FGLM algorithm over Tate algebras

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

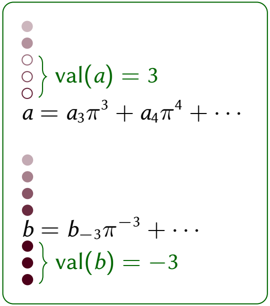
1. Université de Bordeaux, CNRS, Inria, Bordeaux, France
2. Université de Limoges, CNRS, XLIM, Limoges, France
3. Johannes Kepler University, Institute for Algebra, Linz, Austria

Journées Nationales de Calcul Formel 2021, 2021/03/04

Setting and definitions

Valued field, valuation ring

- Field with a valuation $\mathrm{val} : K \to \mathbb{Z} \cup \infty$ — $\mathbb{Q}_p$ — $k((X))$
- Integer ring $K^\circ = \{x : \mathrm{val}(x) \geq 0\}$ — $\mathbb{Z}_p$ — $k[[X]]$
- Uniformizer π s.t. $\pi K^\circ = \{x : \mathrm{val}(x) \geq 1\}$ — p — X



Metric and topology

- "a is small" $\iff$ "$\mathrm{val}(a)$ is large"
- Non-archimedean metric: "small + small = small"
- $\mathbb{Q}_p$, $\mathbb{Z}_p$, $k((X))$, $k[[X]]$ are complete for that topology

Rigid geometry and Tate series

- "Algebraic geometry, analytic geometry" bridge for non-archimedean geometry
- Main object: Tate series

Tate series

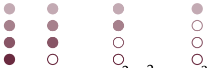
$\mathbf{r} \in \mathbb{Q}^n$: convergence (log)-radii

Definitions

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

Examples:

- Polynomials are Tate series for all radii (finite sums)



- $f = \sum_{i,j=0}^{\infty} \pi^i X^i = 1 + \pi X + \pi^2 X^2 + \pi^3 X^3 + \cdots$
  - $f \in K\{X\} = K\{X; 0\}$
  - $f \notin K\{X; 1\}$: for all terms, $\mathrm{val}(\pi^\alpha) - \alpha = 0 \not\to \infty$

Gröbner bases over Tate algebras

Gröbner bases:

- Multi-purpose tool for ideal arithmetic in polynomial algebras
- Membership testing, elimination, intersection...
- Uses successive (terminating) reductions
- Requires the definition of an ordering on terms

Construction for Tate series

- Term order considering terms according to the valuation of their coefficient
- First compare $\mathrm{val}(a_\alpha) - \sum r_j \alpha_j$, break ties with a monomial order

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

- Convergent reductions (interrupted at the precision bound) instead of terminating ones
- Allows to use usual algorithms (Buchberger, F4) to compute Gröbner bases

Complexity bottleneck: reductions

Cost of reductions

- Not unusual with Gröbner bases
- Tate case: reductions are interrupted at the precision bound
- The cost grows badly with the precision
- **Question:** can we compute reductions in time quasi-linear in the precision?

Ideas for possible improvement:

- Avoid useless reductions to zero
- Speed-up interreductions
- Exploit overconvergence

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

Complexity bottleneck: reductions

Cost of reductions

- Not unusual with Gröbner bases
- Tate case: reductions are interrupted at the precision bound
- The cost grows badly with the precision
- **Question:** can we compute reductions in time quasi-linear in the precision?

Ideas for possible improvement:

- Avoid useless reductions to zero ⟶ Signature algorithms [CVV 2020]
- Speed-up interreductions
- Exploit overconvergence

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

Complexity bottleneck: reductions

Cost of reductions

- Not unusual with Gröbner bases
- Tate case: reductions are interrupted at the precision bound
- The cost grows badly with the precision
- **Question:** can we compute reductions in time quasi-linear in the precision?

