Signature Gröbner bases over 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

Seminar *Algebra and Discrete Mathematics*, ~~30 January 2020~~
~~12 March 2020~~
26 March 2020

Precision and Gröbner bases

- Question: in $\mathbb{R}[X]$, reduce $f = X^2$ modulo $g = 0.01X - 1$

Precision and Gröbner bases

- Question: in $\mathbb{R}[X]$, reduce $f = X^2$ modulo $g = \underbrace{0.01X}_{\mathrm{LT}(g)} - 1$

- The usual way:

$$f = X^2 \xrightarrow{-100Xg} 100X \xrightarrow{-10\,000g} 10\,000$$

- It terminates, but...

- $g \simeq 1$, but $f \bmod g \not\simeq 0$

Precision and Gröbner bases

- Question: in $\mathbb{R}[X]$, reduce $f = X^2$ modulo $g = \underbrace{0.0001X}_{\mathrm{LT}(g)} - 1$

- The usual way:

$$f = X^2 \xrightarrow{-10\,000Xg} 10\,000X \xrightarrow{-100\,000\,000g} 100\,000\,000$$

- It terminates, but...

- $g \simeq 1$, but $f \bmod g \not\simeq 0$

Precision and Gröbner bases

- Question: in $\mathbb{R}[X]$, reduce $f = X^2$ modulo $g = \underbrace{0.000\,001X}_{\mathrm{LT}(g)} - 1$

- The usual way:

$$f = X^2 \xrightarrow{-1\,000\,000Xg} 1\,000\,000X \xrightarrow{-1\,000\,000\,000\,000g} 1\,000\,000\,000\,000$$

- It terminates, but...

- $g \simeq 1$, but $f \bmod g \not\simeq 0$

Precision and Gröbner bases

- **Question:** in $\mathbb{R}[X]$, reduce $f = X^2$ modulo $g = 0.01X - \underbrace{1}_{\mathrm{LT}(g)}$

- The usual way:

$$f = X^2 \xrightarrow{-100Xg} 100X \xrightarrow{-10\,000g} 10\,000$$

- It terminates, but...
- $g \simeq 1$, but $f \bmod g \not\simeq 0$

- Another way?

$$f = X^2 \xrightarrow{+X^2 g} 0.01X^3 \xrightarrow{+0.01X^3 g} 0.0001X^4 \xrightarrow{\cdots} \cdots$$

- It does not terminate, but...
- The sequence of reductions tends to 0

- Question: in $\mathbb{R}[X]$, reduce $f = X^2$ modulo $g = 0.0001X - \underbrace{1}_{\mathrm{LT}(g)}$

- The usual way:

$$f = X^2 \xrightarrow{-10\,000Xg} 10\,000X \xrightarrow{-100\,000\,000g} 100\,000\,000$$

- It terminates, but...
- $g \simeq 1$, but $f \bmod g \not\simeq 0$

- Another way?

$$f = X^2 \xrightarrow{+X^2 g} 0.0001X^3 \xrightarrow{+0.0001X^3 g} 0.000\,000\,01X^4 \xrightarrow{\cdots} \cdots$$

- It does not terminate, but...
- The sequence of reductions tends to 0

Precision and Gröbner bases

- **Question:** in $\mathbb{R}[X]$, reduce $f = X^2$ modulo $g = 0.000\,001X - \underbrace{1}_{\mathrm{LT}(g)}$

- The usual way:

$$f = X^2 \xrightarrow{-1\,000\,000Xg} 1\,000\,000X \xrightarrow{-1\,000\,000\,000\,000g} 1\,000\,000\,000\,000$$

- It terminates, but...

- $g \simeq 1$, but $f \bmod g \not\simeq 0$

- Another way?

$$f = X^2 \xrightarrow{+X^2 g} 0.000\,001X^3 \xrightarrow{+0.000\,001X^3 g} 0.000\,000\,000\,001X^4 \xrightarrow{\cdots} \cdots$$

- It does not terminate, but...

- The sequence of reductions tends to 0

Precision and Gröbner bases

- Question: in $\mathbb{R}[X]$, reduce $f = X^2$ modulo $g = 0.000\,001X - 1$

- The usual way:

$$\begin{array}{l} f = X^2 \\ \quad\big\downarrow -1\,000\,000Xg \\ 1\,000\,000X \\ \quad\big\downarrow -1\,000\,000\,000\,000g \\ 1\,000\,000\,000\,000 \end{array}$$

- It terminates, but...
- $g \simeq 1$, but $f \bmod g \not\simeq 0$

- Another way?

$$\begin{array}{l} f = X^2 \\ \quad\big\downarrow +X^2g \\ 0.000\,001X^3 \\ \quad\big\downarrow +0.000\,001X^3g \\ 0.000\,000\,000\,001X^4 \\ \quad\big\downarrow \cdots \\ \cdots \end{array}$$

- It does not terminate, but...
- The sequence of reductions tends to 0

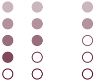
- This work: make sense of this process for convergent power series in $\mathbb{Z}_p[[X]]$

Valued fields and rings: basic definitions

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

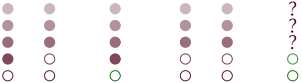
0

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



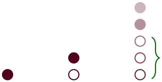
$a \cdot b = ab$

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



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

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



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

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

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	$\mathbb{F}_p$	✓
$\mathbb{C}[x]_{(x-\alpha)}$	$\mathbb{C}(x)$	$x - \alpha$	$\mathbb{C}$	×
$\mathbb{C}[[x-\alpha]]$	$\mathbb{C}((x-\alpha))$	$x - \alpha$	$\mathbb{C}$	✓

