

Non-commutative Gröbner bases in SINGULAR

Viktor Levandovskyy

SFB Project F1301 of the Austrian FWF
Research Institute for Symbolic Computation (RISC)
Johannes Kepler University
Linz, Austria

Special Semester on Gröbner Bases and Related Methods

8.02.2006, Linz

Preliminaries

Let \mathbb{K} be a field and R be a commutative ring $R = \mathbb{K}[x_1, \dots, x_n]$.

$$\text{Mon}(R) \ni x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \mapsto (\alpha_1, \alpha_2, \dots, \alpha_n) = \alpha \in \mathbb{N}^n.$$

Definition

- 1 a total ordering \prec on \mathbb{N}^n is called a **well-ordering**, if
 - ▶ $\forall F \subseteq \mathbb{N}^n$ there exists a minimal element of F ,
in particular $\forall a \in \mathbb{N}^n, 0 \prec a$
- 2 an ordering \prec is called a **monomial ordering on R** , if
 - ▶ $\forall \alpha, \beta \in \mathbb{N}^n \alpha \prec \beta \Rightarrow x^\alpha \prec x^\beta$
 - ▶ $\forall \alpha, \beta, \gamma \in \mathbb{N}^n$ such that $x^\alpha \prec x^\beta$ we have $x^{\alpha+\gamma} \prec x^{\beta+\gamma}$.
- 3 Any $f \in R \setminus \{0\}$ can be written uniquely as $f = cx^\alpha + f'$, with $c \in \mathbb{K}^*$ and $x^{\alpha'} \prec x^\alpha$ for any non-zero term $c'x^{\alpha'}$ of f' . We define
$$\begin{aligned} \text{lm}(f) &= x^\alpha, & \text{the leading monomial of } f \\ \text{lc}(f) &= c, & \text{the leading coefficient of } f \end{aligned}$$

Computational Objects

Suppose we are given the following data

- 1 a field \mathbb{K} and a commutative ring $R = \mathbb{K}[x_1, \dots, x_n]$,
- 2 a set $C = \{c_{ij}\} \subset \mathbb{K}^*$, $1 \leq i < j \leq n$
- 3 a set $D = \{d_{ij}\} \subset R$, $1 \leq i < j \leq n$

Assume, that there exists a monomial well-ordering \prec on R such that

$$\forall 1 \leq i < j \leq n, \text{Im}(d_{ij}) \prec x_i x_j.$$

The Construction

To the data (R, C, D, \prec) we associate an algebra

$$A = \mathbb{K}\langle x_1, \dots, x_n \mid \{x_j x_i = c_{ij} x_i x_j + d_{ij}\} \forall 1 \leq i < j \leq n \rangle$$

PBW Bases and G -algebras

Define the (i, j, k) -nondegeneracy condition to be the polynomial

$$NDC_{ijk} := c_{ik}c_{jk} \cdot d_{ij}x_k - x_kd_{ij} + c_{jk} \cdot x_jd_{ik} - c_{ij} \cdot d_{ik}x_j + d_{jk}x_i - c_{ij}c_{ik} \cdot x_id_{jk}.$$

Theorem

$A = A(R, C, D, \prec)$ has a PBW basis $\{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}\}$ if and only if

$$\forall 1 \leq i < j < k \leq n, \quad NDC_{ijk} \text{ reduces to } 0 \text{ w.r.t. relations}$$

Curious fact $NDC_{ijk} = x_k(x_jx_i) - (x_kx_j)x_i$.

Definition

An algebra $A = A(R, C, D, \prec)$, where nondegeneracy conditions vanish, is called a **G -algebra** (in n variables).

Filtration by Ordering

Any admissible well-ordering \prec induces a filtration on a G -algebra A . For $\alpha \in \mathbb{N}^n$, let $A_\alpha = \{f \in A \mid \text{Im}(f) \preceq x^\alpha\}$. Note, that $\dim_{\mathbb{K}} A_\alpha \leq \infty$.

A is a multi-filtered algebra

- $A_{\bar{0}} = \mathbb{K}$ and $\forall \beta \prec \alpha \quad A_\beta \subset A_\alpha \subset A$,
- $A = \bigcup_{\alpha \in \mathbb{N}^n} A_\alpha$,
- $A_\alpha \cdot A_\beta \subseteq A_{\alpha+\beta}$ (since $\text{Im}(x^\alpha x^\beta) = x^{\alpha+\beta}$).

Let $\sigma(\alpha) = \max_{\prec} \{\gamma \mid \gamma \prec \alpha\}$, $\sigma(\bar{0}) = \emptyset$. Then $G_\alpha = A_\alpha / A_{\sigma(\alpha)} = \{x^\alpha\}$.

$$\text{Hence, } \text{Gr}_{\prec}(A) = \bigoplus_{\alpha \in \mathbb{N}^n} G_\alpha \cong \mathbb{K}\langle \bar{x}_1, \dots, \bar{x}_n \mid \bar{x}_j \bar{x}_i = c_{ij} \bar{x}_i \bar{x}_j \forall j > i \rangle,$$

where $\bar{x}_i = x_i + A_{\sigma(e_i)}$ and $\text{Gr}_{\prec}(A)$ is an **associated graded algebra** of A .

Gel'fand–Kirillov dimension

Let R be an associative \mathbb{K} –algebra with generators x_1, \dots, x_m .

