Introduction to linear rewriting: Gröbner bases and reduction operators

Cyrille Chenavier

Algebraic rewriting Seminar

February 25, 2021





I. Motivations

- ▷ Effective algebraic computation
- ▷ Formalisation of algebraic computation

II. Commutative Gröbner bases

- > Polynomial reduction and Gröbner bases
- ▷ Completion algorithms

III. Noncommutative Gröbner bases

- Noncommutative polynomial reduction
- ▷ Anick's resolution and Koszulness

IV. Reduction operators

- > Functional representation of linear rewriting systems
- $\triangleright~$ Lattice characterisation of confluence and completion

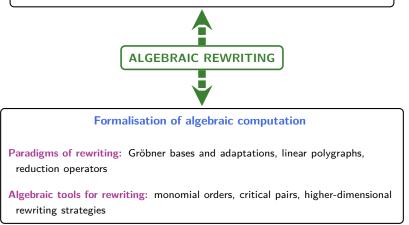
I. MOTIVATIONS

Effective algebraic computation

Objective: compute with (non)commutative/Lie/tree polynomials

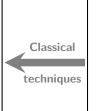
 $\boldsymbol{\rightarrow}$ membership problem, computation of representatives and linear bases

Application scopes: algebraic geometry/combinatorics, homological algebra, formal analysis of functional equations, cryptography



Some algorithmic problems in algebra

- solve decision problems (*e.g.*, membership problem)
- compute homological invariants (*e.g.*, Tor, Ext groups)
- analysis of functional systems (*e.g.*, integrability conditions)

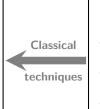


Constructive methods in algebra

- compute set of representatives for congruence classes
- construct free resolutions of modules
- elimination theory for systems of equations

Some algorithmic problems in algebra

- solve decision problems (*e.g.*, membership problem)
- compute homological invariants (*e.g.*, Tor, Ext groups)
- analysis of functional systems (*e.g.*, integrability conditions)



Constructive methods in algebra

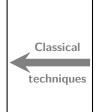
- compute set of representatives for congruence classes
- construct free resolutions of modules
- elimination theory for systems of equations

ALGEBRAIC REWRITING

Approach: orientation of relations \rightarrow notion of normal formexample: chosen orientation in $\mathbb{K}[x, y]$ \rightarrow induced by $yx \rightarrow xy$ NF computation: $3 yxx + xyx - xy \rightarrow 4 xyx - xy \rightarrow 4 xxy - xy$

Some algorithmic problems in algebra

- solve decision problems (*e.g.*, membership problem)
- compute homological invariants (*e.g.*, Tor, Ext groups)
- analysis of functional systems (*e.g.*, integrability conditions)



Constructive methods in algebra

- compute set of representatives for congruence classes
- construct free resolutions of modules
- elimination theory for systems of equations

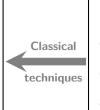
ALGEBRAIC REWRITING

Approach: orientation of relations \rightarrow notion of normal form example: chosen orientation in $\mathbb{K}[x, y] \rightarrow$ induced by $yx \rightarrow xy$

NF computation: 3 $yxx + xyx - xy \rightarrow 4 xyx - xy \rightarrow 4 xxy - xy$

Some algorithmic problems in algebra

- solve decision problems (*e.g.*, membership problem)
- compute homological invariants (*e.g.*, Tor, Ext groups)
- analysis of functional systems (*e.g.*, integrability conditions)



Constructive methods in algebra

- compute set of representatives for congruence classes
- construct free resolutions of modules
- elimination theory for systems of equations

ALGEBRAIC REWRITING

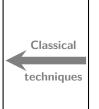
Approach: orientation of relations \rightarrow notion of normal form

example: chosen orientation in $\mathbb{K}[x, y] \rightarrow$ induced by $yx \rightarrow xy$

NF computation: $3 yxx + xyx - xy \rightarrow 4 xyx - xy \rightarrow 4 xxy - xy$

Some algorithmic problems in algebra

- solve decision problems (*e.g.*, membership problem)
- compute homological invariants (*e.g.*, Tor, Ext groups)
- analysis of functional systems (*e.g.*, integrability conditions)



Constructive methods in algebra

- compute set of representatives for congruence classes
- construct free resolutions of modules
- elimination theory for systems of equations

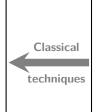
ALGEBRAIC REWRITING

Approach: orientation of relations \rightarrow notion of normal form example: chosen orientation in $\mathbb{K}[x, y] \rightarrow$ induced by $yx \rightarrow xy$

NF computation: $3 yxx + xyx - xy \rightarrow 4 xyx - xy \rightarrow 4 xxy - xy$

Some algorithmic problems in algebra

- solve decision problems (*e.g.*, membership problem)
- compute homological invariants (*e.g.*, Tor, Ext groups)
- analysis of functional systems (*e.g.*, integrability conditions)



Constructive methods in algebra

- compute set of representatives for congruence classes
- construct free resolutions of modules
- elimination theory for systems of equations

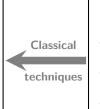
ALGEBRAIC REWRITING

Approach: orientation of relations \rightarrow notion of normal form example: chosen orientation in $\mathbb{K}[x, y] \rightarrow$ induced by $yx \rightarrow xy$

NF computation: $3 yxx + xyx - xy \rightarrow 4 xyx - xy \rightarrow 4 xxy - xy$

Some algorithmic problems in algebra

- solve decision problems (*e.g.*, membership problem)
- compute homological invariants (*e.g.*, Tor, Ext groups)
- analysis of functional systems (*e.g.*, integrability conditions)



Constructive methods in algebra

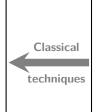
- compute set of representatives for congruence classes
- construct free resolutions of modules
- elimination theory for systems of equations

