Polynomial Ideals and Order Ideals

Sylvain Schmitz

based on joint work with Lia Schütze

Loop Invariants and Algebraic Reasoning, July 7, 2025

Outline

Hilbert's Basis Theorem

- involved e.g., in computing Zariski closures

order ideals

- over well-quasi-orders
- allows to derive complexity statements

connection

- illustration on polynomial automata
- invertible polynomial automata and the dimension of ideals
- what about Buchberger's algorithm?

Outline

Hilbert's Basis Theorem

- involved e.g., in computing Zariski closures

order ideals

- over well-quasi-orders
- allows to derive complexity statements

connection

- illustration on polynomial automata
- invertible polynomial automata and the dimension of ideals
- what about Buchberger's algorithm?

Outline

Hilbert's Basis Theorem

- involved e.g., in computing Zariski closures

order ideals

- over well-quasi-orders
- allows to derive complexity statements

connection

- illustration on polynomial automata
- invertible polynomial automata and the dimension of ideals
- what about Buchberger's algorithm?

Motivating Example

A loop with polynomial updates

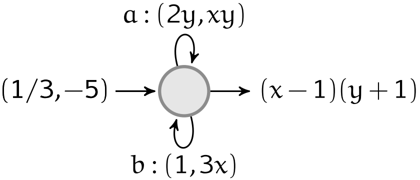
```
x := 1/3;
y := -5;
while (*) {
  choose
    (x,y) := (2y,y*x);
    or
    (x,y) := (1, 3x);
}
return (x-1)*(y+1);
```

Motivating Example

A loop with polynomial updates

```
x := 1/3;
y := -5;
while (*) {
  choose
    (x,y) := (2y,y*x);
    or
    (x,y) := (1, 3x);
}
return (x-1)*(y+1);
```

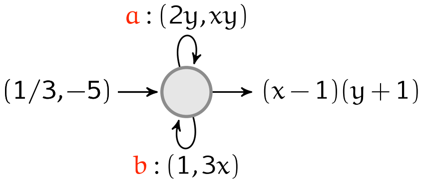
... seen as a polynomial automaton



Polynomial Automata

A polynomial automaton $\mathcal{A}$ of dimension d

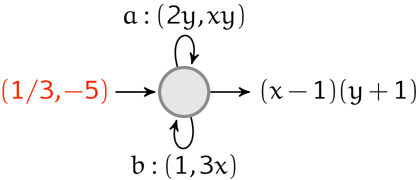
- finite alphabet Σ
- initial configuration $\alpha \in \mathbb{Q}^d$
- polynomial updates $(p_a)_{a \in \Sigma} : \mathbb{Q}^d \to \mathbb{Q}^d$
- polynomial output $\gamma : \mathbb{Q}^d \to \mathbb{Q}$



Polynomial Automata

A polynomial automaton $\mathcal{A}$ of dimension d

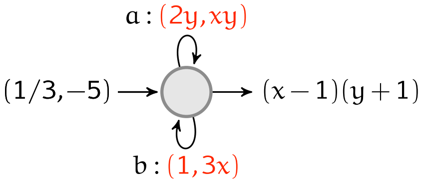
- finite alphabet Σ
- initial configuration $\alpha \in \mathbb{Q}^d$
- polynomial updates $(p_a)_{a \in \Sigma} : \mathbb{Q}^d \to \mathbb{Q}^d$
- polynomial output $\gamma : \mathbb{Q}^d \to \mathbb{Q}$



Polynomial Automata

A polynomial automaton $\mathcal{A}$ of dimension d

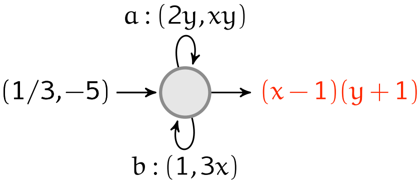
- finite alphabet Σ
- initial configuration $\alpha \in \mathbb{Q}^d$
- polynomial updates $(p_a)_{a\in\Sigma} \colon \mathbb{Q}^d \to \mathbb{Q}^d$
- polynomial output $\gamma \colon \mathbb{Q}^d \to \mathbb{Q}$



Polynomial Automata

A polynomial automaton $\mathcal{A}$ of dimension d

- finite alphabet Σ
- initial configuration $\alpha \in \mathbb{Q}^d$
- polynomial updates $(p_a)_{a\in\Sigma} \colon \mathbb{Q}^d \to \mathbb{Q}^d$
- polynomial output $\gamma \colon \mathbb{Q}^d \to \mathbb{Q}$



Zeroness of Polynomial Automata

Semantics

- $p_w \colon \mathbb{Q}^d \to \mathbb{Q}^d$ for $w \in \Sigma^*$

$$p_\varepsilon \stackrel{\text{def}}{=} \text{identity} \qquad\qquad p_{aw} \stackrel{\text{def}}{=} p_w \circ p_a$$

- $[\![\mathcal{A}]\!](w) \stackrel{\text{def}}{=} \gamma(p_w(\alpha))$

Zeroness

input polynomial automaton $\mathcal{A}$

question does $[\![\mathcal{A}]\!](w) = 0$ for all $w \in \Sigma^*$?

Zeroness of Polynomial Automata

Semantics

- $p_w : \mathbb{Q}^d \to \mathbb{Q}^d$ for $w \in \Sigma^*$

$$p_\varepsilon \stackrel{\text{def}}{=} \text{identity} \qquad\qquad p_{aw} \stackrel{\text{def}}{=} p_w \circ p_a$$

- $[\![\mathcal{A}]\!](w) \stackrel{\text{def}}{=} \gamma(p_w(\alpha))$

Zeroness

input polynomial automaton $\mathcal{A}$

question does $[\![\mathcal{A}]\!](w) = 0$ for all $w \in \Sigma^*$?

Zeroness of Polynomial Automata

Zeroness

input polynomial automaton $\mathcal{A}$

question does $[\![\mathcal{A}]\!](w) = 0$ for all $w \in \Sigma^*$?

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for polynomial automata is ACKERMANN-*complete.*

Zeroness of Polynomial Automata

Zeroness

input polynomial automaton $\mathcal{A}$

question does $[\![\mathcal{A}]\!](w) = 0$ for all $w \in \Sigma^*$?

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for polynomial automata is ACKERMANN*-complete.*

Corollary (Benedikt, Duff, Sharad, and Worrell, 2017)

The equivalence problem for polynomial automata is ACKERMANN*-complete.*

Analysing Polynomial Automata

(Benedikt et al., 2017)

Define polynomial ideals $J_0 \subsetneq J_1 \subsetneq \cdots$ by

$$J_k \stackrel{\text{def}}{=} \langle \gamma \circ p_w \mid w \in \Sigma^{\leqslant k} \rangle$$

Inductively,

$$J_0 = \langle \gamma \rangle$$
$$J_{k+1} = \langle f \circ p_a \mid f \in J_k, a \in \Sigma \cup \{\varepsilon\} \rangle$$

By Hilbert's Basis Theorem, this stabilises to

$$J_* = \langle \gamma \circ p_w \mid w \in \Sigma^* \rangle$$

and we can detect stabilisation using reduced Gröbner bases for the J_k.

