Gröbner bases in the free algebra: Introduction & advanced topics

Clemens Hofstadler · Institute of Mathematics · University of Kassel

Séminaire Calcul Formel

Limoges, France, January 12, 2023

UNI KASSEL VERSITÄT

FWF Der Wissenschaftsfonds.

Gröbner bases in the free algebra: Introduction

Why noncommutative Gröbner bases?

Why noncommutative Gröbner bases?

Ideal theoretic problems

- Ideal membership
- Elimination ideals
- Ideal/subalgebra intersections
- ...

(Mora '85, Borges, Borges '98, Nordbeck '98)

Why noncommutative Gröbner bases?

Ideal theoretic problems

- Ideal membership
- Elimination ideals
- Ideal/subalgebra intersections
- ...

(Mora '85, Borges, Borges '98, Nordbeck '98)

Studying finitely presented algebras

If $\mathcal{A} = K\langle X \mid R\rangle$, then Gröbner bases allow to

- decide whether $\mathcal{A}$ is trivial, commutative, finite dim.,...
- compute K-basis of $\mathcal{A}$
- decide word problem $f \stackrel{?}{=} g$ in $\mathcal{A}$

Why noncommutative Gröbner bases?

Ideal theoretic problems

- Ideal membership
- Elimination ideals
- Ideal/subalgebra intersections
- ...

(Mora '85, Borges, Borges '98, Nordbeck '98)

Studying operator statements

- Model lin. operators by noncomm. polies
- Simplify and prove operator statements
- Validity of first-order operator statements
  $\Longleftrightarrow$
  nc ideal membership

(Helton, Stankus, Wavrik '98, Schmitz, Levandovskyy '20, Raab, Regensburger, Hossein Poor '21, H, Raab, Regensburger '22)

Studying finitely presented algebras

If $\mathcal{A} = K\langle X \mid R\rangle$, then Gröbner bases allow to

- decide whether $\mathcal{A}$ is trivial, commutative, finite dim.,...
- compute K-basis of $\mathcal{A}$
- decide word problem $f \stackrel{?}{=} g$ in $\mathcal{A}$

Algebraic setting

Free monoid $\langle X \rangle$ (on $X = \{x_1, \ldots, x_n\}$)

- finite words (including empty word 1) over X
- concatenation $x_1 \cdot x_2 = x_1 x_2 \neq x_2 x_1 = x_2 \cdot x_1$

Algebraic setting

Free monoid $\langle X \rangle$ (on $X = \{x_1, \dots, x_n\}$)

- finite words (including empty word 1) over X
- concatenation $x_1 \cdot x_2 = x_1x_2 \neq x_2x_1 = x_2 \cdot x_1$

Free algebra $K\langle X \rangle$ (over field K)

- K-vector space with basis $\langle X \rangle$
- $c_1m_1 \cdot c_2m_2 = (c_1c_2)(m_1m_2)$, with $c_i \in K, m_i \in \langle X \rangle$

Algebraic setting

Free monoid $\langle X \rangle$ (on $X = \{x_1, \dots, x_n\}$)

- finite words (including empty word 1) over X
- concatenation $x_1 \cdot x_2 = x_1 x_2 \neq x_2 x_1 = x_2 \cdot x_1$

Free algebra $K\langle X \rangle$ (over field K)

- K-vector space with basis $\langle X \rangle$
- $c_1 m_1 \cdot c_2 m_2 = (c_1 c_2)(m_1 m_2)$, with $c_i \in K, m_i \in \langle X \rangle$
- For $F \subseteq K\langle X \rangle$,

$$(F) = \left\{ \sum a_i f_i b_i \mid a_i, b_i \in K\langle X \rangle,\ f_i \in F \right\}$$

Algebraic setting

Free monoid $\langle X \rangle$ (on $X = \{x_1, \ldots, x_n\}$)

- finite words (including empty word 1) over X
- concatenation $x_1 \cdot x_2 = x_1 x_2 \neq x_2 x_1 = x_2 \cdot x_1$

Free algebra $K\langle X \rangle$ (over field K)

- K-vector space with basis $\langle X \rangle$
- $c_1 m_1 \cdot c_2 m_2 = (c_1 c_2)(m_1 m_2)$, with $c_i \in K, m_i \in \langle X \rangle$
- For $F \subseteq K\langle X \rangle$,

$$(F) = \left\{ \sum a_i f_i b_i \mid a_i, b_i \in K\langle X \rangle,\ f_i \in F \right\}$$

Caution If $|X| > 1$, then $K\langle X \rangle$ is not Noetherian!