ALGEBRAIC REWRITING

Approach: orientation of relations \rightarrow notion of normal formexample: chosen orientation in $\mathbb{K}[x, y]$ \rightarrow induced by $yx \rightarrow xy$ NF computation: $3 yxx + xyx - xy \rightarrow 4 xyx - xy \rightarrow 4 xxy - xy$

Some algorithmic problems in algebra

- solve decision problems (*e.g.*, membership problem)
- compute homological invariants (*e.g.*, Tor, Ext groups)
- analysis of functional systems (*e.g.*, integrability conditions)



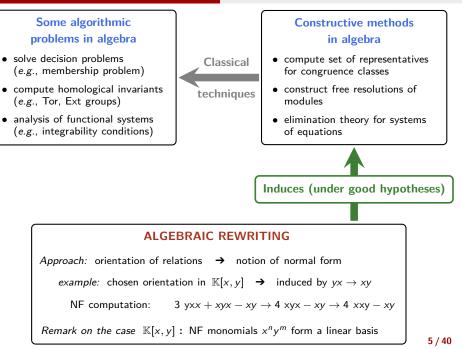
Constructive methods in algebra

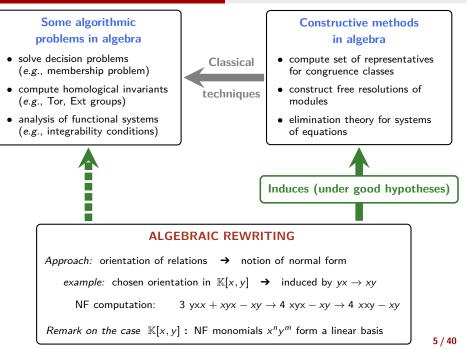
- compute set of representatives for congruence classes
- construct free resolutions of modules
- elimination theory for systems of equations

ALGEBRAIC REWRITING

Approach: orientation of relations \rightarrow notion of normal form example: chosen orientation in $\mathbb{K}[x, y] \rightarrow$ induced by $yx \rightarrow xy$

NF computation: $3 yxx + xyx - xy \rightarrow 4 xyx - xy \rightarrow 4 xxy - xy$





MOTIVATING PROBLEM

Given an algebra $\mathbf{A} := \mathbb{K} \langle X \mid R \rangle$ presented by generators X and relations R

 $\mathbf{A} := \mathbb{K} \langle X \rangle / I(R) \qquad \left(e.g., \quad \mathbb{K}[x, y] = \mathbb{K} \langle x, y \mid yx - xy \rangle \right)$

Question: given an orientation of *R* (*e.g.*, $yx \rightarrow xy$)

do NF monomials form a linear basis of A?

MOTIVATING PROBLEM

Given an algebra $\mathbf{A} := \mathbb{K} \langle X \mid R \rangle$ presented by generators X and relations R

 $\mathbf{A} := \mathbb{K} \langle X \rangle / I(R) \qquad \left(e.g., \quad \mathbb{K}[x, y] = \mathbb{K} \langle x, y \mid yx - xy \rangle \right)$

Question: given an orientation of R (e.g., $yx \rightarrow xy$)

do NF monomials form a linear basis of A?

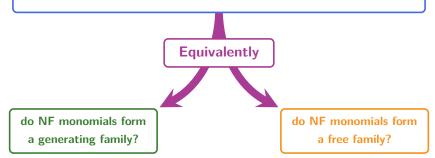
MOTIVATING PROBLEM

Given an algebra $\mathbf{A} := \mathbb{K} \langle X \mid R \rangle$ presented by generators X and relations R

 $\mathbf{A} := \mathbb{K} \langle X \rangle / I(R) \qquad \left(e.g., \quad \mathbb{K}[x, y] = \mathbb{K} \langle x, y \mid yx - xy \rangle \right)$

Question: given an orientation of *R* (*e.g.*, $yx \rightarrow xy$)

do NF monomials form a linear basis of A?



NF monomials do not form a generating family $A := \mathbb{K}\langle x \mid x - xx \rangle$ orientation: $x \to xx$ $\rightarrow \dim_{\mathbb{K}}(A) = 2$ $(\overline{1} \text{ and } \overline{x} \text{ form a basis})$ $\rightarrow 1$ is the only NF monomial $(\forall n \ge 1 : x^n \to x^{n+1})$

 $\begin{array}{l} \text{Definition:} \ \rightarrow \ \text{is called terminating} \\ \text{if} \end{array}$

 \nexists infinite rewriting sequence

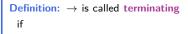
$$f_1 \rightarrow f_2 \rightarrow \cdots \rightarrow f_n \rightarrow f_{n+1} \rightarrow \ldots$$

NF monomials do not form a generating family $A := \mathbb{K}\langle x \mid x - xx \rangle$ orientation: $x \to xx$ $\Rightarrow \dim_{\mathbb{K}}(A) = 2$ $(\overline{1} \text{ and } \overline{x} \text{ form a basis})$ $\Rightarrow 1$ is the only NF monomial $(\forall n \ge 1 : x^n \to x^{n+1})$

∄ infinite rewriting sequence

$$f_1 \rightarrow f_2 \rightarrow \cdots \rightarrow f_n \rightarrow f_{n+1} \rightarrow \ldots$$

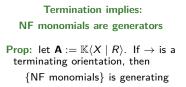
NF monomials do not form a generating family $A := \mathbb{K}\langle x \mid x - xx \rangle$ orientation: $x \to xx$ $\rightarrow \dim_{\mathbb{K}}(A) = 2$ $(\overline{1} \text{ and } \overline{x} \text{ form a basis})$ $\rightarrow 1$ is the only NF monomial $(\forall n \ge 1 : x^n \to x^{n+1})$

