On FGLM algorithms over Tate algebras

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

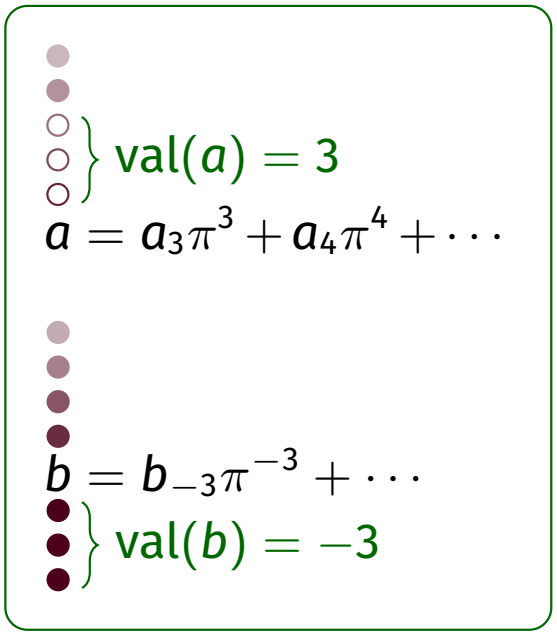
1. Université de Bordeaux, CNRS, Inria, Bordeaux, France
2. Université de Limoges, CNRS, XLIM, Limoges, France
3. Johannes Kepler University, Institute for Algebra, Linz, Austria

International Symposium on Symbolic and Algebraic Computation, 2021/07/23

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

Definitions

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

- 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: $r_i = \infty$ if 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, $\mathrm{val}(\pi^\alpha) - \alpha = 0 \not\to \infty$
- If $K = \mathbb{Q}_p$, $\exp(X)$ is a Tate series with $r < \frac{1}{p-1}$

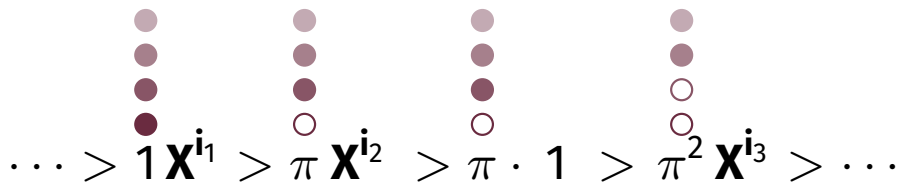
Gröbner bases over Tate algebras

Gröbner bases

- Multi-purpose tool for ideal arithmetic in polynomial algebras
- Ex: membership testing, elimination, intersection...
- Uses successive (terminating) reductions
- Requires the definition of a term ordering

Construction for Tate series

- Term ordering compatible with the topology
- First compare $\mathrm{val}(a_\alpha) - \sum r_j \alpha_j$ and break ties with a monomial order



- Non-terminating but convergent reduction (+ precision bound)
- 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 do better?

Possible improvements?

- 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 do better?

Possible improvements?

- Avoid useless reductions to zero $\longrightarrow$ 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 do better?

Possible improvements?

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

→ In dim. 0: with FGLM **[this work]**

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

Change of ordering and the FGLM algorithm

Change of ordering

- Useful in the classical case for two-steps strategies
- For zero-dimensional ideals, can be done efficiently with the FGLM algorithm [Faugère, Gianni, Lazard, Mora 1993]
- Complexity cubic (or faster) in the degree (number of solutions)

For Tate algebras

- Change of term ordering (monomial ordering and convergence radii)
- Complexity cubic in the degree, quasi-linear in the precision
- Can reduce partially reduced bases

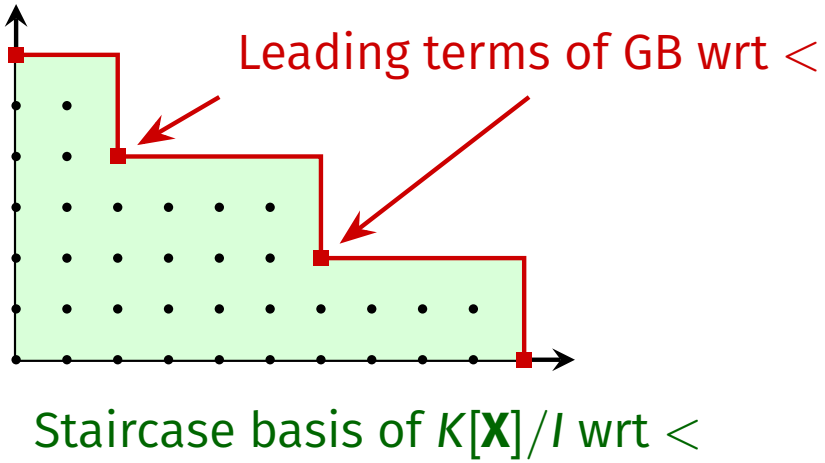
Idea for overconvergence

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

FGLM algorithm

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

- Finitely many solutions
- $K[\mathbf{X}]/I$ has finite dimension δ as a K-vector space
- Key object: matrices of $P \mapsto X_i P \bmod I$



Algorithm FGLM

G_1 reduced GB of $I \subset K[\mathbf{X}]$ wrt the order $<_1$

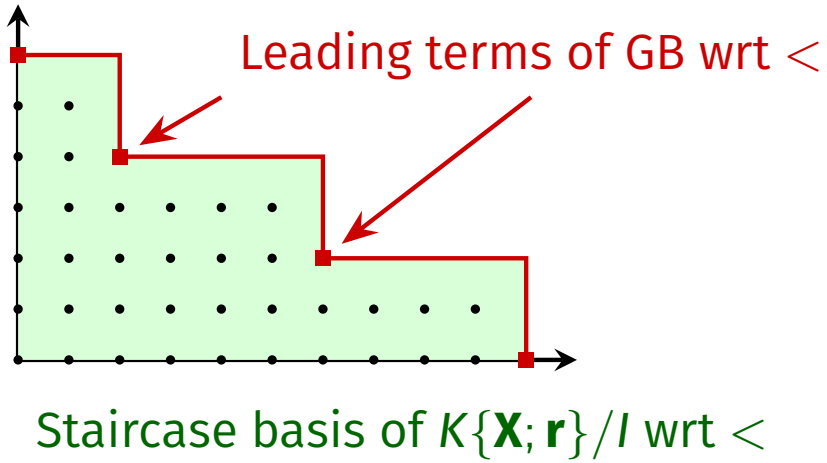
Mult. matrices by $X_1, \ldots, X_n$ in staircase B_1

