Grobner Bases for polytopal affinoid algebras

Legrand Lucas

Joint work with M. Barkatou and T. Vaccon

JNCF 2024

Outline

1. Introducing polytopal affinoid algebras (PAA)

Outline

1. Introducing polytopal affinoid algebras (PAA)
2. Grobner theory for ideals in PAA
    - Definition of Grobner bases
    - Multivariate division algorithm
    - S-pairs criterion
    - Buchberger-like algorithm

Non-archimedean setting

K a non-archimedean field :

Non-archimedean setting

K a non-archimedean field :

- K a field
- $val : K \to \mathbb{R}$ a **discrete** valuation for which K is **complete**
- val is **normalized**: $val(K) = \mathbb{Z}$.
- π uniformizer, i.e val$(\pi) = 1$.

Non-archimedean setting

K a non-archimedean field :

- K a field
- $val : K \to \mathbb{R}$ a **discrete** valuation for which K is **complete**
- val is **normalized**: $val(K) = \mathbb{Z}$.
- π uniformizer, i.e $\text{val}(\pi) = 1$.

Example

$K = \mathbb{Q}_p$, p-adic valuation, $\pi = p$

Non-archimedean setting

K a non-archimedean field :

- K a field
- $val : K \to \mathbb{R}$ a **discrete** valuation for which K is **complete**
- val is **normalized**: $val(K) = \mathbb{Z}$.
- π uniformizer, i.e val$(\pi) = 1$.

Example

$K = \mathbb{Q}_p$, p-adic valuation, $\pi = p$

Example

$K = A((T))$, A field, T-adic valuation, $\pi = T$.

Non-archimedean setting

K a non-archimedean field :

- K a field
- $val : K \to \mathbb{R}$ a **discrete** valuation for which K is **complete**
- val is **normalized**: $val(K) = \mathbb{Z}$.
- π uniformizer, i.e $\text{val}(\pi) = 1$.

Example

$K = \mathbb{Q}_p$, p-adic valuation, $\pi = p$

Example

$K = A((T))$, A field, T-adic valuation, $\pi = T$.

Notations :

- $n \in \mathbb{N}^*$
- $\mathbf{X} := (X_1, \ldots, X_n)$
- $u \in \mathbb{Z}^n, \mathbf{X}^u := X_1^{u_1} \cdots X_n^{u_n}$

Reminder: affinoid algebras

- Tate's 1971 famous paper: "Rigid analytic spaces"

Let $r = (r_1, \cdots, r_n) \in \mathbb{Q}^n$

Definition (Tate Algebra)

$$K_r\{\mathbf{X}\} := \{ \sum_{u \in \mathbb{N}^n} a_u \mathbf{X}^u \ : \ a_u \in K, \ \mathrm{val}(a_u) - r \cdot u \xrightarrow[|u| \to +\infty]{} +\infty \}$$

Elements of $K_r\{X\}$ are power series converging on the product of closed balls $B(0, |\pi|^{r_1}) \times \cdots \times B(0, |\pi|^{r_n})$.
Gauss valuation : $\mathrm{val}_r(\sum a_u \mathbf{X}^u) := \min_u (val(a_u) - r \cdot u)$

Definition (Affinoid Algebra)

Any quotient of a Tate algebra equipped with the induced norm.

Polytopal affinoid algebras

Polytopal affinoid algebras

P a rational polytope in $\mathbb{R}^n := \mathrm{Conv}(\{s_1, \ldots, s_k\}), s_i \in \mathbb{Q}^n$

Polytopal affinoid algebras

P a rational polytope in $\mathbb{R}^n := \mathrm{Conv}(\{s_1, \ldots, s_k\}), s_i \in \mathbb{Q}^n$

Definition (PAA)

$K\{\mathbf{X}; P\} :=$

Polytopal affinoid algebras

P a rational polytope in $\mathbb{R}^n := \mathrm{Conv}(\{s_1, \dots, s_k\}), s_i \in \mathbb{Q}^n$