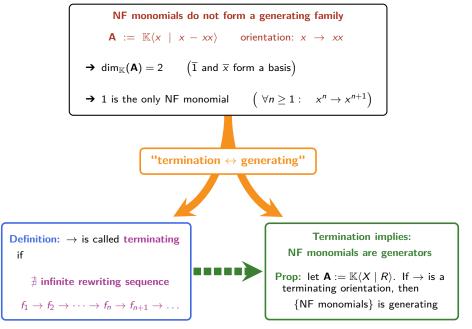


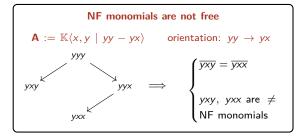
∄ infinite rewriting sequence

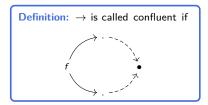
$$f_1 \rightarrow f_2 \rightarrow \cdots \rightarrow f_n \rightarrow f_{n+1} \rightarrow \ldots$$

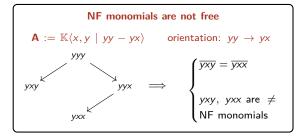


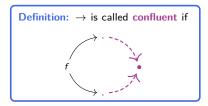


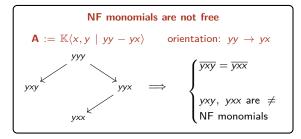


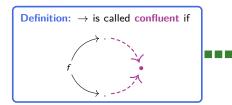


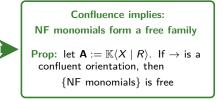


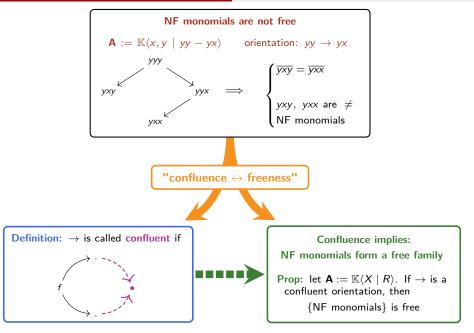








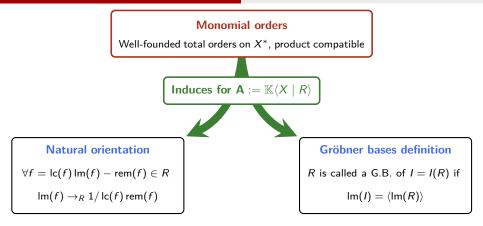




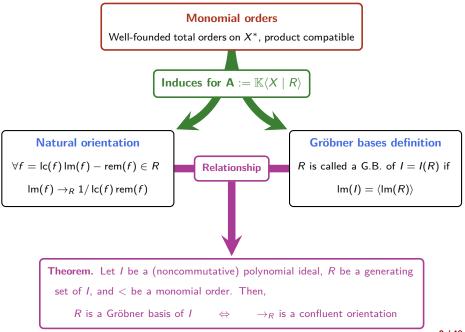
Monomial orders

Well-founded total orders on X^* , product compatible

Gröbner bases and confluent orientations



Gröbner bases and confluent orientations



Objective and plan of the talk

Sections II and II: basics of (noncommutative) Gröbner bases

- → define Gröbner bases in terms of monomials ideals
- → show rewriting characterisation of Gröbner bases
- → present completion algorithms and Anick's resolution

Remark. Gröbner bases have adaptations to many other structures, *e.g.*, Lie algebras, operads, Weyl/Ore algebras, tensor rings

Section IV: introduction to reduction operators

- → definition of reduction operators for vector spaces
- → lattice characterisations of confluence and completion

II. COMMUTATIVE GRÖBNER BASES

Membership problem

Question: given
$$I \subseteq \mathbb{K}[X]$$
 and $g \subseteq \mathbb{K}[X]$

how to compute f mod /?

USING REWRITING!

Case of one variable: we recover Euclidean division, e.g.,

$$f := x^4 + 3x^3 + 2x + 1$$
 and $g := x^2 + 1$

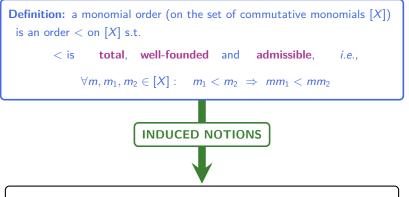
 $f \mod (g)$ is computed by reducing f into NF w.r.t. $x^2
ightarrow -1$

$$x^4 + 3x^3 + 2x + 1 \longrightarrow 3x^3 - x^2 + 2x + 1 \longrightarrow -x^2 - x + 1 \longrightarrow -x + 2$$

→
$$f = (x^2 + 3x - 1) \cdot (x^2 + 1) - x + 2$$

Case of many variables: requires a suitable notion of "leading monomial"

→ based on monomial orders



Leading monomial, leading coefficient and remainder

 $\forall f \in \mathbb{K}[X] \setminus \{0\}$, we define

- → the leading monomial Im(f) of f as being max(supp(f))
- → the leading coefficient lc(f) of f as being the coefficient of lm(f) in f
- → the remainder of f by $\operatorname{rem}(f) = \operatorname{lc}(f) \operatorname{Im}(f) f$

Generalisation of Euclidean division

Let $f, g \in \mathbb{K}[X]$ and $G \subseteq \mathbb{K}[X]$ **Reducing** f w.r.t. g: if $f = \lambda m + f'$, with m = Im(g)m', $m \notin \text{supp}(f')$ and $\lambda \neq 0$, then, we have: $f \rightarrow_g \frac{\lambda}{\operatorname{lc}(f)} \Big(m' . \operatorname{rem}(g) \Big) + f'$ **Reducing** f w.r.t. G: $f \rightarrow_G f'$ iff $\exists g \in G : f \rightarrow_g f'$ A NF of f for \rightarrow_G is also called a remainder of f w.r.t. G THE REMAINDER IS NOT UNIQUE IN GENERAL Example: $G := \{g_1, g_2\}$ with $g_1 := xy^2 + x$ and $g_2 := 2y^3 + xy - 1$ xy^3 has two remainders: -xy and -x/2.(xy-1)

