Signature Gröbner bases and cofactor computation in the free algebra

Clemens Hofstadler[1, 2], Thibaut Verron[1]

Algebraic Rewriting Seminar, 21 April 2022

1. Institute for Algebra, Johannes Kepler University, Linz, Autriche
2. Institute of Mathematics, University of Kassel, Kassel, Allemagne

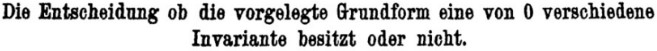
JOHANNES KEPLER UNIVERSITÄT LINZ

FWF Der Wissenschaftsfonds.

UNI KASSEL VERSITÄT

The Ideal Membership Problem and Gröbner bases

Question:



Die Entscheidung ob die vorgelegte Grundform eine von 0 verschiedene Invariante besitzt oder nicht.

[Hilbert 1893]

David Hilbert

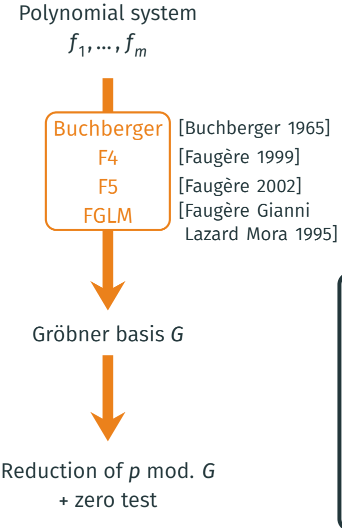
The Ideal Membership Problem and Gröbner bases

Question: Given $f_1, \ldots, f_m, p \in K[X_1, \ldots, X_n]$, decide if $p \in \langle f_1, \ldots, f_m \rangle$. [Hilbert 1893]

David Hilbert

The Ideal Membership Problem and Gröbner bases

Question: Given $f_1,\dots,f_m, p \in K[X_1,\dots,X_n]$, decide if $p \in \langle f_1,\dots,f_m \rangle$. [Hilbert 1893]


Polynomial system $f_1,\dots,f_m$

Buchberger [Buchberger 1965]

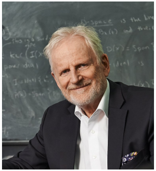
F4 [Faugère 1999]

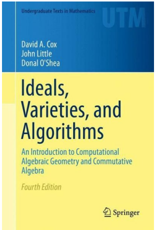
F5 [Faugère 2002]

FGLM [Faugère Gianni Lazard Mora 1995]

Gröbner basis G

Reduction of p mod. G + zero test


Bruno Buchberger


Undergraduate Texts in Mathematics UTM

David A. Cox
John Little
Donal O'Shea

Ideals, Varieties, and Algorithms

An Introduction to Computational Algebraic Geometry and Commutative Algebra

Fourth Edition

Springer

Central in effective algebra and geometry

- List the solutions of a system
- Eliminate variables, compute projections
- Parametrization, implicitization
- Bases for differential operators, for word polynomials in the free algebra...
- Bases for modules

Gröbner bases in the noncommutative case

Setting:

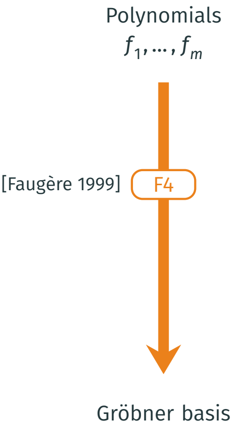
- R field, $A = R\langle X_1, \dots, X_n\rangle$ free algebra over R
- Monomials are words: $X_{i_1} X_{i_2} \cdots X_{i_d}$
- Monomial ordering and reduction are defined as usual
- Gröbner bases are defined as usual
- Application: proof of formulas
  "Does a relation follow from a prescribed set of axioms?"

What is not usual:

- The free algebra is not Noetherian
- Most ideals do not admit a finite Gröbner basis
- It is not decidable whether an ideal admits a finite Gröbner basis

Why signature Gröbner bases?

Commutative case



Polynomials
$f_1, \dots, f_m$

[Faugère 1999] F4

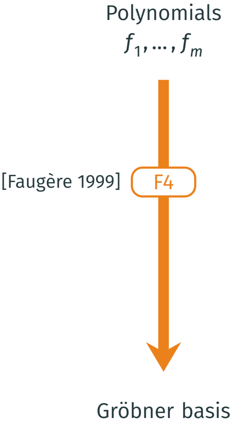
Gröbner basis

Ideal Membership Problem

*“Does there exist (a_i)
such that
$p = a_1 f_1 + \cdots + a_m f_m$?”*

Why signature Gröbner bases?

Commutative case



Polynomials

$f_1, \dots, f_m$

[Faugère 1999]

F4

Gröbner basis

Ideal Membership Problem

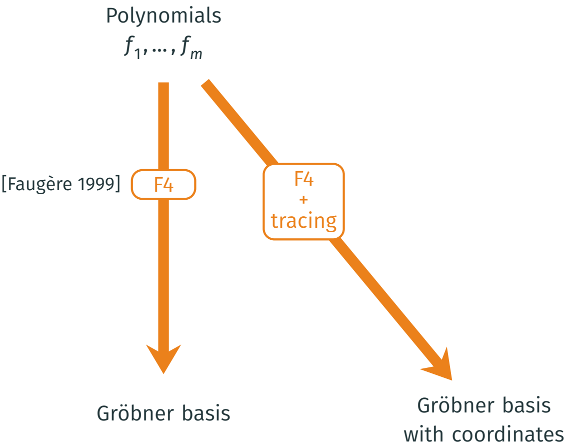
“Does there exist (a_i)
such that
$p = a_1 f_1 + \cdots + a_m f_m$?”

IMP with certificate

“Compute (a_i)
such that
$p = a_1 f_1 + \cdots + a_m f_m$”

Why signature Gröbner bases?

Commutative case



Ideal Membership Problem

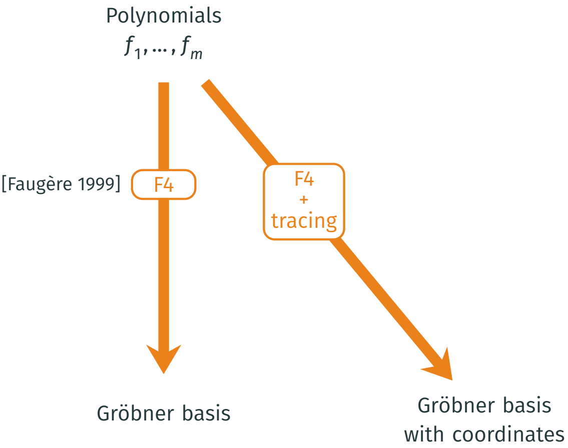
*"Does there exist (a_i)
such that
$p = a_1 f_1 + \dots + a_m f_m$?"*

IMP with certificate

*"Compute (a_i)
such that
$p = a_1 f_1 + \dots + a_m f_m$"*

Why signature Gröbner bases?