Basic definitions

Momial order $=$ total, well-founded, compatible order $\preceq$ on $\langle X \rangle$

Basic definitions

$\mathfrak{m} \preceq \mathfrak{m}' \Rightarrow \mathfrak{a}\mathfrak{m}\mathfrak{b} \preceq \mathfrak{a}\mathfrak{m}'\mathfrak{b}$

Momial order $=$ total, well-founded, compatible order $\preceq$ on $\langle X \rangle$

Basic definitions

$m \preceq m' \Rightarrow amb \preceq am'b$

Momial order $=$ total, well-founded, compatible order $\preceq$ on $\langle X \rangle$

$$\Rightarrow \quad f \quad = \quad \overbrace{\underbrace{c}_{\mathrm{lc}(f)} \cdot \underbrace{m}_{\mathrm{lm}(f)}}^{\mathrm{lt}(f)} \quad + \quad \text{smaller terms}$$

Basic definitions

$m \preceq m' \Rightarrow amb \preceq am'b$

Momial order = total, well-founded, compatible order $\preceq$ on $\langle X \rangle$

$$\Rightarrow \quad f = \overbrace{\underbrace{c}_{\mathrm{lc}(f)} \cdot \underbrace{m}_{\mathrm{lm}(f)}}^{\mathrm{lt}(f)} + \text{ smaller terms}$$

Polynomial reduction

Let $f, g \in K\langle X \rangle$ with $g \neq 0$ and $G \subseteq K\langle X \rangle$.

Reduction by g: If $\exists a, b \in \langle X \rangle : \mathrm{lm}(agb) = \mathrm{lm}(f)$, then

$$f \quad \to_g \quad f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb.$$

Basic definitions

$m \preceq m' \Rightarrow amb \preceq am'b$

Momial order $=$ total, well-founded, compatible order $\preceq$ on $\langle X \rangle$

$$\Rightarrow \quad f \;=\; \overbrace{\underbrace{c}_{\mathrm{lc}(f)} \cdot \underbrace{m}_{\mathrm{lm}(f)}}^{\mathrm{lt}(f)} \;+\; \text{smaller terms}$$

Polynomial reduction

Let $f, g \in K\langle X \rangle$ with $g \neq 0$ and $G \subseteq K\langle X \rangle$.

Reduction by g: If $\exists a, b \in \langle X \rangle : \mathrm{lm}(agb) = \mathrm{lm}(f)$, then

$$f \quad \rightarrow_g \quad f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb.$$

Example: $f = xyzy + xz, \quad g = yz - 1$

Basic definitions

$m \preceq m' \Rightarrow amb \preceq am'b$

Momial order = total, well-founded, compatible order $\preceq$ on $\langle X \rangle$

$$\Rightarrow \quad f = \overbrace{\underbrace{c}_{\mathrm{lc}(f)} \cdot \underbrace{m}_{\mathrm{lm}(f)}}^{\mathrm{lt}(f)} + \text{ smaller terms}$$

Polynomial reduction

Let $f, g \in K\langle X \rangle$ with $g \neq 0$ and $G \subseteq K\langle X \rangle$.

Reduction by g: If $\exists a, b \in \langle X \rangle : \mathrm{lm}(agb) = \mathrm{lm}(f)$, then

$$f \quad \to_g \quad f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb.$$

Example: $f = xyzy + xz, \quad g = yz - 1$

Basic definitions

$m \preceq m' \Rightarrow amb \preceq am'b$

Momial order = total, well-founded, $\boxed{\text{compatible}}$ order $\preceq$ on $\langle X \rangle$

$$\Rightarrow \quad f = \underbrace{\overbrace{\underset{\mathrm{lc}(f)}{c} \cdot \underset{\mathrm{lm}(f)}{m}}^{\mathrm{lt}(f)}} + \text{ smaller terms}$$

Polynomial reduction

Let $f, g \in K\langle X \rangle$ with $g \neq 0$ and $G \subseteq K\langle X \rangle$.

Reduction by g: If $\exists a, b \in \langle X \rangle : \mathrm{lm}(agb) = \mathrm{lm}(f)$, then

$$f \quad \to_g \quad f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb.$$

Example:

$$f = xyzy + xz, \quad g = yz - 1$$
$$f \quad \to_g \quad f - xgy = xz + xy$$

Basic definitions

$m \preceq m' \Rightarrow amb \preceq am'b$

Momial order = total, well-founded, compatible order $\preceq$ on $\langle X \rangle$

$$\Rightarrow \quad f = \overbrace{\underbrace{c}_{\mathrm{lc}(f)} \cdot \underbrace{m}_{\mathrm{lm}(f)}}^{\mathrm{lt}(f)} + \text{ smaller terms}$$

Polynomial reduction

Let $f, g \in K\langle X \rangle$ with $g \neq 0$ and $G \subseteq K\langle X \rangle$.

Reduction by g: If $\exists a, b \in \langle X \rangle : \mathrm{lm}(agb) = \mathrm{lm}(f)$, then

$$f \quad \to_g \quad f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb.$$

Example:

$$f = xyzy + xz, \quad g = yz - 1$$
$$f \quad \to_g \quad f - xgy = xz + xy$$

Reduction by G: $f \to_G f' \quad \iff \quad \exists g \in G : f \to_g f'$

Basic definitions

$$m \preceq m' \Rightarrow amb \preceq am'b$$

Momial order $=$ total, well-founded, $\boxed{\text{compatible}}$ order $\preceq$ on $\langle X \rangle$

$$\Rightarrow \quad f = \overbrace{\underbrace{c}_{\mathrm{lc}(f)} \cdot \underbrace{m}_{\mathrm{lm}(f)}}^{\mathrm{lt}(f)} + \text{ smaller terms}$$

Polynomial reduction

Let $f, g \in K\langle X \rangle$ with $g \neq 0$ and $G \subseteq K\langle X \rangle$.