Generalisation of Euclidean division

Let $f, g \in \mathbb{K}[X]$ and $G \subseteq \mathbb{K}[X]$ **Reducing** f w.r.t. g: if $f = \lambda m + f'$, with m = Im(g)m', $m \notin \text{supp}(f')$ and $\lambda \neq 0$, then, we have: $f \rightarrow_g \frac{\lambda}{\operatorname{lc}(f)} \Big(m' . \operatorname{rem}(g) \Big) + f'$ **Reducing** f w.r.t. G: $f \rightarrow_G f'$ iff $\exists g \in G : f \rightarrow_g f'$ A NF of f for \rightarrow_G is also called a remainder of f w.r.t. G THE REMAINDER IS NOT UNIQUE IN GENERAL Example: $G := \{g_1, g_2\}$ with $g_1 := xy^2 + x$ and $g_2 := 2y^3 + xy - 1$ xy^3 has two remainders: -xy and -x/2.(xy-1)

Definition: let $I \subseteq \mathbb{K}[X]$ and let < be a monomial order on [X].

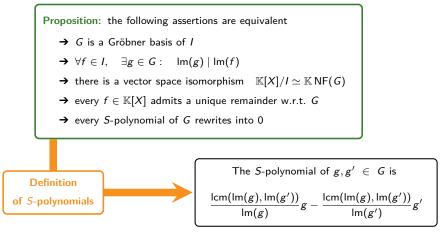
A (commutative) Gröbner basis of I is a subset $G \subseteq I$ s.t.

G is a generating set of *I* and $Im(I) = \langle Im(G) \rangle$

Definition: let $I \subseteq \mathbb{K}[X]$ and let < be a monomial order on [X].

A (commutative) **Gröbner basis of I** is a subset $G \subseteq I$ s.t.

G is a generating set of *I* and $Im(I) = \langle Im(G) \rangle$



Theorem. Let I be a polynomial ideal, G be a generating set of I, and < be a monomial order. Then,

G is a Gröbner basis of $I \Leftrightarrow$ the polynomial reduction is confluent

Ideas of the proof

Step 1: G is a G.B. of $I \Leftrightarrow \operatorname{Im}(I) \cap \operatorname{NF}(G) = \emptyset \Leftrightarrow \mathbb{K}[X] = I \oplus \mathbb{K}\operatorname{NF}(G)$

Step 2: \rightarrow_G is confluent \Leftrightarrow every $f \in \mathbb{K}[X]$ has a unique NF \Leftrightarrow $\mathbb{K}[X] = I \oplus \mathbb{K} \operatorname{NF}(G)$

THE ALGORITHM

```
Input: a set of monic polynomials f_1, \ldots, f_r \in \mathbb{K}[X]

Output: a G.B. G of l(f_1, \ldots, f_r)

Init: G := \{f_1, \ldots, f_r\} and P := G \times G

While P \neq \emptyset:

\rightarrow remove p from P and reduce spol(p) into NF w.r.t. G

\rightarrow add \widehat{spol(p)} to G and add all the corresponding pairs to P

Return G
```

Proof of termination: follows from Dickson's lemma

Proof of correctness: $G \subseteq I$ and every *S*-polynomials rewrites into 0

EXAMPLE

Input: $G := \{g_1, g_2\}$ with $g_1 := xy^2 + x$ and $g_2 := y^3 + (xy)/2 - 1/2$ <: the deglex order induced by y < x

While loop:

- → spol $(g_1, g_2) = -(x^2 y)/2 + xy + x/2 \quad \rightsquigarrow \quad g_3 := x^2 y 2xy x \in G$
- → spol $(g_1, g_3) = 2xy^2 + x^2 + xy$ rewrites into $g_4 := x^2 + xy 2x \in G$
- → spol $(g_2, g_3) = -(x^3y)/2 + x^2/2 2xy^3 xy^2$ rewrites into 0
- → spol $(g_1, g_4) = xy^3 2xy^2 x^2$ rewrites into 0
- → spol $(g_2, g_4) = xy^4 (x^3y)/2 xy^3 + x^2/2$ rewrites into 0
- → spol $(g_3, g_4) = xy^2 + x$ rewrites into 0

Return
$$\left\{ xy^2 + x, \quad y^3 + (xy)/2 - 1/2, \quad x^2y - 2xy - x, \quad x^2 + xy - 2x \right\}$$

18/40

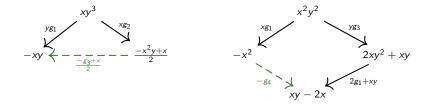
1st Buchberger's criterion: if gcd(Im(g), Im(g')) = 1, spol(g, g') rewrites into 0

 \rightarrow we may restrict the algorithm by computing S-pol. with nontrivial gcd

Alternatively: we obtain a linear adaptation of Knuth-Bendix algorithm

→ with
$$g_1 := xy^2 + x$$
 and $g_2 := y^3 + (xy)/2 - 1/2$, we get

$$g_3 := \mathbf{x}^2 \mathbf{y} - 2xy - x$$
 and $g_4 := \mathbf{x}^2 + xy - 2x$ from



Remark. Gröbner bases may be computed by Gaussian elimination

- → consider a critical pair $I \leftarrow m \rightarrow r$
- \rightarrow reduce *l* and *r* into NF and store the reductions into a matrix *M*
- \rightarrow compute the row echelon form \overline{M} of M by Gaussian elimination
- → if some $Im(\overline{M}_{i\bullet})$ does not belong to (Im(G)), then add $\overline{M}_{i\bullet}$ to G