G_2 reduced GB of $I \subset K[\mathbf{X}]$ wrt the order $<_2$

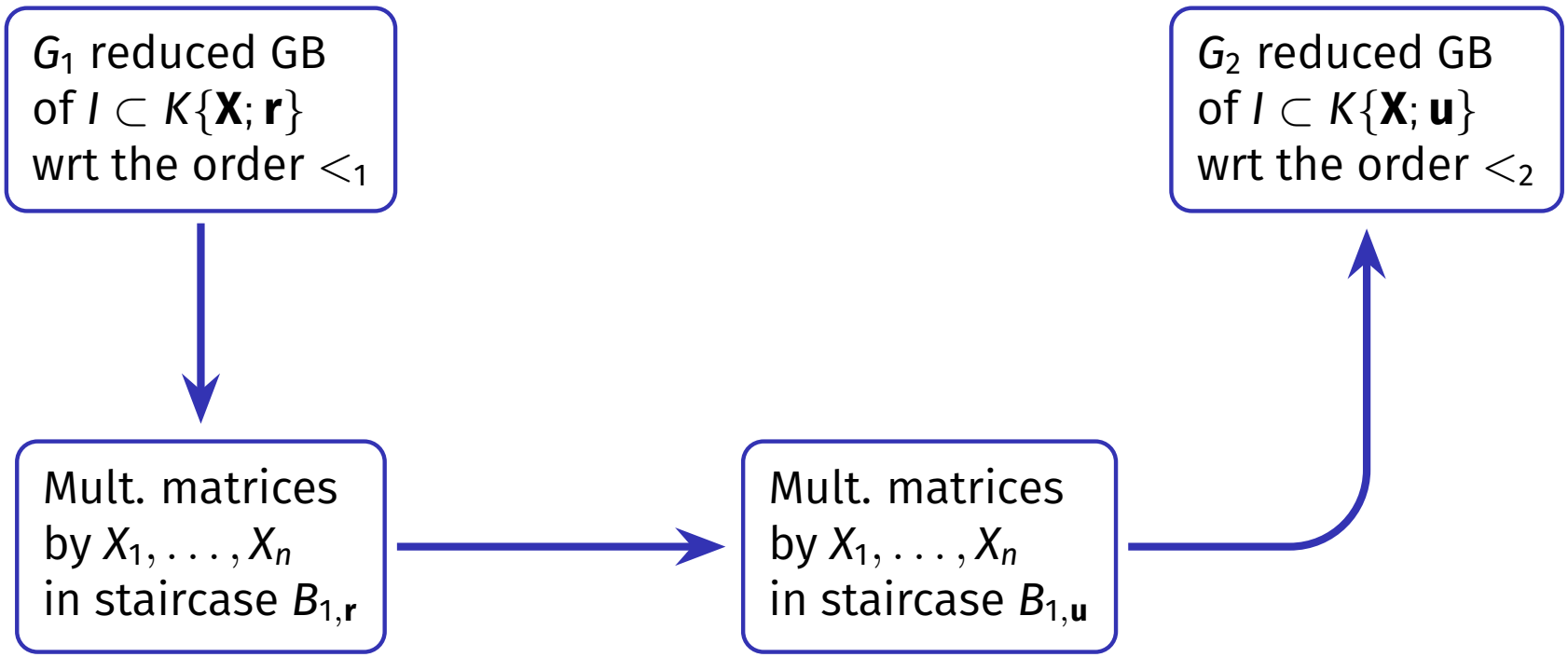
FGLM algorithm

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

- Finitely many solutions
- $K\{\mathbf{X};\mathbf{r}\}/I$ has finite dimension δ as a K-vector space
- Key object: matrices of $P \mapsto X_i P \bmod I$