Reduction by g: If $\exists a, b \in \langle X \rangle : \mathrm{lm}(agb) = \mathrm{lm}(f)$, then

$$f \quad \to_g \quad f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb.$$

Example:
$$f = xyzy + xz, \quad g = yz - 1$$
$$f \quad \to_g \quad f - xgy = xz + xy$$

Reduction by G: $f \to_G f' \qquad \Longleftrightarrow \qquad \exists g \in G : f \to_g f'$

Observe Since $\preceq$ is well-founded, $\to_G$ is terminating.

Gröbner bases

Definition Generating set G of ideal $I \subseteq K\langle X\rangle$ s.t. $\to_G$ is confluent

Gröbner bases

Definition Generating set G of ideal $I \subseteq K\langle X\rangle$ s.t. $\to_G$ is confluent

Equiv. characterisations G is a Gröbner basis of I

$\iff$ $\mathrm{LM}(I) = \mathrm{LM}(G)$

$\iff$ $f \in I$ iff $f \xrightarrow{*}_G 0$

$\iff$ $\{m + I \mid m$ is in normal form w.r.t. $\to_G\}$ is a K-basis of $K\langle X\rangle/I$

Gröbner bases

Definition Generating set G of ideal $I \subseteq K\langle X\rangle$ s.t. $\to_G$ is confluent

Equiv. characterisations G is a Gröbner basis of I

$\iff \quad \mathrm{LM}(I) = \mathrm{LM}(G)$

$\iff \quad f \in I$ iff $f \xrightarrow{*}_G 0$

$\iff \quad \{m + I \mid m$ is in normal form w.r.t. $\to_G\}$ is a K-basis of $K\langle X\rangle / I$

Applications

K-basis: K-basis of $K\langle X \mid R\rangle$ is given by K-basis of $K\langle X\rangle/(R)$

Commutativity: $K\langle X \mid R\rangle$ is comm. iff $[x_i, x_j] \in (R)$ for all $i < j$

Algebraicity: $p \in K\langle X \mid R\rangle$ is alg. iff $(R + (p - y)) \cap K[y] \neq \emptyset$

Gröbner bases and the word problem

Caution Not all fin. gen. ideals in $K\langle X\rangle$ have finite Gröbner bases!

Gröbner bases and the word problem

Caution Not all fin. gen. ideals in $K\langle X\rangle$ have finite Gröbner bases!

$\Rightarrow$ Ideal membership (and many other problems) in $K\langle X\rangle$ only semidecidable

Gröbner bases and the word problem

Caution Not all fin. gen. ideals in $K\langle X\rangle$ have finite Gröbner bases!

$\Rightarrow$ Ideal membership (and many other problems) in $K\langle X\rangle$ only semidecidable

Well-behaved special cases

- $\dim_K(K\langle X\rangle/I) < \infty \Rightarrow$ every minimal GB of I is finite
- I homogeneous and finitely generated $\Rightarrow$ ideal membership decidable
- Many infinite GBs are finitely parametrisable $\Rightarrow$ ideal membership decidable
- Verifying ideal membership is always possible in finite time, and in practice this is often all we need.

Ambiguities & S-polynomials

Overlap ambiguity

$$f = \qquad + \cdots$$
$$g = \qquad + \cdots$$

$$f \qquad - \qquad g \quad \in \ \mathrm{SPol}(f, g)$$

Inclusion ambiguity

$$f = \qquad + \cdots$$
$$g = \qquad + \cdots$$

$$f \qquad - g \quad \in \ \mathrm{SPol}(f, g)$$

Ambiguities & S-polynomials

Overlap ambiguity

Inclusion ambiguity

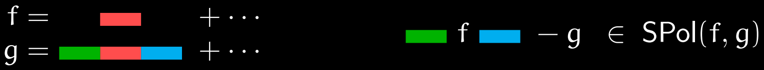
Remarks

- Central part has to be non-trivial (coprime criterion)
- S-polynomials are not unique but finite!

Ambiguities & S-polynomials

Overlap ambiguity

Inclusion ambiguity



Remarks

- Central part has to be non-trivial (coprime criterion)
- S-polynomials are not unique but finite!
- $xxyx$ and xy have two ambiguities: $\begin{array}{l} xxyx \\ xy \end{array}$ $\quad$ $\begin{array}{l} xxyx \\ xy \end{array}$

Ambiguities & S-polynomials

Overlap ambiguity

Inclusion ambiguity

Remarks

- Central part has to be non-trivial (coprime criterion)
- S-polynomials are not unique but finite!
- $xxyx$ and xy have two ambiguities: $\begin{matrix} xxyx \\ xy \end{matrix} \qquad \begin{matrix} xxyx \\ xy \end{matrix}$
- $xyxy$ has an (overlap) ambiguity with itself: $\begin{matrix} xyxy \\ xyxy \end{matrix}$

