fields and rings

Ring K° $\underset{\text{val} \geq 0}{\overset{\text{Frac}}{\rightleftarrows}}$	Field K	Uniformizer π	Residue field K°/π	Complete
$\mathbb{Z}_{(p)}$	$\mathbb{Q}$	p prime	$\mathbb{F}_p$	×
$\mathbb{Z}_p$	$\mathbb{Q}_p$	p prime	$\mathbb{F}_p$	✓
$\mathbb{C}[x]_{(x-\alpha)}$	$\mathbb{C}(x)$	$x - \alpha$	$\mathbb{C}$	×
$\mathbb{C}[[x-\alpha]]$	$\mathbb{C}((x-\alpha))$	$x - \alpha$	$\mathbb{C}$	✓

- Metric and topology defined by "a is small" $\iff$ "val(a) is large"
- Complete rings and fields: $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{C}[[x-\alpha]]$, $\mathbb{C}((x-\alpha))$
- In a complete valuation ring,
  a series is convergent
  iff its general term goes to 0:

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

Examples of valued fields and rings

Ring K° $\underset{\mathrm{val} \geq 0}{\overset{\mathrm{Frac}}{\rightleftarrows}}$	Field K	Uniformizer π	Residue field K°/π	Complete
$\mathbb{Z}_{(p)}$	$\mathbb{Q}$	p prime	$\mathbb{F}_p$	×
$\mathbb{Z}_p$	$\mathbb{Q}_p$	p prime	$\mathbb{F}_p$	✓
$\mathbb{C}[x]_{(x-\alpha)}$	$\mathbb{C}(x)$	$x - \alpha$	$\mathbb{C}$	×
$\mathbb{C}[[x-\alpha]]$	$\mathbb{C}((x-\alpha))$	$x - \alpha$	$\mathbb{C}$	✓

- Metric and topology defined by "a is small" $\iff$ "$\mathrm{val}(a)$ is large"
- Complete rings and fields: $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{C}[[x-\alpha]]$, $\mathbb{C}((x-\alpha))$
- In a complete valuation ring,
  a series is convergent
  iff its general term goes to 0:

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

Examples of valued fields and rings

Ring K° $\underset{\mathrm{val} \geq 0}{\overset{\mathrm{Frac}}{\rightleftarrows}}$	Field K	Uniformizer π	Residue field K°/π	Complete
$\mathbb{Z}_{(p)}$	$\mathbb{Q}$	p prime	$\mathbb{F}_p$	×
$\mathbb{Z}_p$	$\mathbb{Q}_p$	p prime	$\mathbb{F}_p$	✓
$\mathbb{C}[x]_{(x-\alpha)}$	$\mathbb{C}(x)$	$x-\alpha$	$\mathbb{C}$	×
$\mathbb{C}[[x-\alpha]]$	$\mathbb{C}((x-\alpha))$	$x-\alpha$	$\mathbb{C}$	✓

- Metric and topology defined by “a is small” $\iff$ “$\mathrm{val}(a)$ is large”
- Complete rings and fields: $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{C}[[x-\alpha]]$, $\mathbb{C}((x-\alpha))$
- In a complete valuation ring,
  a series is convergent
  iff its general term goes to 0:

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

Examples of valued fields and rings

Ring K° $\underset{\mathrm{val} \geq 0}{\overset{\mathrm{Frac}}{\rightleftarrows}}$	Field K	Uniformizer π	Residue field K°/π	Complete
$\mathbb{Z}_{(p)}$	$\mathbb{Q}$	p prime	$\mathbb{F}_p$	×
$\mathbb{Z}_p$	$\mathbb{Q}_p$	p prime	$\mathbb{F}_p$	✓
$\mathbb{C}[x]_{(x-\alpha)}$	$\mathbb{C}(x)$	$x-\alpha$	$\mathbb{C}$	×
$\mathbb{C}[[x-\alpha]]$	$\mathbb{C}((x-\alpha))$	$x-\alpha$	$\mathbb{C}$	✓

- Metric and topology defined by "a is small" $\iff$ "val(a) is large"
- Complete rings and fields: $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{C}[[x-\alpha]]$, $\mathbb{C}((x-\alpha))$
- In a complete valuation ring,
  a series is convergent
  iff its general term goes to 0:

