Signature-based Gröbner basis algorithms 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

Journées Nationales de Calcul Formel, 2 mars 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:

$$\begin{tikzcd} f = X^2 \arrow[d, bend right, "-100Xg"] \\ 100X \arrow[d, bend right, "-10\,000g"] \\ 10\,000 \end{tikzcd}$$

- 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:

$$\begin{tikzcd}
f = X^2 \arrow[d, bend right, "-10\,000Xg"] \\
10\,000X \arrow[d, bend right, "-100\,000\,000g"] \\
100\,000\,000
\end{tikzcd}$$

- 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

Precision and Gröbner bases

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

- The usual way:

$$
\begin{aligned}
& f = X^2 \\
& \quad \downarrow {\scriptstyle -10\,000Xg} \\
& 10\,000X \\
& \quad \downarrow {\scriptstyle -100\,000\,000g} \\
& 100\,000\,000
\end{aligned}
$$

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

- Another way?

$$
\begin{aligned}
& f = X^2 \\
& \quad \downarrow {\scriptstyle +X^2g} \\
& 0.0001X^3 \\
& \quad \downarrow {\scriptstyle +0.0001X^3g} \\
& 0.000\,000\,01X^4 \\
& \quad \downarrow {\scriptstyle \cdots} \\
& \cdots
\end{aligned}
$$

- 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?

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

- 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:

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

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

- Another way?

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

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

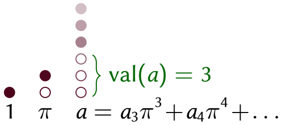
- This work: make sense of this process for convergent power series in $\mathbb{Z}_p[[X]]$

A recap on Complete Discrete Valuation Rings

- DVR = principal local domain K° with maximal ideal $\langle \pi \rangle$, residue field $\mathbb{F} = K^\circ / \langle \pi \rangle$

K°	π	$\mathbb{F}$
$\mathbb{Z}_p$	p	$\mathbb{F}_p$
$\mathbb{C}[[X]]$	X	$\mathbb{C}$

- Elements can be written $a = \sum_{n=0}^{\infty} a_n \pi^n$, $a_n \in \mathbb{F}$
- Valuation of a = max n such that π^n divides a
- Metric defined by "a is small $\iff$ val(a) is large"
- $\mathbb{Z}_p$ and $\mathbb{C}[[X]]$ are complete for this topology

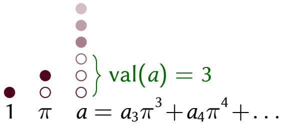


A recap on Complete Discrete Valuation Rings

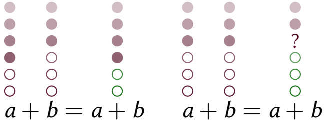
- DVR = principal local domain K° with maximal ideal $\langle\pi\rangle$, residue field $\mathbb{F} = K^\circ/\langle\pi\rangle$

K°	π	$\mathbb{F}$
$\mathbb{Z}_p$	p	$\mathbb{F}_p$
$\mathbb{C}[[X]]$	X	$\mathbb{C}$

- Elements can be written $a = \sum_{n=0}^{\infty} a_n \pi^n$, $a_n \in \mathbb{F}$
- Valuation of a = max n such that π^n divides a
- Metric defined by "a is small $\iff$ val(a) is large"
- $\mathbb{Z}_p$ and $\mathbb{C}[[X]]$ are complete for this topology



- No loss of precision possible:
  if a and b are small, $a + b$ is small

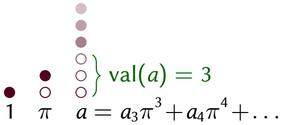


A recap on Complete Discrete Valuation Rings

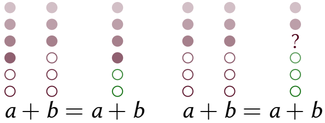
- DVR = principal local domain K° with maximal ideal $\langle\pi\rangle$, residue field $\mathbb{F} = K^\circ/\langle\pi\rangle$

K°	π	$\mathbb{F}$
$\mathbb{Z}_p$	p	$\mathbb{F}_p$
$\mathbb{C}[[X]]$	X	$\mathbb{C}$