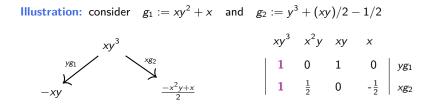
Illustration: consider

$$g_1 := xy^2 + x$$
 and
 $g_2 := y^3 + (xy)/2 - 1/2$
 xy^3
 xy^3
 x^2y
 xy
 xy^3
 x^{2y}
 xy
 xy^3
 $-xy$
 $\frac{-x^2y+x}{2}$
 1
 0
 yg_1

By Gaussian elimination

Remark. Gröbner bases may be computed by Gaussian elimination

- → consider a critical pair $I \leftarrow m \rightarrow r$
- \rightarrow reduce *l* and *r* into NF and store the reductions into a matrix *M*
- \rightarrow compute the row echelon form \overline{M} of M by Gaussian elimination
- → if some $\operatorname{Im}(\overline{M}_{i\bullet})$ does not belong to $(\operatorname{Im}(G))$, then add $\overline{M}_{i\bullet}$ to G



By Gaussian elimination

Remark. Gröbner bases may be computed by Gaussian elimination

- → consider a critical pair $I \leftarrow m \rightarrow r$
- \rightarrow reduce *l* and *r* into NF and store the reductions into a matrix *M*
- \rightarrow compute the row echelon form \overline{M} of M by Gaussian elimination
- → if some $\operatorname{Im}(\overline{M}_{i\bullet})$ does not belong to $(\operatorname{Im}(G))$, then add $\overline{M}_{i\bullet}$ to G

Illustration: consider
$$g_1 := xy^2 + x$$
 and $g_2 := y^3 + (xy)/2 - 1/2$
 $xy^3 \qquad x^{2}y \qquad xy \qquad x$
 $yg_1 \qquad yg_1 \qquad yg_1$
 $-xy \qquad -xy \qquad -xy \qquad -x^{2}y+x \qquad | 1 \qquad 0 \qquad 1 \qquad 0 \qquad yg_1$
 $0 \qquad 1 \qquad -2 \qquad -1 \qquad | 2(xg_2 - yg_1)$

By Gaussian elimination we get

$$g_3 := x^2y - 2xy - x$$
 20 / 40

THE ALGORITHM

Input: a set of monic polynomials $f_1, \ldots, f_r \in \mathbb{K}[X]$

Output: a G.B. G of $I(f_1, \ldots, f_r)$

Init: $G := \{f_1, \ldots, f_r\}$ and $P := G \times G$

While $P \neq \emptyset$:

→ remove from P a selected subset P' of P

- \rightarrow reduce the spol of elements of P' into normal form
- \rightarrow store all reductions into a matrix M
- → compute the row echelon form \overline{M} of M
- → add to G each $\overline{M}_{i\bullet}$ with leading monomial not in $(\operatorname{Im}(G))$
- \rightarrow add the corresponding pairs to P

Return G

II. NONCOMMUTATIVE GRÖBNER BASES

OBJECTIVE: adapt G.B. theory to the noncommutative framework

One need noncommutative adaptations of

- monomial orders \rightarrow definition of noncommutative G.B.
- polynomial reduction \rightarrow rewriting characterisation of noncommutative G.B.
- S-polynomials \rightarrow noncommutative Buchberger's/F4 procedures

We apply noncommutative G.B. to homological algebra \rightarrow Anick's resolution

Monomial order: total, well-founded order < on noncommutative monomials $\langle X \rangle$, that is admissible *i.e.*,

$$\forall m, m', m_1, m_2 \in [X]: \quad m_1 < m_2 \Rightarrow mm_1m' < mm_2m'$$

Gröbner bases: a generating subset G of the ideal $I \subseteq \mathbb{K}\langle X \rangle$ s.t. $\operatorname{Im}(I) = \langle \operatorname{Im}(G) \rangle$ (for a fixed monomial order <)

Polynomial reduction: given $G \subseteq \mathbb{K}\langle X \rangle$ and a monomial order <:

$$\lambda \Big(m \operatorname{Im}(g)m' \Big) + f \quad \rightarrow_{G} \quad \frac{\lambda}{\operatorname{lc}(g)} \Big(m \operatorname{rem}(g)m' \Big) + f$$

where $g \in G$, $\lambda \neq 0$, $m, m' \in \langle X \rangle$ and $m \operatorname{Im}(g)m' \notin \operatorname{supp}(f)$

Theorem. Let *I* be a noncommutative polynomial ideal, *G* be a generating set of *I*, and < be a monomial order. Then,

G is a Gröbner basis of $I \qquad \Leftrightarrow \qquad \rightarrow_G$ is confluent

Theorem. Let *I* be a noncommutative polynomial ideal, *G* be a generating set of *I*, and < be a monomial order. Then,

G is a Gröbner basis of $I \qquad \Leftrightarrow \qquad \rightarrow_G$ is confluent

Remark. If $\mathbf{A} = \mathbb{K}\langle X \mid R \rangle := \mathbb{K}\langle X \rangle / \langle R \rangle$ is an algebra and \langle is a monomial order, then R is a Gröbner basis of $\langle R \rangle$ iff \rightarrow_R is a confluent orientation of R.

In this case, A admits as a basis

 $\{m \mod \langle R \rangle \mid m \text{ is a normal form for } \rightarrow_R \}$

"Gröbner bases \leftrightarrow confluent orientations"

Ideal membership problem: given a G.B. G of I and $f \in \mathbb{K}\langle X \rangle$, how to decide $f \in I$?

- → reduce f into normal form \hat{f} using G and test $\hat{f} = 0$
- $\rightarrow \hat{f}$ is independent from the reduction path!

"Gröbner bases \leftrightarrow confluent orientations"

Ideal membership problem: given a G.B. G of I and $f \in \mathbb{K}\langle X \rangle$, how to decide $f \in I$?

- → reduce f into normal form \hat{f} using G and test $\hat{f} = 0$
- $\rightarrow \hat{f}$ is independent from the reduction path!