Buchberger's algorithm

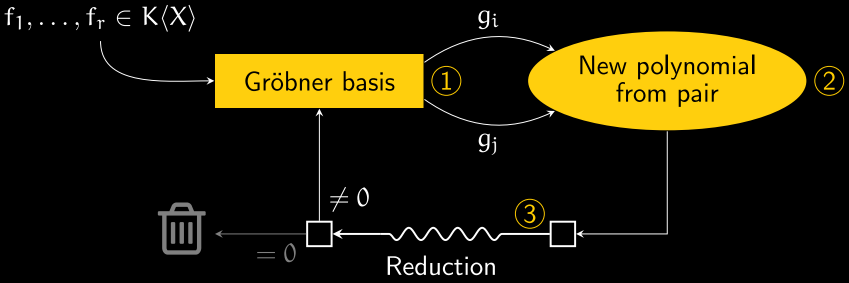
Diamond lemma (Bergman '78)

$$G \subseteq K\langle X\rangle \text{ is GB of } (G) \quad \text{iff} \quad \forall \text{ S-poly } p \text{ of } G : p \xrightarrow{*}_G 0$$

Buchberger's algorithm

Diamond lemma (Bergman '78)

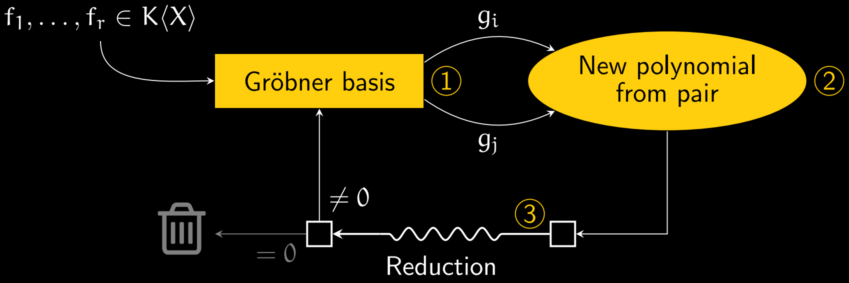
$$G \subseteq K\langle X\rangle \text{ is GB of } (G) \quad \text{iff} \quad \forall \text{ S-poly } p \text{ of } G : p \xrightarrow{*}_G 0$$



Buchberger's algorithm

Diamond lemma (Bergman '78)

$$G \subseteq K\langle X\rangle \text{ is GB of } (G) \quad \text{iff} \quad \forall \text{ S-poly } p \text{ of } G : p \xrightarrow{*}_G 0$$

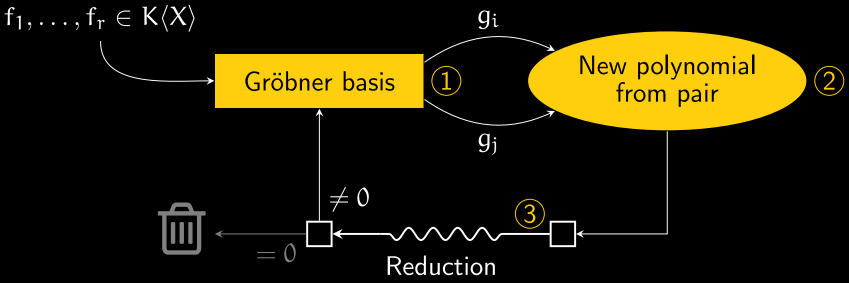


1. Selection: fair strategy *"Every S-poly is selected eventually"*

Buchberger's algorithm

Diamond lemma (Bergman '78)

$$G \subseteq K\langle X\rangle \text{ is GB of } (G) \quad \text{iff} \quad \forall \text{ S-poly } p \text{ of } G : p \xrightarrow{*}_G 0$$



1. Selection: fair strategy *"Every S-poly is selected eventually"*
2. Construction: form S-polynomials from ambiguities
3. Reduction: reduction using (partial) Gröbner basis

Software

- Bergman: Gröbner bases in noncommutative algebras and in modules over them (Backelin et al. '06)
- Letterplace: SINGULAR package for noncommutative Gröbner bases (+ cofactor repr.) in free algebras, finitely presented algebras, and modules. Allows computations over $\mathbb{Z}$ (Levandovskyy, La Scala '09)
- Magma: Noncommutative F4 algorithm (Steel ~'09)
- NCAlgebra: MATHEMATICA package for simplification and reduction modulo noncommutative Gröbner bases (Helton, Stankus '01)
- GBNP: GAP package for noncommutative Gröbner bases for free and path algebras (Cohen, Gijsbers '03)
- OperatorGB: MATHEMATICA and SAGEMATH package for noncommutative Gröbner bases (+ cofactor repr.) and for automatically proving operator statements (H., Raab, Regensburger '19)
- SignatureGB (soon): SAGEMATH package for noncommutative signature Gröbner bases

Gröbner bases in the free algebra: Advanced topics

Hot topics

Hot topics

Efficient computation

- $\rightsquigarrow$ Linear algebra reductions (Steel ~'09, Xiu '12)
- $\rightsquigarrow$ Signature-based algorithms (H., Verron '22)

Hot topics

Efficient computation

- $\rightsquigarrow$ Linear algebra reductions (Steel ~'09, Xiu '12)
- $\rightsquigarrow$ Signature-based algorithms (H., Verron '22)

Expanding applicability

- $\rightsquigarrow$ Coefficient rings (Mikhalev, Zolotykh '98, Levandovskyy, Metzlaff, Abou Zeid '20)

Linear algebra reductions – F4

Idea Use linear algebra for polynomial reduction!