Ideas for possible improvement:

- Avoid useless reductions to zero ⟶ Signature algorithms [CVV 2020]
- Speed-up interreductions
- Exploit overconvergence

(Speed-up interreductions, Exploit overconvergence) ⟶ In dim. 0: with FGLM **[this work]**

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

FGLM algorithm and applications

Zero-dimensional ideal in $K[\mathbf{X}]$

- Variety = finitely many points
- Quotient $K[\mathbf{X}]/I$ has finite dimension as a vector space over K
- Given a Gröbner basis G, the staircase under G is
  $B = \{m$ monomial not divisible by any LT of $G\}$
- B is a K-basis of $K[\mathbf{X}]/I$
- Key object: matrices of multiplications by $X_1, \ldots, X_n$ in the basis B

Outline of the algorithm:

In: G_1 a reduced Gröbner basis of $I \subset K[\mathbf{X}]$ wrt an order $<_1$

$<_2$ a monomial order

Out: G_2 a reduced Gröbner basis of $I \subset K[\mathbf{X}]$ wrt $<_2$

1. Compute the matrices of multiplication by $X_1, \ldots, X_n$ in the basis B_1 (computing B_1)

2. Convert them into the Gröbner basis G_2 (computing B_2)

FGLM algorithm and applications

Zero-dimensional ideal in $K\{\mathbf{X};\mathbf{r}\}$

- Variety = finitely many points
- Quotient $K\{\mathbf{X};\mathbf{r}\}/I$ has finite dimension as a vector space over K
- Given a Gröbner basis G, the staircase under G is
  $B = \{m \text{ monomial not divisible by any LT of } G\}$
- B is a K-basis of $K\{\mathbf{X};\mathbf{r}\}/I$
- Key object: matrices of multiplications by $X_1, \ldots, X_n$ in the basis B

Outline of the algorithm for Tate algebras:

In: G_1 a reduced Gröbner basis of $I \subset K\{\mathbf{X};\mathbf{r}\}$ wrt an order $<_1$
$<_2$ a monomial order, $\mathbf{u} \leq \mathbf{r}$

Out: G_2 a reduced Gröbner basis of $I \cdot K\{\mathbf{X};\mathbf{u}\} \subset K\{\mathbf{X};\mathbf{u}\}$ wrt $<_2$

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

FGLM algorithm and applications

Zero-dimensional ideal in $K\{\mathbf{X};\mathbf{r}\}$

- Variety = finitely many points
- Quotient $K\{\mathbf{X};\mathbf{r}\}/I$ has finite dimension as a vector space over K
- Given a Gröbner basis G, the staircase under G is
  $B = \{m \text{ monomial not divisible by any LT of } G\}$
- B is a K-basis of $K\{\mathbf{X};\mathbf{r}\}/I$
- Key object: matrices of multiplications by $X_1, \dots, X_n$ in the basis B

Outline of the algorithm for Tate algebras:

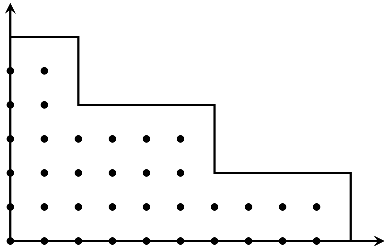
In: G_1 a Gröbner basis reduced mod π of $I \subset K\{\mathbf{X};\mathbf{r}\}$ wrt an order $<_1$
$<_2$ a monomial order, $\mathbf{u} \leq \mathbf{r}$

Out: G_2 a reduced Gröbner basis of $I \cdot K\{\mathbf{X};\mathbf{u}\} \subset K\{\mathbf{X};\mathbf{u}\}$ wrt $<_2$

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

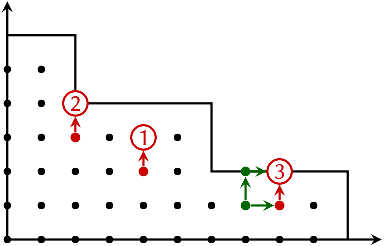
Step 1: computing the multiplication matrices

Idea: we want $\mathrm{NF}(X_i m)$ for all $i \in \{1, \ldots, n\}$, $m \in B$ without computing the NF



Step 1: computing the multiplication matrices

Idea: we want $\mathrm{NF}(X_i m)$ for all $i \in \{1, \ldots, n\}$, $m \in B$ without computing the NF