Proposition

Benedikt et al., 2017 $[\![\mathcal{A}]\!](w) = 0$ *for all* $w \in \Sigma^*$ *iff* $\alpha \in \mathbf{V}(J_*)$.

Analysing Polynomial Automata

(Benedikt et al., 2017)

Define polynomial ideals $J_0 \subsetneq J_1 \subsetneq \cdots$ by

$$J_k \stackrel{\text{def}}{=} \langle \gamma \circ p_w \mid w \in \Sigma^{\leqslant k} \rangle$$

Inductively,

$$J_0 = \langle \gamma \rangle$$
$$J_{k+1} = \langle f \circ p_a \mid f \in J_k, a \in \Sigma \cup \{\varepsilon\} \rangle$$

By Hilbert's Basis Theorem, this stabilises to

$$J_* = \langle \gamma \circ p_w \mid w \in \Sigma^* \rangle$$

and we can detect stabilisation using reduced Gröbner bases for the J_k.

Proposition

Benedikt et al., 2017 $[\![\mathcal{A}]\!](w) = 0$ *for all* $w \in \Sigma^*$ *iff* $\alpha \in \mathbf{V}(J_*)$.

Analysing Polynomial Automata

(Benedikt et al., 2017)

Define polynomial ideals $J_0 \subsetneq J_1 \subsetneq \cdots$ by

$$J_k \stackrel{\text{def}}{=} \langle \gamma \circ p_w \mid w \in \Sigma^{\leqslant k} \rangle$$

Inductively,

$$J_0 = \langle \gamma \rangle$$
$$J_{k+1} = \langle f \circ p_a \mid f \in J_k, a \in \Sigma \cup \{\varepsilon\} \rangle$$

By Hilbert's Basis Theorem, this stabilises to

$$J_* = \langle \gamma \circ p_w \mid w \in \Sigma^* \rangle$$

and we can detect stabilisation using reduced Gröbner bases for the J_k.

Proposition

Benedikt et al., 2017 $[\![\mathcal{A}]\!](w) = 0$ *for all* $w \in \Sigma^*$ *iff* $\alpha \in \mathbf{V}(J_*)$.

- thus zeroness is decidable
- what about complexity upper bounds?
- turn to order ideals

- thus zeroness is decidable
- what about complexity upper bounds?
- turn to order ideals

- thus zeroness is decidable
- what about complexity upper bounds?
- turn to order ideals

Descending Chains

over a wqo

- well-quasi-order $(X, \leqslant)$: every descending chain of downwards-closed sets is finite
- $(\mathbb{N}, \sqsubseteq)$ is a wqo by Dickson's Lemma

Descending Chains

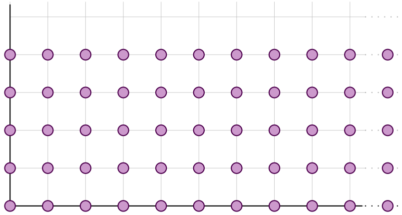
over a wqo

- well-quasi-order $(X, \leqslant)$: every descending chain of downwards-closed sets is finite
- $(\mathbb{N}, \sqsubseteq)$ is a wqo by Dickson's Lemma

Descending Chains

over a wqo

- well-quasi-order $(X, \leqslant)$: every descending chain of downwards-closed sets is finite
- $(\mathbb{N}, \sqsubseteq)$ is a wqo by Dickson's Lemma

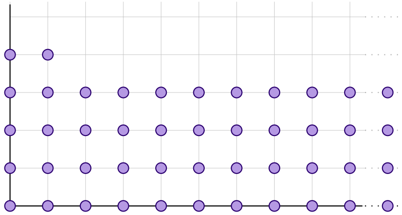


D_0

Descending Chains

over a wqo

- well-quasi-order $(X, \leqslant)$: every descending chain of downwards-closed sets is finite
- $(\mathbb{N}, \sqsubseteq)$ is a wqo by Dickson's Lemma

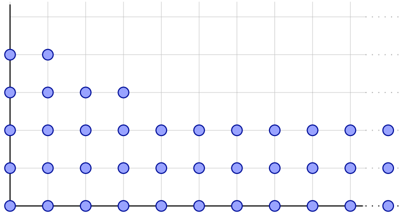


$D_0 \supsetneq D_1$

Descending Chains

over a wqo

- well-quasi-order $(X, \leqslant)$: every descending chain of downwards-closed sets is finite
- $(\mathbb{N}, \sqsubseteq)$ is a wqo by Dickson's Lemma

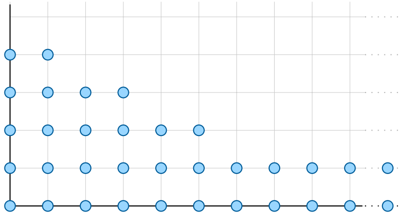


$D_0 \supsetneq D_1 \supsetneq D_2$

Descending Chains

over a wqo

- well-quasi-order $(X, \leqslant)$: every descending chain of downwards-closed sets is finite
- $(\mathbb{N}, \sqsubseteq)$ is a wqo by Dickson's Lemma

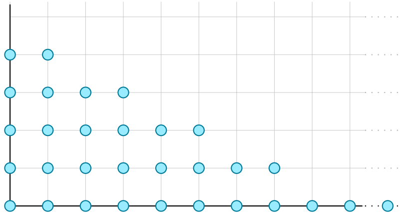


$D_0 \supsetneq D_1 \supsetneq D_2 \supsetneq D_3$

Descending Chains

over a wqo

- well-quasi-order $(X, \leqslant)$: every descending chain of downwards-closed sets is finite
- $(\mathbb{N}, \sqsubseteq)$ is a wqo by Dickson's Lemma

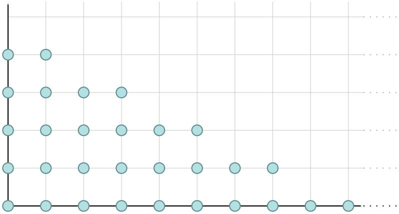


$D_0 \supsetneq D_1 \supsetneq D_2 \supsetneq D_3 \supsetneq D_4$

Descending Chains

over a wqo

- well-quasi-order $(X, \leqslant)$: every descending chain of downwards-closed sets is finite
- $(\mathbb{N}, \sqsubseteq)$ is a wqo by Dickson's Lemma