Commutative case



Polynomials

$f_1, \dots, f_m$

[Faugère 1999]

F4

F4 + tracing

Gröbner basis

Gröbner basis with coordinates

Ideal Membership Problem

“Does there exist (a_i) such that $p = a_1 f_1 + \dots + a_m f_m$?”

IMP with certificate

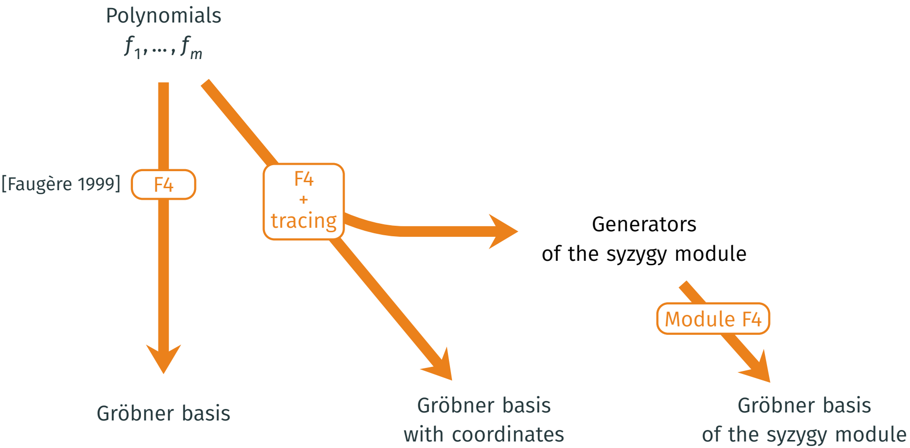
“Compute (a_i) such that $p = a_1 f_1 + \dots + a_m f_m$”

Module of syzygies

“Find all (a_i) such that $a_1 f_1 + \dots + a_m f_m = 0$”

WHY SIGNATURE GRÖBNER BASES?

Commutative case



Polynomials $f_1, \dots, f_m$

[Faugère 1999]

F4

F4 + tracing

Generators of the syzygy module

Module F4

Gröbner basis

Gröbner basis with coordinates

Gröbner basis of the syzygy module

Ideal Membership Problem

“Does there exist (a_i) such that $p = a_1 f_1 + \dots + a_m f_m$?”

IMP with certificate

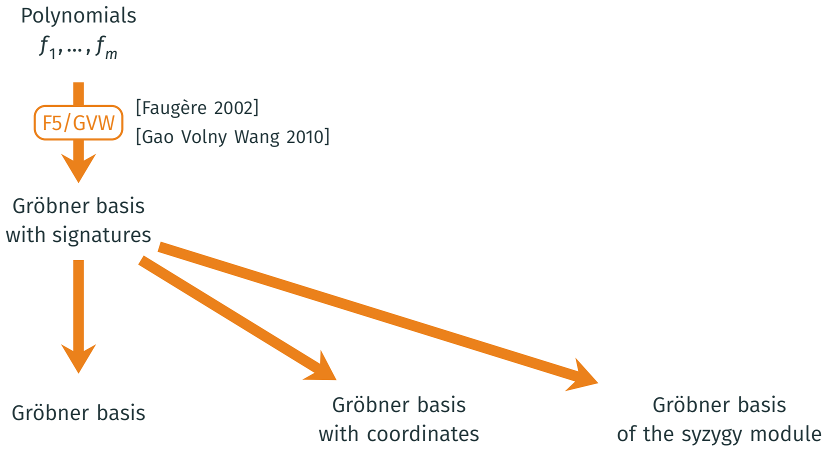
“Compute (a_i) such that $p = a_1 f_1 + \dots + a_m f_m$”

Module of syzygies

“Find all (a_i) such that $a_1 f_1 + \dots + a_m f_m = 0$”

Why signature Gröbner bases?

Commutative case



Polynomials
$f_1, \dots, f_m$

F5/GVW

[Faugère 2002]
[Gao Volny Wang 2010]

Gröbner basis
with signatures

Gröbner basis

Gröbner basis
with coordinates

Gröbner basis
of the syzygy module

Ideal Membership Problem

*“Does there exist (a_i)
such that
$p = a_1 f_1 + \dots + a_m f_m$?”*

IMP with certificate

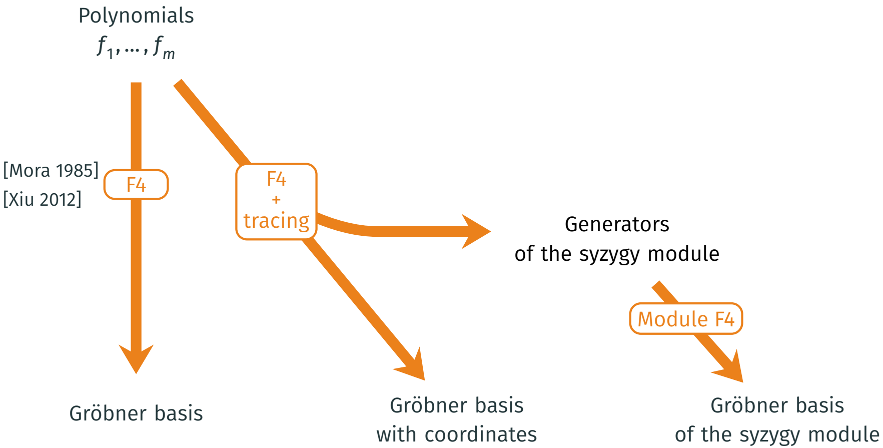
*“Compute (a_i)
such that
$p = a_1 f_1 + \dots + a_m f_m$”*

Module of syzygies

*“Find all (a_i)
such that
$a_1 f_1 + \dots + a_m f_m = 0$”*

Why signature Gröbner bases?

