

Signature Gröbner Bases in Free Algebras over Rings

Clemens Hofstadler¹, Thibaut Verron²

ISSAC 2023

Tromsø, Norway, July 25th, 2023

1. Institute of Mathematics, University of Kassel, Germany
2. Institute for Algebra, Johannes Kepler University, Linz, Austria

U N I K A S S E L
V E R S I T Ä T

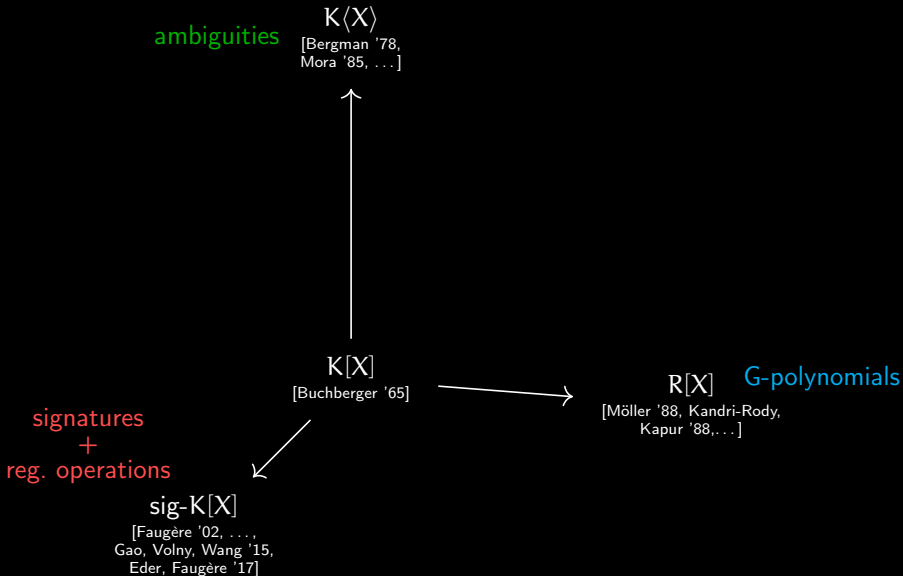
FWF

Der Wissenschaftsfonds.

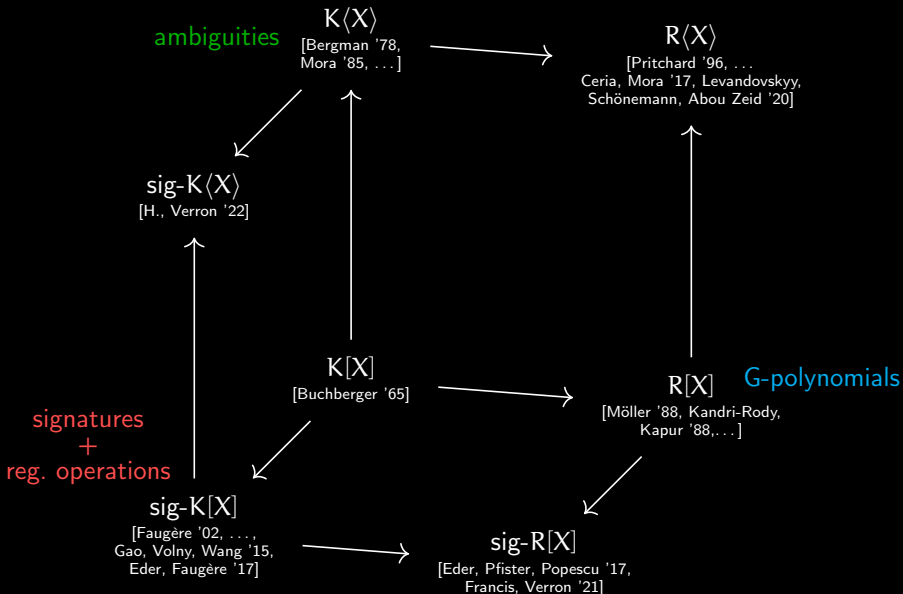
The (vast) world of Gröbner theories

$K[X]$
[Buchberger '65]

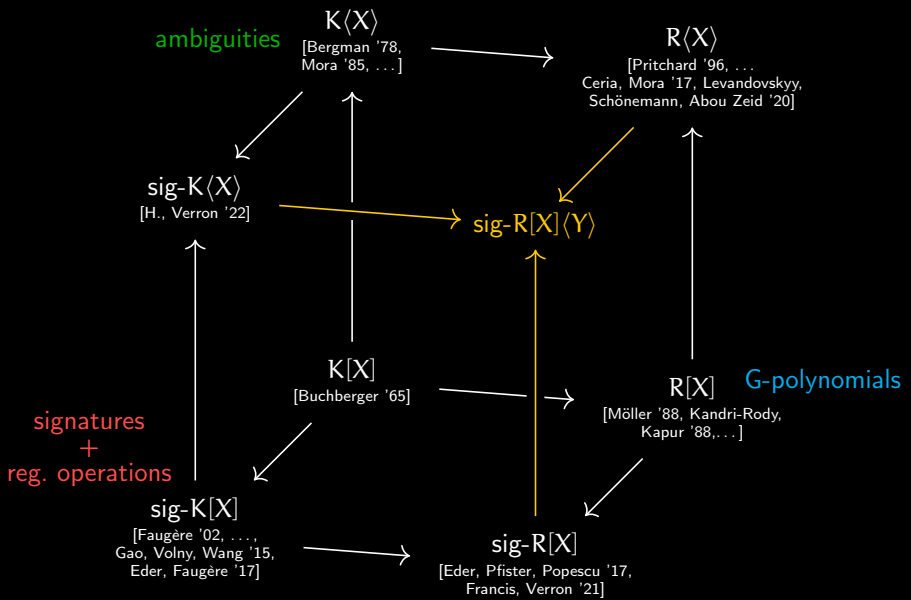
The (vast) world of Gröbner theories



The (vast) world of Gröbner theories



The (vast) world of Gröbner theories



Signature Gröbner Bases in ~~Free~~ Algebras over Rings Mixed

Clemens Hofstadler¹, Thibaut Verron²

ISSAC 2023

Tromsø, Norway, July 25th, 2023

1. Institute of Mathematics, University of Kassel, Germany
2. Institute for Algebra, Johannes Kepler University, Linz, Austria

U N I K A S S E L
V E R S I T Ä T

FWF

Der Wissenschaftsfonds.