Linear algebra reductions – F4

Idea Use linear algebra for polynomial reduction!

$$f \rightarrow_{a,g,b} f' \qquad \Longleftrightarrow \qquad \begin{pmatrix} — & f & — \\ — & agb & — \end{pmatrix}$$

Linear algebra reductions – F4

Idea Use linear algebra for polynomial reduction!

$$f \rightarrow_{a,g,b} f' \qquad \Longleftrightarrow \qquad \begin{pmatrix} — & f & — \\ — & agb & — \end{pmatrix} \overset{\text{RRef}}{\rightsquigarrow} \begin{pmatrix} — & f & — \\ — & f' & — \end{pmatrix}$$

Linear algebra reductions – F4

Idea Use linear algebra for polynomial reduction!

$$f \to_{a,g,b} f' \quad \Longleftrightarrow \quad \begin{pmatrix} — & f & — \\ — & agb & — \end{pmatrix} \overset{\text{RRef}}{\rightsquigarrow} \begin{pmatrix} — & f & — \\ — & f' & — \end{pmatrix}$$

- Allows to reduce many S-polies simultaneously

  1. Say we want to reduce $\{p_1, \dots, p_m\}$
  2. Find multiples of reducers needed for reductions (Symbolic preprocessing) $\rightsquigarrow$ $\{a_1 g_1 b_1, \dots, a_k g_k b_k\}$
  3. Form Macaulay style matrix & row-reduce
  4. Rows with new leading monomials get added to Gröbner basis

Linear algebra reductions – F4

Idea Use linear algebra for polynomial reduction!

$$f \to_{a,g,b} f' \quad \Longleftrightarrow \quad \begin{pmatrix} - & f & - \\ - & agb & - \end{pmatrix} \overset{\text{RRef}}{\rightsquigarrow} \begin{pmatrix} - & f & - \\ - & f' & - \end{pmatrix}$$

- Allows to reduce many S-polies simultaneously
  1. Say we want to reduce $\{p_1, \ldots, p_m\}$
  2. Find multiples of reducers needed for reductions (Symbolic preprocessing) $\rightsquigarrow$ $\{a_1 g_1 b_1, \ldots, a_k g_k b_k\}$
  3. Form Macaulay style matrix & row-reduce
  4. Rows with new leading monomials get added to Gröbner basis

$$\begin{array}{c|c} \left(\begin{array}{cccc} * & \cdots & \cdots & * \\ \vdots & & & \vdots \\ * & \cdots & \cdots & * \\ \hline * & \cdots & \cdots & * \\ \vdots & & & \vdots \\ * & \cdots & \cdots & * \end{array}\right) & \begin{array}{c} p_1 \\ \vdots \\ p_m \\ a_1 g_1 b_1 \\ \vdots \\ a_k g_k b_k \end{array} \end{array}$$

Linear algebra reductions – F4

Idea Use linear algebra for polynomial reduction!

$$f \to_{a,g,b} f' \quad \Longleftrightarrow \quad \begin{pmatrix} — & f & — \\ — & agb & — \end{pmatrix} \overset{\text{RRef}}{\rightsquigarrow} \begin{pmatrix} — & f & — \\ — & f' & — \end{pmatrix}$$

- Allows to reduce many S-polies simultaneously
  1. Say we want to reduce $\{p_1, \dots, p_m\}$
  2. Find multiples of reducers needed for reductions (Symbolic preprocessing) $\rightsquigarrow$ $\{a_1 g_1 b_1, \dots, a_k g_k b_k\}$
  3. Form Macaulay style matrix & row-reduce
  4. Rows with new leading monomials get added to Gröbner basis

$$\begin{array}{cc} \left(\begin{array}{cccc} * & \cdots & \cdots & * \\ \vdots & & & \vdots \\ * & \cdots & \cdots & * \\ \hline * & \cdots & \cdots & * \\ \vdots & & & \vdots \\ * & \cdots & \cdots & * \end{array}\right) & \begin{array}{c} p_1 \\ \vdots \\ p_m \\ a_1 g_1 b_1 \\ \vdots \\ a_k g_k b_k \end{array} \end{array}$$

$$\Big\downarrow \text{RRef}$$

$$\begin{pmatrix} 1 & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & 1 \\ & & & \end{pmatrix}$$

Linear algebra reductions – F4

Idea Use linear algebra for polynomial reduction!

$$f \to_{a,g,b} f' \quad \Longleftrightarrow \quad \begin{pmatrix} — & f & — \\ — & agb & — \end{pmatrix} \overset{\text{RRef}}{\rightsquigarrow} \begin{pmatrix} — & f & — \\ — & f' & — \end{pmatrix}$$