Non-commutative case



Polynomials
$f_1, \dots, f_m$

[Mora 1985]
[Xiu 2012]

F4

F4
+
tracing

Generators
of the syzygy module

Module F4

Gröbner basis

Gröbner basis
with coordinates

Gröbner basis
of the syzygy module

Ideal Membership Problem

*“Does there exist (a_i, b_j)
such that
$p = a_1 f_1 b_1 + \dots + a_m f_m b_m$?”*

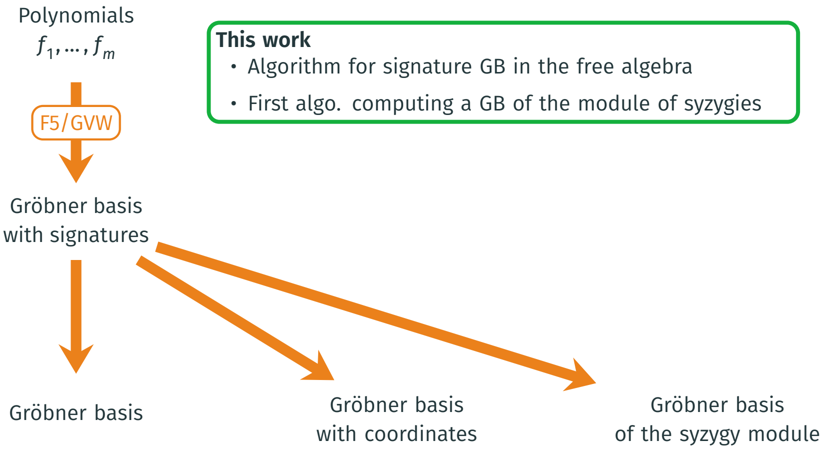
IMP with certificate

*“Compute (a_i, b_j)
such that
$p = a_1 f_1 b_1 + \dots + a_m f_m b_m$”*

Module of syzygies

*“Find all (a_i, b_j)
such that
$a_1 f_1 b_1 + \dots + a_m f_m b_m = 0$”*

Why signature Gröbner bases?



Polynomials
$f_1, \dots, f_m$

F5/GVW

Gröbner basis
with signatures

This work

- Algorithm for signature GB in the free algebra
- First algo. computing a GB of the module of syzygies

Gröbner basis

Gröbner basis
with coordinates

Gröbner basis
of the syzygy module

Ideal Membership Problem

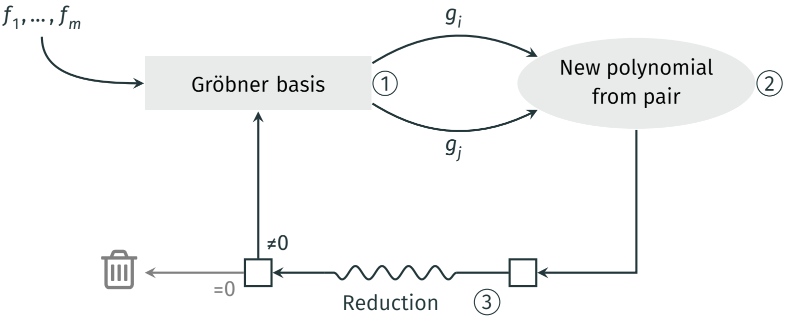
*"Does there exist (a_i, b_j)
such that
$p = a_1 f_1 b_1 + \dots + a_m f_m b_m$?"*

IMP with certificate

*"Compute (a_i, b_j)
such that
$p = a_1 f_1 b_1 + \dots + a_m f_m b_m$"*

Module of syzygies

*"Find all (a_i, b_j)
such that
$a_1 f_1 b_1 + \dots + a_m f_m b_m = 0$"*



1. **Selection**: selection strategy
2. **Construction**: S-polynomials
3. **Reduction**

Signatures

Problem: useless computations: 🗑 → ♻

$p = p_1 f_1 + p_2 f_2 + \cdots + p_m f_m$

$q = q_1 f_1 + q_2 f_2 + \cdots + q_m f_m$

$p - q = 0$?

Signatures

Problem: useless computations: 🗑 ⟶ ♻

- 1st idea: keep track of the representation of the ideal elements
  [Möller, Mora, Traverso 1992]

$$p = p_1 f_1 + p_2 f_2 + \dots + p_m f_m$$
$$\boldsymbol{p} = p_1 \boldsymbol{e}_1 + p_2 \boldsymbol{e}_2 + \dots + p_m \boldsymbol{e}_m$$

$$q = q_1 f_1 + q_2 f_2 + \dots + q_m f_m$$
$$\boldsymbol{q} = q_1 \boldsymbol{e}_1 + q_2 \boldsymbol{e}_2 + \dots + q_m \boldsymbol{e}_m$$

$p - q = 0$?

$$\boldsymbol{p} - \boldsymbol{q} = \left(p_1 \boldsymbol{e}_1 + \dots + p_m \boldsymbol{e}_m\right) - \left(q_1 \boldsymbol{e}_1 + \dots + q_m \boldsymbol{e}_m\right)$$

Signatures

Problem: useless computations: 🗑 ⟶ ♻

- 1st idea: keep track of the representation of the ideal elements
  [Möller, Mora, Traverso 1992]
- 2nd idea: we do not need the full representation, the largest term is enough
  [Faugère 2002 ; Gao, Volny, Wang 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_m f_m$$

$$\boldsymbol{p} = p_1 \boldsymbol{e}_1 + p_2 \boldsymbol{e}_2 + \cdots + p_m \boldsymbol{e}_m$$

$$= \mathrm{LT}(p_k)\boldsymbol{e}_k + \text{smaller terms}$$

$$q = q_1 f_1 + q_2 f_2 + \cdots + q_m f_m$$

$$\boldsymbol{q} = q_1 \boldsymbol{e}_1 + q_2 \boldsymbol{e}_2 + \cdots + q_m \boldsymbol{e}_m$$

$$= \mathrm{LT}(q_l)\boldsymbol{e}_l + \text{smaller terms}$$

$p - q = 0?$

$$\boldsymbol{p} - \boldsymbol{q} = \left(p_1 \boldsymbol{e}_1 + \cdots + p_m \boldsymbol{e}_m\right) - \left(q_1 \boldsymbol{e}_1 + \cdots + q_m \boldsymbol{e}_m\right)$$

$$= \mathrm{LT}(p_k)\boldsymbol{e}_k - \mathrm{LT}(q_l)\boldsymbol{e}_l + \text{smaller terms}$$

Signatures

Problem: useless computations: 🗑 ⟶ ♻

- 1st idea: keep track of the representation of the ideal elements
  [Möller, Mora, Traverso 1992]
- 2nd idea: we do not need the full representation, the largest term is enough
  [Faugère 2002 ; Gao, Volny, Wang 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_m f_m$$

$$\boldsymbol{p} = p_1 \boldsymbol{e}_1 + p_2 \boldsymbol{e}_2 + \cdots + p_m \boldsymbol{e}_m$$

$$= \mathrm{LT}(p_k)\boldsymbol{e}_k + \text{smaller terms}$$

$$q = q_1 f_1 + q_2 f_2 + \cdots + q_m f_m$$

$$\boldsymbol{q} = q_1 \boldsymbol{e}_1 + q_2 \boldsymbol{e}_2 + \cdots + q_m \boldsymbol{e}_m$$

$$= \mathrm{LT}(q_l)\boldsymbol{e}_l + \text{smaller terms}$$

$p - q = 0$?