The mixed algebra

[Mikhalev, Zolotykh '98]

Mixed algebra = $\mathbb{R}[X]\langle Y \rangle$

The mixed algebra

[Mikhalev, Zolotykh '98]

$$\text{Mixed algebra} = \mathbb{R}[X]\langle Y \rangle$$

comm. PID

The mixed algebra

[Mikhalev, Zolotykh '98]

Mixed algebra = $\mathbb{F}[\mathbf{X}]\langle Y \rangle$

$$\{\mathbf{x}^{\mathbf{a}} = x_1^{\mathbf{a}_1} \dots x_k^{\mathbf{a}_k} \mid \mathbf{a} \in \mathbb{N}^k\}$$

The mixed algebra

[Mikhalev, Zolotykh '98]

$$\text{Mixed algebra} = \mathbb{R}[X \langle Y \rangle \{y_{i_1} \dots y_{i_l} \mid l \in \mathbb{N}\}]$$

The mixed algebra

[Mikhalev, Zolotykh '98]

$$\begin{aligned} \text{Mixed algebra} &= \mathbb{R}[X]\langle Y \rangle \\ &\cong \mathbb{R}\langle X, Y \rangle / (\chi z - z \chi \mid x \in X, z \in X \cup Y) \end{aligned}$$

The mixed algebra

[Mikhalev, Zolotykh '98]

$$\begin{aligned} \text{Mixed algebra} &= \mathbb{R}[X]\langle Y \rangle \\ &\cong \mathbb{R}\langle X, Y \rangle / (\chi z - z \chi \mid \chi \in X, z \in X \cup Y) \end{aligned}$$

$$\text{(Mixed) polynomial} = \sum_{i=1}^d c_i \cdot \chi^{\alpha_i} w_i$$

$$\text{Multiplication} : \chi^{\alpha} v \cdot \chi^{\beta} w = \chi^{\alpha+\beta} vw$$

The mixed algebra

[Mikhalev, Zolotykh '98]

$$\begin{aligned} \text{Mixed algebra} &= \mathbb{R}[X]\langle Y \rangle \\ &\simeq \mathbb{R}\langle X, Y \rangle / (\chi z - z \chi \mid \chi \in X, z \in X \cup Y) \end{aligned}$$

$$\text{(Mixed) polynomial} = \sum_{i=1}^d c_i \cdot \chi^{\alpha_i} w_i$$

$$\text{Multiplication} : \chi^{\alpha} v \cdot \chi^{\beta} w = \chi^{\alpha+\beta} vw$$

Two-sided ideals For $f_1, \dots, f_r \in \mathbb{R}[X]\langle Y \rangle$

$$(f_1, \dots, f_r) = \left\{ \sum_i \sum_j p_{i,j} \cdot f_i \cdot q_{i,j} \mid p_{i,j}, q_{i,j} \in \mathbb{R}[X]\langle Y \rangle \right\}$$

Why the mixed algebra?

In the free algebra. . .

Why the mixed algebra?

In the free algebra...

Observation 1: ...commutators appear frequently (modelling scalars, ideal arithmetic, homogenisation, etc.)

Why the mixed algebra?

In the free algebra...

Observation 1: ... commutators appear frequently (modelling scalars, ideal arithmetic, homogenisation, etc.)

Observation 2: ... commutators = bad

- Problem: Lots of (redundant) S-polynomials from commutators


Why the mixed algebra?

In the free algebra...

Observation 1: ... commutators appear frequently (modelling scalars, ideal arithmetic, homogenisation, etc.)

Observation 2: ... commutators = bad

- Problem: Lots of (redundant) S-polynomials from commutators

Observation 3: ... signatures = good f  ← signature

- Powerful elimination criteria → detect most(/all) reductions to 0


Why the mixed algebra?

In the free algebra...

Observation 1: ... commutators appear frequently (modelling scalars, ideal arithmetic, homogenisation, etc.)

Observation 2: ... commutators = bad

- Problem: Lots of (redundant) S-polynomials from commutators

Observation 3: ... signatures = good f  ← signature

- Powerful elimination criteria → detect most(/all) reductions to 0

Idea Use signatures to detect the redundant S-polynomials

Why the mixed algebra?

In the free algebra...

Observation 1: ... commutators appear frequently (modelling scalars, ideal arithmetic, homogenisation, etc.)

Observation 2: ... commutators = **bad**

- Problem: Lots of (redundant) S-polynomials from commutators

Observation 3: ... signatures = **good** $f \blacksquare \leftarrow$ signature

- Powerful elimination criteria \rightarrow detect most(/all) reductions to 0

Idea Use signatures to detect the redundant S-polynomials

Observation 4: ... commutators + signatures = **even worse**

- Problem: Signatures do not see commutator information

Why the mixed algebra?

In the free algebra...

Observation 1: ... commutators appear frequently (modelling scalars, ideal arithmetic, homogenisation, etc.)