Definition (PAA)

$K\{\mathbf{X}; P\} :=$

$$\{\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u \ : \ a_u \in K, \ \forall r \in P, \ \mathrm{val}(a_u) - r \cdot u \xrightarrow[|u| \to +\infty]{} +\infty\}$$

Polytopal affinoid algebras

P a rational polytope in $\mathbb{R}^n := \mathrm{Conv}(\{s_1, \ldots, s_k\}), s_i \in \mathbb{Q}^n$

Definition (PAA)

$K\{\mathbf{X}; P\} :=$

$$\{\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u \ : \ a_u \in K, \ \forall r \in P, \ \mathrm{val}(a_u) - r \cdot u \xrightarrow[|u| \to +\infty]{} +\infty\}$$

Elements of $K\{\mathbf{X}; P\} =$ "series $\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u$ converging on $\mathrm{val}^{-1}(P) \subset (K^\times)^n$".

Polytopal affinoid algebras

P a rational polytope in $\mathbb{R}^n := \mathrm{Conv}(\{s_1, \ldots, s_k\}), s_i \in \mathbb{Q}^n$

Definition (PAA)

$K\{\mathbf{X}; P\} :=$

$$\{\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u \ : \ a_u \in K, \ \forall r \in P, \ \mathrm{val}(a_u) - r \cdot u \xrightarrow[|u| \to +\infty]{} +\infty\}$$

Elements of $K\{\mathbf{X}; P\}$ = "series $\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u$ converging on $\mathrm{val}^{-1}(P) \subset (K^\times)^n$".

$$\forall r \in P,$$

Polytopal affinoid algebras

P a rational polytope in $\mathbb{R}^n := \mathrm{Conv}(\{s_1, \dots, s_k\}), s_i \in \mathbb{Q}^n$

Definition (PAA)

$K\{\mathbf{X}; P\} :=$

$$\{\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u \ : \ a_u \in K, \ \forall r \in P, \ \mathrm{val}(a_u) - r \cdot u \xrightarrow[|u| \to +\infty]{} +\infty\}$$

Elements of $K\{\mathbf{X}; P\}$ = "series $\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u$ converging on $\mathrm{val}^{-1}(P) \subset (K^\times)^n$".

$$\forall r \in P, \quad \mathrm{val}_{\mathbf{r}}\left(\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u\right) := \min_{u \in \mathbb{Z}^n} \mathrm{val}(a_u) - r \cdot u,$$

Polytopal affinoid algebras

P a rational polytope in $\mathbb{R}^n := \mathrm{Conv}(\{s_1, \ldots, s_k\}), s_i \in \mathbb{Q}^n$

Definition (PAA)

$K\{\mathbf{X}; P\} :=$

$$\{\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u \ : \ a_u \in K, \ \forall r \in P, \ \mathrm{val}(a_u) - r \cdot u \xrightarrow[|u| \to +\infty]{} +\infty\}$$

Elements of $K\{\mathbf{X}; P\}$ = "series $\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u$ converging on $\mathrm{val}^{-1}(P) \subset (K^\times)^n$".

$$\forall r \in P, \quad \mathrm{val}_{\mathbf{r}} \left(\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u \right) := \min_{u \in \mathbb{Z}^n} \mathrm{val}(a_u) - r \cdot u,$$

$$\forall f \in K\{\mathbf{X}; P\},$$

Polytopal affinoid algebras

P a rational polytope in $\mathbb{R}^n := \text{Conv}(\{s_1, \ldots, s_k\}), s_i \in \mathbb{Q}^n$

Definition (PAA)

$K\{\mathbf{X}; P\} :=$

$$\{\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u \ : \ a_u \in K, \ \forall r \in P, \ \text{val}(a_u) - r \cdot u \xrightarrow[|u| \to +\infty]{} +\infty\}$$