$$\boldsymbol{p} - \boldsymbol{q} = \left(p_1 \boldsymbol{e}_1 + \cdots + p_m \boldsymbol{e}_m\right) - \left(q_1 \boldsymbol{e}_1 + \cdots + q_m \boldsymbol{e}_m\right)$$

$$= \mathrm{LT}(p_k)\boldsymbol{e}_k - \mathrm{LT}(q_l)\boldsymbol{e}_l + \text{smaller terms}$$

$$= \mathrm{LT}(p_k)\boldsymbol{e}_k + \text{smaller terms} \qquad \text{if } \mathrm{LT}(p_k)\boldsymbol{e}_k > \mathrm{LT}(q_l)\boldsymbol{e}_l$$

Signatures

Problem: useless computations: 🗑 ⟶ ♻

- 1st idea: keep track of the representation of the ideal elements
  [Möller, Mora, Traverso 1992]
- 2nd idea: we do not need the full representation, the largest term is enough
  [Faugère 2002 ; Gao, Volny, Wang 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_m f_m$$

$$\boldsymbol{p} = p_1 \boldsymbol{e}_1 + p_2 \boldsymbol{e}_2 + \cdots + p_m \boldsymbol{e}_m$$

$$= \mathrm{LT}(p_k)\boldsymbol{e}_k + \text{smaller terms}$$

$\mathrm{sig}(\boldsymbol{p}) =$ signature of $\boldsymbol{p}$

$$q = q_1 f_1 + q_2 f_2 + \cdots + q_m f_m$$

$$\boldsymbol{q} = q_1 \boldsymbol{e}_1 + q_2 \boldsymbol{e}_2 + \cdots + q_m \boldsymbol{e}_m$$

$$= \mathrm{LT}(q_l)\boldsymbol{e}_l + \text{smaller terms}$$

$p - q = 0$?

$$\boldsymbol{p} - \boldsymbol{q} = \left(p_1 \boldsymbol{e}_1 + \cdots + p_m \boldsymbol{e}_m\right) - \left(q_1 \boldsymbol{e}_1 + \cdots + q_m \boldsymbol{e}_m\right)$$

$$= \mathrm{LT}(p_k)\boldsymbol{e}_k - \mathrm{LT}(q_l)\boldsymbol{e}_l + \text{smaller terms}$$

$$= \mathrm{LT}(p_k)\boldsymbol{e}_k + \text{smaller terms} \quad \text{if } \mathrm{LT}(p_k)\boldsymbol{e}_k > \mathrm{LT}(q_l)\boldsymbol{e}_l$$

Regular addition

Module framework

Setting:

- Input: $f_1, \dots, f_m \in A = R[\boldsymbol{X}]$ spanning the ideal I
- Module $M = A\boldsymbol{e}_1 \oplus \cdots \oplus A\boldsymbol{e}_m \simeq A^m$ with the map $M \to I$, $\boldsymbol{e}_i \mapsto f_i$
- Monomials in M are ordered with an ordering compatible with that on A
- Signature-polynomial pair: $(\boldsymbol{s}, f)$ with $f = \sum a_i f_i$ and $\boldsymbol{s} = \mathrm{LM}(\sum a_i \boldsymbol{e}_i)$
- Syzygy in M: $\boldsymbol{z} = \sum z_i \boldsymbol{e}_i \in M$ such that $\sum z_i f_i = 0$

Module framework

Setting:

- Input: $f_1, \dots, f_m \in A = R[\boldsymbol{X}]$ spanning the ideal I
- Module $M = A\boldsymbol{e}_1 \oplus \cdots \oplus A\boldsymbol{e}_m \simeq A^m$ with the map $M \to I$, $\boldsymbol{e}_i \mapsto f_i$
- Monomials in M are ordered with an ordering compatible with that on A
- Signature-polynomial pair: $(\boldsymbol{s}, f)$ with $f = \sum a_i f_i$ and $\boldsymbol{s} = \mathrm{LM}(\sum a_i \boldsymbol{e}_i)$
- Syzygy in M: $\boldsymbol{z} = \sum z_i \boldsymbol{e}_i \in M$ such that $\sum z_i f_i = 0$

Regular operations:

- Multiplying a sig-poly pair by a term in A is easy
- We can only compute the result of regular additions: $(\boldsymbol{s}, f) + (\boldsymbol{t}, g) = (\max(\boldsymbol{s}, \boldsymbol{t}), f + g)$ if $\boldsymbol{s} \neq \boldsymbol{t}$
- We define regular S-polynomials and regular reductions in that way

Module framework

Setting:

- Input: $f_1, \dots, f_m \in A = R[\boldsymbol{X}]$ spanning the ideal I
- Module $M = A\boldsymbol{e}_1 \oplus \dots \oplus A\boldsymbol{e}_m \simeq A^m$ with the map $M \to I$, $\boldsymbol{e}_i \mapsto f_i$
- Monomials in M are ordered with an ordering compatible with that on A
- Signature-polynomial pair: $(\boldsymbol{s}, f)$ with $f = \sum a_i f_i$ and $\boldsymbol{s} = \mathrm{LM}(\sum a_i \boldsymbol{e}_i)$
- Syzygy in M: $\boldsymbol{z} = \sum z_i \boldsymbol{e}_i \in M$ such that $\sum z_i f_i = 0$

Regular operations:

- Multiplying a sig-poly pair by a term in A is easy
- We can only compute the result of regular additions: $(\boldsymbol{s}, f) + (\boldsymbol{t}, g) = (\max(\boldsymbol{s}, \boldsymbol{t}), f + g)$ if $\boldsymbol{s} \neq \boldsymbol{t}$
- We define regular S-polynomials and regular reductions in that way

s-reductions: $(\mathrm{sig}(\boldsymbol{f}), f)$ s-reduces to $(\mathrm{sig}(\boldsymbol{h}), h)$ modulo $(\mathrm{sig}(\boldsymbol{g}), g)$ if:

- $t\mathrm{LT}(f) = \mathrm{LT}(f)$
- $h = f - tg$
- $t\,\mathrm{sig}(\boldsymbol{g}) \leq \mathrm{sig}(\boldsymbol{f})$

“A s-reduction doesn’t increase the signature, a regular reduction doesn’t change it.”

