Signature Gröbner bases in the free algebra

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

Journées Nationales de Calcul Formel 2022, 3 mars 2022

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

Gröbner bases

Gröbner bases for commutative polynomials:

- Ideal Membership Problem: decide if a polynomial lies in an ideal
- Leads to solving equations (parametrization, elimination, dimension of the solutions...)
- Also simplifications, reductions, computations in modules

Gröbner bases in the non commutative case:

- 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
$p = a_1 f_1 + \dots + a_m f_m$?"

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

Polynomials
$f_1, \dots, f_m$

[Faugère 1999] F4

F4 + tracing

Gröbner basis

Gröbner basis
with coordinates

Ideal Membership Problem

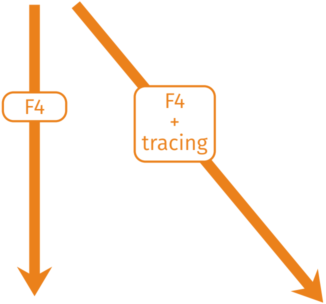
“Does there exist (a_i)
such that
$p = a_1 f_1 + \dots + a_m f_m$?”

IMP with certificate

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

Polynomials
$f_1, \dots, f_m$

[Faugère 1999]



Gröbner basis

Gröbner basis
with coordinates

Ideal Membership Problem

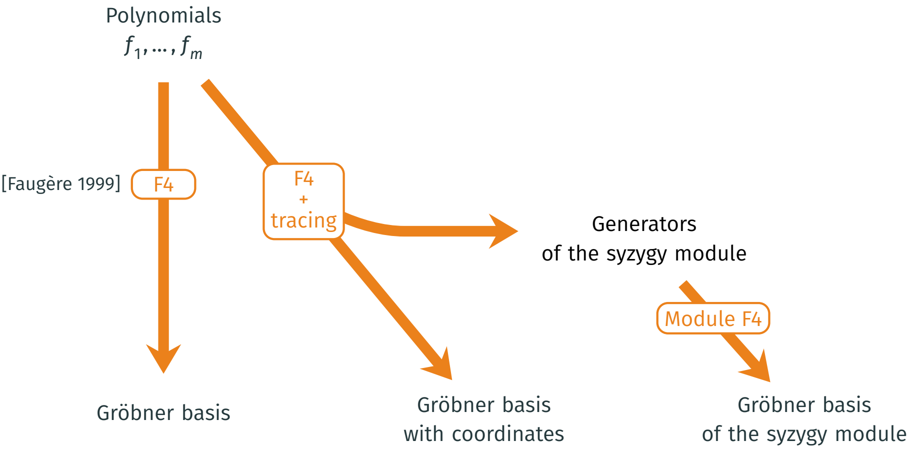
"Does there exist (a_i) such that $p = a_1 f_1 + \dots + a_m f_m$?"

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 $a_1 f_1 + \dots + a_m f_m = 0$"



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

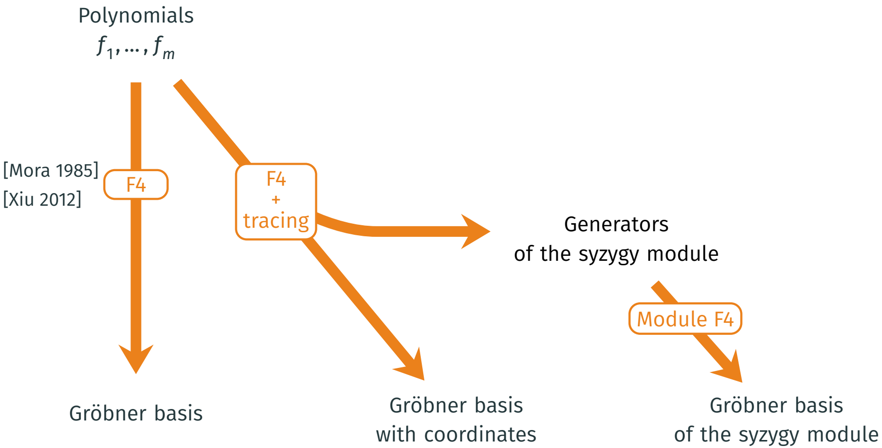
*"Does there exist (a_i)
such that
$p = a_1 f_1 + \cdots + a_m f_m$?"*