Elements of $K\{\mathbf{X}; P\}$ = "series $\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u$ converging on $\text{val}^{-1}(P) \subset (K^\times)^n$".

$$\forall r \in P, \quad \text{val}_\mathbf{r}\left(\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u\right) := \min_{u \in \mathbb{Z}^n} \text{val}(a_u) - r \cdot u,$$

$$\forall f \in K\{\mathbf{X}; P\}, \quad \text{val}_P(f)$$

Polytopal affinoid algebras

P a rational polytope in $\mathbb{R}^n := \mathrm{Conv}(\{s_1, \ldots, s_k\}), s_i \in \mathbb{Q}^n$

Definition (PAA)

$K\{\mathbf{X}; P\} :=$

$$\{\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u \ : \ a_u \in K, \ \forall r \in P, \ \mathrm{val}(a_u) - r \cdot u \xrightarrow[|u| \to +\infty]{} +\infty\}$$

Elements of $K\{\mathbf{X}; P\}$ = "series $\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u$ converging on $\mathrm{val}^{-1}(P) \subset (K^\times)^n$".

$$\forall r \in P, \quad \mathrm{val}_{\mathbf{r}} \left(\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u \right) := \min_{u \in \mathbb{Z}^n} \mathrm{val}(a_u) - r \cdot u,$$

$$\forall f \in K\{\mathbf{X}; P\}, \quad \mathrm{val}_P(f) := \min_{r \in Vert(P)} \mathrm{val}_{\mathbf{r}}(f)$$

Polytopal affinoid algebras

P a rational polytope in $\mathbb{R}^n := \mathrm{Conv}(\{s_1, \dots, s_k\}), s_i \in \mathbb{Q}^n$

Definition (PAA)

$K\{\mathbf{X}; P\} :=$

$$\{\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u \ : \ a_u \in K, \ \forall r \in P, \ \mathrm{val}(a_u) - r \cdot u \xrightarrow[|u| \to +\infty]{} +\infty\}$$

Elements of $K\{\mathbf{X}; P\}$ = "series $\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u$ converging on $\mathrm{val}^{-1}(P) \subset (K^\times)^n$".

$$\forall r \in P, \quad \mathrm{val}_\mathbf{r}\left(\sum_{u \in \mathbb{Z}^n} a_u \mathbf{X}^u\right) := \min_{u \in \mathbb{Z}^n} \mathrm{val}(a_u) - r \cdot u,$$

$$\forall f \in K\{\mathbf{X}; P\}, \quad \mathrm{val}_P(f) := \min_{r \in Vert(P)} \mathrm{val}_\mathbf{r}(f)$$

$\mathrm{val}_P(f)$ is the minimum valuation reached by f on $\mathrm{val}^{-1}(P)$.

Motivations behind PAA

- Polytopal **affinoid** algebras are **affinoid** algebras !
- Introduced in :
  - Manfred Einsiedler, Mikhail Kapranov, and Douglas Lind. "Non-archimedean amoebas and tropical varieties". In: (2006)
  - Walter Gubler. "Tropical varieties for non-Archimedean analytic spaces". In: *Inventiones mathematicae* 169.2 (2007), pp. 321–376
- Tropical analytic geometry

Related previous work

Grobner bases for ideals in affinoid algebras (local team):

1. Xavier Caruso, Tristan Vaccon, and Thibaut Verron. "Gröbner bases over Tate algebras". In: ISSAC 2019 - Beijing, China
2. Xavier Caruso, Tristan Vaccon, and Thibaut Verron. "Signature-Based Algorithms for Gröbner Bases over Tate Algebras". In: ISSAC 2020 - Kalamata, Greece
3. Xavier Caruso, Tristan Vaccon, and Thibaut Verron. "On FGLM Algorithms with Tate Algebras". In: ISSAC 2021 - Virtual Event, Russian Federation
4. Xavier Caruso, Tristan Vaccon, and Thibaut Verron. "On Polynomial Ideals and Overconvergence in Tate Algebras". In: ISSAC 2022 - Villeneuve-d'Ascq, France
5. Tristan Vaccon and Thibaut Verron. "Universal Analytic Gröbner Bases and Tropical Geometry". In: ISSAC 2023 - Tromsø, Norway