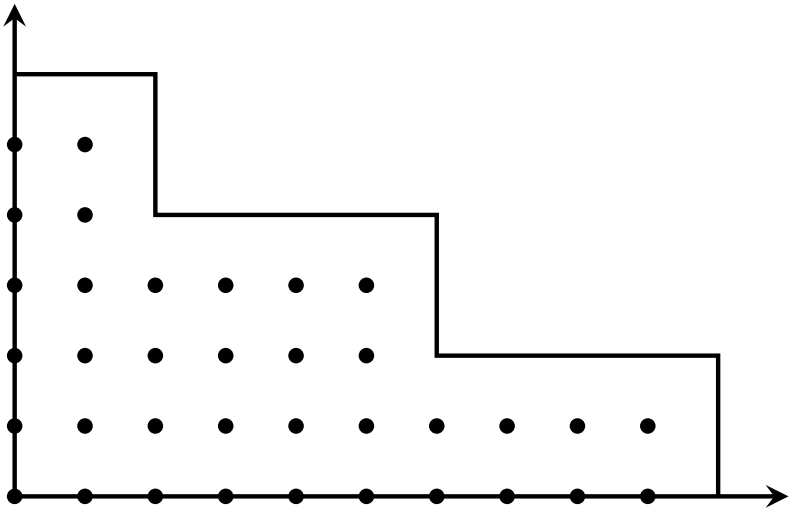
Algorithm FGLM



Iterative computation of the multiplication matrices

$\mathbf{r} = (0, \ldots, 0)$

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

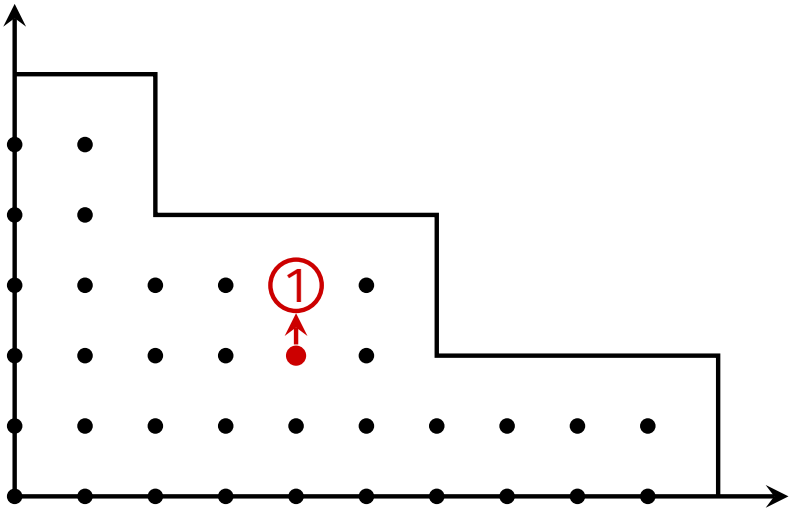


3 cases

Iterative computation of the multiplication matrices

$\mathbf{r} = (0, \ldots, 0)$

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



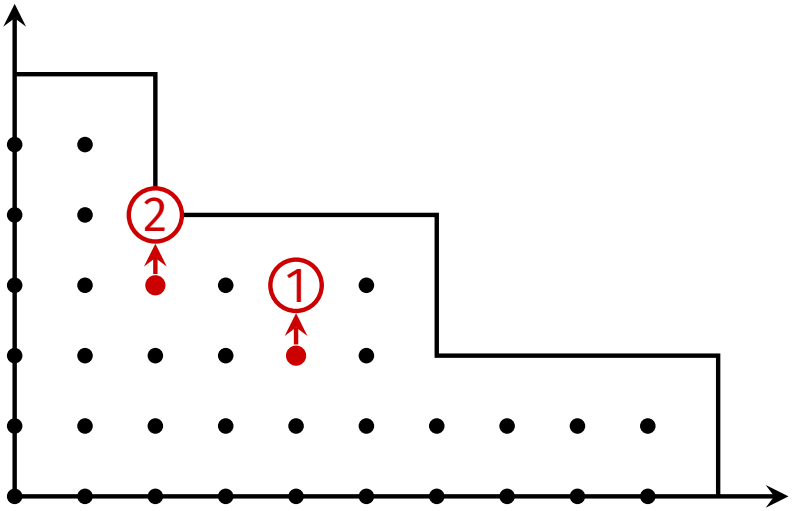
3 cases

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

Iterative computation of the multiplication matrices

$\mathbf{r} = (0, \ldots, 0)$

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



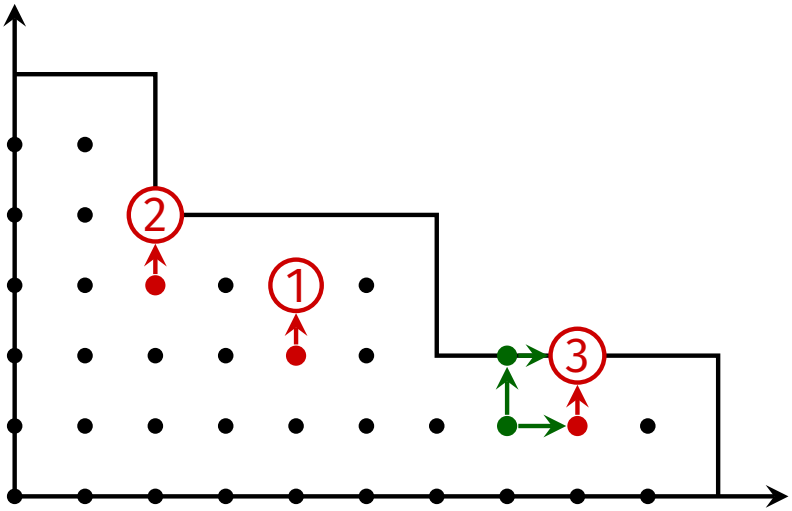
3 cases

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

Iterative computation of the multiplication matrices

$\mathbf{r} = (0, \ldots, 0)$

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



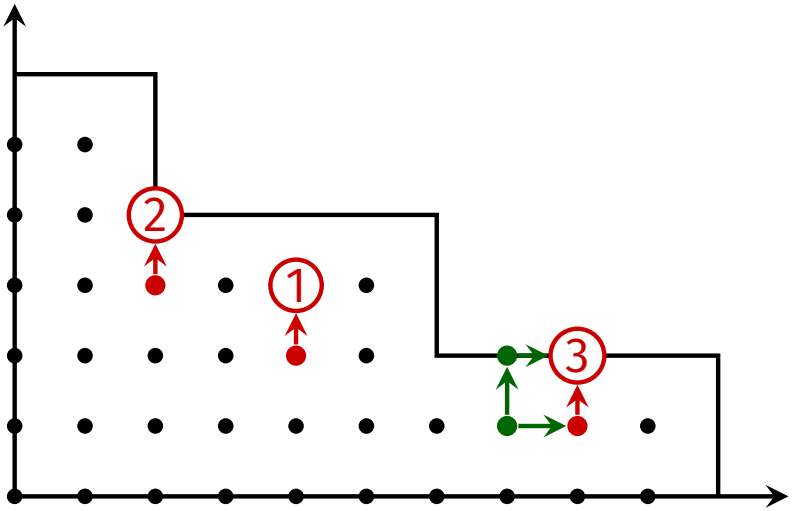
3 cases

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

Iterative computation of the multiplication matrices