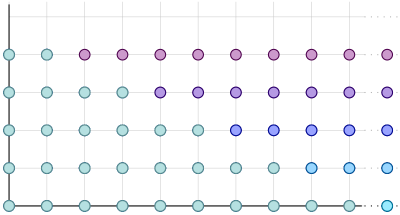


$D_0 \supsetneq D_1 \supsetneq D_2 \supsetneq D_3 \supsetneq D_4 \supsetneq D_5$

Descending Chains

over a wqo

- well-quasi-order $(X, \leqslant)$: every descending chain of downwards-closed sets is finite
- $(\mathbb{N}, \sqsubseteq)$ is a wqo by Dickson's Lemma

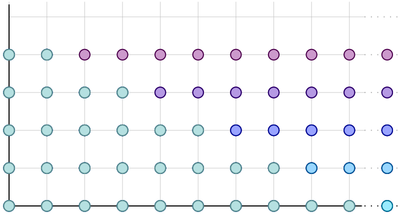


$$D_0 \supsetneq D_1 \supsetneq D_2 \supsetneq D_3 \supsetneq D_4 \supsetneq D_5$$

Descending Chains

over a wqo

- well-quasi-order $(X, \leqslant)$: every descending chain of downwards-closed sets is finite
- $(\mathbb{N}, \sqsubseteq)$ is a wqo by Dickson's Lemma



$D_0 \supsetneq D_1 \supsetneq D_2 \supsetneq D_3 \supsetneq D_4 \supsetneq D_5$

Order Ideals

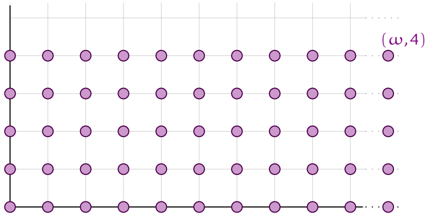
- downwards-closed sets over a wqo have a unique decomposition as finite unions of ideals
- ideals are the irreducible downwards-closed sets: $I \subseteq D_1 \cup D_2$ implies $I \subseteq D_1$ or $I \subseteq D_2$
- over $\mathbb{N}^d$: ideals represented as vectors in $(\mathbb{N} \cup \{\omega\})^d$

Order Ideals

- downwards-closed sets over a wqo have a unique decomposition as finite unions of ideals
- ideals are the irreducible downwards-closed sets: $I \subseteq D_1 \cup D_2$ implies $I \subseteq D_1$ or $I \subseteq D_2$
- over $\mathbb{N}^d$: ideals represented as vectors in $(\mathbb{N} \cup \{\omega\})^d$

Order Ideals

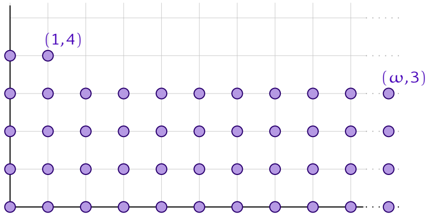
- downwards-closed sets over a wqo have a unique decomposition as finite unions of ideals
- ideals are the irreducible downwards-closed sets: $I \subseteq D_1 \cup D_2$ implies $I \subseteq D_1$ or $I \subseteq D_2$
- over $\mathbb{N}^d$: ideals represented as vectors in $(\mathbb{N} \cup \{\omega\})^d$



$D_0 = \{(\omega, 4)\}$

Order Ideals

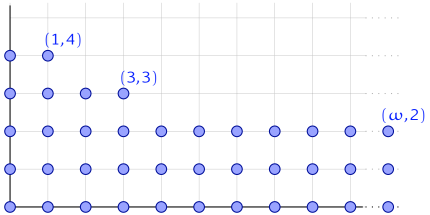
- downwards-closed sets over a wqo have a unique decomposition as finite unions of ideals
- ideals are the irreducible downwards-closed sets: $I \subseteq D_1 \cup D_2$ implies $I \subseteq D_1$ or $I \subseteq D_2$
- over $\mathbb{N}^d$: ideals represented as vectors in $(\mathbb{N} \cup \{\omega\})^d$



$D_1 = \{(1,4),(\omega,3)\}$

Order Ideals

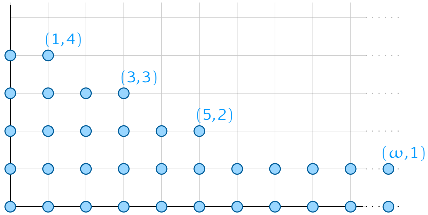
- downwards-closed sets over a wqo have a unique decomposition as finite unions of ideals
- ideals are the irreducible downwards-closed sets: $I \subseteq D_1 \cup D_2$ implies $I \subseteq D_1$ or $I \subseteq D_2$
- over $\mathbb{N}^d$: ideals represented as vectors in $(\mathbb{N} \cup \{\omega\})^d$



$D_2 = \{(1,4),(3,3),(\omega,2)\}$

Order Ideals

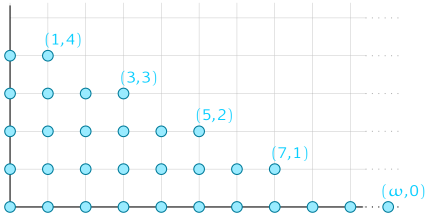
- downwards-closed sets over a wqo have a unique decomposition as finite unions of ideals
- ideals are the irreducible downwards-closed sets: $I \subseteq D_1 \cup D_2$ implies $I \subseteq D_1$ or $I \subseteq D_2$
- over $\mathbb{N}^d$: ideals represented as vectors in $(\mathbb{N} \cup \{\omega\})^d$



$$D_3 = \{(1,4),(3,3),(5,2),(\omega,1)\}$$

Order Ideals

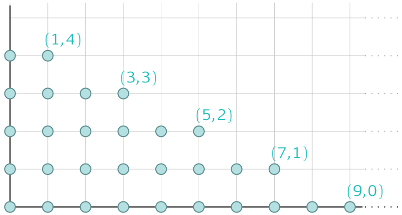
- downwards-closed sets over a wqo have a unique decomposition as finite unions of ideals
- ideals are the irreducible downwards-closed sets: $I \subseteq D_1 \cup D_2$ implies $I \subseteq D_1$ or $I \subseteq D_2$
- over $\mathbb{N}^d$: ideals represented as vectors in $(\mathbb{N} \cup \{\omega\})^d$



$$D_4 = \{(1,4),(3,3),(5,2),(7,1),(\omega,0)\}$$

Order Ideals

- downwards-closed sets over a wqo have a unique decomposition as finite unions of ideals
- ideals are the irreducible downwards-closed sets: $I \subseteq D_1 \cup D_2$ implies $I \subseteq D_1$ or $I \subseteq D_2$
- over $\mathbb{N}^d$: ideals represented as vectors in $(\mathbb{N} \cup \{\omega\})^d$



$$D_5 = \{(1,4),(3,3),(5,2),(7,1),(9,0)\}$$

Dimension of Ideals over $\mathbb{N}^d$

For an ideal I seen as a vector in $(\mathbb{N} \cup \{\omega\})^d$

$$\omega(I) \stackrel{\text{def}}{=} \{1 \leqslant i \leqslant d \mid I(i) = \omega\}$$
$$\dim I \stackrel{\text{def}}{=} |\omega(I)|$$