Main idea: use the valution to order terms

*Tate algebra setting

Fix $\leq_m$ a monomial order on $\mathbb{N}^n$.
Order terms $a\mathbf{X}^u, b\mathbf{X}^v \in K_r\{\mathbf{X}\}$ by the following:

$$a\mathbf{X}^u \leq b\mathbf{X}^v \iff (\mathrm{val}_r(a\mathbf{X}^u) > \mathrm{val}_r(b\mathbf{X}^v)) \text{ or } (\mathrm{val}_r(a\mathbf{X}^u) = \mathrm{val}_r(b\mathbf{X}^v) \text{ and } \mathbf{X}^u \leq_m \mathbf{X}^v)$$

Main idea continued

There is no "monomial order on $\mathbb{Z}^n$".
Recall that a monomial order is a total order that satisfies, for all r, s, t:

1. $0 \leq t$
2. $r < s \implies r + t < s + t$

Main idea continued

There is no "monomial order on $\mathbb{Z}^n$".
Recall that a monomial order is a total order that satisfies, for all r, s, t:

1. $0 \leq t$
2. $r < s \implies r + t < s + t$

Proof.
Assume such an order exists. Take any $a \neq 0$. By (1), $0 < a$, and by (2) $-a < 0$, contradiction. □

Main idea continued

There is no "monomial order on $\mathbb{Z}^n$".
Recall that a monomial order is a total order that satisfies, for all r, s, t:

1. $0 \leq t$
2. $r < s \implies r + t < s + t$

Proof.
Assume such an order exists. Take any $a \neq 0$. By (1), $0 < a$, and by (2) $-a < 0$, contradiction. □

But we can use "generalized monomial order" as defined by Pauer-Unterkircher in:
Franz Pauer and Andreas Unterkircher. "Gröbner bases for ideals in Laurent polynomial rings and their application to systems of difference equations". In: (1999)

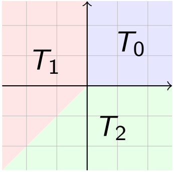
Generalized monomial order

Put $T := \{\mathbf{X}^u,\ u \in \mathbb{Z}^n\}$.

Definition

A conic decomposition of T is a finite family $(T_i)_{i \in I}$ of finitely generated submonoids of T such that

1. for each i, the only invertible element in the monoid T_i is 1 and the group generated by T_i is T.
2. the union of all the T_i's equal T



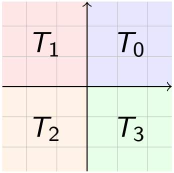


Figure: Conic decompositions for $n = 2$

Generalized monomial order

Definition

Let $(T_i)_{i\in I}$ be a conic decomposition of T. A generalized monomial order (or g.m.o) on T for the decomposition $(T_i)_{i\in I}$ is a total order $<$ on T such that

1. $\forall t \in T, 1 \leq t$
2. $\forall r \in T, \forall i \in I, (s, t \in T_i \text{ and } r < s) \implies rt < st$

For $f \in K[\mathbf{X}^{\pm 1}], K\{\mathbf{X}; P\}\ldots$ and $t \in T$, we generally have :

$$\mathrm{lt}(tf) \neq t\mathrm{lt}(f)$$

Definition

For $i \in I$ define $T_i(f) := \{t \in T,\ \mathrm{lm}(tf) \in T_i\}$.

The compatibility condition implies ...

Take $i \in I$, $f \in K\{\mathbf{X}; P\}$, $u, v \in T_i(f)$.