$\mathbf{r} = (0, \dots, 0)$

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



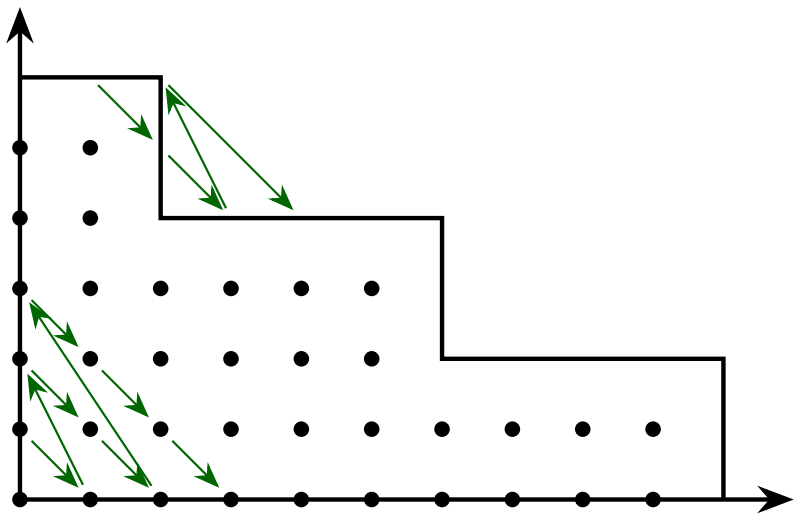
3 cases

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

Why does it work?

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

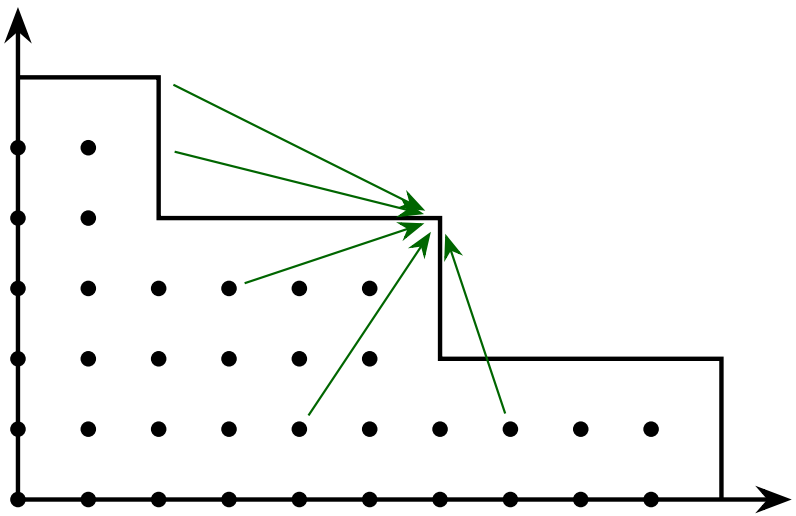
Improvements on the computation of the multiplication matrices



Incremental algorithm

- Follows the monomial ordering
- Cubic in δ, quadratic in precision
- Fast arithmetic does not help!

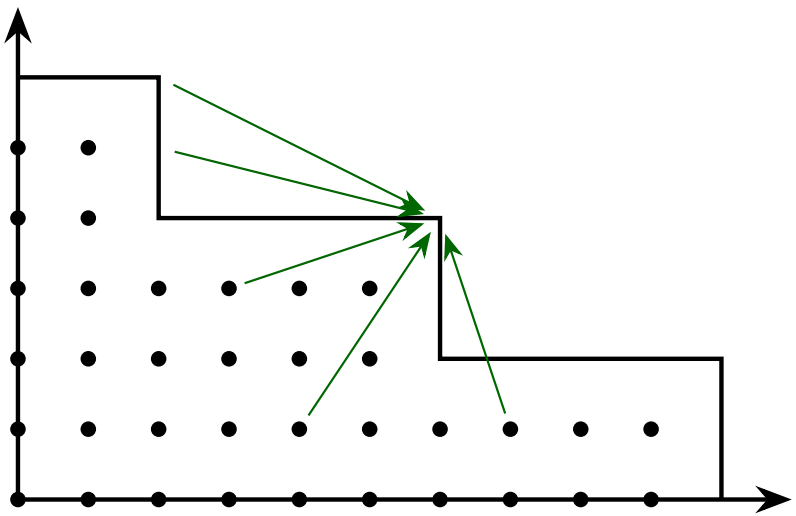
Improvements on the computation of the multiplication matrices



Recursive algorithm

- Query digits of the coefs as needed
- Functionally equivalent to incr. algo.
- Cubic in δ, quadratic in precision
- Order-agnostic (e.g. for other radii)

Improvements on the computation of the multiplication matrices



Recursive algorithm

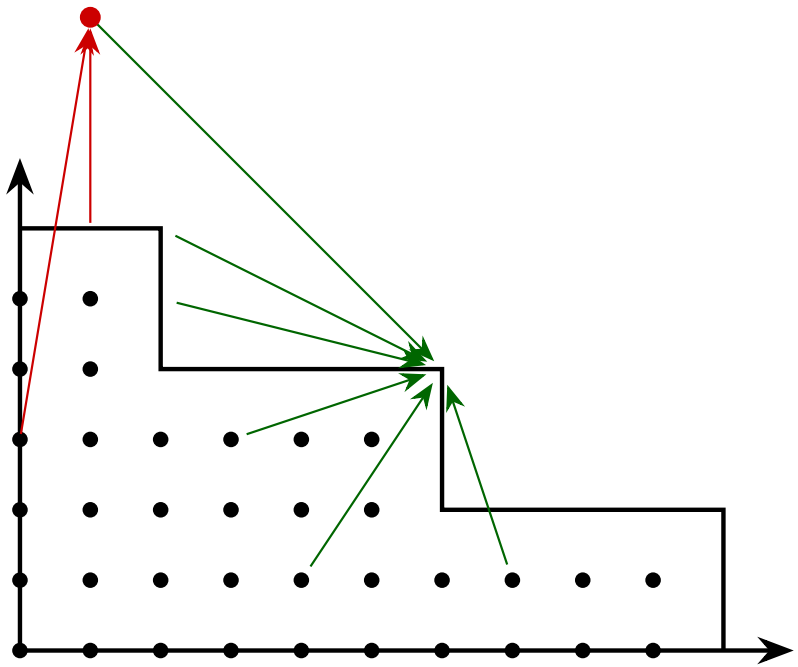
- Query digits of the coefs as needed
- Functionally equivalent to incr. algo.
- Cubic in δ, quadratic in precision
- Order-agnostic (e.g. for other radii)