Example

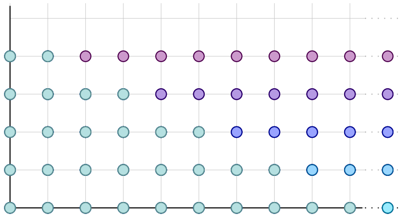
For $d = 3$, $\omega((2,10,\omega)) = \{3\}$ and $\dim(2,10,\omega) = 1$.

Monotonicity

[Lazić and S., 2021]

- at every step k, since $D_k \supsetneq D_{k+1}$, there must exist an ideal in D_k but not in D_{k+1}: we say it is proper at step k
- the chain is strongly monotone if, $\forall I_{k+1}$ proper at step $k+1$, $\exists I_k$ proper at step k s.t.

$$\dim I_{k+1} \leqslant \dim I_k$$



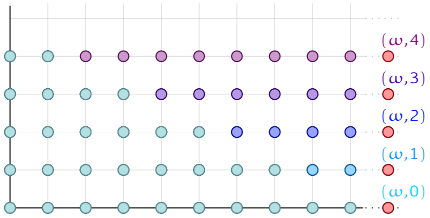
$D_0 \supsetneq D_1 \supsetneq D_2 \supsetneq D_3 \supsetneq D_4 \supsetneq D_5$

MONOTONICITY

[Lazić and S., 2021]

- at every step k, since $D_k \supsetneq D_{k+1}$, there must exist an ideal in D_k but not in D_{k+1}: we say it is proper at step k
- the chain is strongly monotone if, $\forall I_{k+1}$ proper at step $k+1$, $\exists I_k$ proper at step k s.t.

$$\dim I_{k+1} \leqslant \dim I_k$$



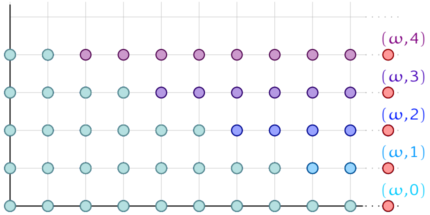
$$D_0 \supsetneq D_1 \supsetneq D_2 \supsetneq D_3 \supsetneq D_4 \supsetneq D_5$$

Monotonicity

[Lazić and S., 2021]

- at every step k, since $D_k \supsetneq D_{k+1}$, there must exist an ideal in D_k but not in D_{k+1}: we say it is proper at step k
- the chain is ω- monotone if, $\forall I_{k+1}$ proper at step $k+1$, $\exists I_k$ proper at step k s.t.

$$\omega(I_{k+1}) \subseteq \omega(I_k)$$



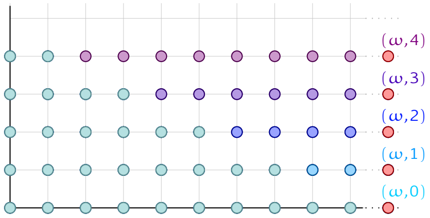
$$D_0 \supsetneq D_1 \supsetneq D_2 \supsetneq D_3 \supsetneq D_4 \supsetneq D_5$$

Monotonicity

[Novikov and Yakovenko, 1999; Benedikt et al., 2017]

- at every step k, since $D_k \supsetneq D_{k+1}$, there must exist an ideal in D_k but not in D_{k+1}: we say it is proper at step k
- the chain is strongly monotone if, $\forall I_{k+1}$ proper at step $k+1$, $\exists I_k$ proper at step k s.t.

$$\dim I_{k+1} \leqslant \dim I_k$$



$D_0 \supsetneq D_1 \supsetneq D_2 \supsetneq D_3 \supsetneq D_4 \supsetneq D_5$

The Length of Descending Chains

Issue

The length can be arbitrary (also for strongly monotone chains): for all n,

$$\{(0,\omega)\} \supsetneq \{(0,n)\} \supsetneq \{(0,n-1)\} \supsetneq \cdots \supsetneq \{(0,1)\} \supsetneq \{(0,0)\}$$

Control

$$|D| \stackrel{\text{def}}{=} \max_{I \in D} |I|$$

$$|I| \stackrel{\text{def}}{=} \max_{i \notin \omega(I)} I(i)$$

For $g \colon \mathbb{N} \to \mathbb{N}$ and $n_0 \in \mathbb{N}$: a chain $D_0 \supsetneq D_1 \supsetneq \cdots$ is (g, n_0)-controlled if, $\forall k$,

$$|D_k| \leqslant g^k(n_0)$$

The Length of Descending Chains

Issue

The length can be arbitrary (also for strongly monotone chains): for all n,

$$\{(0,\omega)\} \supsetneq \{(0,n)\} \supsetneq \{(0,n-1)\} \supsetneq \cdots \supsetneq \{(0,1)\} \supsetneq \{(0,0)\}$$

Control

$$|D| \stackrel{\text{def}}{=} \max_{I \in D} |I|$$

$$|I| \stackrel{\text{def}}{=} \max_{i \notin \omega(I)} I(i)$$

For $g\colon \mathbb{N} \to \mathbb{N}$ and $n_0 \in \mathbb{N}$: a chain $D_0 \supsetneq D_1 \supsetneq \cdots$ is (g,n_0)-controlled if, $\forall k$,

$$|D_k| \leqslant g^k(n_0)$$

The Length of Descending Chains

Issue

The length can be arbitrary (also for strongly monotone chains): for all n,

$$\{(0,\omega)\} \supsetneq \{(0,n)\} \supsetneq \{(0,n-1)\} \supsetneq \cdots \supsetneq \{(0,1)\} \supsetneq \{(0,0)\}$$

Control

$$|D| \stackrel{\text{def}}{=} \max_{I \in D} |I|$$

$$|I| \stackrel{\text{def}}{=} \max_{i \notin \omega(I)} I(i)$$

For $g\colon \mathbb{N} \to \mathbb{N}$ and $n_0 \in \mathbb{N}$: a chain $D_0 \supsetneq D_1 \supsetneq \cdots$ is (g, n_0)-controlled if, $\forall k$,

$$|D_k| \leqslant g^k(n_0)$$

The Length of Descending Chains

Issue

The length can be arbitrary (also for strongly monotone chains): for all n,

$$\{(0,\omega)\} \supsetneq \{(0,n)\} \supsetneq \{(0,n-1)\} \supsetneq \cdots \supsetneq \{(0,1)\} \supsetneq \{(0,0)\}$$