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

Examples of valued fields and rings

Ring K° $\underset{\text{val} \geq 0}{\overset{\text{Frac}}{\rightleftarrows}}$	Field K	Uniformizer π	Residue field K°/π	Complete
$\mathbb{Z}_{(p)}$	$\mathbb{Q}$	p prime	$\mathbb{F}_p$	×
$\mathbb{Z}_p$	$\mathbb{Q}_p$	p prime	$\mathbb{F}_p$	✓
$\mathbb{C}[x]_{(x-\alpha)}$	$\mathbb{C}(x)$	$x-\alpha$	$\mathbb{C}$	×
$\mathbb{C}[[x-\alpha]]$	$\mathbb{C}((x-\alpha))$	$x-\alpha$	$\mathbb{C}$	✓

- Metric and topology defined by "a is small" $\iff$ "val(a) is large"
- Complete rings and fields: $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{C}[[x-\alpha]]$, $\mathbb{C}((x-\alpha))$
- In a complete valuation ring, a series is convergent iff its general term goes to 0:

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

Examples of valued fields and rings

Ring $K^\circ \underset{\text{val} \geq 0}{\overset{\text{Frac}}{\rightleftarrows}}$ Field K		Uniformizer π	Residue field K°/π	Complete
$\mathbb{Z}_{(p)}$	$\mathbb{Q}$	p prime	$\mathbb{F}_p$	×
$\mathbb{Z}_p$	$\mathbb{Q}_p$	p prime	$\mathbb{F}_p$	✓
$\mathbb{C}[x]_{(x-\alpha)}$	$\mathbb{C}(x)$	$x-\alpha$	$\mathbb{C}$	×
$\mathbb{C}[[x-\alpha]]$	$\mathbb{C}((x-\alpha))$	$x-\alpha$	$\mathbb{C}$	✓

- Metric and topology defined by "a is small" $\iff$ "val(a) is large"
- Complete rings and fields: $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{C}[[x-\alpha]]$, $\mathbb{C}((x-\alpha))$
- 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 $\iff$ $F \in \mathbb{C}[\mathbf{X}][[Y]]$

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 valued 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 valued 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

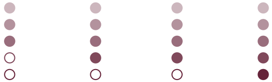
$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

- Starting from a usual monomial ordering $1 <_m \mathbf{X}^{\mathbf{i}_1} <_m \mathbf{X}^{\mathbf{i}_2} <_m \ldots$
- 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:



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

Term ordering for Tate algebras

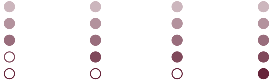
$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

- 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:

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

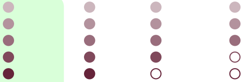
Term ordering for Tate series:



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

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

$\mathrm{LT}(f)$



$$f = \boxed{a_2 XY} + a_1 X + a_0 \cdot 1 + a_3 X^2 Y^2 + \dots$$

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

$$f = \underbrace{\boxed{a_2 XY + a_1 X}}_{}^{\mathrm{LT}(f)\text{ on } a_2XY} + a_0 \cdot 1 + a_3 X^2 Y^2 + \ldots$$

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

- Isomorphism

$$\begin{array}{ccc} K\{\mathbf{X}\}^\circ / \langle \pi \rangle & \simeq & \mathbb{F}[\mathbf{X}] \\ f & \mapsto & \bar{f} \end{array}$$

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 $\quad$ $\exists$ 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 $\quad$ $\exists$ sequence of reductions converging to 0

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

  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 $\quad$ $\exists$ sequence of reductions converging to 0

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

  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

Buchberger's algorithm

$G \leftarrow \{f_1, \ldots, f_m\}$
$B \leftarrow \{$S-pol of g_1 and g_2 for $g_1, g_2 \in G\}$
While $B \neq \varnothing$:
  Pop v from B
  $w \leftarrow$ reduction of v modulo G
  If $w = 0$:
    Pass
  Else:
    $B \leftarrow B \cup \{$S-pol of w and g for $g \in G\}$
    $G \leftarrow G \cup \{w\}$
Return G

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°

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

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

What about valued fields?