Observation 2: ... commutators = **bad**

- Problem: Lots of (redundant) S-polynomials from commutators

Observation 3: ... signatures = **good** $f \blacksquare \leftarrow$ signature

- Powerful elimination criteria \rightarrow detect most(/all) reductions to 0

Idea Use signatures to detect the redundant S-polynomials

Observation 4: ... commutators + signatures = **even worse**

- Problem: Signatures do not see commutator information

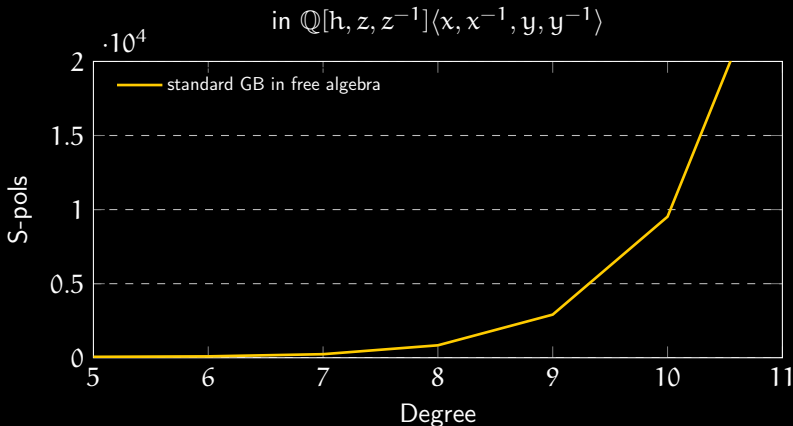
Solution New setting for signatures \rightarrow **Mixed algebra**

Experiments

Prototype implementation for SAGEMATH (when R is a field).

Consider **homogenisation** of the **discrete Heisenberg group**

$$\langle x, y, z \mid z = xyx^{-1}y^{-1}, xz = zx, yz = zy \rangle.$$

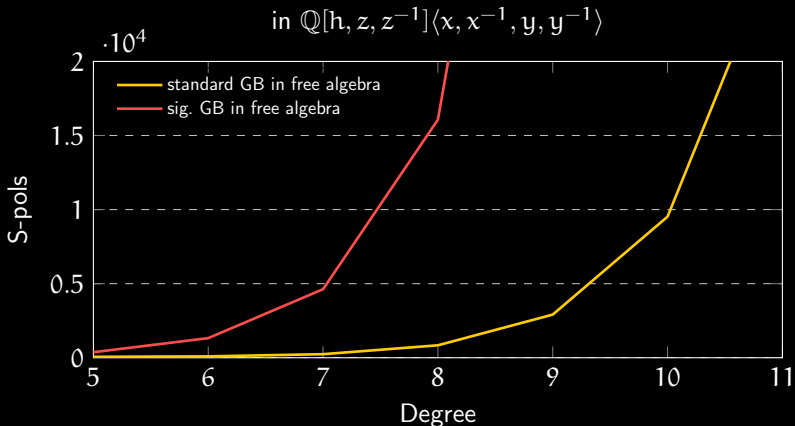


Experiments

Prototype implementation for SAGEMATH (when R is a field).

Consider **homogenisation** of the **discrete Heisenberg group**

$$\langle x, y, z \mid z = xyx^{-1}y^{-1}, xz = zx, yz = zy \rangle.$$

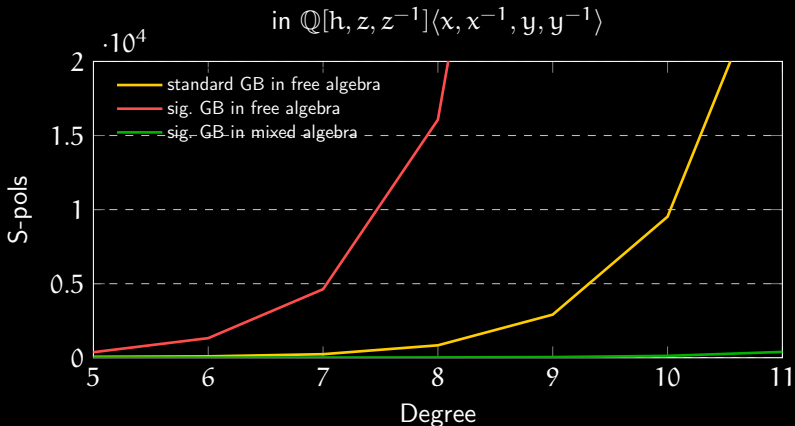


Experiments

Prototype implementation for SAGEMATH (when R is a field).

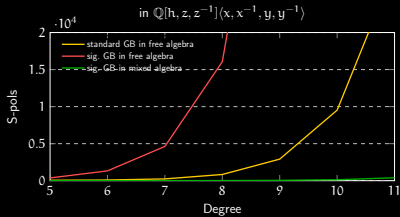
Consider **homogenisation** of the **discrete Heisenberg group**

$$\langle x, y, z \mid z = xyx^{-1}y^{-1}, xz = zx, yz = zy \rangle.$$



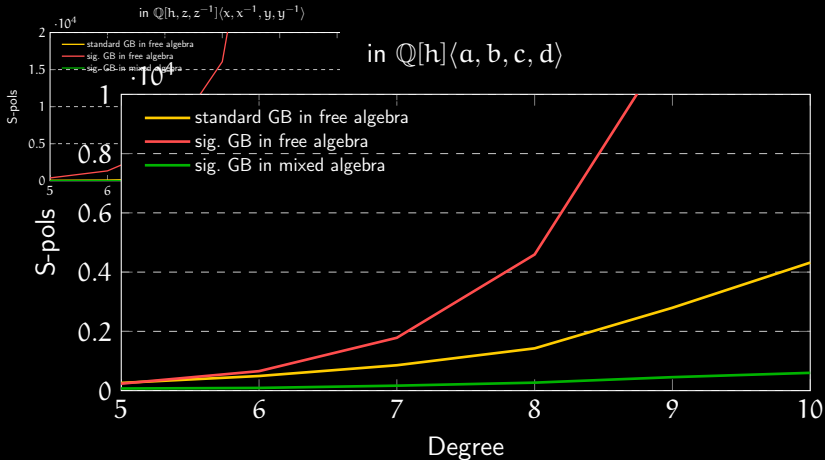
Experiments

Prototype implementation for SAGEMATH (when R is a field).