IMP with certificate

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

Module of syzygies

*"Find all (a_i)
such that
$a_1 f_1 + \cdots + a_m f_m = 0$"*



Ideal Membership Problem

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

IMP with certificate

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

Module of syzygies

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

Polynomials
$f_1, \dots, f_m$

F5/GVW

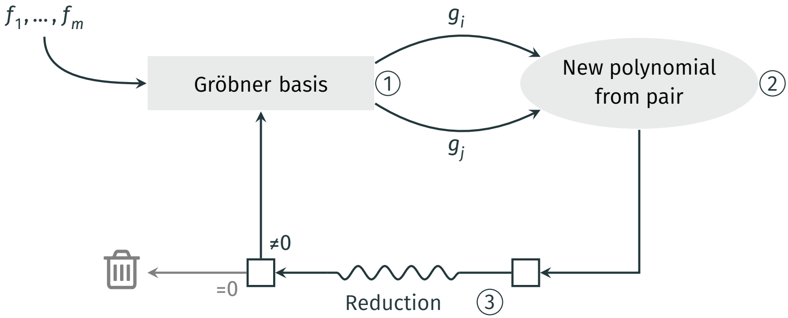
Gröbner basis
with signatures

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	**IMP with certificate**	**Module of syzygies**
"Does there exist (a_i, b_j) such that $p = a_1 f_1 b_1 + \dots + a_m f_m b_m$?"	*"Compute (a_i, b_j) such that $p = a_1 f_1 b_1 + \dots + a_m f_m b_m$"*	*"Find all (a_i, b_j) such that $a_1 f_1 b_1 + \dots + a_m f_m b_m = 0$"*

Non-commutative Buchberger's algorithm



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

Several ways to make S-polynomials

- **Overlap ambiguity**

- **Inclusion ambiguity**

Several ways to make S-polynomials

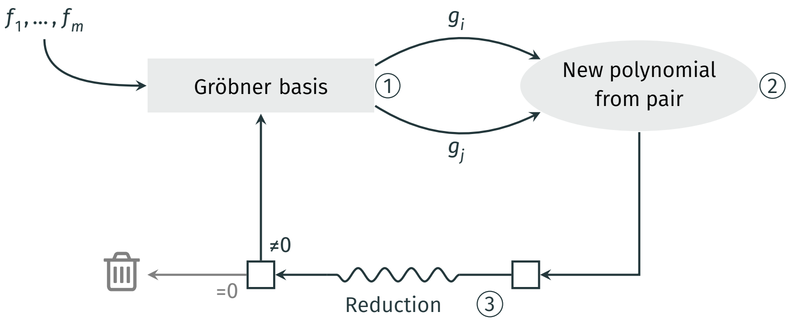
- **Overlap ambiguity**

- **Inclusion ambiguity**

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**

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 $\boldsymbol{s} = \mathrm{LM}(\sum a_i \boldsymbol{e}_i)$

Constructions with signatures

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 $\boldsymbol{s} = \mathrm{LM}(\sum a_i \boldsymbol{e}_i)$

Regular operations:

- Multiplying sig-poly pair by a term in A is easy
- Additions are required to be regular: $(\boldsymbol{s}, f) + (\boldsymbol{t}, g) = (\max(\boldsymbol{s}, \boldsymbol{t}), f + g)$ if $\boldsymbol{s} \neq \boldsymbol{t}$
- We define regular S-polynomials and regular reductions in that way

Setting:

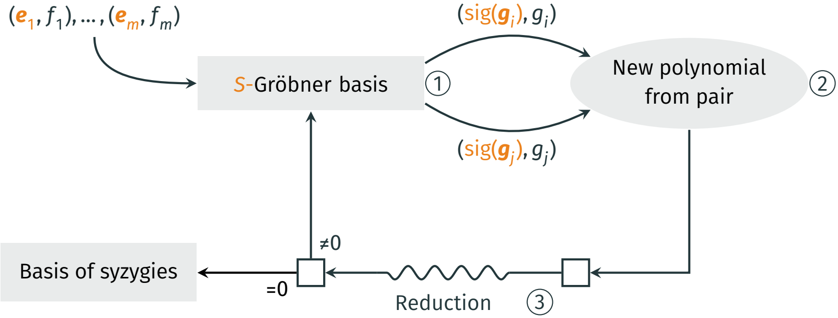
- Input: $f_1, \dots, f_m \in A = R[\boldsymbol{X}]$ spanning the ideal I
- Module $M = A\boldsymbol{e}_1 \oplus \cdots \oplus A\boldsymbol{e}_m \simeq A^m$ with the map $M \to I$, $\boldsymbol{e}_i \mapsto f_i$
- Monomials in M are ordered with an ordering compatible with that on A
- Signature-polynomial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