- Recall: K = fraction field of K°

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

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

- 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°

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

$$\text{val}(a) = -3$$

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

$$\pi^{-2} + \pi^{-1}X + 1X^2 + \pi^2 X^3 + \cdots$$

- Another surprising equivalence
  1. G is a normalized GB of I
  2. $G \subset K\{\mathbf{X}\}^\circ$ is a GB of $I \cap K\{\mathbf{X}\}^\circ$

$\forall g \in G$, $\mathrm{LC}(g) = 1$ (in part., $G \subset K\{\mathbf{X}\}^\circ$)

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

Why signatures?

Problem: useless and redundant computations, infinite reductions to 0

Example with a S-polynomial

$p = p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + p_m f_m$ $\qquad$ $q = q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + q_m f_m$

$\text{S-Pol}(p, q) = \mu p - \nu q$

Why signatures?

Problem: useless and redundant computations, infinite reductions to 0

- 1st idea: keep track of the representation of the ideal elements [Möller, Mora, Traverso 1992]

Example with a S-polynomial

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + p_m f_m \qquad q = q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + q_m f_m$$

$$\mathbf{p} = p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_k \mathbf{e}_k + \cdots + p_m \mathbf{e}_m \qquad \mathbf{q} = q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_l \mathbf{e}_l + \cdots + q_m \mathbf{e}_m$$

$$\text{S-Pol}(p, q) = \mu p - \nu q$$

$$\text{S-Pol}(\mathbf{p}, \mathbf{q}) = \mu \left(p_1 \mathbf{e}_1 + \cdots + p_k \mathbf{e}_k + \cdots + p_m \mathbf{e}_m \right) - \nu \left(q_1 \mathbf{e}_1 + \cdots + q_l \mathbf{e}_l + \cdots + q_m \mathbf{e}_m \right)$$

Why signatures?

Problem: useless and redundant computations, infinite reductions to 0

- 1^{st} idea: keep track of the representation of the ideal elements
  [Möller, Mora, Traverso 1992]
- 2^{nd} idea: the largest term of the representation is enough
  [Faugère 2002 ; Gao, Volny, Wang 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

Example with a S-polynomial

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + 0\, f_m$$
$$\mathbf{p} = p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m$$
$$= \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms}$$

$$q = q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + 0\, f_m$$
$$\mathbf{q} = q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m$$
$$= \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms}$$

$$\text{S-Pol}(p, q) = \mu p - \nu q$$
$$\text{S-Pol}(\mathbf{p}, \mathbf{q}) = \mu\,(p_1 \mathbf{e}_1 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m) - \nu\,(q_1 \mathbf{e}_1 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m)$$
$$= \mu \mathrm{LT}(p_k)\mathbf{e}_k - \nu \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms}$$

Why signatures?

Problem: useless and redundant computations, infinite reductions to 0

- 1^{st} idea: keep track of the representation of the ideal elements
  [Möller, Mora, Traverso 1992]
- 2^{nd} idea: the largest term of the representation is enough
  [Faugère 2002 ; Gao, Volny, Wang 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

Example with a S-polynomial

$$
\begin{aligned}
p &= p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + 0\, f_m \\
\mathbf{p} &= p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m \\
&= \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms}
\end{aligned}
$$

$$
\begin{aligned}
q &= q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + 0\, f_m \\
\mathbf{q} &= q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m \\
&= \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms}
\end{aligned}
$$

$$\text{S-Pol}(p, q) = \mu p - \nu q$$

$$
\begin{aligned}
\text{S-Pol}(\mathbf{p}, \mathbf{q}) &= \mu \left(p_1 \mathbf{e}_1 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m\right) - \nu \left(q_1 \mathbf{e}_1 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m\right) \\
&= \mu \mathrm{LT}(p_k)\mathbf{e}_k - \nu \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms} \\
&= \mu \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms} \quad \text{if } \mu \mathrm{LT}(p_k)\mathbf{e}_k \gneqq \nu \mathrm{LT}(q_l)\mathbf{e}_l
\end{aligned}
$$

Why signatures?