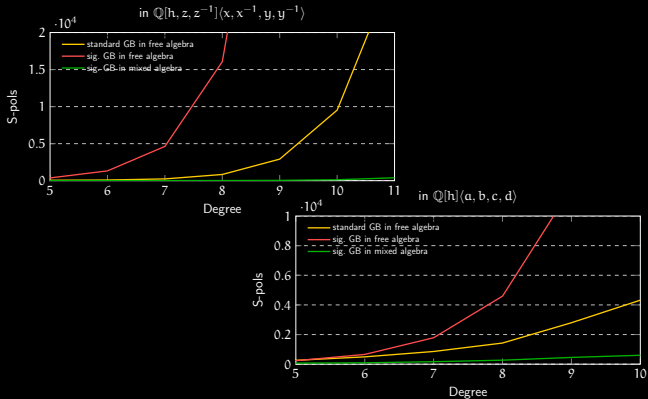
Experiments

Prototype implementation for SAGEMATH (when R is a field).



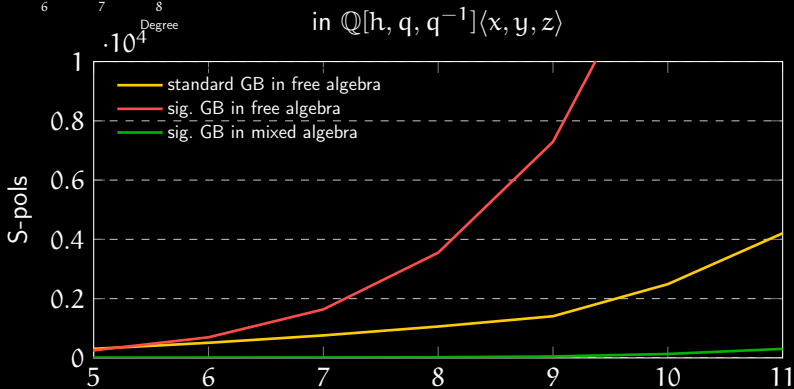
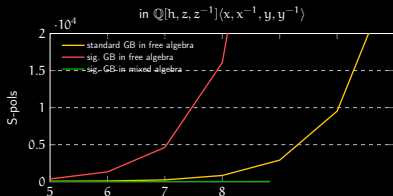
Experiments

Prototype implementation for SAGEMATH (when R is a field).



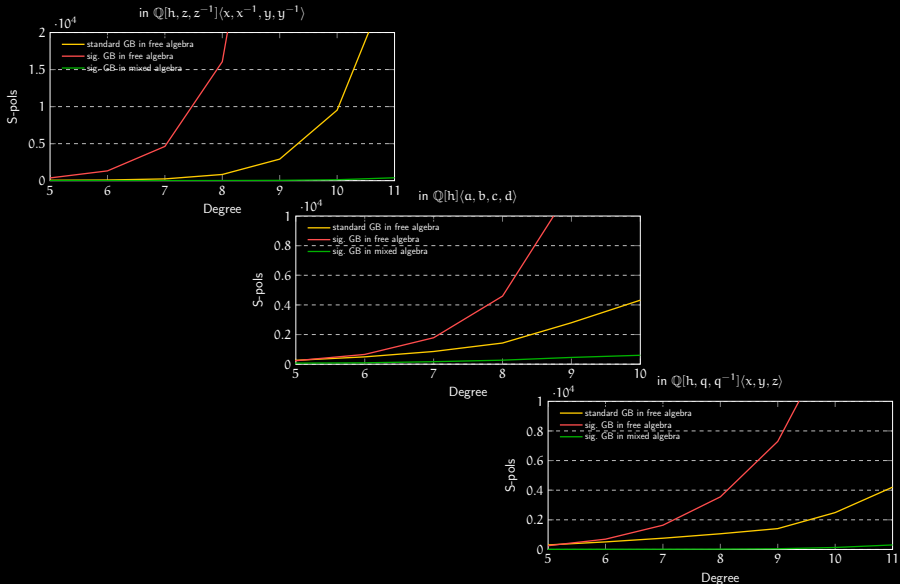
Experiments

Prototype implementation for SAGEMATH (when R is a field).



Experiments

Prototype implementation for SAGEMATH (when R is a field).



The mixed algebra

What's standard?

- Monomial order and leading coefficient/monomial/term

$$\begin{array}{c} \text{lt}(f) \\ \Rightarrow f = \underbrace{c}_{\text{lc}(f)} \cdot \underbrace{x^\alpha w}_{\text{lm}(f)} + \text{smaller terms} \end{array}$$

- Reductions: if $\text{lt}(f) = s \cdot \text{lt}(g) \cdot t$, then $f \rightarrow f - sgt$
- Gröbner bases: $G \subseteq I \trianglelefteq R[X]\langle Y \rangle$ is

Gröbner basis if $f \xrightarrow{*}_G 0$ for all $f \in I$

The mixed algebra

What's not so standard?

... because of $\langle Y \rangle$

... because of $[X]$

... because of R

The mixed algebra

What's not so standard?

- Most ideals do not have finite Gröbner basis ... because of $\langle Y \rangle$
⇒ enumeration procedures

... because of $[X]$

... because of R

The mixed algebra

What's not so standard?

- Most ideals do not have finite Gröbner basis ... because of $\langle Y \rangle$
⇒ enumeration procedures
- lcm of leading monomials not unique
For zyz and yz both $zyzyz$ and $zyzy$ are minimal multiples.

... because of $[X]$

... because of R

The mixed algebra

What's not so standard?