"Gröbner bases \leftrightarrow confluent orientations"

Ideal membership problem: given a G.B. G of I and $f \in \mathbb{K}\langle X \rangle$, how to decide $f \in I$?

- → reduce f into normal form \hat{f} using G and test $\hat{f} = 0$
- $\rightarrow \hat{f}$ is independent from the reduction path!

"Gröbner bases \leftrightarrow confluent orientations"

Ideal membership problem: given a G.B. G of I and $f \in \mathbb{K}\langle X \rangle$, how to decide $f \in I$?

- → reduce f into normal form \hat{f} using G and test $\hat{f} = 0$
- $\rightarrow \hat{f}$ is independent from the reduction path!

PBW theorem: let \mathscr{L} be a Lie algebra and let X be a totally well-ordered basis of \mathscr{L} .

Then, the universal enveloping algebra $U(\mathcal{L})$ of \mathcal{L} admits as a basis

$$\left\{ x_1^{\alpha_1} \dots x_k^{\alpha_k} \mid \quad x_i < x_{i+1} \in X, \ \alpha_i \in \mathbb{N} \right\}$$

"Gröbner bases \leftrightarrow confluent orientations"

Ideal membership problem: given a G.B. G of I and $f \in \mathbb{K}\langle X \rangle$, how to decide $f \in I$?

- → reduce f into normal form \hat{f} using G and test $\hat{f} = 0$
- $\rightarrow \hat{f}$ is independent from the reduction path!

PBW theorem: let \mathscr{L} be a Lie algebra and let X be a totally well-ordered basis of \mathscr{L} .

Then, the universal enveloping algebra $U(\mathscr{L})$ of \mathscr{L} admits as a basis

$$\left\{x_1^{\alpha_1} \dots x_k^{\alpha_k} \mid \quad x_i < x_{i+1} \in X, \ \alpha_i \in \mathbb{N}\right\}$$

Ideas of the proof:

- → presentation of $U(\mathscr{L})$: $\mathbb{K}\langle X \mid yx xy [y, x], x \neq y \in X \rangle$
- → choice of orientation: $yx \rightarrow xy + [y, x]$, where x < y
- → this orientation is confluent (equivalent to Jacobi identity)
- → a basis of $U(\mathscr{L})$ is composed of NF monomials: $x_1^{\alpha_1} \dots x_k^{\alpha_k}$ s.t. $x_i < x_{i+1}$

S-polynomials

Ambiguities of $G \subseteq \mathbb{K}\langle X \rangle$: tuples $\mathfrak{a} = (w_1, w_2, w_3, g, g')$ such that

- $w_1, w_2, w_3 \in \langle X \rangle$ with $w_2 \neq 1$ and $g, g' \in G$
- one of the following two conditions holds

→
$$w_1w_2 = \text{Im}(g)$$
 and $w_2w_3 = \text{Im}(g')$ (overlapping)

→
$$w_1w_2w_3 = Im(g)$$
 and $w_2 = Im(g')$ (inclusion)

S-polynomials: spol(\mathfrak{a}) = $gw_3 - w_1g'$ if \mathfrak{a} is an overlapping

 $spol(\mathfrak{a}) = w_1gw_3 - g'$ if \mathfrak{a} is an inclusion

Proposition: G is a noncommutative G.B. iff every spol rewrites into 0

Completion procedures: adaptations of Buchberger's and F₄ procedures

Fix $G \subseteq \mathbb{K}\langle X \rangle$ and a monomial order

Definition: Anick's n-chains and their tails are defined by induction

→ the unique (-1)-chain is 1, which is its own tail 0-chains are elements of X, which are their own tails

→ if $n \ge 1$: a *n*-chain with tail *t* is a monomial *mt* such that

i. *m* is a (n-1)-chain with tail t'

ii. t is a normal form w.r.t. G

iii. t't is uniquely reducible, on its right

Example: if Im(G) = {xyx, yxy}
0-chains: x and y
1-chains: xyx and yxy
2-chains: xyxy and yxyx yx
3-chains: xyxyxy and yxyxyx
4-chains: xyxyxy and yxyxyx

Framework:

We fix: $\mathbf{A} = \mathbb{K}\langle X \mid R \rangle \xrightarrow{\varepsilon} \mathbb{K}$ (with ker $(\varepsilon) = \langle X \rangle$) and a monomial order <

Assumption: R is a reduced noncommutative Gröbner basis of $\langle R \rangle$

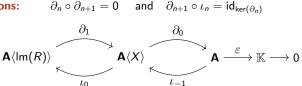
Construction of Anick's resolution: main steps

→ consider the free (left A–)modules $\mathbf{A}\langle C_n \rangle$ generated by *n*-chains $(\mathbf{A}\langle C_{-1} \rangle \simeq \mathbf{A}, \qquad \mathbf{A}\langle C_0 \rangle = \mathbf{A}\langle X \rangle, \qquad \mathbf{A}\langle C_1 \rangle \simeq \mathbf{A}\langle R \rangle)$

→ boundaries ∂_n are constructed simultaneously with the contracting homotopy ι_n they satisfy the identities: $\partial_n \circ \partial_{n+1} = 0$ and $\partial_{n+1} \circ \iota_n = id_{ker(\partial_n)}$

$$\ldots \rightarrow \mathbf{A} \langle \mathcal{C}_n \rangle \overbrace{\overset{\partial_n}{\underset{\iota_{n-1}}{\overset{}{\longrightarrow}}}}^{\partial_n} \mathbf{A} \langle \mathcal{C}_{n-1} \rangle \rightarrow \ldots \rightarrow \mathbf{A} \langle \mathcal{C}_1 \rangle \overbrace{\overset{\partial_1}{\underset{\iota_0}{\overset{}{\longrightarrow}}}}^{\partial_1} \mathbf{A} \langle \mathcal{C}_0 \rangle \overbrace{\overset{\partial_0}{\underset{\iota_{n-1}}{\overset{}{\longrightarrow}}}}^{\partial_0} \mathbf{A} \langle \mathcal{C}_{-1} \rangle \xrightarrow{\varepsilon} \mathbb{K} \rightarrow 0$$