Problem: useless and redundant computations, infinite reductions to 0

- 1st idea: keep track of the representation of the ideal elements
  [Möller, Mora, Traverso 1992]
- 2nd idea: the largest term of the representation is enough
  [Faugère 2002 ; Gao, Volny, Wang 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

Example with a S-polynomial

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + 0\, f_m \qquad q = q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + 0\, f_m$$

$$\mathbf{p} = p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m \qquad \mathbf{q} = q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m$$

$$= \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms} \qquad = \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms}$$

$\mathfrak{s}(p) =$ signature of p

$$\text{S-Pol}(p, q) = \mu p - \nu q$$

$$\begin{aligned}
\text{S-Pol}(\mathbf{p}, \mathbf{q}) &= \mu\,(p_1 \mathbf{e}_1 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m) - \nu\,(q_1 \mathbf{e}_1 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m) \\
&= \mu \mathrm{LT}(p_k)\mathbf{e}_k - \nu \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms} \\
&= \mu \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms} \quad \text{if } \mu \mathrm{LT}(p_k)\mathbf{e}_k \gneq \nu \mathrm{LT}(q_l)\mathbf{e}_l
\end{aligned}$$

Regular S-polynomial

Buchberger's algorithm, with signatures

1. $G \leftarrow \{(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)\}$
2. $B \leftarrow \{$S-pol of p_1 and p_2 for $p_1, p_2 \in G\}$
3. While $B \neq \varnothing$:
4. Pop $(\mathbf{u}, v)$ from B with smallest $\mathbf{u}$
5. $w \leftarrow$ regular reduction of $(\mathbf{u}, v)$ modulo G
6. If $w = 0$:
7. Pass
8. Else:
9. $B \leftarrow B \cup \{$regular S-pol of $(\mathbf{u}, w)$ and p for $p \in G\}$
10. $G \leftarrow G \cup \{(\mathbf{u}, w)\}$
11. Return G

Buchberger's algorithm, with signatures

- $G \leftarrow \{(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)\}$
- $B \leftarrow \{$S-pol of p_1 and p_2 for $p_1, p_2 \in G\}$
- While $B \neq \varnothing$:
  - Pop $(\mathbf{u}, v)$ from B with smallest $\mathbf{u}$
  - $w \leftarrow$ regular reduction of $(\mathbf{u}, v)$ modulo G
  - If $w = 0$:
    - Pass
  - Else:
    - $B \leftarrow B \cup \{$regular S-pol of $(\mathbf{u}, w)$ and p for $p \in G\}$
    - $G \leftarrow G \cup \{(\mathbf{u}, w)\}$
- Return G

Buchberger's algorithm, with signatures

1. $G \leftarrow \{(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)\}$
2. $B \leftarrow \{$S-pol of p_1 and p_2 for $p_1, p_2 \in G\}$
3. While $B \neq \varnothing$:
4.   Pop $(\mathbf{u}, v)$ from B with smallest $\mathbf{u}$ Need to order the signatures!
5. $w \leftarrow$ regular reduction of $(\mathbf{u}, v)$ modulo G
6.   If $w = 0$:
7.   Pass
8.   Else:
9. $B \leftarrow B \cup \{$regular S-pol of $(\mathbf{u}, w)$ and p for $p \in G\}$
10. $G \leftarrow G \cup \{(\mathbf{u}, w)\}$
11. Return G

Signature orderings

Signature orderings:

- Necessary for correctness and termination of the algorithms
- Different choices lead to different performances

Examples (polynomial case):

- $\mu\mathbf{e}_i <_{\mathrm{PoTe}} \nu\mathbf{e}_j \iff i < j$, or if equal, $\mu < \nu$

  Position over Term

- $\mu\mathbf{e}_i <_{\mathrm{ToP}} \nu\mathbf{e}_j \iff \mu < \nu$, or if equal, $i < j$

  Term over Position

- $\mu\mathbf{e}_i <_{\mathrm{DePoTe}} \nu\mathbf{e}_j \iff \deg(p) < \deg(q)$, or if equal, $i < j$, or if equal, $\mu < \nu$

  Degree over Position over Term

Signature orderings

Signature orderings:

- Necessary for correctness and termination of the algorithms
- Different choices lead to different performances

Examples (polynomial case):

- $\mu \mathbf{e}_i <_{\text{PoTe}} \nu \mathbf{e}_j \iff i < j$, or if equal, $\mu < \nu$

  Position over Term

  - Incremental
  - Fails to optimize globally

- $\mu \mathbf{e}_i <_{\text{ToP}} \nu \mathbf{e}_j \iff \mu < \nu$, or if equal, $i < j$

  Term over Position

  - Non incremental
  - More efficient by using all polynomials at once

- $\mu \mathbf{e}_i <_{\text{DePoTe}} \nu \mathbf{e}_j \iff \deg(p) < \deg(q)$, or if equal, $i < j$, or if equal, $\mu < \nu$