Control

$$|D| \stackrel{\text{def}}{=} \max_{I \in D} |I|$$

$$|I| \stackrel{\text{def}}{=} \max_{i \notin \omega(I)} I(i)$$

For $g \colon \mathbb{N} \to \mathbb{N}$ and $n_0 \in \mathbb{N}$: a chain $D_0 \supsetneq D_1 \supsetneq \cdots$ is (g, n_0)-controlled if, $\forall k$,

$$|D_k| \leqslant g^k(n_0)$$

The Length of Descending Chains

Control

$$|D| \stackrel{\text{def}}{=} \max_{I \in D} |I|$$

$$|I| \stackrel{\text{def}}{=} \max_{i \notin \omega(I)} I(i)$$

For $g\colon \mathbb{N} \to \mathbb{N}$ and $n_0 \in \mathbb{N}$: a chain $D_0 \supsetneq D_1 \supsetneq \cdots$ is (g, n_0)-controlled if, $\forall k$,

$$|D_k| \leqslant g^k(n_0)$$

Example (Vector Addition Systems)

The descending chains in the dual backward coverability algorithm are ω-monotone and (g, n_0)-controlled by

$$g(x) \stackrel{\text{def}}{=} x + n \qquad n_0 \stackrel{\text{def}}{=} n$$

(n the size of the coverability instance)

The Length of Descending Chains

Example (Vector Addition Systems)

The descending chains in the dual backward coverability algorithm are ω-monotone and (g, n_0)-controlled by

$$g(x) \stackrel{\text{def}}{=} x + n \qquad\qquad n_0 \stackrel{\text{def}}{=} n$$

(n the size of the coverability instance)

Theorem (Length function theorem (Lazić and S., 2021))

(g, n)-controlled descending chains over $(\mathbb{N}^d, \sqsubseteq)$ for g primitive-recursive are of length bounded by

$$F_{\mathcal{O}(d)}(n)$$

in the fast-growing hierarchy.

The Length of Descending Chains

Theorem (Length function theorem (Lazić and S., 2021))

(g, n)-controlled descending chains over $(\mathbb{N}^d, \sqsubseteq)$ for g primitive-recursive are of length bounded by

$$F_{\mathcal{O}(d)}(n)$$

in the fast-growing hierarchy.

Theorem (Length function theorem (S. and Schütze, 2024))

Strongly monotone (g, n)-controlled descending chains over $(\mathbb{N}^d, \sqsubseteq)$ for $g(x) \stackrel{\text{def}}{=} x + n$ are of length bounded by

$$n^{2^{\mathcal{O}(d)}} .$$

The Length of Descending Chains

Theorem (Length function theorem (S. and Schütze, 2024))

Strongly monotone (g,n)-controlled descending chains over $(\mathbb{N}^d, \sqsubseteq)$ for $g(x) \stackrel{\text{def}}{=} x + n$ are of length bounded by

$$n^{2^{\mathcal{O}(d)}}.$$

Remark ((S. and Schütze, 2024))

Strongly monotone (g,n)-controlled descending chains over $(\mathbb{N}^d, \sqsubseteq)$ for $g(x) \stackrel{\text{def}}{=} x \cdot n$ are of length bounded by

$$(dn)^d \uparrow\uparrow d\,,$$

i.e., a tower of exponentials of height $d+1$.

Setup

- work over an algebraically closed field $\mathbb{A}$
- multivariate polynomials over $\mathbf{x} = x_1, \ldots, x_d$
- monomial $x_1^{u_1} \cdots x_d^{u_d}$ written as $\mathbf{x}^{\mathbf{u}}$ for $\mathbf{u} = u_1, \ldots, u_d \in \mathbb{N}^d$
- monomial ordering $\preceq$ over $\mathbb{N}^d$ that is graded:
  $\sum_{1 \leqslant i \leqslant d} \mathbf{u}(i) < \sum_{1 \leqslant i \leqslant d} \mathbf{u}'(i)$ implies $\mathbf{u} \prec \mathbf{u}'$

Setup

- work over an algebraically closed field $\mathbb{A}$
- multivariate polynomials over $\mathbf{x} = x_1, \ldots, x_d$
- monomial $x_1^{u_1} \cdots x_d^{u_d}$ written as $\mathbf{x}^{\mathbf{u}}$ for $\mathbf{u} = u_1, \ldots, u_d \in \mathbb{N}^d$
- monomial ordering $\preceq$ over $\mathbb{N}^d$ that is graded: $\sum_{1 \leqslant i \leqslant d} \mathbf{u}(i) < \sum_{1 \leqslant i \leqslant d} \mathbf{u}'(i)$ implies $\mathbf{u} \prec \mathbf{u}'$

Setup

- work over an algebraically closed field $\mathbb{A}$
- multivariate polynomials over $\boldsymbol{x} = x_1, \dots, x_d$
- monomial $x_1^{u_1} \cdots x_d^{u_d}$ written as $\boldsymbol{x}^{\boldsymbol{u}}$ for $\boldsymbol{u} = u_1, \dots, u_d \in \mathbb{N}^d$
- monomial ordering $\preceq$ over $\mathbb{N}^d$ that is graded: $\sum_{1 \leqslant i \leqslant d} \boldsymbol{u}(i) < \sum_{1 \leqslant i \leqslant d} \boldsymbol{u}'(i)$ implies $\boldsymbol{u} \prec \boldsymbol{u}'$

Setup

- work over an algebraically closed field $\mathbb{A}$
- multivariate polynomials over $\mathbf{x} = x_1, \ldots, x_d$
- monomial $x_1^{u_1} \cdots x_d^{u_d}$ written as $\mathbf{x}^{\mathbf{u}}$ for $\mathbf{u} = u_1, \ldots, u_d \in \mathbb{N}^d$
- monomial ordering $\preceq$ over $\mathbb{N}^d$ that is graded:
  $\sum_{1 \leqslant i \leqslant d} \mathbf{u}(i) < \sum_{1 \leqslant i \leqslant d} \mathbf{u}'(i)$ implies $\mathbf{u} \prec \mathbf{u}'$

Leading Monomials and Multidegrees

- for a polynomial $f = \sum_{u \in \mathbb{N}^d} c_u x^u$ in $\mathbb{A}[x]$,

$$\mathrm{multideg}(f) \stackrel{\text{def}}{=} \max_{\preceq}\{u \in \mathbb{N}^d \mid c_u \neq 0\} \quad \mathrm{LM}(f) \stackrel{\text{def}}{=} x^{\mathrm{multideg}(f)}$$