Required relations:



 ∂_0 and ι_{-1} : $\partial_0([x]) := \overline{x}$ and $\iota_{-1}(\overline{mx}) := \overline{m}.[x]$ ($mx \in NF$) $\rightarrow \ker(\varepsilon) = \operatorname{im}(\partial_0)$ and $\partial_0 \circ \iota_{-1} = \operatorname{id}_{\ker(\varepsilon)}$

$$\partial_1 \text{ and } \iota_0$$
: $\partial_1([\operatorname{Im}(g)]) := \overline{m}.[x] - \sum \lambda_i \overline{m_i}.[x_i] \text{ where } g = mx - \sum \lambda_i m_i x_i$

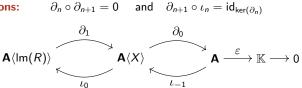
→ $\partial_0 \circ \partial_1 = 0$ since $\partial_1[\operatorname{Im}(g)] = \overline{m}.[x] - \iota_{-1} \circ \partial_0(\overline{m}.[x])$

 $\forall h \in \ker(\partial_0)$ with leading term $\overline{m}[x]$, there is a factorisation $mx = m' \operatorname{Im}(g)$

$$\iota_0(h):=\overline{m'}.[\mathsf{Im}(g)]+\iota_0\Bigl((h-\partial_1ig(\overline{m'}.[\mathsf{Im}(g)]ig)\Bigr)$$

→ $\partial_1 \circ \iota_0 = id_{ker(\partial_0)}$ is proven by induction

Required relations:



 ∂_0 and ι_{-1} : $\partial_0([x]) := \overline{x}$ and $\iota_{-1}(\overline{mx}) := \overline{m}.[x]$ ($mx \in NF$) $\rightarrow \ker(\varepsilon) = \operatorname{im}(\partial_0)$ and $\partial_0 \circ \iota_{-1} = \operatorname{id}_{\ker(\varepsilon)}$

$$\partial_1 \text{ and } \iota_0$$
: $\partial_1([\operatorname{Im}(g)]) := \overline{m}.[x] - \sum \lambda_i \overline{m_i}.[x_i] \text{ where } g = mx - \sum \lambda_i m_i x_i$

→ $\partial_0 \circ \partial_1 = 0$ since $\partial_1[\operatorname{Im}(g)] = \overline{m}.[x] - \iota_{-1} \circ \partial_0(\overline{m}.[x])$

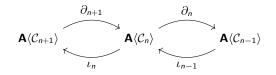
 $\forall h \in \ker(\partial_0)$ with leading term $\overline{m}[x]$, there is a factorisation $mx = m' \operatorname{Im}(g)$

$$\iota_0(h):=\overline{m'}.[\mathsf{Im}(g)]+\iota_0\Bigl((h-\partial_1ig(\overline{m'}.[\mathsf{Im}(g)]ig)\Bigr)$$

→ $\partial_1 \circ \iota_0 = id_{ker(\partial_0)}$ is proven by induction

Required relations:

$$\partial_n \circ \partial_{n+1} = 0$$
 and $\partial_{n+1} \circ \iota_n = \mathrm{id}_{\mathrm{ker}(\partial_n)}$



 $\mathsf{A}\langle \mathcal{C}_{n+1}\rangle \xrightarrow{\partial_{n+1}} \mathsf{A}\langle \mathcal{C}_n\rangle \colon \quad \partial_{n+1}([m \mid t]) := \overline{m}.[t] - \iota_{n-1} \circ \partial_n(\overline{m}.[t])$

→ $\partial_n \circ \partial_{n+1} = 0$ (using the induction hypothesis $\partial_n \circ \iota_{n-1} = 0$)

 $\mathbf{A}\langle \mathcal{C}_n \rangle \xrightarrow{\iota_n} \mathbf{A} \langle \mathcal{C}_{n+1} \rangle : \quad \forall h \in \ker(\partial_n) \text{ with leading term } \overline{m}.[c], \ mc = m'c', \text{ with } c' \in \mathcal{C}_{n+1}$

$$\iota_n(h) := \overline{m'}.[c'] + \iota_0\Big((c - \partial_1\big(\overline{m'}.[c']\big)\Big)$$

→ $\partial_{n+1} \circ \iota_n = id_{ker(\partial_n)}$ is proven by induction

Using the Anick'resolution, we can prove:

→ if $\mathbf{A} = \mathbb{K}\langle X \mid R \rangle$ is a monomial algebra, *i.e.* $R \subseteq \langle X \rangle$, then

$$\mathsf{Tor}^{\mathsf{A}}(\mathbb{K},\mathbb{K})=\bigoplus_{n}\mathbb{K}\mathcal{C}_{n}$$

 \rightarrow if **A** is presented by a quadratic Gröbner basis, then it is Koszul

→ if A is presented by an N-homogeneous Gröbner basis and satisfies the extra-condition, then it is N-Koszul

IV. REDUCTION OPERATORS

A brief overview on reduction operators

Bergman, 1978: formalism for rewriting noncommutative polynomials

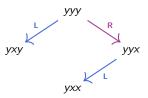
Berger 1998, 2001: lattice characterisation of homogeneous G.B. applied to Koszul duality

C. 2016, 2018: lattice characterisations of confluence and completion with the following applications

- → constructive proof of Koszulness
- \rightarrow lattice formulation of the noncommutative F_4 completion procedure
- \rightarrow computation of syzygies and detection of useless critical pairs



Example: $yy \rightarrow yx \quad \rightsquigarrow \quad \text{left/right reduction operators on 3 letter words}$