Relaxed algorithm for $\mathbb{Q}_p$ or $\mathbb{Q}((X))$

- Lazy representation of objects
  + recursive definition
- Amortized log cost for each digit
- Complexity quasi-linear in precision

[v. d. Hoeven 1997] [Berthomieu, Lebreton 2012]
[Berthomieu, v. d. Hoeven, Lecerf 2011]

Improvements on the computation of the multiplication matrices



Recursive algorithm

- Query digits of the coefs as needed
- Functionally equivalent to incr. algo.
- Cubic in δ, quadratic in precision
- Order-agnostic (e.g. for other radii)

Relaxed algorithm for $\mathbb{Q}_p$ or $\mathbb{Q}((X))$

- Lazy representation of objects + recursive definition
- Amortized log cost for each digit
- Complexity quasi-linear in precision

[v. d. Hoeven 1997] [Berthomieu, Lebreton 2012] [Berthomieu, v. d. Hoeven, Lecerf 2011]

What about non-reduced bases?

- We may need elements out of the staircase
- If reduced mod π, their coefficient is div. by π
- The relaxed algorithm still works!
- Complexity quasi-linear in precision, but unbounded in δ

Changing convergence radii: what happens to the staircase?

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

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

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

Changing convergence radii: what happens to the staircase?

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

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

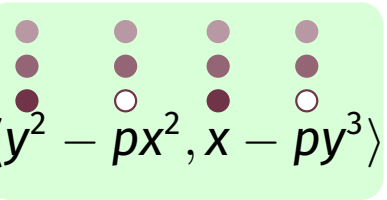
- $K\{x, y\}$: $\mathbf{u} = (0, 0)$
- $J = \langle y^2 - px^2, x - py^3 \rangle$ Gröbner bases
- $B_2 = \{1, y\}$, degree 2

Changing convergence radii: what happens to the staircase?

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

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

- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $J = \langle y^2 - px^2, x - py^3 \rangle$ Gröbner bases



- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2

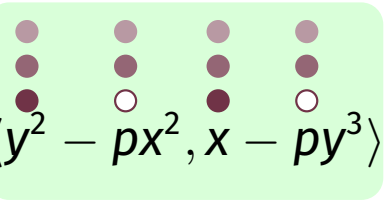
- Why does x disappear from the staircase?

  Consider $x^4 \cdot x$

Changing convergence radii: what happens to the staircase?

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

- $K[x, y]$: $\mathbf{r} = (\infty, \infty)$
- $K\{x, y\}$: $\mathbf{u} = (0, 0)$
- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $J = \langle y^2 - px^2, x - py^3 \rangle$ Gröbner bases



- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2

- Why does x disappear from the staircase?

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

Changing convergence radii: what happens to the staircase?

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

- $K[x, y]$: $\mathbf{r} = (\infty, \infty)$
- $K\{x, y\}$: $\mathbf{u} = (0, 0)$
- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $J = \langle y^2 - px^2, x - py^3 \rangle$ Gröbner bases
- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2
- Why does x disappear from the staircase?

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

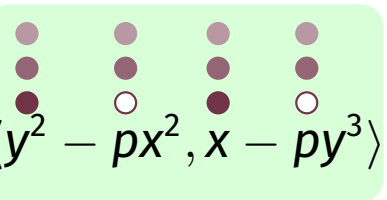
  

  so $x = p^5 x^5$

Changing convergence radii: what happens to the staircase?

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

- $K[x, y]$: $\mathbf{r} = (\infty, \infty)$
- $K\{x, y\}$: $\mathbf{u} = (0, 0)$
- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $J = \langle y^2 - px^2, x - py^3 \rangle$ Gröbner bases



- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2

- Why does x disappear from the staircase?

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

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

Changing convergence radii: what happens to the staircase?

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

- $K[x, y]$: $\mathbf{r} = (\infty, \infty)$
- $K\{x, y\}$: $\mathbf{u} = (0, 0)$
- $I = \langle px^2 - y^2, py^3 - x \rangle$
- $J = \langle y^2 - px^2, x - py^3 \rangle$ Gröbner bases
- $B_1 = \{1, x, y, y^2, xy, xy^2\}$, degree 6
- $B_2 = \{1, y\}$, degree 2
- Why does x disappear from the staircase?

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

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

  Invertible in $K\{x, y\}$

Multiplication matrices and slope factorization

- **Problem**: how to detect this phenomenon in general?

Multiplication matrices and slope factorization

- **Problem**: how to detect this phenomenon in general?