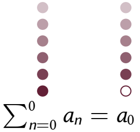
- Elements can be written $a = \sum_{n=0}^{\infty} a_n\pi^n$, $a_n \in \mathbb{F}$
- Valuation of a = max n such that π^n divides a
- Metric defined by "a is small $\iff$ val(a) is large"
- $\mathbb{Z}_p$ and $\mathbb{C}[[X]]$ are complete for this topology



- No loss of precision possible:
  if a and b are small, $a + b$ is small



- In a CDVR, a series is convergent
  iff its general term tends to 0

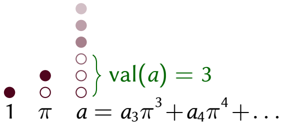


A recap on Complete Discrete Valuation Rings

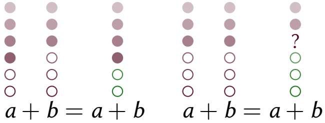
- DVR = principal local domain K° with maximal ideal $\langle \pi \rangle$, residue field $\mathbb{F} = K^\circ / \langle \pi \rangle$

K°	π	$\mathbb{F}$
$\mathbb{Z}_p$	p	$\mathbb{F}_p$
$\mathbb{C}[[X]]$	X	$\mathbb{C}$

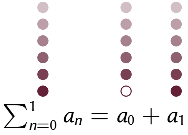
- Elements can be written $a = \sum_{n=0}^{\infty} a_n \pi^n$, $a_n \in \mathbb{F}$
- Valuation of a = max n such that π^n divides a
- Metric defined by "a is small $\iff$ val(a) is large"
- $\mathbb{Z}_p$ and $\mathbb{C}[[X]]$ are complete for this topology



- No loss of precision possible:
  if a and b are small, $a + b$ is small



- In a CDVR, a series is convergent
  iff its general term tends to 0

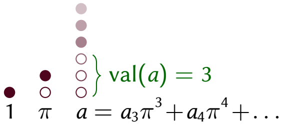


A recap on Complete Discrete Valuation Rings

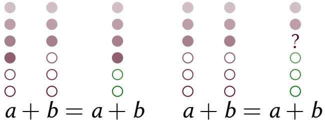
- DVR = principal local domain K° with maximal ideal $\langle \pi \rangle$, residue field $\mathbb{F} = K^\circ / \langle \pi \rangle$

K°	π	$\mathbb{F}$
$\mathbb{Z}_p$	p	$\mathbb{F}_p$
$\mathbb{C}[[X]]$	X	$\mathbb{C}$

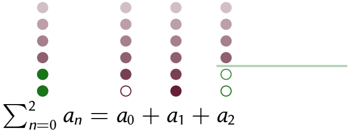
- Elements can be written $a = \sum_{n=0}^{\infty} a_n \pi^n$, $a_n \in \mathbb{F}$
- Valuation of a = max n such that π^n divides a
- Metric defined by "a is small $\iff$ val(a) is large"
- $\mathbb{Z}_p$ and $\mathbb{C}[[X]]$ are complete for this topology



- No loss of precision possible:
  if a and b are small, $a + b$ is small



- In a CDVR, a series is convergent
  iff its general term tends to 0

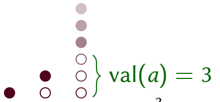


A recap on Complete Discrete Valuation Rings

- DVR = principal local domain K° with maximal ideal $\langle \pi \rangle$, residue field $\mathbb{F} = K^\circ / \langle \pi \rangle$

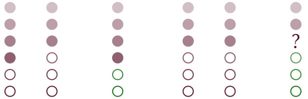
$\mathbb{Z}_p$	p	$\mathbb{F}_p$
$\mathbb{C}[[X]]$	X	$\mathbb{C}$

- Elements can be written $a = \sum_{n=0}^{\infty} a_n \pi^n$, $a_n \in \mathbb{F}$
- Valuation of a = max n such that π^n divides a
- Metric defined by "a is small $\iff$ val(a) is large"
- $\mathbb{Z}_p$ and $\mathbb{C}[[X]]$ are complete for this topology