Lemma

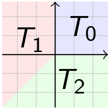
Write $\mathrm{Im}(uf) = ut_u \in T_i$ *and* $\mathrm{Im}(vf) = vt_v \in T_i$ *for some monomials* t_u, t_v *of* f*. Then* $t_u = t_v$*.*

Definition

For $t \in T_i(f)$, define $\mathrm{Im}_i(f) := \mathrm{Im}(tf)t^{-1}$.

An example

Take the conic decomposition:



Define a g.m.o for this decomposition by the formula :

$$(x_1, y_1) \leq (x_2, y_2) \iff -\min(0, x_1, y_1) \leq -\min(0, x_2, y_2) \text{ or }$$
$$-\min(x_1, y_1) = -\min(x_2, y_2) \text{ and } (x_1, y_1) \leq_{lex} ($$

For $f = xy^{-2} + x^{-2}y^{-2} + x^{-1}y^{-2} + y^2$:

- $xy^{-2} > x^{-1}y^{-2} > x^{-2}y^{-2} > y^2$,
- $\mathrm{lm}_0(f) = \mathrm{lm}_2(f) = \mathrm{lm}(f) = xy^{-2}$
- $\mathrm{lm}_1(f) = x^{-2}y^{-2}$
- $T_0(f) = x^2y^2T_0$
- $T_1(f) = xy^2T_1, \; T_2(f) = x^2y^2T_2$

Main idea revisited

*polytopal algebra setting

Fix $\leq_\omega$ a generalized monomial order on $\mathbb{Z}^n$.
Order terms $a\mathbf{X}^u, b\mathbf{X}^v \in K\{\mathbf{X}; P\}$ by the following:

$$a\mathbf{X}^u \leq b\mathbf{X}^v \iff (\mathrm{val}_P(a\mathbf{X}^u) > \mathrm{val}_P(b\mathbf{X}^v)) \text{ or } (\mathrm{val}_P(a\mathbf{X}^u) = \mathrm{val}_P(b\mathbf{X}^v) \text{ and } \mathbf{X}^u \leq_\omega \mathbf{X}^v)$$

Grobner basis

Fix a g.m.o $\leq$ for a conic decomposition $(T_i)_{i\in I}$.
Let J be an ideal in $K\{\mathbf{X}; P\}$ and G be a finite subset of $J \setminus \{0\}$.
We always have the containment:

$$\{\mathrm{lm}(f), f \in J\} \supset \bigcup_{g\in G} \{\mathrm{lm}(tg), t \in T\} = \bigcup_{g\in G, i\in I} T_i(g)\mathrm{lm}_i(g)$$

Definition

We say that G is a Gröbner basis of J when:

$$\{\mathrm{lm}(f), f \in J\} = \bigcup_{g\in G} \{\mathrm{lm}(tg), t \in T\} = \bigcup_{g\in G, i\in I} T_i(g)\mathrm{lm}_i(g)$$

Multivariate division algorithm in $K\{\mathbf{X}; P\}$

input : $f, g_1, \ldots, g_m \in K\{\mathbf{X}; P\}$
output: $q_1, \ldots, q_m, r$

$q_1, \ldots, q_m, r \leftarrow 0$;
while $f \neq 0$ **do**
  while $\exists (i,j) \in I \times [1, m]$ *such that* $\operatorname{lm}\left(\frac{\operatorname{lm}(f)}{\operatorname{lm}_i(g_j)} g_j\right) = \operatorname{lm}(f)$ **do**
    $t \leftarrow \frac{\operatorname{lt}(f)}{\operatorname{lt}_i(g_j)}$;
    $q_j \leftarrow q_j + t$;
    $f \leftarrow f - tg_j$;
  $r \leftarrow r + \operatorname{lt}(f)$
  $f \leftarrow f - \operatorname{lt}(f)$;
return $q_1, \ldots, q_m, r \in K\{\mathbf{X}; P\}$