Signature Gröbner bases

Signature Gröbner basis:

- set $\mathcal{G}$ of sig-poly pairs such that every sig-poly pair of M is s-reducible modulo $\mathcal{G}$
- Property: the polynomial parts of a S-GB form a Gröbner basis

Signature basis of syzygies:

- set $\mathcal{Z}$ of signatures such that every syzygy in M is reducible modulo $\mathcal{Z}$
- equivalently, generating set for the leading terms of the syzygies in M

Signature Gröbner bases

Signature Gröbner basis:

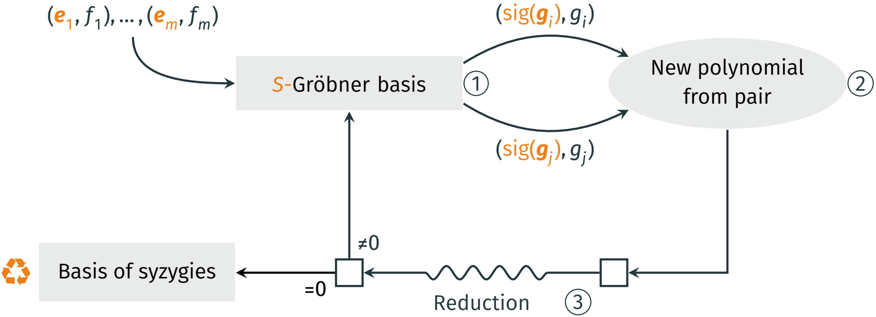
- set $\mathcal{G}$ of sig-poly pairs such that every sig-poly pair of M is s-reducible modulo $\mathcal{G}$
- Property: the polynomial parts of a S-GB form a Gröbner basis

Signature basis of syzygies:

- set $\mathcal{Z}$ of signatures such that every syzygy in M is reducible modulo $\mathcal{Z}$
- equivalently, generating set for the leading terms of the syzygies in M

Buchberger's algorithm, with signatures and restricted to regular operations, computes both of those

Buchberger's algorithm with signatures


$(\boldsymbol{e}_1, f_1), \ldots, (\boldsymbol{e}_m, f_m)$
S-Gröbner basis
①
$(\mathrm{sig}(\boldsymbol{g}_i), g_i)$
$(\mathrm{sig}(\boldsymbol{g}_j), g_j)$
New polynomial from pair
②
$\neq 0$
$=0$
Basis of syzygies
Reduction
③

1. **Selection**: non-decreasing signatures
2. **Construction**: regular S-polynomials
3. **Reduction** (regular)

Why do we care? 1: Criteria

Singular criterion

- if two regular-reduced elements have the same signature, they s-reduce each other
- Consequence: it is enough to add one of them
- Consequence: we can discard singular reducible elements after reduction

Syzygy criterion

- if $(\boldsymbol{s}, 0)$ is a sig-poly pair, any element with signature divisible by $\boldsymbol{s}$ regular-reduces to 0
- Consequence: we can discard such elements before computing the S-pol

F5 criterion

- $\operatorname{sig}(f_i \boldsymbol{e}_j - f_j \boldsymbol{e}_i) = \max\big(\mathrm{LM}(f_i)\boldsymbol{e}_j, \mathrm{LM}(f_j)\boldsymbol{e}_i\big)$ is the signature of a syzygy
- Consequence: we can add them to the basis of syzygies early

Why do we care? 2: Module computations

Theorem [Gao, Volny, Wang 2015]

Given $\mathcal{G}$ a signature Gröbner basis and $\mathcal{Z}$ a signature basis of syzygies, one can reconstruct:

- a Gröbner basis with coordinates $\mathcal{G}_{\text{full}}$;
- a Gröbner basis of the module of syzygies $\mathcal{Z}_{\text{full}}$.

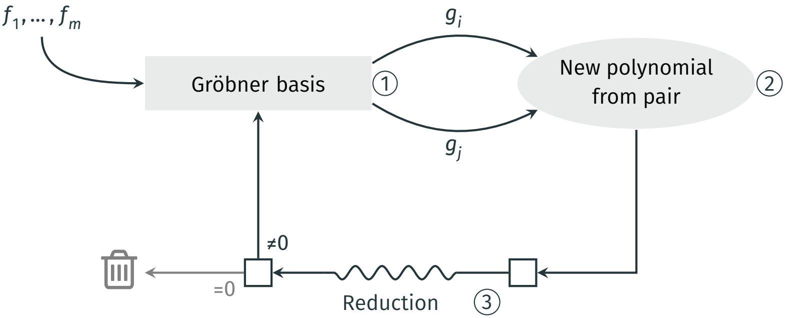
Reconstructing the module elements from the signatures

In
- $\mathcal{G} = \{(\boldsymbol{s}_i, g_i)\}$ a signature Gröbner basis
- $\mathcal{Z} = \{(\boldsymbol{z}_i, 0)\}$ a signature basis of syzygies

Out
- $\mathcal{G}_{\text{full}}$ a Gröbner basis with coordinates
- $\mathcal{Z}_{\text{full}}$ a Gröbner basis of the module of syzygies

```
1. $\mathcal{G}_{\text{full}} \leftarrow \{(\boldsymbol{e}_i, f_i) : i \in \{1, \dots, m\}\}$ (reducing if needed)
2. For $(\boldsymbol{s}_i, g_i) \in \mathcal{G}$ in increasing order of signatures, do
   2.1 Find $\boldsymbol{g}_j \in \mathcal{G}_{\text{full}}$ s.t. there exists a term $t$ with $t\text{sig}(\boldsymbol{g}_j) = \boldsymbol{s}_i$ (and $t\text{LM}(\boldsymbol{g}_j)$ minimal)
   2.2 Perform regular reductions of $t\boldsymbol{g}_j$ by $\mathcal{G}_{\text{full}}$ until not reducible
   2.3 Add the result to $\mathcal{G}_{\text{full}}$
3. With $\mathcal{G}_{\text{full}}$ known, reconstruct $\mathcal{Z}_{\text{full}}$ in the same way
```

Non-commutative Buchberger's algorithm



1. **Selection**: fair selection strategy *"Every S-polynomial is selected eventually."*
2. **Construction**: S-polynomials
3. **Reduction**