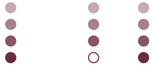
- Metric and topology defined by "a is small" $\iff$ "$\text{val}(a)$ is large"
- Complete rings and fields: $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{C}[[x-\alpha]]$, $\mathbb{C}((x-\alpha))$
- In a complete valuation ring, a series is convergent iff its general term goes to 0:

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

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" $\iff$ "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° $\underset{\text{val} \geq 0}{\overset{\text{Frac}}{\rightleftarrows}}$ 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" $\iff$ "$\mathrm{val}(a)$ 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" $\iff$ "$\mathrm{val}(a)$ 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:

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

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° $\underset{\mathrm{val} \geq 0}{\overset{\mathrm{Frac}}{\rightleftarrows}}$	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:

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

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

Motivation

- Introduced by Tate in 1971 for rigid geometry
  (p-adic equivalent of the bridge between algebraic and analytic geometry over $\mathbb{C}$)

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 $\iff$ $F \in \mathbb{C}[\mathbf{X}][[Y]]$

Term ordering for Tate algebras

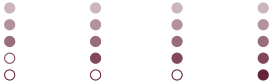
$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

- 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

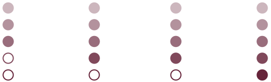
$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

- 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

$$f = \overbrace{a_2 XY}^{\mathrm{LT}(f)} + a_1 X + a_0 \cdot 1 + a_3 X^2 Y^2 + \ldots$$

Term ordering for Tate algebras

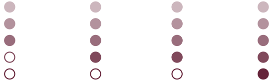
$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}$

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

Usual term ordering:

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

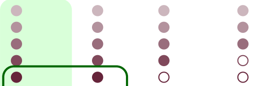
Term ordering for Tate series:



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

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

$\mathrm{LT}(f)$



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

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

- Isomorphism

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

compatible with the term order

Gröbner bases

- 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

- 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 $\mathbb{F}[\mathbf{X}]$

Gröbner bases

- 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 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

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°

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

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

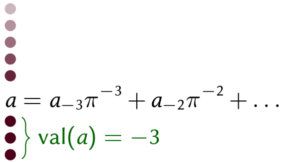
What about valued fields?

- Recall: K = fraction field of K°

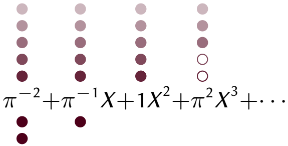
  $\mathbb{Q}_p$ — $\mathbb{Z}_p$

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

- 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°



- 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
  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

- 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

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

$$\begin{aligned}\mathbf{p} &= p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m \\ &= \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms}\end{aligned} \qquad \begin{aligned}\mathbf{q} &= q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m \\ &= \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms}\end{aligned}$$

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

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

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

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

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

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

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

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

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

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):

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

  Position over Term

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

  Term over Position

- $\mu \mathbf{e}_i <_{\text{dopot}} \nu \mathbf{e}_j \iff \deg(p) < \deg(q)$, 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):

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

  Position over Term

  - Theoretically convenient
  - Incremental
  - Rarely the most efficient

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

  Term over Position

  - Better in practice
  - Theoretically complicated

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

  Degree over Position over Term

  - "F5-ordering" for homogeneous systems and degree order
  - Avoid going too high in degree, still incremental
  - Best of both worlds

Buchberger's algorithm, incremental variant

```
Q ← (f_1, ..., f_m)
G ← ∅
For f ∈ Q
    G ← G ∪ {f}
    B ← {S-pol of f and g for g ∈ G}
    While B ≠ ∅:
        Pop v from B
        w ← reduction of v modulo G
        If w = 0:
            Pass
        Else:
            B ← B ∪ {S-pol of w and g for g ∈ G}
            G ← G ∪ {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:

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

  Position over Term

  - Theoretically convenient
  - Incremental
  - Rarely the most efficient

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

  Term over Position

  - Better in practice
  - Theoretically complicated

Signature-based algorithm, PoT ordering

1. $Q \leftarrow (f_1, \ldots, f_m)$
2. $G \leftarrow \varnothing$
3. For $f \in Q$
4. $G_S \leftarrow \{(0, g) : g \in G_S\} \cup \{1, f)\}$
5. $B \leftarrow \{$S-pol of $(1, f)$ and p for $p \in G_S\}$
6.   While $B \neq \varnothing$:
7.   Pop (u, v) from B with smallest u
8. $w \leftarrow$ regular reduction of (u, v) modulo G_S
9.   If $w = 0$:
10.   Pass
11.   Else:
12. $B \leftarrow B \cup \{$regular S-pol of (u, w) and p for $p \in G_S\}$
13. $G_S \leftarrow G_S \cup \{(u, w)\}$
14. $G \leftarrow \{v : (u, v) \in G_S\}$
15. 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:

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

  Position over Term

  - Theoretically convenient
  - Incremental
  - Rarely the most efficient

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

  Term over Position

  - Better in practice
  - Theoretically complicated

- $\mu\mathbf{e}_i <_{\text{vopot}} \nu\mathbf{e}_j \iff \mathrm{val}(p) < \mathrm{val}(q)$, 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

- $Q \leftarrow (f_1, \ldots, f_m)$
- $G \leftarrow \varnothing$
- 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

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

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 and using those Gröbner bases (also with signatures)
- Data structure and algorithms implemented in Sage (version 8.5, 22/12/2018)

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 and using those Gröbner bases (also with signatures)
- Data structure and algorithms implemented in Sage (version 8.5, 22/12/2018)

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: *ISSAC'19*, arXiv:1901.09574. arXiv: `1901.09574 [math.AG]`
- 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]