- Most ideals do not have finite Gröbner basis ... because of $\langle Y \rangle$
⇒ enumeration procedures
- lcm of leading monomials not unique
For zyz and yz both $zyzy$ and zyz are minimal multiples.

ambiguity a

... because of $[X]$

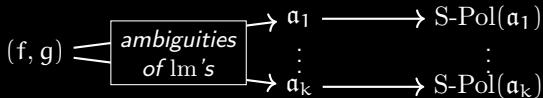
... because of R

The mixed algebra

What's not so standard?

- Most ideals do not have finite Gröbner basis ... because of $\langle Y \rangle$
⇒ enumeration procedures
- lcm of leading monomials not unique

ambiguity a
For zyz and yz both $zyzy$ and zyz are minimal multiples.



... because of $[X]$

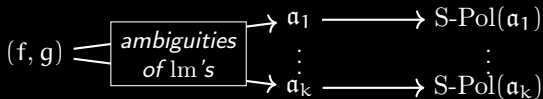
... because of R

The mixed algebra

What's not so standard?

- Most ideals do not have finite Gröbner basis ... because of $\langle Y \rangle$
 \Rightarrow enumeration procedures
- lcm of leading monomials not unique

For zyz and yz both $zyzy$ and zyz are minimal multiples.



- Non-minimal ambiguities corresponding to

$$\text{lm}(f) \text{ --- } \text{lm}(g) \quad \forall \text{ --- } \in \langle Y \rangle$$

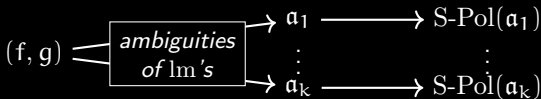
\Rightarrow two elements have infinitely many S-polynomials ... because of $[X]$

The mixed algebra

What's not so standard?

- Most ideals do not have finite Gröbner basis ... because of $\langle Y \rangle$
 \Rightarrow enumeration procedures

- lcm of leading monomials not unique
 For zyz and yz both $zyzy$ and zyz are minimal multiples.

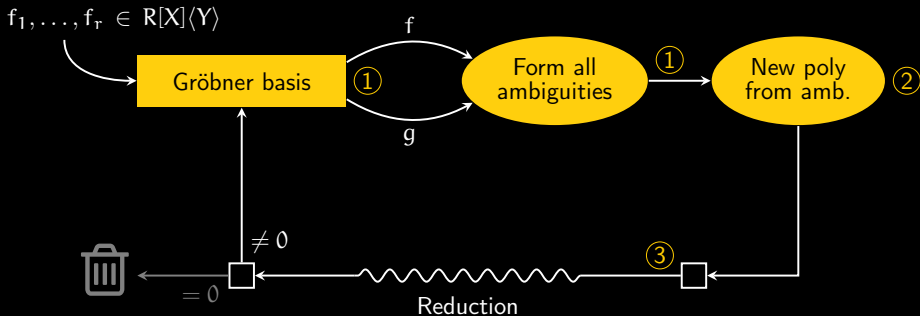


- Non-minimal ambiguities corresponding to
 $\text{lm}(f) \text{ --- } \text{lm}(g) \quad \forall \text{ ---} \in \langle Y \rangle$
 \Rightarrow two elements have infinitely many S-polynomials ... because of $[X]$

- G-polynomials to introduce new leading coefficients
 - S-Pol(α): $\text{lm}(\text{S-Pol}) = \text{new}$ and $\text{lc}(\text{S-Pol}) = ?$
 - G-Pol(α): $\text{lm}(\text{G-Pol}) = \text{old}$ and $\text{lc}(\text{G-Pol}) = \text{minimal}$

... because of R

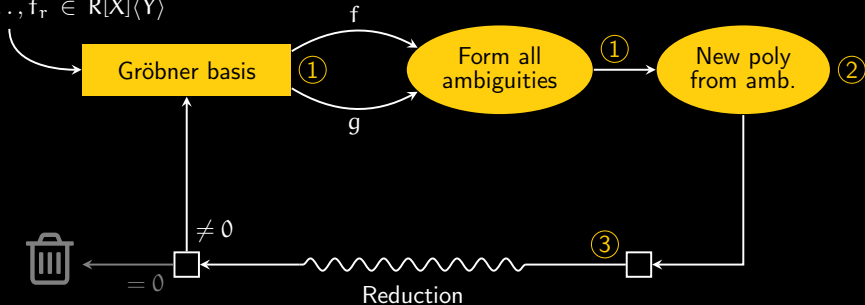
Buchberger's algorithm



- 1. Selection:** fair strategy “Every S/G -poly is selected eventually”
- 2. Construction:** $S\text{-Pol}(a)$ and $G\text{-Pol}(a)$ from ambiguity a
- 3. Reduction:** if $\text{lt}(f) = s \cdot \text{lt}(g) \cdot t$, then $f \rightarrow f - sgt$

Buchberger's algorithm

$f_1, \dots, f_r \in R[X]\langle Y \rangle$



1. **Selection:** fair strategy “Every S/G -poly is selected eventually”
2. **Construction:** $S\text{-Pol}(a)$ and $G\text{-Pol}(a)$ from ambiguity a
3. **Reduction:** if $\text{lt}(f) = s \cdot \text{lt}(g) \cdot t$, then $f \rightarrow f - sgt$

Theorem [Mikhalev, Zolotykh '98]

This enumerates a (possibly infinite) GB

Signatures

Idea Add module perspective to polynomial computations

Signatures

Idea Add module perspective to polynomial computations

$$\mathcal{A} = \mathbb{R}[X]\langle Y \rangle$$

mixed algebra

$$I = (f_1, \dots, f_r)$$

$$f = \sum_i c_i \cdot \mathbf{x}^{\alpha_i} v_i f_{j_i} w_i \quad v_i, w_i \in \langle Y \rangle$$