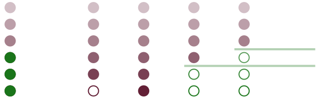
$1 \quad \pi \quad a = a_3\pi^3 + a_4\pi^4 + \dots$

- No loss of precision possible:
  if a and b are small, $a + b$ is small



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

- In a CDVR, a series is convergent
  iff its general term tends to 0



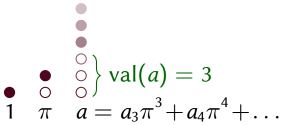
$\sum_{n=0}^{3} a_n = a_0 + a_1 + a_2 + a_3$

A recap on Complete Discrete Valuation Rings

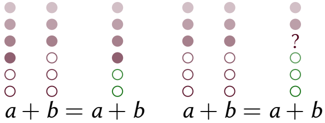
- DVR = principal local domain K° with maximal ideal $\langle \pi \rangle$, residue field $\mathbb{F} = K^\circ / \langle \pi \rangle$

$\mathbb{Z}_p$	p	$\mathbb{F}_p$
$\mathbb{C}[[X]]$	X	$\mathbb{C}$

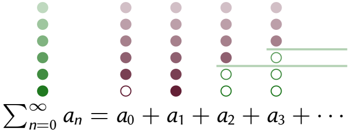
- Elements can be written $a = \sum_{n=0}^{\infty} a_n \pi^n$, $a_n \in \mathbb{F}$
- Valuation of a = max n such that π^n divides a
- Metric defined by "a is small $\iff$ val(a) is large"
- $\mathbb{Z}_p$ and $\mathbb{C}[[X]]$ are complete for this topology



- No loss of precision possible:
  if a and b are small, $a + b$ is small



- In a CDVR, a series is convergent iff its general term tends to 0



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

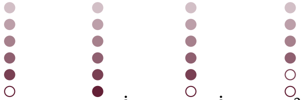
- Polynomials (finite sums are convergent)
- $\displaystyle\sum_{i,j=0}^{\infty} \pi^{i+j} X^i Y^j = 1 + \pi X + \pi Y + \pi^2 X^2 + \pi^2 XY + \pi^2 Y^2 + \cdots$
- Not a Tate series: $\displaystyle\sum_{i=0}^{\infty} X^i = 1 + 1X + 1X^2 + 1X^3 + \cdots$

Term ordering for Tate algebras

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

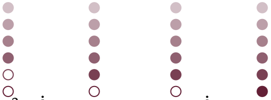
- Starting from a usual monomial ordering $1 <_m \mathbf{X}^{\mathbf{i}_1} <_m \mathbf{X}^{\mathbf{i}_2} <_m \dots$
- We define a term ordering putting more weight on large coefficients

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:



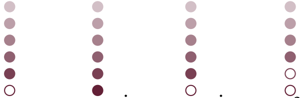
$$\cdots < \pi^2\,\mathbf{X}^{\mathbf{i}_3} < \underbrace{\pi\cdot 1 \; < \; \pi\,\mathbf{X}^{\mathbf{i}_2}}_{<_m} < 1\,\mathbf{X}^{\mathbf{i}_1} < \cdots$$

Term ordering for Tate algebras

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

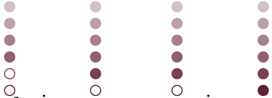
- Starting from a usual monomial ordering $1 <_m \mathbf{X}^{\mathbf{i}_1} <_m \mathbf{X}^{\mathbf{i}_2} <_m \dots$
- We define a term ordering putting more weight on large coefficients

Usual term ordering:



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

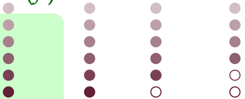
Term ordering for Tate series:



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

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

$\mathrm{LT}(f)$



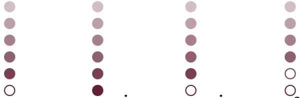
$$f = \boxed{a_2 XY} + a_1 X + a_0 \cdot 1 + a_3 X^2 Y^2 + \dots$$