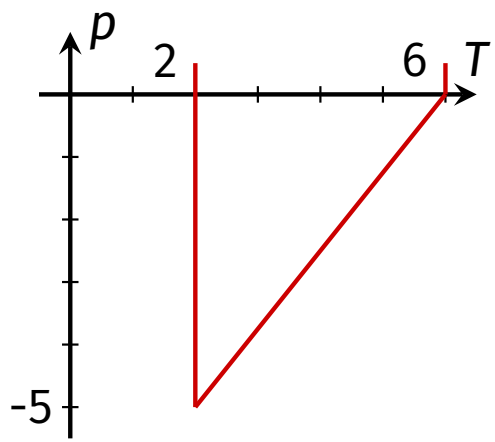
Multiplication matrix by x

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

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

Characteristic poly.

$$T_x^6 - p^{-5} T_x^2 = 0$$



Multiplication matrices and slope factorization

- **Problem**: how to detect this phenomenon in general?

Multiplication matrix by x

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

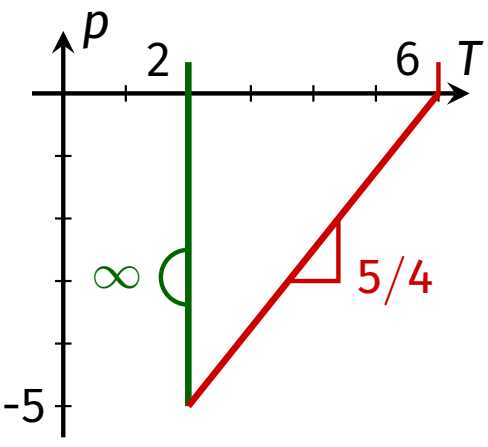
$$\begin{matrix} 1 & x & y & xy & y^2 & xy^2 \end{matrix}$$

Characteristic poly.

$$T_x^6 - p^{-5} T_x^2 = 0$$

Slope factorization

$$T_x^2 \cdot (T_x^4 - p^{-5}) = 0$$



Multiplication matrices and slope factorization

- **Problem**: how to detect this phenomenon in general?

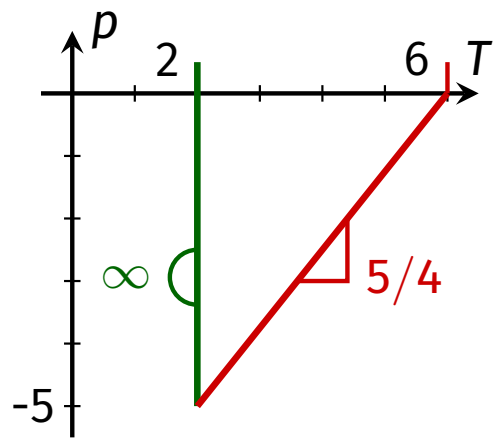
Multiplication matrix by x

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

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

Characteristic poly.

$$T_x^6 - p^{-5} T_x^2 = 0$$



Slope factorization

$$T_x^2 \cdot (T_x^4 - p^{-5}) = 0$$

$\ker(T_x^2)$

Eigenvalues with valuation $\infty \geq 0$

Vectors in the staircase

$\ker(T_x^4 - p^{-5})$

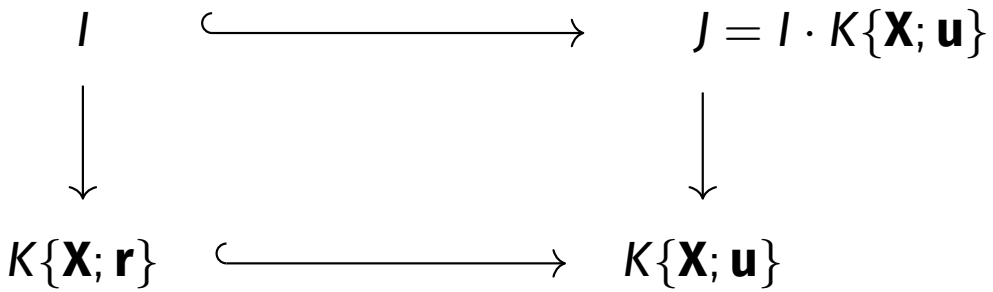
"Eigenvalues" with valuation $-5/4 < 0$

Vectors sent to 0

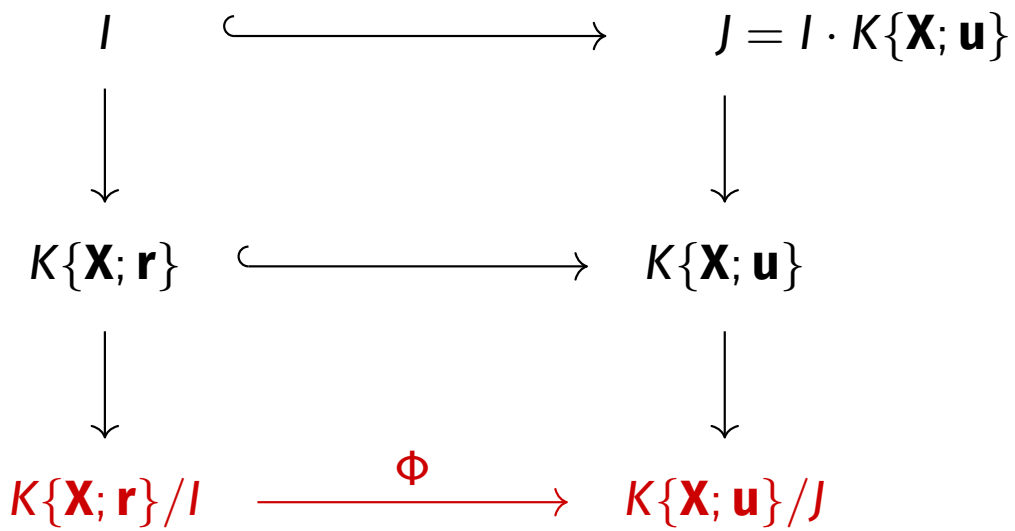
Construction of the new staircase: theoretical point of view