Regular operations:

- Multiplying sig-poly pair by a term in A is easy
- Additions are required to be regular: $(\boldsymbol{s}, f) + (\boldsymbol{t}, g) = (\max(\boldsymbol{s}, \boldsymbol{t}), f + g)$ if $\boldsymbol{s} \neq \boldsymbol{t}$
- We define regular S-polynomials and regular reductions in that way

Criteria:

- Syzygy criterion: if $(\boldsymbol{s}, 0)$ is a sig-poly pair,
  any element with signature divisible by $\boldsymbol{s}$ regular-reduces to 0
- F5 criterion: any element with signature divisible by
  $\mathrm{LM}(f_i\boldsymbol{e}_j - f_j\boldsymbol{e}_i) = \max\left(\mathrm{LM}(f_i)\boldsymbol{e}_j, \mathrm{LM}(f_j)\boldsymbol{e}_i\right)$ regular-reduces to 0

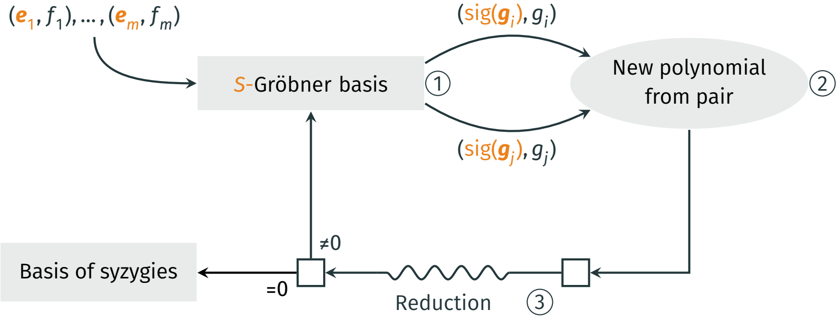


1. **Selection**: non-decreasing signatures
2. **Construction**: regular S-polynomials
3. **Reduction** (regular)

Non-commutative setting:

- Bimodule $M = A\boldsymbol{e}_1A \oplus \cdots \oplus A\boldsymbol{e}_mA$ 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



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

Question 1: Does the algorithm always terminate?

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 $\blacksquare$
- 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

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?

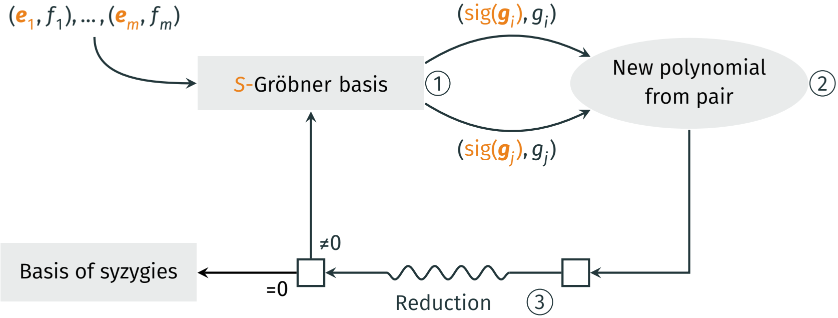
- Still not. In most cases, the module of syzygies does not have a finite Gröbner basis
- Conjecture: it's always the case if $n > 1$ (non-commutative) and $m > 1$ (non-principal)

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: $\max\bigl(\mathrm{sig}(\boldsymbol{f}) \blacksquare \mathrm{LM}(g), \mathrm{LM}(f) \blacksquare \mathrm{sig}(\boldsymbol{g})\bigr)$
- 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



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 such a signature Gröbner basis
- 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!

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*, `ArXiV:2107.14675`

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*, `ArXiV:2107.14675`

Merci pour votre attention !