Term ordering for Tate algebras

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

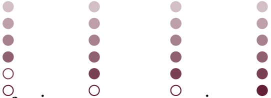
- Starting from a usual monomial ordering $1 <_m \mathbf{X}^{\mathbf{i}_1} <_m \mathbf{X}^{\mathbf{i}_2} <_m \ldots$
- We define a term ordering putting more weight on large coefficients

Usual term ordering:



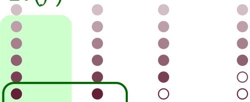
$$\pi \cdot 1 <_m 1\,\mathbf{X}^{\mathbf{i}_1} <_m \pi\,\mathbf{X}^{\mathbf{i}_2} <_m \pi^2\,\mathbf{X}^{\mathbf{i}_3} <_m \cdots$$

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



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

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

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

$$f \quad \mapsto \quad \bar{f}$$

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:

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

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

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 $\quad$ $\exists$ 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

What about Tate series over a field?

- CDVF = fraction field K of a CDVR K°

$$\begin{array}{ll} \mathbb{Q}_p & \mathbb{Z}_p \\ \mathbb{C}((X)) & \mathbb{C}[[X]] \end{array}$$

- Elements can be written $a = \sum_{n=-r}^{\infty} a_n \pi^n$, $a_n \in \mathbb{F}$
- The valuation can be negative but not infinite
- Same metric, same topology as K°

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

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

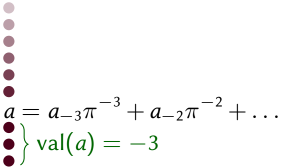
What about Tate series over a field?

- CDVF = fraction field K of a CDVR K°

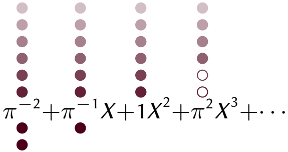
  $\mathbb{Q}_p$ $\qquad$ $\mathbb{Z}_p$

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

- Elements can be written $a = \sum_{n=-r}^{\infty} a_n \pi^n$, $a_n \in \mathbb{F}$
- 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

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

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

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

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

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

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

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

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

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

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

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

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + 0\, f_m$$

$$\mathbf{p} = p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m$$

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

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

$$q = q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + 0\, f_m$$

$$\mathbf{q} = q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m$$

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

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

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

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

$$= \text{smaller terms} + \mu \mathrm{LT}(p_k)\mathbf{e}_k \quad \text{if } \mu \mathrm{LT}(p_k)\mathbf{e}_k \gneqq \nu \mathrm{LT}(q_l)\mathbf{e}_l$$

Regular S-polynomial

Signatures for Tate algebra

Main properties of signatures:

- Ordered (in a way compatible with monomials)
- Example: Position over Term: $\mu \mathbf{e}_i < \nu \mathbf{e}_j \iff i < j$ or $i = j$ and $\mu < \nu$
- Never decreasing in the course of the algorithms

Difficulties with Tate series:

- Need to order them with their coefficients
- The order is mixed: $1 > \pi$

Results:

- Proof of correctness and termination for two orders:
  - Position over Term
  - Valuation over Position over Term: analogue of the F5 order for the valuation
- No need to multiply signatures by π

Conclusion and perspectives

Main results

- Definitions of Gröbner bases for Tate series
- Algorithms for computing and using those Gröbner bases
- Data structure and algorithms implemented in Sage (version 8.5, 22/12/2018)
- Two signature-based algorithms with significant performance improvements

Perspectives

- Reduction of Tate series is very different from reduction of polynomials
- Design algorithms to perform those reductions more efficiently
- Goal: being able to take advantage of e.g. delaying reductions using signatures

Conclusion and perspectives

Main results

- Definitions of Gröbner bases for Tate series
- Algorithms for computing and using those Gröbner bases
- Data structure and algorithms implemented in Sage (version 8.5, 22/12/2018)
- Two signature-based algorithms with significant performance improvements

Perspectives

- Reduction of Tate series is very different from reduction of polynomials
- Design algorithms to perform those reductions more efficiently
- Goal: being able to take advantage of e.g. delaying reductions using signatures

---

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

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

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

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