- Allows to reduce many S-polies simultaneously
  1. Say we want to reduce $\{p_1, \ldots, p_m\}$
  2. Find multiples of reducers needed for reductions (Symbolic preprocessing) $\rightsquigarrow \{a_1 g_1 b_1, \ldots, a_k g_k b_k\}$
  3. Form Macaulay style matrix & row-reduce
  4. Rows with new leading monomials get added to Gröbner basis

$$\begin{array}{cc} \left(\begin{array}{cccc} * & \cdots & \cdots & * \\ \vdots & & & \vdots \\ * & \cdots & \cdots & * \\ \hline * & \cdots & \cdots & * \\ \vdots & & & \vdots \\ * & \cdots & \cdots & * \end{array}\right) & \begin{array}{c} p_1 \\ \vdots \\ p_m \\ a_1 g_1 b_1 \\ \vdots \\ a_k g_k b_k \end{array} \end{array}$$

$$\Big\downarrow \text{RRef}$$

$$\begin{pmatrix} 1 & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & 1 \end{pmatrix}$$

- Exploit efficient (sparse) linear algebra techniques and matrix structure

Signature-based algorithms – F5, GVW

Observation A lot of time is spent on zero reductions.

Goal Detect such useless computations!

Signature-based algorithms – F5, GVW

Observation A lot of time is spent on zero reductions.

Goal Detect such useless computations! $\Rightarrow$ Signatures

Signature-based algorithms – F5, GVW

Observation A lot of time is spent on zero reductions.

Goal Detect such useless computations! $\Rightarrow$ Signatures

Setting

- Given $f_1, \ldots, f_r \in K\langle X \rangle$ generating ideal $I = (f_1, \ldots, f_r)$
- Free $K\langle X \rangle$-bimodule $\Sigma = \bigoplus_{i=1}^{r} K\langle X \rangle \otimes K\langle X \rangle$ with basis $\varepsilon_1, \ldots, \varepsilon_r$
- $K\langle X \rangle$-bimodule homomorphism $\bar{\cdot} : \Sigma \to I, \varepsilon_i \mapsto f_i$

Signature-based algorithms – F5, GVW

Observation A lot of time is spent on zero reductions.

Goal Detect such useless computations! $\Rightarrow$ Signatures

Setting

- Given $f_1, \dots, f_r \in K\langle X\rangle$ generating ideal $I = (f_1, \dots, f_r)$
- Free $K\langle X\rangle$-bimodule $\Sigma = \bigoplus_{i=1}^{r} K\langle X\rangle \otimes K\langle X\rangle$ with basis $\varepsilon_1, \dots, \varepsilon_r$
- $K\langle X\rangle$-bimodule homomorphism $\bar{\cdot} : \Sigma \to I, \varepsilon_i \mapsto f_i$

Signature of $\alpha \in \Sigma$ $\mathrm{sig}(\alpha) =$ leading monomial of α (w.r.t. module order)

Signature-based algorithms – F5, GVW

Observation A lot of time is spent on zero reductions.

Goal Detect such useless computations! $\Rightarrow$ Signatures

Setting

- Given $f_1, \ldots, f_r \in K\langle X\rangle$ generating ideal $I = (f_1, \ldots, f_r)$
- Free $K\langle X\rangle$-bimodule $\Sigma = \bigoplus_{i=1}^{r} K\langle X\rangle \otimes K\langle X\rangle$ with basis $\varepsilon_1, \ldots, \varepsilon_r$
- $K\langle X\rangle$-bimodule homomorphism $\bar{\cdot} : \Sigma \to I, \varepsilon_i \mapsto f_i$

Signature of $\alpha \in \Sigma$ $\mathrm{sig}(\alpha)$ = leading monomial of α (w.r.t. module order)

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

Signature-based algorithms – F5, GVW

Observation A lot of time is spent on zero reductions.

Goal Detect such useless computations! $\Rightarrow$ Signatures

Setting

- Given $f_1, \ldots, f_r \in K\langle X\rangle$ generating ideal $I = (f_1, \ldots, f_r)$
- Free $K\langle X\rangle$-bimodule $\Sigma = \bigoplus_{i=1}^{r} K\langle X\rangle \otimes K\langle X\rangle$ with basis $\varepsilon_1, \ldots, \varepsilon_r$
- $K\langle X\rangle$-bimodule homomorphism $\bar{\cdot} : \Sigma \to I, \varepsilon_i \mapsto f_i$

Signature of $\alpha \in \Sigma$ $\mathrm{sig}(\alpha) =$ leading monomial of α (w.r.t. module order)

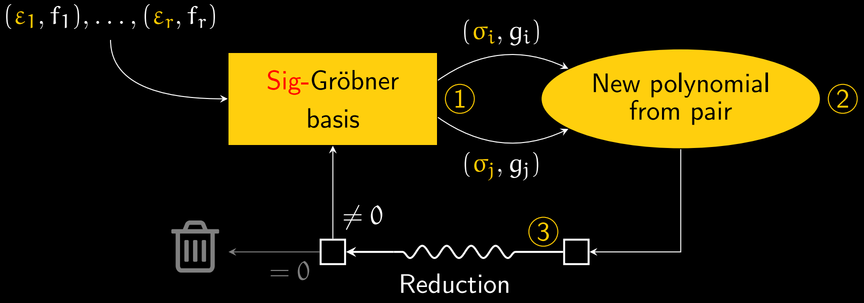
Sig-based algorithms work with pairs $(\mathrm{sig}(\alpha), f)$ where $\overline{\alpha} = f$