Constructions in the non-commutative case

Several ways to make S-polynomials

- **Overlap ambiguity**

  f = 🟩🟥 + ⋯

  g = 🟥🟦 + ⋯

  SPol(f, g) = f 🟦 − 🟩 g

- **Inclusion ambiguity**

  f = 🟥 + ⋯

  g = 🟩🟥🟦 + ⋯

  SPol(f, g) = 🟩 f 🟦 − g

Constructions in the non-commutative case

Several ways to make S-polynomials

- **Overlap ambiguity**

  $f =$ 🟩🟥 $+ \cdots$

  $g =$ 🟥🟦 $+ \cdots$

  $\mathrm{SPol}(f,g) = f$ 🟦 $-$ 🟩 g

- **Inclusion ambiguity**

  $f =$ 🟥 $+ \cdots$

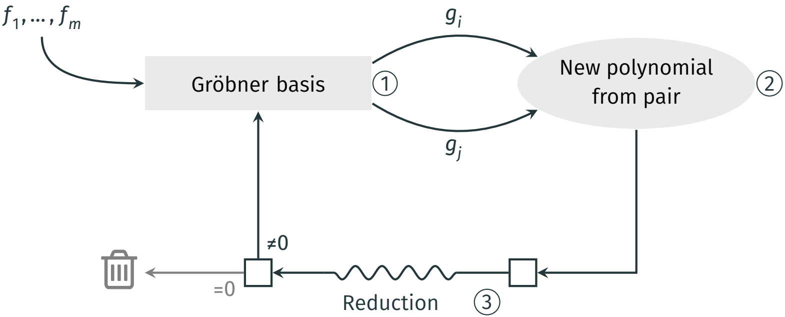
  $g =$ 🟩🟥🟦 $+ \cdots$

  $\mathrm{SPol}(f,g) =$ 🟩 f 🟦 $- g$

Remarks:

- The combination need not be minimal, and S-polynomials are not unique!
- $xyxy$ has an (overlap) ambiguity with itself: $xyxy$
  $xyxy$
- $xxyx$ and xy have two ambiguities: $xxyx$ / xy and $xxyx$ / xy
- Two polynomials can only give rise to finitely many S-polynomials
- It is required that the central part is non-trivial (coprime criterion)

Non-commutative Buchberger's algorithm



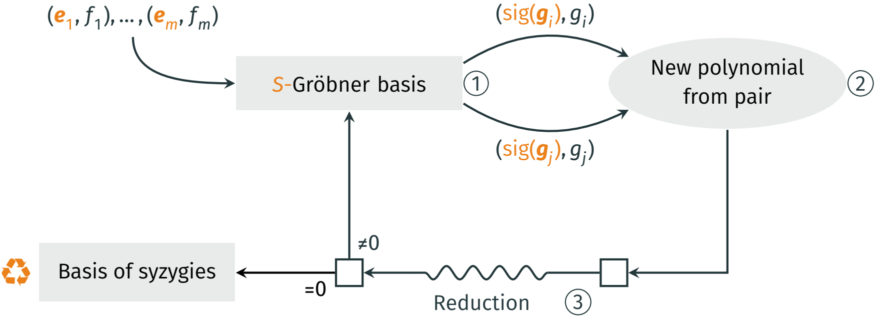
1. **Selection**: fair selection strategy *“Every S-polynomial is selected eventually.”*
2. **Construction**: S-polynomials
3. **Reduction**

Signatures for non-commutative polynomials

Non-commutative setting:

- Bimodule $M = A\boldsymbol{e}_1 A \oplus \cdots \oplus A\boldsymbol{e}_m A$ with the expected morphism $M \to A$ with image I
- Equipped with a module monomial ordering as before
- The ordering must additionally be fair (isomorphic to $\mathbb{N}$)
- Sig-poly pairs $(\boldsymbol{s}, f)$ with $f = \sum a_i f_i b_i$ and $\boldsymbol{s} = \mathrm{LM}(\sum a_i \boldsymbol{e}_i b_i)$
- Regular S-polynomials and reductions are defined as before

Non-commutative Buchberger's algorithm with signatures



$(\boldsymbol{e}_1, f_1), \dots, (\boldsymbol{e}_m, f_m)$
S-Gröbner basis
①
$(\mathrm{sig}(\boldsymbol{g}_i), g_i)$
$(\mathrm{sig}(\boldsymbol{g}_j), g_j)$
New polynomial from pair
②
≠0
=0
Basis of syzygies
Reduction
③

1. **Selection**: non-decreasing signatures for a fair ordering
2. **Construction**: regular S-polynomials
3. **Reduction** (regular)

Termination

Question 1: Does the algorithm always terminate?

Termination

Question 1: Does the algorithm always terminate?

- Of course not, because most ideals do not have a finite Gröbner basis.

Termination: trivial syzygies

Question 1: Does the algorithm always terminate?

- Of course not, because most ideals do not have a finite Gröbner basis.

Question 2: Okay, but what if they do?

Termination: trivial syzygies and how to find them

Question 1: Does the algorithm always terminate?

- Of course not, because most ideals do not have a finite Gröbner basis.

Question 2: Okay, but what if they do?

- Still not. In most cases, the module of syzygies does not have a finite Gröbner basis
- Conjecture: it's always the case if $n > 1$ (non-commutative) and $m > 1$ (non-principal)

Termination: trivial syzygies and how to find them

Question 1: Does the algorithm always terminate?

- Of course not, because most ideals do not have a finite Gröbner basis.

Question 2: Okay, but what if they do?

- Still not. In most cases, the module of syzygies does not have a finite Gröbner basis
- Conjecture: it's always the case if $n > 1$ (non-commutative) and $m > 1$ (non-principal)

Obstruction: Trivial syzygies! [Hofstadler V. 2021] [Chenavier Léonard Vaccon 2021]

- Syzygies of the form $\boldsymbol{f} \blacksquare g - f \blacksquare \boldsymbol{g}$ for any monomial ■
- Signature: $\max\big(\mathrm{sig}(\boldsymbol{f}) \blacksquare \mathrm{LM}(g), \mathrm{LM}(f) \blacksquare \mathrm{sig}(\boldsymbol{g})\big)$
- Because ■ is put in the middle, this set is usually not finitely generated

Termination: trivial syzygies and how to find them

Question 1: Does the algorithm always terminate?

- Of course not, because most ideals do not have a finite Gröbner basis.

Question 2: Okay, but what if they do?

- Still not. In most cases, the module of syzygies does not have a finite Gröbner basis
- Conjecture: it's always the case if $n > 1$ (non-commutative) and $m > 1$ (non-principal)

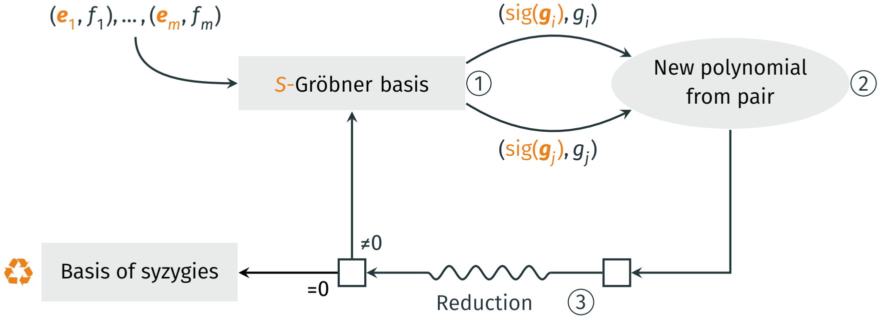
Obstruction: Trivial syzygies! [Hofstadler V. 2021] [Chenavier Léonard Vaccon 2021]

- Syzygies of the form $\boldsymbol{f} \blacksquare g - f \blacksquare \boldsymbol{g}$ for any monomial $\blacksquare$
- Signature: $\max\big(\mathrm{sig}(\boldsymbol{f}) \blacksquare \mathrm{LM}(g), \mathrm{LM}(f) \blacksquare \mathrm{sig}(\boldsymbol{g})\big)$
- Because $\blacksquare$ is put in the middle, this set is usually not finitely generated

Solution: Signatures!