$$K\{\mathbf{X};\mathbf{r}\} \hookrightarrow K\{\mathbf{X};\mathbf{u}\}$$

Construction of the new staircase: theoretical point of view

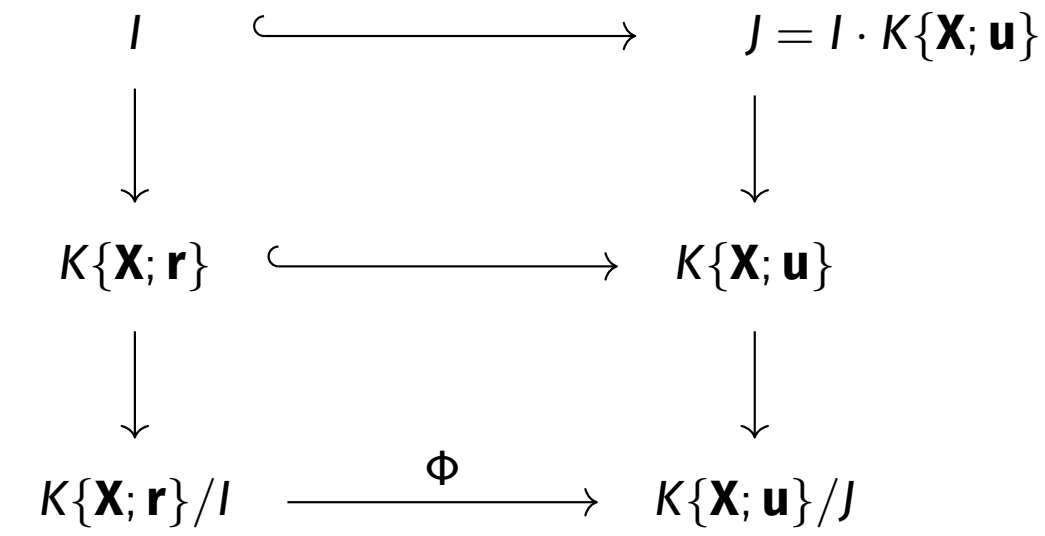


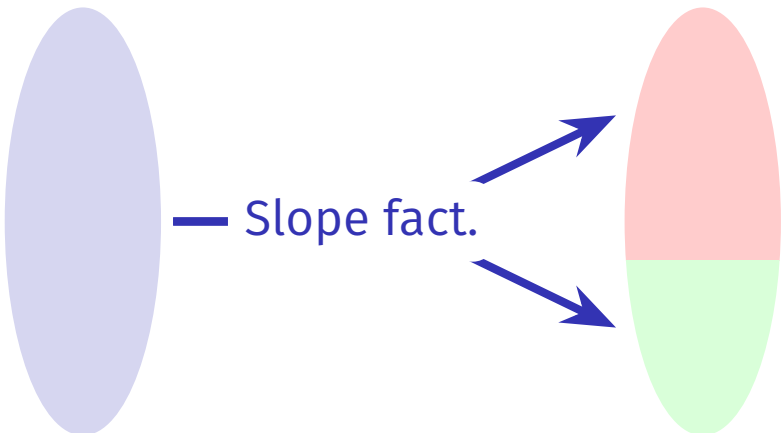
Construction of the new staircase: theoretical point of view