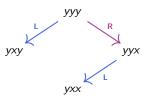


Properties of L and R: they are linear projectors of $\mathbb{K}X^{(3)}$ (or $\mathbb{K}\langle X \rangle$) and

compatible with the deglex order induced by x < y



Example: $yy \rightarrow yx \quad \rightsquigarrow \quad \text{left/right reduction operators on 3 letter words}$

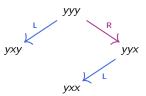


Properties of L and R: they are linear projectors of $\mathbb{K}X^{(3)}$ (or $\mathbb{K}\langle X \rangle$) and

compatible with the deglex order induced by x < y

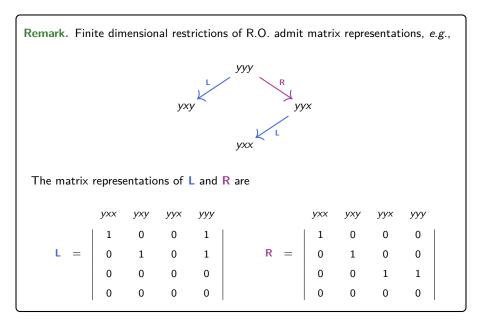


Example: $yy \rightarrow yx \quad \rightsquigarrow \quad \text{left/right reduction operators on 3 letter words}$



Properties of L and R: they are linear projectors of $\mathbb{K}X^{(3)}$ (or $\mathbb{K}\langle X \rangle$) and compatible with the deglex order induced by x < y

Definition: a reduction operator on a vector space V equipped with a well-ordered basis (G, <) is a linear projector of V s.t. $\forall g \in G : T(g) = g \text{ or } Im(T(g)) < g$



Proposition: the kernel map induces a bijection between R.O. and subspaces

$$\mathsf{ker}: \qquad \Big\{\mathsf{reduction \ operators \ on \ }V\Big\} \quad \leftrightarrow \quad \Big\{\mathsf{subspaces \ of \ }V\Big\}$$

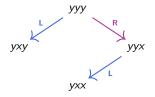
In particular, reduction operators admit the following lattice operations

→
$$T_1 \leq T_2$$
 iff ker $(T_2) \subseteq$ ker (T_1)

→ $T_1 \wedge T_2$ is the reduction operator with kernel ker (T_1) + ker (T_2)

→ $T_1 \lor T_2$ is the reduction operator with kernel ker $(T_1) \cap$ ker (T_2)

Moreover, $T_1 \wedge T_2$ computes minimal normal forms



Proposition: the kernel map induces a bijection between R.O. and subspaces

$$\mathsf{ker}: \qquad \Big\{\mathsf{reduction \ operators \ on \ }V\Big\} \quad \leftrightarrow \quad \Big\{\mathsf{subspaces \ of \ }V\Big\}$$

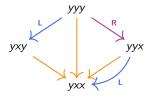
In particular, reduction operators admit the following lattice operations

→
$$T_1 \leq T_2$$
 iff ker $(T_2) \subseteq$ ker (T_1)

→ $T_1 \wedge T_2$ is the reduction operator with kernel ker (T_1) + ker (T_2)

→ $T_1 \lor T_2$ is the reduction operator with kernel ker(T_1) \cap ker(T_2)

Moreover, $T_1 \wedge T_2$ computes minimal normal forms



Computing lower bound using Gaussian elimination

Example: consider

$$\mathbf{L} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \qquad \mathbf{R} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

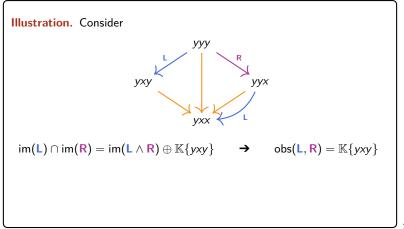
 $ker(L \wedge R) = ker(L) + ker(R) = \mathbb{K}\{yyx - yxx, yyy - yxy, yyy - yyx\}$

 $= \quad \mathbb{K} \{ \mathbf{y} \mathbf{x} \mathbf{y} - \mathbf{y} \mathbf{x} \mathbf{x}, \quad \mathbf{y} \mathbf{y} \mathbf{x} - \mathbf{y} \mathbf{x} \mathbf{x}, \quad \mathbf{y} \mathbf{y} \mathbf{y} - \mathbf{y} \mathbf{x} \mathbf{x} \}$

Hence

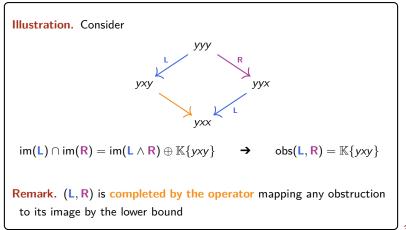
Lemma/Definition. For a familly F of R.O., we have

$$\operatorname{im}(\wedge F) \subseteq \bigcap_{T \in F} \operatorname{im}(T) \longrightarrow \bigcap_{T \in F} \operatorname{im}(T) = \operatorname{im}(\wedge F) \oplus \mathbb{K} \operatorname{obs}(F)$$



Lemma/Definition. For a familly F of R.O., we have

$$\operatorname{im}(\wedge F) \subseteq \bigcap_{T \in F} \operatorname{im}(T) \longrightarrow \bigcap_{T \in F} \operatorname{im}(T) = \operatorname{im}(\wedge F) \oplus \mathbb{K} \operatorname{obs}(F)$$



Theorem. Let *F* be a family of reduction operators and \rightarrow_F be the induced rewriting relation on *V*. Then, \rightarrow_F is confluent if and only if

$$\operatorname{im}(\wedge F) = \bigcap_{T \in F} \operatorname{im}(T)$$

Moreover, if \rightarrow_F is not confluent, then F is completed by

$$C(F) := \wedge F \lor (\lor \overline{F})$$

where

$$\forall \overline{F} := \ker^{-1} \left(\bigcap_{T \in F} \operatorname{im}(T) \right)$$