- Identifying trivial syzygies is what signatures were made for (F5 criterion)
- Not just an optimization, but necessary for termination for some ideals

Non-commutative Buchberger's algorithm with signatures


$(\boldsymbol{e}_1, f_1), \dots, (\boldsymbol{e}_m, f_m)$
S-Gröbner basis
①
$(\mathrm{sig}(\boldsymbol{g}_i), g_i)$
$(\mathrm{sig}(\boldsymbol{g}_j), g_j)$
New polynomial from pair
②
$\neq 0$
$=0$
Basis of syzygies
Reduction
③

1. **Selection**: non-decreasing signatures
2. **Construction**: regular S-polynomials which are not eliminated by the F5 criterion
3. **Reduction** (regular)

What do we get?

Output of the algorithm: a Gröbner basis with signatures, allowing to recover

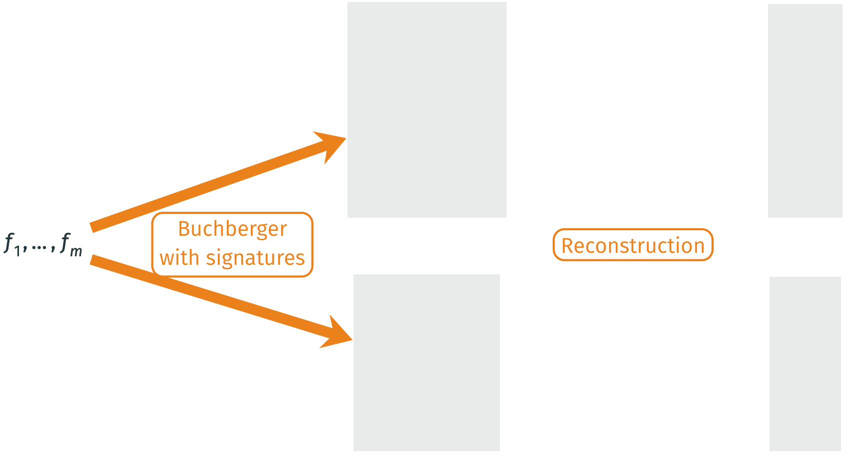
- a Gröbner basis $\mathcal{G}$ with the coordinates
- a set $\mathcal{H}$ of syzygies such that $\mathcal{H} \cup \{\text{trivial syzygies of } \mathcal{G}\}$ is a basis of the module of syzygies
- a way to test if any module monomial is the leading term of a syzygy

Results:

- The algorithm enumerates a signature Gröbner basis, by increasing order of signatures
- The algorithm terminates iff the ideal admits a finite signature Gröbner basis
- This implies that the ideal admits a finite GB and a finite "basis of non-trivial syzygies" $\mathcal{H}$
- **Conjecture**: the converse holds

This is the first algorithm producing an effective representation
of some modules of syzygies in the free algebra!

Reconstruction in the non-commutative case



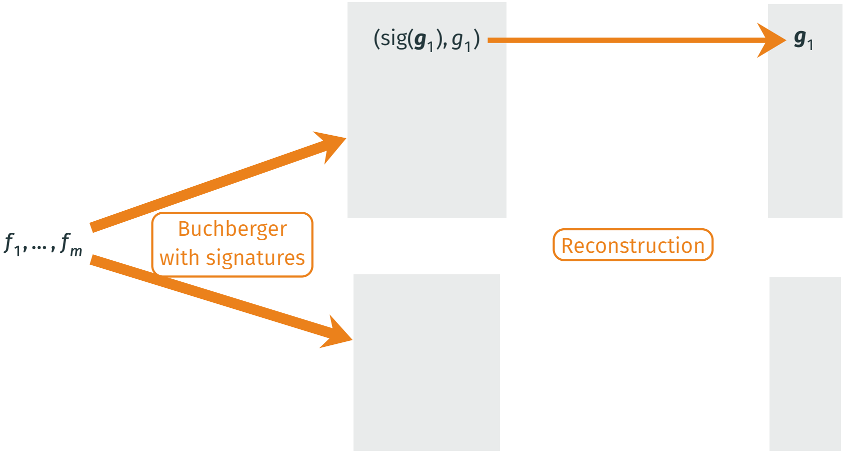
$f_1, \dots, f_m$

Buchberger with signatures

Reconstruction

- The reconstruction can work with partial output from Buchberger+signatures
- The reconstruction terminates with finite input

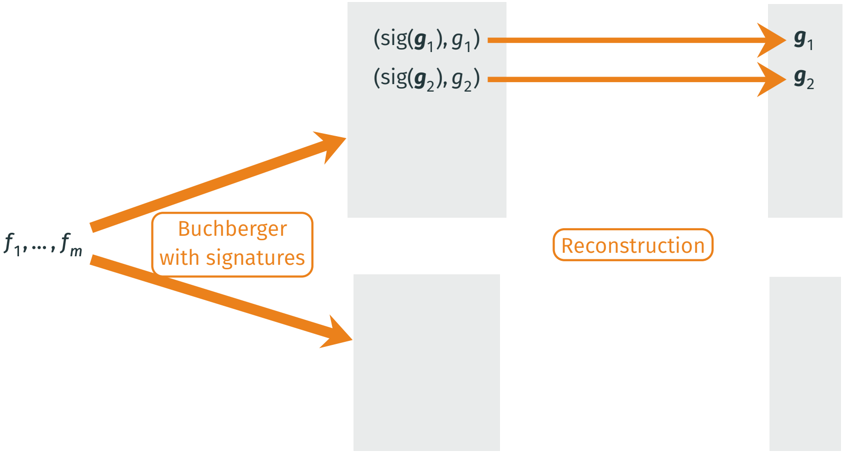
Reconstruction in the non-commutative case



$(\mathrm{sig}(\boldsymbol{g}_1), g_1)$
$\boldsymbol{g}_1$
$f_1, \dots, f_m$
Buchberger with signatures
Reconstruction