Staircase $B_{\mathbf{r}}$

Construction of the new staircase: theoretical point of view





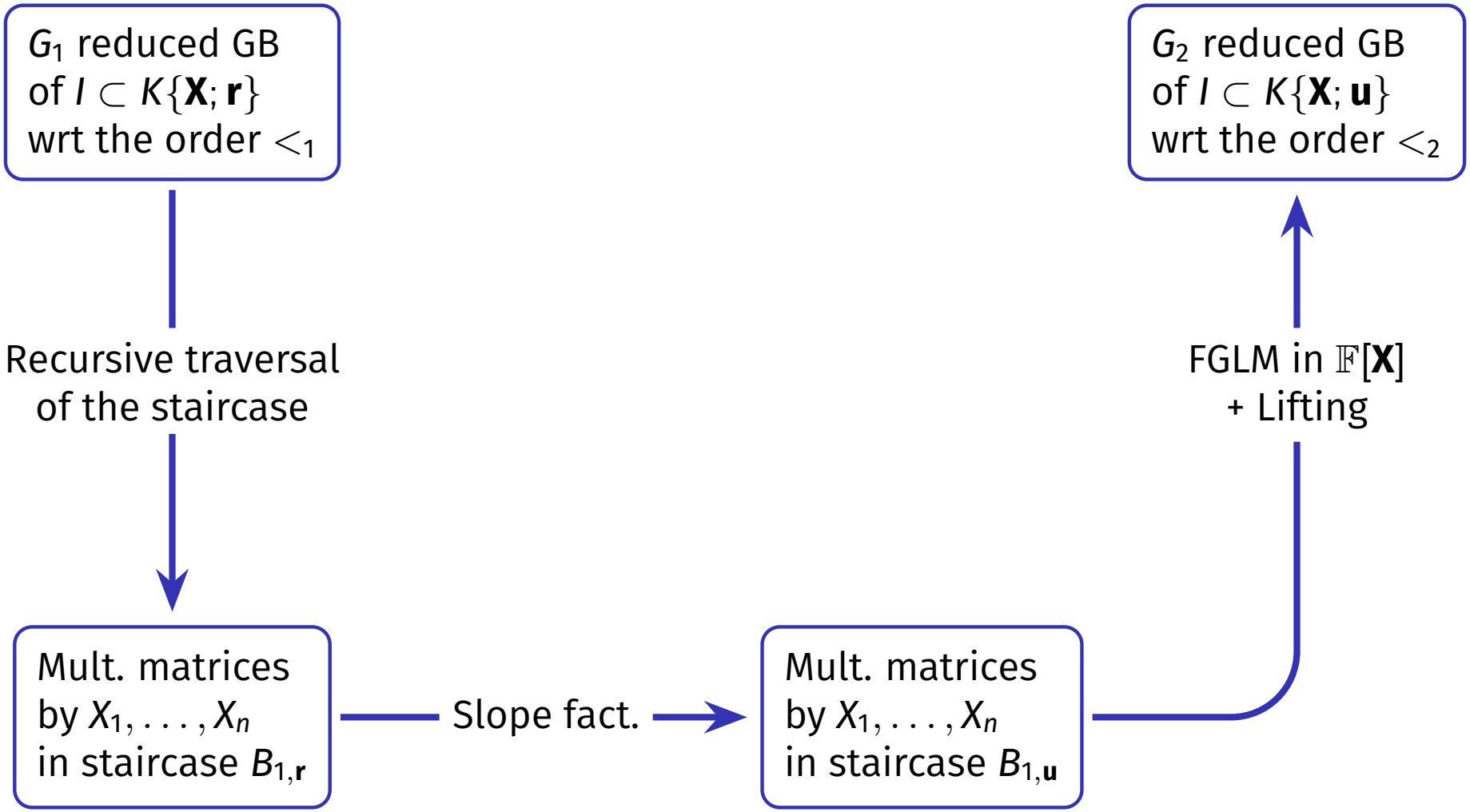
Staircase $B_{\mathbf{r}}$

Basis of $\ker(\Phi)$
$= \sum$ "Eigenspace" of T_i with val. $< u_i$

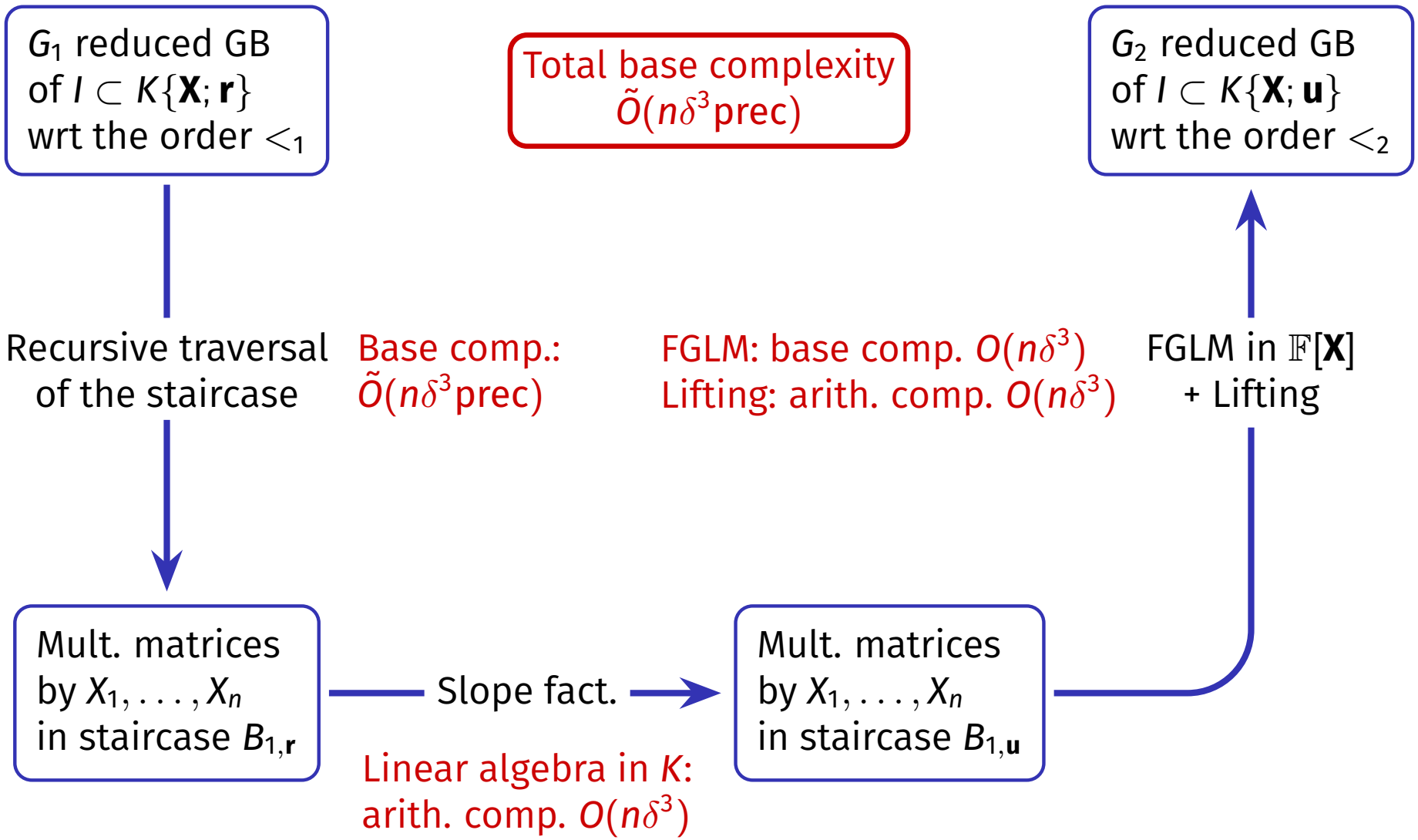
Staircase $B_{\mathbf{u}}$: basis of
$\bigcap$ "Eigenspace" of T_i with val. $\geq u_i$

Topological computation (completion+separation) using linear algebra!

Full FGLM algorithm for Tate algebras



Full FGLM algorithm for Tate algebras



Conclusion

Summary

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

Conclusion

Summary

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

Future work

- Implement FGLM for Tate series in SageMath
- Generalizations of interreductions before a basis is complete
- Improve the complexity of reduction in positive dimension

Conclusion

Summary

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

Future work

- Implement FGLM for Tate series in SageMath
- Generalizations of interreductions before a basis is complete
- Improve the complexity of reduction in positive dimension

Thank you for your attention!