  Degree over Position over Term

  - “F5-ordering” for homogeneous systems and degree order
  - Avoids too high-degree calculations, still incremental
  - Best of both worlds

$Q \leftarrow (f_1, \ldots, f_m)$
$G \leftarrow \varnothing$
For $f \in Q$
  $G \leftarrow G \cup \{f\}$
  $B \leftarrow \{\text{S-pol of } f \text{ and } g \text{ for } g \in G\}$
  While $B \neq \varnothing$:
    Pop v from B
    $w \leftarrow$ reduction of v modulo G
    If $w = 0$:
      Pass
    Else:
      $B \leftarrow B \cup \{\text{S-pol of } w \text{ and } g \text{ for } g \in G\}$
      $G \leftarrow G \cup \{w\}$
Return G

Signature orderings for Tate series

Signature orderings:

- Necessary for correctness and termination of the algorithms
- Different choices lead to different performances

Orders for Tate series:

- $\mu \mathbf{e}_i <_{\text{PoTe}} \nu \mathbf{e}_j \iff i < j$, or if equal, $\mu < \nu$
  Position over Term
  - Incremental
  - Fails to optimize globally

- $\mu \mathbf{e}_i <_{\text{ToP}} \nu \mathbf{e}_j \iff \mu < \nu$, or if equal, $i < j$
  Term over Position
  - Non incremental
  - More efficient by using all polynomials at once

Signature-based algorithm, PoT ordering

- $Q \leftarrow (f_1, \ldots, f_m)$
- $G \leftarrow \varnothing$
- For $f \in Q$
  - $G_S \leftarrow \{(0, g) : g \in G_S\} \cup \{(1, f)\}$
  - $B \leftarrow \{$S-pol of $(1, f)$ and p for $p \in G_S\}$
  - While $B \neq \varnothing$:
    - Pop (u, v) from B with smallest u
    - $w \leftarrow$ regular reduction of (u, v) modulo G_S
    - If $w = 0$:
      - Pass
    - Else:
      - $B \leftarrow B \cup \{$regular S-pol of (u, w) and p for $p \in G_S\}$
      - $G_S \leftarrow G_S \cup \{(u, w)\}$
  - $G \leftarrow \{v : (u, v) \in G_S\}$
- Return G

Signature-based algorithm, PoT ordering

$Q \leftarrow (f_1, \ldots, f_m)$
$G \leftarrow \varnothing$
For $f \in Q$
    $G_S \leftarrow \{(0, g) : g \in G_S\} \cup \{(1, f)\}$ Incremental order: only the last coefficient matters
    $B \leftarrow \{$S-pol of $(1, f)$ and p for $p \in G_S\}$
    While $B \neq \varnothing$:
        Pop (u, v) from B with smallest u
        $w \leftarrow$ regular reduction of (u, v) modulo G_S
        If $w = 0$:
            Pass
        Else:
            $B \leftarrow B \cup \{$regular S-pol of (u, w) and p for $p \in G_S\}$
            $G_S \leftarrow G_S \cup \{(u, w)\}$
    $G \leftarrow \{v : (u, v) \in G_S\}$ Throwing away the signatures
Return G

Signature orderings for Tate series

Signature orderings:

- Necessary for correctness and termination of the algorithms
- Different choices lead to different performances

Orders for Tate series:

- $\mu \mathbf{e}_i <_{\mathrm{PoTe}} \nu \mathbf{e}_j \iff i < j$, or if equal, $\mu < \nu$

  Position over Term

  - Incremental
  - Fails to optimize globally

- $\mu \mathbf{e}_i <_{\mathrm{ToP}} \nu \mathbf{e}_j \iff \mu < \nu$, or if equal, $i < j$

  Term over Position

  - Non incremental
  - More efficient by using all polynomials at once

- $\mu \mathbf{e}_i <_{\mathrm{VaPoTe}} \nu \mathbf{e}_j \iff \mathrm{val}(p) < \mathrm{val}(q)$, or if equal, $i < j$, or if equal, $\mu < \nu$

  Valuation over Position over Term

  - Analogue of the F5 ordering for the valuation
  - Allows to delay (or avoid) high valuation computations