$\text{lt}(f)$ = largest term in f

leading term

Signatures

Idea Add module perspective to polynomial computations

$$\Sigma = \bigoplus_{i=1}^r \mathcal{A} \otimes_{\mathbb{R}[X]} \mathcal{A}$$

free \mathcal{A} -bimodule

$$\varepsilon_1, \dots, \varepsilon_r$$

$$\alpha = \sum_i c_i \cdot \mathbf{x}^{\mathbf{a}_i} v_i \varepsilon_{j_i} w_i$$

$\text{sig}(\alpha)$ = largest term in α
signature

$$\mathcal{A} = \mathbb{R}[X] \langle Y \rangle$$

mixed algebra

$$I = (f_1, \dots, f_r)$$

$$f = \sum_i c_i \cdot \mathbf{x}^{\mathbf{a}_i} v_i f_{j_i} w_i \quad v_i, w_i \in \langle Y \rangle$$

$\text{lt}(f)$ = largest term in f
leading term

Signatures

Idea Add module perspective to polynomial computations

$$\Sigma = \bigoplus_{i=1}^r \mathcal{A} \otimes_{\mathbb{R}[X]} \mathcal{A}$$

free \mathcal{A} -bimodule

$$\varepsilon_1, \dots, \varepsilon_r$$

$$\alpha = \sum_i c_i \cdot \mathbf{x}^{\mathbf{a}_i} v_i \varepsilon_{j_i} w_i$$

$\text{sig}(\alpha)$ = largest term in α
signature

$$\mathcal{A} = \mathbb{R}[X] \langle Y \rangle$$

mixed algebra

$$I = (f_1, \dots, f_r)$$

$$f = \sum_i c_i \cdot \mathbf{x}^{\mathbf{a}_i} v_i f_{j_i} w_i \quad v_i, w_i \in \langle Y \rangle$$

$\text{lt}(f)$ = largest term in f
leading term

Note: $x\alpha = \alpha x$ but $y\alpha \neq \alpha y \Rightarrow$ signature sees commutators

Signatures

Idea Add module perspective to polynomial computations

$$\Sigma = \bigoplus_{i=1}^r \mathcal{A} \otimes_{\mathbb{R}[X]} \mathcal{A}$$

free \mathcal{A} -bimodule

$$\varepsilon_1, \dots, \varepsilon_r$$

$$\alpha = \sum_i c_i \cdot x^{\alpha_i} v_i \varepsilon_{j_i} w_i$$

$\text{sig}(\alpha)$ = largest term in α
signature

$$\mathcal{A} = \mathbb{R}[X] \langle Y \rangle$$

mixed algebra

$$I = (f_1, \dots, f_r)$$

$$f = \sum_i c_i \cdot x^{\alpha_i} v_i f_{j_i} w_i \quad v_i, w_i \in \langle Y \rangle$$

$\text{lt}(f)$ = largest term in f
leading term

$$\mathcal{A}\text{-bimodule hom.} \quad \bar{\cdot} : \Sigma \rightarrow I, \quad \varepsilon_i \mapsto f_i$$

Signatures

Idea Add module perspective to polynomial computations

$\Sigma = \bigoplus_{i=1}^r \mathcal{A} \otimes_{\mathbb{R}[X]} \mathcal{A}$ <p style="text-align: center;">free \mathcal{A}-bimodule</p> <p style="text-align: center;">$\varepsilon_1, \dots, \varepsilon_r$</p> $\alpha = \sum_i c_i \cdot \mathbf{x}^{\mathbf{a}_i} v_i \varepsilon_{j_i} w_i$ <p style="text-align: center;">sig(α) = largest term in α signature</p>	\longmapsto	$\mathcal{A} = \mathbb{R}[X] \langle Y \rangle$ <p style="text-align: center;">mixed algebra</p> <p style="text-align: center;">$I = (f_1, \dots, f_r)$</p> $f = \sum_i c_i \cdot \mathbf{x}^{\mathbf{a}_i} v_i f_{j_i} w_i \quad v_i, w_i \in \langle Y \rangle$ <p style="text-align: center;">lt(f) = largest term in f leading term</p>
\mathcal{A} -bimodule hom.: $\bar{\cdot} : \Sigma \rightarrow I, \quad \varepsilon_i \mapsto f_i$		

Sig-based algorithms work with pairs $(f, \text{sig}(\alpha))$ where $\bar{\alpha} = f$

Regular operations

$$\begin{aligned} \sigma \succ \mu &\Rightarrow (f, \sigma) \pm (g, \mu) = (f \pm g, \sigma) \\ &\Rightarrow \text{regular reductions, regular S/G-polynomials} \\ &(f, \sigma) \rightarrow (f - \text{sgt}, \sigma) \end{aligned}$$

Signature based algorithms

To add signatures to the classical Buchberger algorithm, we have to . . .

1. Replace polynomials by signature polynomials
2. Restrict to regular operations
3. Exploit elimination criteria

Signature based algorithms

To add signatures to the classical Buchberger algorithm, we have to . . .

1. Replace polynomials by signature polynomials $f \rightsquigarrow (f, \sigma)$
2. Restrict to regular operations
3. Exploit elimination criteria

Signature based algorithms

To add signatures to the classical Buchberger algorithm, we have to...

1. Replace polynomials by signature polynomials $f \rightsquigarrow (f, \sigma)$
2. Restrict to regular operations $(f, \sigma) \pm (g, \mu) = (f \pm g, \sigma)$ if $\sigma \succ \mu$
3. Exploit elimination criteria

Signature based algorithms

To add signatures to the classical Buchberger algorithm, we have to...

1. Replace polynomials by signature polynomials $f \rightsquigarrow (f, \sigma)$
2. Restrict to regular operations $(f, \sigma) \pm (g, \mu) = (f \pm g, \sigma)$ if $\sigma \succ \mu$
3. Exploit elimination criteria

Signature based algorithms

To add signatures to the classical Buchberger algorithm, we have to . . .