- for $J \subseteq \mathbb{A}[x]$,

$$\mathrm{multideg}(J) \stackrel{\text{def}}{=} \{\mathrm{multideg}(f) \mid f \in J\} \quad \mathrm{LM}(J) \stackrel{\text{def}}{=} \{\mathrm{LM}(f) \mid f \in J\}$$

Definition

Associate to any polynomial ideal $J \subseteq \mathbb{A}[x]$ its downwards-closed set

$$D \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(J)$$

Leading Monomials and Multidegrees

- for a polynomial $f = \sum_{u \in \mathbb{N}^d} c_u x^u$ in $\mathbb{A}[x]$,

$$\mathrm{multideg}(f) \stackrel{\text{def}}{=} \max_{\preceq}\{u \in \mathbb{N}^d \mid c_u \neq 0\} \quad \mathrm{LM}(f) \stackrel{\text{def}}{=} x^{\mathrm{multideg}(f)}$$

- for $J \subseteq \mathbb{A}[x]$,

$$\mathrm{multideg}(J) \stackrel{\text{def}}{=} \{\mathrm{multideg}(f) \mid f \in J\} \quad \mathrm{LM}(J) \stackrel{\text{def}}{=} \{\mathrm{LM}(f) \mid f \in J\}$$

Definition
Associate to any polynomial ideal $J \subseteq \mathbb{A}[x]$ its downwards-closed set

$$D \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(J)$$

Leading Monomials and Multidegrees

- for a polynomial $f = \sum_{u \in \mathbb{N}^d} c_u x^u$ in $\mathbb{A}[x]$,

$$\mathrm{multideg}(f) \stackrel{\text{def}}{=} \max_{\preceq}\{u \in \mathbb{N}^d \mid c_u \neq 0\} \quad \mathrm{LM}(f) \stackrel{\text{def}}{=} x^{\mathrm{multideg}(f)}$$

- for $J \subseteq \mathbb{A}[x]$,

$$\mathrm{multideg}(J) \stackrel{\text{def}}{=} \{\mathrm{multideg}(f) \mid f \in J\} \quad \mathrm{LM}(J) \stackrel{\text{def}}{=} \{\mathrm{LM}(f) \mid f \in J\}$$

Definition

Associate to any polynomial ideal $J \subseteq \mathbb{A}[x]$ its downwards-closed set

$$D \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(J)$$

Leading Monomials and Multidegrees

Definition

Associate to any polynomial ideal $J \subseteq \mathbb{A}[x]$ its downwards-closed set

$$D \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \operatorname{multideg}(J)$$

Remark

For a Gröbner basis G *of* J, $\langle \mathrm{LM}(G) \rangle = \langle \mathrm{LM}(J) \rangle$, *thus equivalently*

$$D \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \operatorname{multideg}(\mathrm{LM}(\mathrm{Grobner}(J)))$$

General Complexity Upper Bound

Benedikt et al., 2017

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for polynomial automata is in ACKERMANN.

- $J_0 \subsetneq J_1 \subsetneq \cdots \subseteq J_*$ yields $D_0 \supsetneq D_1 \supsetneq \cdots \supseteq D_*$ where $D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \text{multideg}(J_k)$
- Dubé (1990): degree bound of $2(t+1)^{2^d}$ on Gröbner bases of $\langle f_1, \ldots, f_m \rangle$ where the f_i have total degree $\leqslant t$
- Benedikt et al. (2017, Prop. 4) the chain is (g, n)-controlled for $n \stackrel{\text{def}}{=} 2(t+1)^{2^d}$ and $g(x) \stackrel{\text{def}}{=} x \cdot n$
- apply the length function theorem for descending chains: g is primitive-recursive, thus $F_{\mathcal{O}(d)}$ upper bound

General Complexity Upper Bound

Benedikt et al., 2017

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for polynomial automata is in ACKERMANN.

- $J_0 \subsetneq J_1 \subsetneq \cdots \subseteq J_*$ yields $D_0 \supsetneq D_1 \supsetneq \cdots \supseteq D_*$ where $D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(J_k)$
- Dubé (1990): degree bound of $2(t+1)^{2^d}$ on Gröbner bases of $\langle f_1, \ldots, f_m \rangle$ where the f_i have total degree $\leqslant t$
- Benedikt et al. (2017, Prop. 4) the chain is (g, n)-controlled for $n \stackrel{\text{def}}{=} 2(t+1)^{2^d}$ and $g(x) \stackrel{\text{def}}{=} x \cdot n$
- apply the length function theorem for descending chains: g is primitive-recursive, thus $F_{\mathcal{O}(d)}$ upper bound

General Complexity Upper Bound

Benedikt et al., 2017

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for polynomial automata is in ACKERMANN.

- $J_0 \subsetneq J_1 \subsetneq \cdots \subseteq J_*$ yields $D_0 \supsetneq D_1 \supsetneq \cdots \supseteq D_*$ where $D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \text{multideg}(J_k)$
- Dubé (1990): degree bound of $2(t+1)^{2^d}$ on Gröbner bases of $\langle f_1, \ldots, f_m \rangle$ where the f_i have total degree $\leqslant t$
- Benedikt et al. (2017, Prop. 4) the chain is (g, n)-controlled for $n \stackrel{\text{def}}{=} 2(t+1)^{2^d}$ and $g(x) \stackrel{\text{def}}{=} x \cdot n$
- apply the length function theorem for descending chains: g is primitive-recursive, thus $F_{\mathcal{O}(d)}$ upper bound

General Complexity Upper Bound

Benedikt et al., 2017

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for polynomial automata is in ACKERMANN.

- $J_0 \subsetneq J_1 \subsetneq \cdots \subseteq J_*$ yields $D_0 \supsetneq D_1 \supsetneq \cdots \supseteq D_*$ where $D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(J_k)$
- Dubé (1990): degree bound of $2(t+1)^{2^d}$ on Gröbner bases of $\langle f_1, \ldots, f_m \rangle$ where the f_i have total degree $\leqslant t$
- Benedikt et al. (2017, Prop. 4) the chain is (g, n)-controlled for $n \stackrel{\text{def}}{=} 2(t+1)^{2^d}$ and $g(x) \stackrel{\text{def}}{=} x \cdot n$
- apply the length function theorem for descending chains: g is primitive-recursive, thus $F_{\mathcal{O}(d)}$ upper bound

General Complexity Upper Bound

Benedikt et al., 2017

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for polynomial automata is in ACKERMANN.