Signature-based algorithm, VoPoT ordering

$Q \leftarrow (f_1, \ldots, f_m)$

$G \leftarrow \varnothing$

While $\exists f \in Q$ with smallest valuation:

    $G_S \leftarrow \{(0, g) : g \in G_S\} \cup \{(1, f)\}$

    $B \leftarrow \{$S-pol of $(1, f)$ and p for $p \in G_S\}$

    While $B \neq \varnothing$:

        Pop (u, v) from B with smallest u

        $w \leftarrow$ regular reduction of (u, v) modulo G_S

        If $\mathrm{val}(w) > \mathrm{val}(f)$:

            $Q \leftarrow Q \cup \{w\}$

        Else:

            $B \leftarrow B \cup \{$regular S-pol of (u, w) and p for $p \in G_S\}$

            $G_S \leftarrow G_S \cup \{(u, w)\}$

    $G \leftarrow \{v : (u, v) \in G_S\}$

Return G

Signature-based algorithm, VoPoT ordering

$Q \leftarrow (f_1, \dots, f_m)$
$G \leftarrow \varnothing$
While $\exists f \in Q$ with smallest valuation:
    $G_S \leftarrow \{(0, g) : g \in G_S\} \cup \{(1, f)\}$
    $B \leftarrow \{$S-pol of $(1, f)$ and p for $p \in G_S\}$
    While $B \neq \varnothing$:
        Pop (u, v) from B with smallest u
        $w \leftarrow$ regular reduction of (u, v) modulo G_S
        If $\mathrm{val}(w) > \mathrm{val}(f)$:
            $Q \leftarrow Q \cup \{w\}$
        Else:
            $B \leftarrow B \cup \{$regular S-pol of (u, w) and p for $p \in G_S\}$
            $G_S \leftarrow G_S \cup \{(u, w)\}$
    $G \leftarrow \{v : (u, v) \in G_S\}$
Return G

Order by valuation first
then incremental

Conclusion and perspectives

What we presented here

- Tate series = formal power series appearing in algebraic geometry
- Definitions of Gröbner bases for Tate series
- Algorithms for computing those Gröbner bases (also with signatures)
- Data structure and algorithms implemented in Sage

Conclusion and perspectives

What we presented here

- Tate series = formal power series appearing in algebraic geometry
- Definitions of Gröbner bases for Tate series
- Algorithms for computing those Gröbner bases (also with signatures)
- Data structure and algorithms implemented in Sage

Extensions

- Tate series with convergence radius different from 1 (integer or rational log)

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 $\mathrm{val}(a_{\mathbf{i}}) + \mathbf{r} \cdot \mathbf{i} \xrightarrow[|\mathbf{i}| \to \infty]{} +\infty$

- The term order is not the same!

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

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

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

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

- 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 $\mathbb{Q}^n$

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

Definition

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

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

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

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

Log-radii in $\mathbb{Q}^n$ are more complicated, but things still work.

convergent

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

Conclusion and perspectives

What we presented here

- Tate series = formal power series appearing in algebraic geometry
- Definitions of Gröbner bases for Tate series
- Algorithms for computing those Gröbner bases (also with signatures)
- Data structure and algorithms implemented in Sage

Extensions

- Tate series with convergence radius different from 1 (integer or rational log)

Perspectives

- Faster reduction: algorithms for local monomial orderings and standard bases (Mora)

Conclusion and perspectives

What we presented here

- Tate series = formal power series appearing in algebraic geometry
- Definitions of Gröbner bases for Tate series
- Algorithms for computing those Gröbner bases (also with signatures)
- Data structure and algorithms implemented in Sage

Extensions

- Tate series with convergence radius different from 1 (integer or rational log)

Perspectives

- Faster reduction: algorithms for local monomial orderings and standard bases (Mora)

Thank you for your attention!

More information and references:

- Xavier Caruso, Tristan Vaccon and Thibaut Verron (2019). 'Gröbner Bases Over Tate Algebras'. In: *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation - ISSAC '19*. DOI: 10.1145/3326229.3326257. URL: https://arxiv.org/abs/1901.09574
- Xavier Caruso, Tristan Vaccon and Thibaut Verron (Feb. 2020). 'Signature-based algorithms for Gröbner bases over Tate algebras'. In: URL: https://hal.archives-ouvertes.fr/hal-02473665 [preprint]