1. Replace polynomials by signature polynomials $f \rightsquigarrow (f, \sigma)$
2. Restrict to regular operations $(f, \sigma) \pm (g, \mu) = (f \pm g, \sigma)$ if $\sigma \succ \mu$
3. Exploit elimination criteria

Signature based algorithms compute . . .

- Signature Gröbner basis
 - Definition just like in the commutative case
 - Signature GBs are in particular GBs
- $$G \text{ signature GB} \Rightarrow \{f \mid (f, \sigma) \in G\} \text{ GB}$$
- Gröbner basis of the syzygy module

Elimination criteria

Characterisation of sig. GB G and syzygy GB H via **cover criterion**

[Gao, Volny, Wang '15, Francis, Verron, '21, H., Verron '23]

Regular **ambiguity** α **covered** by (G, H) if

“S-Pol(α) not minimal among elements with sig(S-Pol) in span of $G \cup H$ ”

Elimination criteria

Characterisation of sig. GB G and syzygy GB H via **cover criterion**

[Gao, Volny, Wang '15, Francis, Verron, '21, H., Verron '23]

Regular **ambiguity** α **covered** by (G, H) if

“S-Pol(α) not minimal among elements with sig(S-Pol) in span of $G \cup H$ ”

Cover criterion

all regular ambiguities of G covered + enough G -Pol

$\Rightarrow G$ sig. GB, H syz. GB

Elimination criteria

Characterisation of sig. GB G and syzygy GB H via **cover criterion**

[Gao, Volny, Wang '15, Francis, Verron, '21, H., Verron '23]

Regular **ambiguity** α **covered** by (G, H) if

“S-Pol(α) not minimal among elements with sig(S-Pol) in span of $G \cup H$ ”

Cover criterion

all regular ambiguities of G covered + enough G -Pol

$\Rightarrow G$ sig. GB, H syz. GB

Facts

- Ambiguity α is covered by $S\text{-Pol}(\alpha)$...
- ... but can also be covered by other elements \Rightarrow **elimination criterion for S-Pol** (includes syzygy, singular, and F5 criterion)

Elimination criteria

Characterisation of sig. GB G and syzygy GB H via **cover criterion**

[Gao, Volny, Wang '15, Francis, Verron, '21, H., Verron '23]

Regular **ambiguity** α **covered** by (G, H) if

“S-Pol(α) *not minimal among elements with sig(S-Pol) in span of $G \cup H$ ”*”

Cover criterion

all regular ambiguities of G covered + enough G-Pol

$\Rightarrow G$ sig. GB, H syz. GB

Facts

- Ambiguity α is covered by S-Pol(α)...
- ... but can also be covered by other elements \Rightarrow **elimination criterion for S-Pol** (includes syzygy, singular, and F5 criterion)
- G-Pol redundant if reducible

Elimination criteria

Characterisation of sig. GB G and syzygy GB H via **cover criterion**

[Gao, Volny, Wang '15, Francis, Verron, '21, H., Verron '23]

Regular **ambiguity** α **covered** by (G, H) if

“S-Pol(α) not minimal among elements with sig(S-Pol) in span of $G \cup H$ ”

Cover criterion

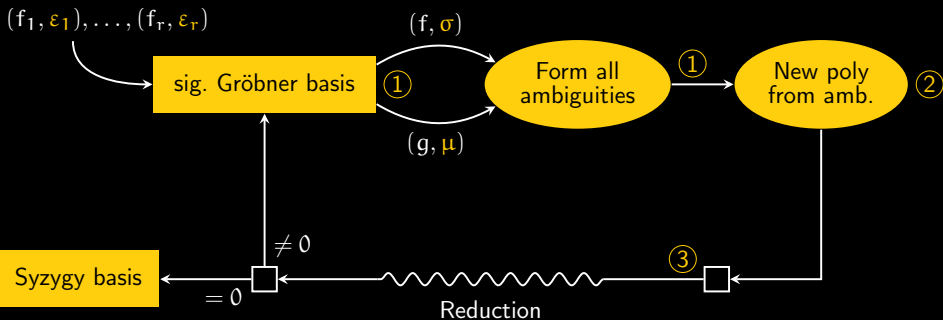
all regular ambiguities of G covered + enough G-Pol

$\Rightarrow G$ sig. GB, H syz. GB

Facts

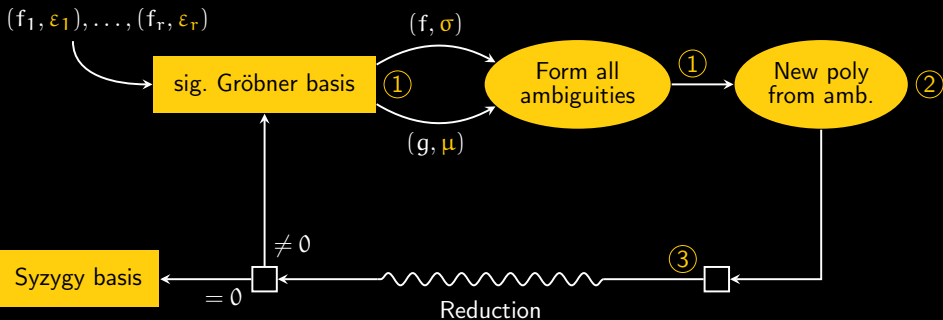
- Ambiguity α is covered by S-Pol(α)...
- ... but can also be covered by other elements \Rightarrow **elimination criterion for S-Pol** (includes syzygy, singular, and F5 criterion)
- G-Pol redundant if reducible
- Cover criterion **decouples selection strategy** from signature order
 - In the commutative case this is nice
 - In the noncommutative case this is **essential**