- $J_0 \subsetneq J_1 \subsetneq \cdots \subseteq J_*$ yields $D_0 \supsetneq D_1 \supsetneq \cdots \supseteq D_*$ where $D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(J_k)$
- Dubé (1990): degree bound of $2(t+1)^{2^d}$ on Gröbner bases of $\langle f_1, \ldots, f_m \rangle$ where the f_i have total degree $\leqslant t$
- Benedikt et al. (2017, Prop. 4) the chain is (g,n)-controlled for $n \stackrel{\text{def}}{=} 2(t+1)^{2^d}$ and $g(x) \stackrel{\text{def}}{=} x \cdot n$
- apply the length function theorem for descending chains: g is primitive-recursive, thus $F_{\mathcal{O}(d)}$ upper bound

- complexity upper bound from the length function theorem on descending chains over $\mathbb{N}^d$
- can we exploit the improved bounds for strongly monotone descending chains?

Dimension of an Algebraic Variety

- multiple equivalent definitions
- over an algebraically closed field with a graded monomial ordering, for a variety $V \subseteq \mathbb{A}^d$:

  $\dim V \stackrel{\text{def}}{=} \max\{\dim I \mid I \text{ order ideal s.t. } I \subseteq \mathbb{N}^d \setminus \text{multideg}(\mathbf{I}(V))\}$

Monotonicity Redux

Consider a descending chain $V_0 \supsetneq V_1 \supsetneq \cdots$ of varieties.

- each V_k is a finite union of incomparable irreducible varieties
- an irreducible variety at step k is proper if it appears in V_k but not V_{k+1}
- $V_0 \supsetneq V_1 \supsetneq \cdots$ is strongly monotone if, $\forall W_{k+1}$ proper at step $k+1$, $\exists W_k$ proper at step k s.t. $\dim W_{k+1} \leqslant \dim W_k$

Proposition

Let $V_0 \supsetneq V_1 \supsetneq \cdots$ be a descending chain of varieties and $D_0 \supsetneq D_1 \supsetneq \cdots$ the corresponding descending chain of downwards-closed sets $D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \text{multideg}(\mathbf{I}(V_k))$. Then one is strongly monotone iff the other is strongly monotone.

Monotonicity Redux

Consider a descending chain $V_0 \supsetneq V_1 \supsetneq \cdots$ of varieties.

- each V_k is a finite union of incomparable irreducible varieties
- an irreducible variety at step k is proper if it appears in V_k but not V_{k+1}
- $V_0 \supsetneq V_1 \supsetneq \cdots$ is strongly monotone if, $\forall W_{k+1}$ proper at step $k+1$, $\exists W_k$ proper at step k s.t. $\dim W_{k+1} \leqslant \dim W_k$

Proposition

Let $V_0 \supsetneq V_1 \supsetneq \cdots$ be a descending chain of varieties and $D_0 \supsetneq D_1 \supsetneq \cdots$ the corresponding descending chain of downwards-closed sets $D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \text{multideg}(\mathbf{I}(V_k))$. Then one is strongly monotone iff the other is strongly monotone.

Monotonicity Redux

Consider a descending chain $V_0 \supsetneq V_1 \supsetneq \cdots$ of varieties.

- each V_k is a finite union of incomparable irreducible varieties
- an irreducible variety at step k is proper if it appears in V_k but not V_{k+1}
- $V_0 \supsetneq V_1 \supsetneq \cdots$ is strongly monotone if, $\forall W_{k+1}$ proper at step $k+1$, $\exists W_k$ proper at step k s.t. $\dim W_{k+1} \leqslant \dim W_k$

Proposition

Let $V_0 \supsetneq V_1 \supsetneq \cdots$ be a descending chain of varieties and $D_0 \supsetneq D_1 \supsetneq \cdots$ the corresponding descending chain of downwards-closed sets $D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(\mathbf{I}(V_k))$. Then one is strongly monotone iff the other is strongly monotone.

Monotonicity Redux

Consider a descending chain $V_0 \supsetneq V_1 \supsetneq \cdots$ of varieties.

- each V_k is a finite union of incomparable irreducible varieties
- an irreducible variety at step k is proper if it appears in V_k but not V_{k+1}
- $V_0 \supsetneq V_1 \supsetneq \cdots$ is strongly monotone if, $\forall W_{k+1}$ proper at step $k+1$, $\exists W_k$ proper at step k s.t. $\dim W_{k+1} \leqslant \dim W_k$

Proposition

Let $V_0 \supsetneq V_1 \supsetneq \cdots$ be a descending chain of varieties and $D_0 \supsetneq D_1 \supsetneq \cdots$ the corresponding descending chain of downwards-closed sets $D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(\mathbf{I}(V_k))$. Then one is strongly monotone iff the other is strongly monotone.

Monotonicity Redux

Consider a descending chain $V_0 \supsetneq V_1 \supsetneq \cdots$ of varieties.

- each V_k is a finite union of incomparable irreducible varieties
- an irreducible variety at step k is proper if it appears in V_k but not V_{k+1}
- $V_0 \supsetneq V_1 \supsetneq \cdots$ is strongly monotone if, $\forall W_{k+1}$ proper at step $k+1$, $\exists W_k$ proper at step k s.t. $\dim W_{k+1} \leqslant \dim W_k$

Proposition

Let $V_0 \supsetneq V_1 \supsetneq \cdots$ be a descending chain of varieties and $D_0 \supsetneq D_1 \supsetneq \cdots$ the corresponding descending chain of downwards-closed sets $D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(\mathbf{I}(V_k))$. Then one is strongly monotone iff the other is strongly monotone.

Invertible Polynomial Automata

Benedikt et al., 2017

- for each $a \in \Sigma$, p_a has a rational inverse $q_a \colon \mathbb{A}^d \to \mathbb{A}^d$
- consequence: each p_a and q_a preserves the dimension
- further consequence: $V_0 \supseteq V_1 \supseteq \cdots$ where $V_k \stackrel{\text{def}}{=} \mathbf{V}(J_k)$ is strongly monotone (Benedikt et al., 2017, Prop. 6)

Complexity Upper Bound

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for invertible polynomial automata is in TOWER.

- consider $V_0 \supseteq V_1 \supseteq \cdots$ and $D_0 \supseteq D_1 \supseteq \cdots$ where $V_k \stackrel{\text{def}}{=} \mathbf{V}(J_k)$ and
$$D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \text{multideg}(\mathbf{I}(V_k)) = \mathbb{N}^d \setminus \text{multideg}(\sqrt{J_k})$$
- Laplagne (2006): degree bound of $2(t+1)^{2^{\mathcal{O}(d^2)}}$ on Gröbner bases of $\sqrt{\langle f_1, \ldots, f_m \rangle}$ where the f_i have total degree $\leqslant t$
- the chain is (g, n)-controlled for $n \stackrel{\text{def}}{=} 2(t+1)^{2^{c \cdot d^2}}$ and $g(x) \stackrel{\text{def}}{=} x \cdot n$ for some c

Complexity Upper Bound

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for invertible polynomial automata is in TOWER.