- The reconstruction can work with partial output from Buchberger+signatures
- The reconstruction terminates with finite input

Reconstruction in the non-commutative case



$f_1, \dots, f_m$

Buchberger with signatures

$(\mathrm{sig}(\boldsymbol{g}_1), g_1)$

$(\mathrm{sig}(\boldsymbol{g}_2), g_2)$

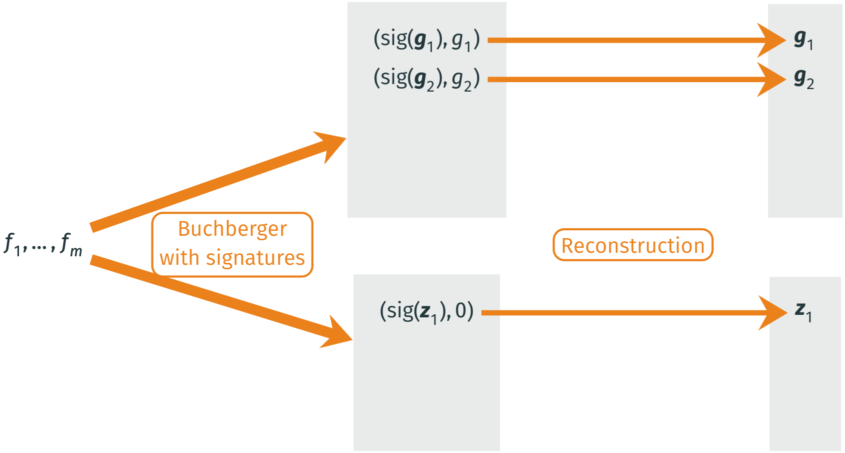
Reconstruction

$\boldsymbol{g}_1$

$\boldsymbol{g}_2$

- The reconstruction can work with partial output from Buchberger+signatures
- The reconstruction terminates with finite input

Reconstruction in the non-commutative case



$f_1, \dots, f_m$

Buchberger with signatures

$(\mathrm{sig}(\boldsymbol{g}_1), g_1)$

$(\mathrm{sig}(\boldsymbol{g}_2), g_2)$

$(\mathrm{sig}(\boldsymbol{z}_1), 0)$

Reconstruction

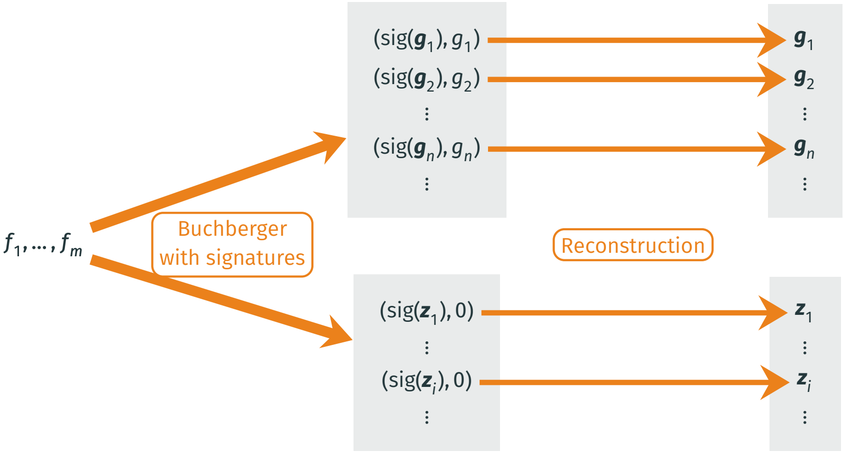
$\boldsymbol{g}_1$

$\boldsymbol{g}_2$

$\boldsymbol{z}_1$

- The reconstruction can work with partial output from Buchberger+signatures
- The reconstruction terminates with finite input

Reconstruction in the non-commutative case



$f_1, \dots, f_m$
Buchberger with signatures
$(\mathrm{sig}(\boldsymbol{g}_1), g_1)$
$(\mathrm{sig}(\boldsymbol{g}_2), g_2)$
$\vdots$
$(\mathrm{sig}(\boldsymbol{g}_n), g_n)$
$\vdots$
$\boldsymbol{g}_1$
$\boldsymbol{g}_2$
$\vdots$
$\boldsymbol{g}_n$
$\vdots$
Reconstruction
$(\mathrm{sig}(\boldsymbol{z}_1), 0)$
$\vdots$
$(\mathrm{sig}(\boldsymbol{z}_i), 0)$
$\vdots$
$\boldsymbol{z}_1$
$\vdots$
$\boldsymbol{z}_i$
$\vdots$

- The reconstruction can work with partial output from Buchberger+signatures
- The reconstruction terminates with finite input

Implementation

What we have

- Toy implementation in Mathematica
- Part of the package `OperatorGB`: `https://clemenshofstadler.com/software/`

Example	Signature			Buchberger			Buchberger + chain		
	S-poly	Red 0	Time	S-poly	Red 0	Time	S-poly	Red 0	Time
`lv2-100`	201	0	60	9702	4990	43	9702	4990	46
`tri1`	335	164	62	9435	8897	16	3480	3288	6

Remarks

- The F5 criterion is necessary to maximize the chances of the algorithm terminating
- The PoT ordering is not fair
- The F5 criterion is expensive! (quadratic in the size of $\mathcal{G}$)
- Reconstruction of the module representation can be very expensive
  (no bound on the rank of the tensors)

Conclusion

This work

- Signature-based algorithm enumerating signature Gröbner bases in the free algebra
- Terminates whenever a finite signature Gröbner basis exists
- Taking care of trivial syzygies is necessary for termination
- Effective and finite representation of the module of syzygies in some non-trivial cases

Open questions and future directions

- Conjecture on characterization of existence of finite signature Gröbner basis
- Use of signatures for the computation of short representations
- Computations in quotients of the algebra, elimination…

More details and references

- Hofstadler and Verron, *Signature Gröbner bases, bases of syzygies and cofactor reconstruction in the free algebra*, Journal of Symbolic Computation 2022

Conclusion

This work

- Signature-based algorithm enumerating signature Gröbner bases in the free algebra
- Terminates whenever a finite signature Gröbner basis exists
- Taking care of trivial syzygies is necessary for termination
- Effective and finite representation of the module of syzygies in some non-trivial cases

Open questions and future directions

- Conjecture on characterization of existence of finite signature Gröbner basis
- Use of signatures for the computation of short representations
- Computations in quotients of the algebra, elimination...

More details and references

- Hofstadler and Verron, *Signature Gröbner bases, bases of syzygies and cofactor reconstruction in the free algebra*, Journal of Symbolic Computation 2022

Merci pour votre attention !