Multivariate division algorithm in $K\{\mathbf{X}; P\}$

input : $f, g_1, \dots, g_m \in K\{\mathbf{X}; P\}$
output: $q_1, \dots, q_m, r$

```
q_1, ..., q_m, r ← 0;
while f ≠ 0 do
    while ∃(i, j) ∈ I × [1, m] such that lm( (lm(f) / lm_i(g_j)) g_j ) = lm(f) do
        t ← lt(f) / lt_i(g_j);
        q_j ← q_j + t;
        f ← f − t g_j;
    r ← r + lt(f)
    f ← f − lt(f);
return q_1, ..., q_m, r ∈ K{X; P}
```

- $f = \sum q_j g_j + r$
- for all monomial t in r, $t \notin \bigcup_{i \in I, g \in G} T_i(g) \mathrm{lm}_i(g)$
- for all g_j and all monomial t in q_j, $\mathrm{lt}(t g_j) \leq \mathrm{lt}(f)$.

S-pairs: definition

Take $i \in I, f, g \in K\{\mathbf{X}; P\}$.

Lemma

The T_i-module

$$\mathrm{lm}_i(f)\, T_i(f) \cap \mathrm{lm}_i(g)\, T_i(g)$$

is finitely generated.

Let $U(i, f, g)$ be a finite system of generator.

Definition (S-pair)

For $v \in U(i, f, g)$:

$$S(i, f, g, v) := \mathrm{lc}_i(g) \frac{v}{\mathrm{lm}_i(f)} f - \mathrm{lc}_i(f) \frac{v}{\mathrm{lm}_i(g)} g.$$

S-pairs criterion

Let $h_1, \dots, h_m \in K\{\mathbf{X}; P\}$ and $i \in I$. For $1 \le j \le m-1$, let $U(i, h_j, h_{j+1})$ be a finite system of generators. Suppose that there are terms $\{t_1, \dots, t_m\}$, $u \in T_i$ and $c \in \mathrm{val}(K^\times)$ such that

- for all $j \in \{1, \dots, m\}$, $\mathrm{lt}(t_j h_j) = c_j u$ with $\mathrm{val}(c_j) = c$
- $\mathrm{lt}(\sum_{i=1}^m t_j h_j) < c_1 u$.

Then there are elements $d_j \in K$, $v_j \in U(i, h_j, h_{j+1})$ for $1 \le j \le m-1$ and $t'_m \in K\{\mathbf{X}; P\}$ such that:

1. $\sum_{j=1}^m t_j h_j = \sum_{j=1}^{m-1} d_j \frac{u}{v_j} S(i, h_j, h_{j+1}, v_j) + t'_m h_m$.
2. $\mathrm{val}_P(t'_m h_m) > \mathrm{val}_P(u c_1)$.
3. $\frac{u}{v_j} \in T_i$ for all $j < m$.
4. For all $j < m$, $\mathrm{val}\left(d_j \mathrm{lc}_i(h_j) \mathrm{lc}_i(h_{j+1})\right) \ge c$.

Buchberger algorithm in $K\{\mathbf{X}; P\}$

input : $J = (h_1, \dots, h_m)$ an ideal of $K\{\mathbf{X}; P\}$
output: a Gröbner basis of J

$H \leftarrow \{h_1, \dots, h_m\}$; $B \leftarrow \{(h_i, h_j),\ 1 \leq i < j \leq m\}$
while $B \neq \emptyset$ **do**
  $(f, g) \leftarrow$ element of B; $B \leftarrow B \setminus \{(f, g)\}$;
  for $i \in I$ **do**
    $U(i, f, g) \leftarrow$ finite set of generators of $\mathrm{lm}_i(f)T_i(f) \cap \mathrm{lm}_i(g)T_i(g)$;
    for $v \in U(i, f, g)$ **do**
      $\_, r \leftarrow$ division$(S(i, f, g, v), H)$;
      if $r \neq 0$ **then**
        $B \leftarrow B \cup \{(h, r),\ h \in H\}$;
        $H \leftarrow H \cup \{r\}$
return H