- consider $V_0 \supseteq V_1 \supseteq \cdots$ and $D_0 \supseteq D_1 \supseteq \cdots$ where $V_k \stackrel{\text{def}}{=} \mathbf{V}(J_k)$ and

$$D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(\mathbf{I}(V_k)) = \mathbb{N}^d \setminus \mathrm{multideg}(\sqrt{J_k})$$

- Laplagne (2006): degree bound of $2(t+1)^{2^{\mathcal{O}(d^2)}}$ on Gröbner bases of $\sqrt{\langle f_1, \ldots, f_m \rangle}$ where the f_i have total degree $\leqslant t$
- the chain is (g,n)-controlled for $n \stackrel{\text{def}}{=} 2(t+1)^{2^{c \cdot d^2}}$ and $g(x) \stackrel{\text{def}}{=} x \cdot n$ for some c

Complexity Upper Bound

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for invertible polynomial automata is in TOWER.

- consider $V_0 \supseteq V_1 \supseteq \cdots$ and $D_0 \supseteq D_1 \supseteq \cdots$ where $V_k \stackrel{\text{def}}{=} \mathbf{V}(J_k)$ and

$$D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \text{multideg}(\mathbf{I}(V_k)) = \mathbb{N}^d \setminus \text{multideg}(\sqrt{J_k})$$

- Laplagne (2006): degree bound of $2(t+1)^{2^{\mathcal{O}(d^2)}}$ on Gröbner bases of $\sqrt{\langle f_1,\ldots,f_m\rangle}$ where the f_i have total degree $\leqslant t$

- the chain is (g,n)-controlled for $n \stackrel{\text{def}}{=} 2(t+1)^{2^{c\cdot d^2}}$ and $g(x) \stackrel{\text{def}}{=} x \cdot n$ for some c

Complexity Upper Bound

Theorem (Benedikt, Duff, Sharad, and Worrell, 2017)

The zeroness problem for invertible polynomial automata is in TOWER.

- consider $V_0 \supseteq V_1 \supseteq \cdots$ and $D_0 \supseteq D_1 \supseteq \cdots$ where $V_k \stackrel{\text{def}}{=} \mathbf{V}(J_k)$ and
$$D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \operatorname{multideg}(\mathbf{I}(V_k)) = \mathbb{N}^d \setminus \operatorname{multideg}(\sqrt{J_k})$$
- Laplagne (2006): degree bound of $2(t+1)^{2^{\mathcal{O}(d^2)}}$ on Gröbner bases of $\sqrt{\langle f_1, \ldots, f_m \rangle}$ where the f_i have total degree $\leqslant t$
- the chain is (g,n)-controlled for $n \stackrel{\text{def}}{=} 2(t+1)^{2^{c \cdot d^2}}$ and $g(x) \stackrel{\text{def}}{=} x \cdot n$ for some c

Complexity Upper Bound

- consider $V_0 \supseteq V_1 \supseteq \cdots$ and $D_0 \supseteq D_1 \supseteq \cdots$ where $V_k \stackrel{\text{def}}{=} \mathbf{V}(J_k)$ and

$$D_k \stackrel{\text{def}}{=} \mathbb{N}^d \setminus \mathrm{multideg}(\mathbf{I}(V_k)) = \mathbb{N}^d \setminus \mathrm{multideg}(\sqrt{J_k})$$

- Laplagne (2006): degree bound of $2(t+1)^{2^{\mathcal{O}(d^2)}}$ on Gröbner bases of $\sqrt{\langle f_1,\ldots,f_m\rangle}$ where the f_i have total degree $\leqslant t$
- the chain is (g,n)-controlled for $n \stackrel{\text{def}}{=} 2(t+1)^{2^{c\cdot d^2}}$ and $g(x) \stackrel{\text{def}}{=} x \cdot n$ for some c
- apply the length function theorem for strongly monotone descending chains: a tower of exponentials of height $d+1$ as upper bound

Outlook

- order ideals as a means to obtain complexity bounds for applications of Hilbert's Basis Theorem
- what about Gröbner basis computations, e.g., by Buchberger's algorithm or F4/F5? They essentially work by computing an ascending chain of polynomial ideals $\langle \mathrm{LM}(G_0)\rangle \subseteq \langle \mathrm{LM}(G_1)\rangle \subseteq \cdots$
  - they can be computed in exponential space (Kühnle and Mayr, 1996), but this relies on the degree bounds of Dubé (1990)
  - for Buchberger's algorithm, all we have are Ackermannian upper bounds (Dubé, Mishra, and Yap, 1995)!

Outlook

- order ideals as a means to obtain complexity bounds for applications of Hilbert's Basis Theorem
- what about Gröbner basis computations, e.g., by Buchberger's algorithm or F4/F5? They essentially work by computing an ascending chain of polynomial ideals $\langle \mathrm{LM}(G_0)\rangle \subseteq \langle \mathrm{LM}(G_1)\rangle \subseteq \cdots$
  - they can be computed in exponential space (Kühnle and Mayr, 1996), but this relies on the degree bounds of Dubé (1990)
  - for Buchberger's algorithm, all we have are Ackermannian upper bounds (Dubé, Mishra, and Yap, 1995)!

Outlook

- order ideals as a means to obtain complexity bounds for applications of Hilbert's Basis Theorem
- what about Gröbner basis computations, e.g., by Buchberger's algorithm or F4/F5? They essentially work by computing an ascending chain of polynomial ideals $\langle \mathrm{LM}(G_0)\rangle \subseteq \langle \mathrm{LM}(G_1)\rangle \subseteq \cdots$
  - they can be computed in exponential space (Kühnle and Mayr, 1996), but this relies on the degree bounds of Dubé (1990)
  - for Buchberger's algorithm, all we have are Ackermannian upper bounds (Dubé, Mishra, and Yap, 1995)!

Outlook

- order ideals as a means to obtain complexity bounds for applications of Hilbert's Basis Theorem
- what about Gröbner basis computations, e.g., by Buchberger's algorithm or F4/F5? They essentially work by computing an ascending chain of polynomial ideals $\langle \mathrm{LM}(G_0)\rangle \subseteq \langle \mathrm{LM}(G_1)\rangle \subseteq \cdots$
  - they can be computed in exponential space (Kühnle and Mayr, 1996), but this relies on the degree bounds of Dubé (1990)
  - for Buchberger's algorithm, all we have are Ackermannian upper bounds (Dubé, Mishra, and Yap, 1995)!