Regular operations

$$\sigma \succ \mu \Rightarrow (\sigma, f) \pm (\mu, g) =: (\sigma, f \pm g) \text{ (sig. preserved)}$$

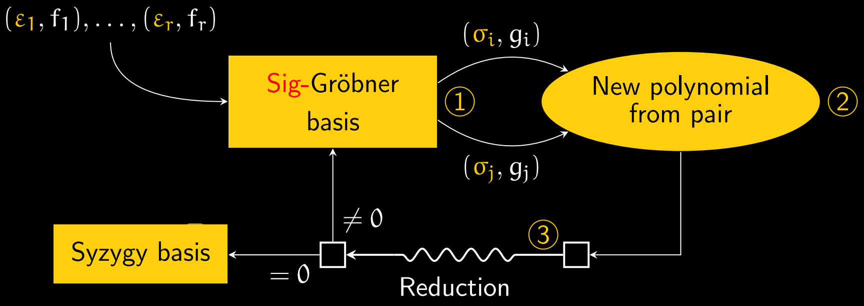
$\Rightarrow$ regular reductions & S-polynomials

Buchberger's algorithm with signatures



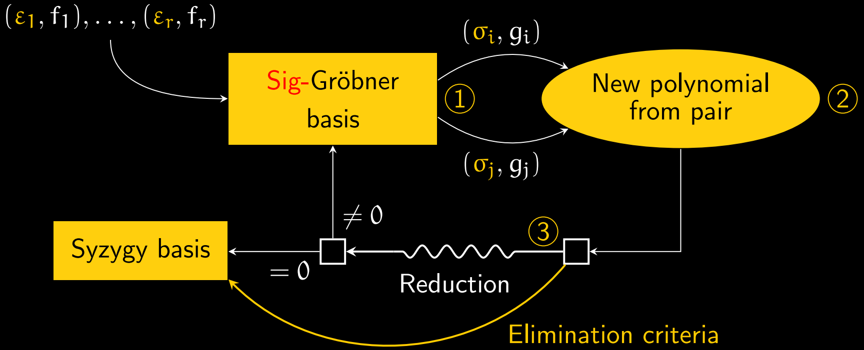
1. Selection: fair strategy
2. Construction: regular S-polynomials
3. Reduction: regular reductions using (partial) Sig-Gröbner basis

Buchberger's algorithm with signatures



1. Selection: fair strategy
2. Construction: regular S-polynomials
3. Reduction: regular reductions using (partial) Sig-Gröbner basis

Buchberger's algorithm with signatures



1. Selection: fair strategy
2. Construction: regular S-polynomials
3. Reduction: regular reductions using (partial) Sig-Gröbner basis

Buchberger's algorithm with signatures

Output Signature Gröbner basis, allowing to recover

- a Gröbner basis of the ideal (+ cofactor representations)
- a Gröbner basis of the syzygy module

Remarks

- Termination is very rare – even less common than standard noncommutative GB algorithms
- Algorithm terminates iff ideal admits finite signature Gröbner basis
- Experimental data suggests performance improvement

Noncommutative Gröbner bases over rings

Setting

$R\langle X \rangle \ldots$ free algebra over comm. PID (e.g. $R = \mathbb{Z}$)

Noncommutative Gröbner bases over rings

Setting

$R\langle X\rangle \ldots$ free algebra over comm. PID (e.g. $R = \mathbb{Z}$)

Reductions

As in the field case, but now also considering coefficients, that is

$$f \to_g f' \quad \Longleftrightarrow \quad \exists a, b \in \langle X\rangle : \mathrm{lm}(f) = \mathrm{lm}(agb) \;\&\; \mathrm{lc}(g) \mid \mathrm{lc}(f)$$

Noncommutative Gröbner bases over rings

Setting

$R\langle X \rangle$ . . . free algebra over comm. PID (e.g. $R = \mathbb{Z}$)

Reductions

As in the field case, but now also considering coefficients, that is

$$f \to_g f' \quad \Longleftrightarrow \quad \exists a, b \in \langle X \rangle : \mathrm{lm}(f) = \mathrm{lm}(agb) \ \& \ \mathrm{lc}(g) \mid \mathrm{lc}(f)$$

Gröbner bases

Different notions, but most relevant are strong Gröbner bases.

Definition: $G \subseteq I$ s.t. $f \xrightarrow{*}_G 0$ for all $f \in I$

Problems over rings

Observation S-polynomials are not enough!

Problems over rings

Observation S-polynomials are not enough!

Example Consider $I = (f = 3x, g = 2y) \subseteq \mathbb{Z}\langle x, y, z\rangle$

Problems over rings

Observation S-polynomials are not enough!