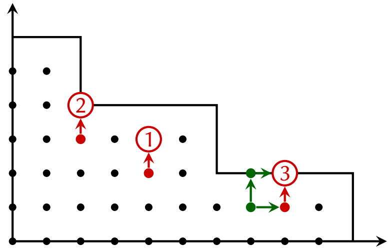
Proceed in increasing order, 3 cases:

1. $X_i m \in B \to \mathrm{NF}(X_i m) = X_i m$
2. $X_i m = \mathrm{LT}(g)$ for $g \in G \to \mathrm{NF}(X_i m) = X_i m - g$
3. Otherwise, write $\mathrm{NF}(X_i m)$ $m = X_j m'$ as linear combination of other normal forms

- Usual case: only involves known normal forms
- Tate case: can involve later monomials, but with coefficients divisible by π
- So we can repeat, increasing the precision by 1 each time

Step 1: computing the multiplication matrices

Idea: we want $\mathrm{NF}(X_i m)$ for all $i \in \{1, \ldots, n\}$, $m \in B$ without computing the NF



Proceed in increasing order, 3 cases:

1. $X_i m \in B \to \mathrm{NF}(X_i m) = X_i m$
2. $X_i m = \mathrm{LT}(g)$ for $g \in G \to \mathrm{NF}(X_i m) = X_i m - g$
3. Otherwise, write $\mathrm{NF}(X_i m)$ $m = X_j m'$ as linear combination of other normal forms

- Usual case: only involves known normal forms
- Tate case: can involve later monomials, but with coefficients divisible by π
- So we can repeat, increasing the precision by 1 each time

Improvements

- Recursive algorithm querying the coefficients as needed (instead of relying on the order)
- Fast arithmetic + relaxed algorithms for base complexity quasi-linear in precision
  [van der Hoeven 1997] [Berthomieu, van der Hoeven, Lecerf 2011] [Berthomieu, Lebreton 2012]
- The algorithm only requires that the basis is reduced modulo π → fast interreduction

Step 2: computing the new staircase

Example

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

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

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

Step 2: computing the new staircase

Example

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

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

- Why does x disappear from the staircase?

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

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

Multiplication matrices and slope factorization

- Problem: how to detect this phenomenon in general?

Consider the multiplication matrix by x:

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

$$\begin{matrix} 1 & x & y & xy & y^2 & xy^2 \end{matrix}$$

Characteristic polynomial:

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

Multiplication matrices and slope factorization

- Problem: how to detect this phenomenon in general?

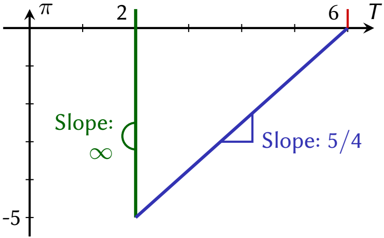
Consider the multiplication matrix by x:

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

$$\begin{matrix} 1 & x & y & xy & y^2 & xy^2 \end{matrix}$$

Characteristic polynomial:

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



Slope factorization: split according to the sign of the generalized eigenvalues

- $\ker(T_x^4 - \pi^{-5})$: generalized eigenvectors with valuation $-5/4 < 0$
  $\rightarrow$ vectors sent to 0
- $\ker(T_x^2)$: generalized eigenvectors with valuation $\infty \geq 0$
  $\rightarrow$ vectors in the staircase

Full algorithm and complexity

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

$<_2$ a monomial order

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

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

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

Full algorithm and complexity

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

$<_2$ a monomial order

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

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

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

Complexity

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

$\delta =$ degree of the ideal $= \#B_{1,\mathbf{r}} \geq \#B_{1,\mathbf{u}}$

Conclusion

Summary

- FGLM algorithm for Tate series
- Allows to perform interreduction and change of log-radii in dimension 0
- Complexity cubic in degree, quasi-linear in precision

Conclusion

Summary

- FGLM algorithm for Tate series
- Allows to perform interreduction and change of log-radii in dimension 0
- Complexity cubic in degree, quasi-linear in precision

Future work

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

Conclusion

Summary

- FGLM algorithm for Tate series
- Allows to perform interreduction and change of log-radii in dimension 0
- Complexity cubic in degree, quasi-linear in precision

Future work

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

Thank you for your attention!

References

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