Sig-based Buchberger's algorithm



1. **Selection:** fair strategy “Every S/G -poly is selected eventually”
2. **Construction:** regular $S\text{-Pol}(a)$ and $G\text{-Pol}(a)$ from ambiguity a
3. **Reduction:** (regular) if $\text{lt}(f) = s \cdot \text{lt}(g) \cdot t$ and $\sigma \succ s \cdot \mu \cdot t$, then $(f, \sigma) \rightarrow (f - \text{sgt}, \sigma)$

Sig-based Buchberger's algorithm

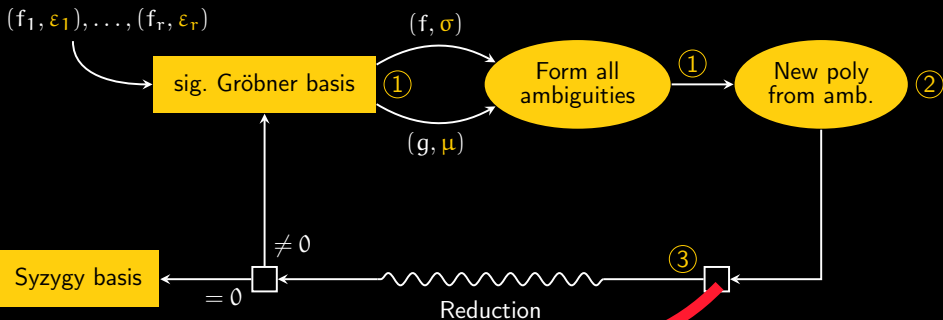


1. **Selection:** fair strategy “Every S/G -poly is selected eventually”
2. **Construction:** regular $S\text{-Pol}(a)$ and $G\text{-Pol}(a)$ from ambiguity a
3. **Reduction:** (regular) if $\text{lt}(f) = s \cdot \text{lt}(g) \cdot t$ and $\sigma \succ s \cdot \mu \cdot t$, then $(f, \sigma) \rightarrow (f - \text{sgt}, \sigma)$

Theorem [H., Verron '23]

This enumerates a (possibly infinite) sig. GB and syzygy basis

Sig-based Buchberger's algorithm



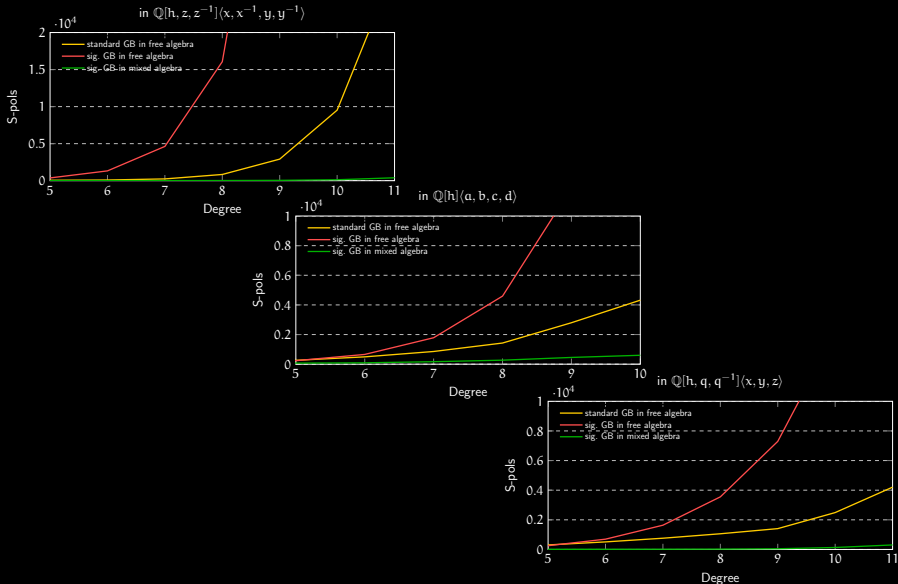
1. Selection: find (f, σ) and (g, μ) such that $f - sgt$ is selected eventually"
2. Construction: regular S-Pol(α) and G-Pol(α) from ambiguity α
3. Reduction: (regular) if $\text{lt}(f) = s \cdot \text{lt}(g) \cdot t$ and $\sigma \succ s \cdot \mu \cdot t$, then $(f, \sigma) \rightarrow (f - sgt, \sigma)$

Theorem [H., Verron '23]

This enumerates a (possibly infinite) sig. GB and syzygy basis

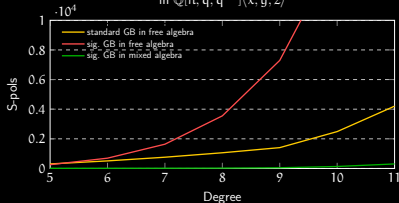
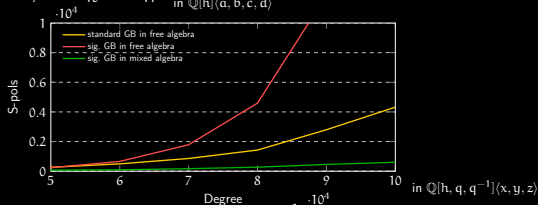
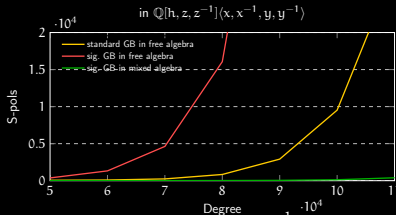
Experiments

Prototype implementation for SAGEMATH (when R is a field).



Experiments

Prototype implementation for SAGEMATH (when R is a field).



+ data that allows to...

- ... obtain representations of ideal elements (almost) for free
- ... compute minimal representations of ideal elements [H., Verron '23]

F

Hi chatGPT



Hello! How can I assist you today?




F

Imagine you want to compute Gröbner bases in the free algebra but some of your variables are commutative. What do you do?



I would use signature Gröbner bases in the mixed algebra.



 Regenerate response

Send a message



Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT July 20 Version](#)