Example Consider $I = (f = 3x, g = 2y) \subseteq \mathbb{Z}\langle x, y, z\rangle$

- $\{f, g\}$ not a strong GB: $xy = fy - xg \in I$ is not reducible

Problems over rings

Observation S-polynomials are not enough!

Example Consider $I = (f = 3x, g = 2y) \subseteq \mathbb{Z}\langle x, y, z\rangle$

- $\{f, g\}$ not a strong GB: $xy = fy - xg \in I$ is not reducible
- Adding $\mathrm{SPol}(f, g) = 0$ does not help

Problems over rings

Observation S-polynomials are not enough!

Example Consider $I = (f = 3x, g = 2y) \subseteq \mathbb{Z}\langle x, y, z\rangle$

- $\{f, g\}$ not a strong GB: $xy = fy - xg \in I$ is not reducible
- Adding $\mathrm{SPol}(f, g) = 0$ does not help
- Look at $\gcd(\mathrm{lc}(f), \mathrm{lc}(g)) \Rightarrow$ $\mathrm{GPol}(f, g) = xy$

Problems over rings

Observation S-polynomials are not enough!

Example Consider $I = (f = 3x, g = 2y) \subseteq \mathbb{Z}\langle x, y, z\rangle$

- $\{f, g\}$ not a strong GB: $xy = fy - xg \in I$ is not reducible
- Adding $\mathrm{SPol}(f, g) = 0$ does not help
- Look at $\gcd(\mathrm{lc}(f), \mathrm{lc}(g)) \Rightarrow$ $\mathrm{GPol}(f, g) = xy$
- $\{f, g, xy\}$ still no strong GB: $xz^n y = fz^n y - xz^n y \in I$ not reducible

Problems over rings

Observation S-polynomials are not enough!

Example Consider $I = (f = 3x, g = 2y) \subseteq \mathbb{Z}\langle x, y, z\rangle$

- $\{f, g\}$ not a strong GB: $xy = fy - xg \in I$ is not reducible
- Adding $\mathrm{SPol}(f, g) = 0$ does not help
- Look at $\gcd(\mathrm{lc}(f), \mathrm{lc}(g)) \Rightarrow \mathrm{GPol}(f, g) = xy$
- $\{f, g, xy\}$ still no strong GB: $xz^n y = fz^n y - xz^n y \in I$ not reducible

$\Rightarrow$ need to look at all combinations $f \quad \mathrm{lm}(g) \pm \mathrm{lm}(f) \quad g$

Problems over rings

Observation S-polynomials are not enough!

Example Consider $I = (f = 3x, g = 2y) \subseteq \mathbb{Z}\langle x, y, z\rangle$

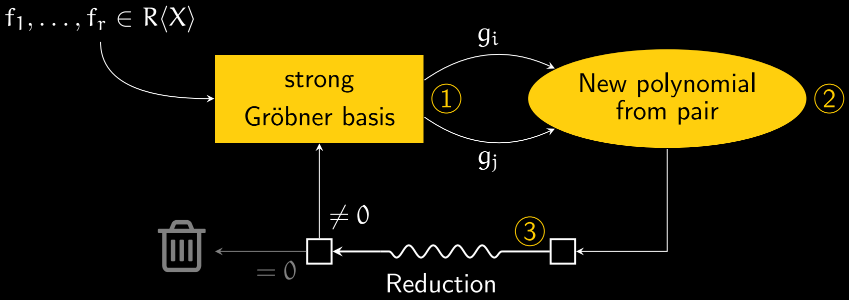
- $\{f, g\}$ not a strong GB: $xy = fy - xg \in I$ is not reducible
- Adding $\mathrm{SPol}(f, g) = 0$ does not help
- Look at $\gcd(\mathrm{lc}(f), \mathrm{lc}(g)) \Rightarrow$ $\mathrm{GPol}(f, g) = xy$
- $\{f, g, xy\}$ still no strong GB: $xz^n y = fz^n y - xz^n y \in I$ not reducible

$\Rightarrow$ need to look at all combinations $f \;\underline{\qquad}\; \mathrm{lm}(g) \pm \mathrm{lm}(f) \;\underline{\qquad}\; g$

Problem $\mathrm{SPol}(f, g)$ and $\mathrm{GPol}(f, g)$ are infinite

$\Rightarrow$ can only compute up to some degree bound

Buchberger's algorithm over rings



1. Selection: fair strategy
2. Construction: S- and G-polynomials up to degree bound
3. Reduction: reduction using (partial) Gröbner basis

Conclusion

Introduction

- Very similar to commutative Gröbner bases
- No termination guarantee $\rightsquigarrow$ Problems only semidecidable
- Many well-behaved special cases

Conclusion

Introduction

- Very similar to commutative Gröbner bases
- No termination guarantee $\rightsquigarrow$ Problems only semidecidable
- Many well-behaved special cases

Advanced topics

- Linear algebra reductions $\rightsquigarrow$ Performance improvement
- Signature-based algorithms
  - Add module perspective to polynomials
  - Gröbner basis of ideal + syzygy module
  - Elimination criteria $\rightsquigarrow$ Performance improvement
- Gröbner bases over rings
  - Infinitely many S- & G-polynomials