A degree filtration

Consider the vector space $V = \mathbb{K}x_1 \oplus \dots \oplus \mathbb{K}x_m$.

Set $V_0 = \mathbb{K}$, $V_1 = \mathbb{K} \oplus V$ and $V_{n+1} = V_n \oplus V^{n+1}$.

Thus, we have an ascending filtration $\{V_n, n \geq 0\}$.

For any fin. gen. left R –module M , there exists a fin.–dim. subspace $M_0 \subset M$ such that $RM_0 = M$.

An ascending filtration on M is defined by $\{H_n := V_n M_0, n \geq 0\}$.

Definition

Let $\{H_n, n \geq 0\}$ be an ascending fin.–dim. filtration on M as before.

The **Gel'fand–Kirillov dimension** of M is defined to be

$$\text{GKdim}(M) = \limsup_{n \rightarrow \infty} \log_n(\dim_{\mathbb{K}} H_n)$$

Definition

Let A be an associative \mathbb{K} -algebra and M be a left A -module.

- 1 The **grade** of M is defined to be $j(M) = \min\{i \mid \text{Ext}_A^i(M, A) \neq 0\}$, or $j(M) = \infty$, if no such i exists or $M = \{0\}$.
- 2 A satisfies the **Auslander condition**, if for every fin. gen. A -module M , for all $i \geq 0$ and for all submodules $N \subseteq \text{Ext}_A^i(M, A)$ the inequality $j(N) \geq i$ holds.
- 3 A is called an **Auslander regular** algebra, if it is Noetherian with $\text{gl. dim}(A) < \infty$ and the Auslander condition holds.
- 4 A is called a **Cohen-Macaulay** algebra, if for every fin. gen. nonzero A -module M , $j(M) + \text{GKdim}(M) = \text{GKdim}(A) < \infty$.

We collect the properties in the following Theorem.

Theorem (Properties of G -algebras)

Let A be a G -algebra in n variables. Then

- A is left and right Noetherian,
- A is an integral domain,
- the Gel'fand–Kirillov dimension $\text{GKdim}(A) = n$,
- the global homological dimension $\text{gl. dim}(A) \leq n$,
- the Krull dimension $\text{Kr.dim}(A) \leq n$,
- A is Auslander-regular and a Cohen-Macaulay algebra.

We say that a **GR-algebra** $\mathcal{A} = A/T_A$ is a factor of a G -algebra in n variables A by a proper two-sided ideal T_A .

Examples of GR -algebras

- algebras of solvable type, skew polynomial rings
- univ. enveloping algebras of fin. dim. Lie algebras
- quasi-commutative algebras, rings of quantum polynomials
- positive (resp. negative) parts of quantized enveloping algebras
- some iterated Ore extensions, some nonstandard quantum deformations, some quantum groups
- Weyl, Clifford, exterior algebras
- Witten's deformation of $U(\mathfrak{sl}_2)$, Smith algebras
- algebras, associated to $(q-)$ differential, $(q-)$ shift, $(q-)$ difference and other linear operators
- ...

Gröbner Basis: Preparations

Definition

We say that monomial x^α **divides** monomial x^β , if $\alpha_i \leq \beta_i \forall i = 1 \dots n$. We use the notation $x^\alpha \mid x^\beta$.

It means that x^β is **reducible** by x^α from the right, from the left and from both sides. A left divisibility means that there exist $c \in \mathbb{K} \setminus \{0\}$, $p \in \text{Mon}(A)$ and $r \in A$ such that $\text{Im}(r) \prec x^\alpha$ and $x^\beta = c \cdot p \cdot x^\alpha + r$.

Definition

Let \prec be a monomial ordering on A^r , $I \subset A^r$ be a left submodule and $G \subset I$ be a finite subset. G is called a **left Gröbner basis** of I , if $\forall f \in I \setminus \{0\}$ there exists a $g \in G$ satisfying $\text{Im}(g) \mid \text{Im}(f)$.

Characterizations of Gröbner bases

Definition

Let S be any subset of A^r .

- We define a **monoideal of leading exponents** $\mathcal{L}(S) \subseteq \mathbb{N}_r \times \mathbb{N}^n$ to be a \mathbb{N}^n -monoideal, generated by the leading exponents of elements of S , $\mathcal{L}(S) = \mathbb{N}^n \langle (i, \alpha) \mid \exists s \in S, \text{lex}(s) = (i, \alpha) \rangle$.
- $L(S)$, the **span of leading monomials of S** , is defined to be the \mathbb{K} -vector space, spanned by the set $\{x^\alpha e_i \mid (i, \alpha) \in \mathcal{L}(S)\} \subseteq A^r$.

Properties

- $\text{Gr}_{\prec}(S) = L(S)$, hence $L(S)$ is a $\text{Gr}_{\prec}(A)$ -module
- G is a left Gröbner basis of $I \Leftrightarrow L(G) = L(I)$ as \mathbb{K} -vector spaces
- G is a left Gröbner basis of $I \Leftrightarrow \mathcal{L}(G) = \mathcal{L}(I)$ as \mathbb{N}^n -monoideals

Filtrations and Gröbner bases

Let \prec_d be a degree ordering with positive weights.

Then for any $a \in A$, its "homogeneous part" with respect to the \mathbb{N} -filtration by degree is the "symbol" of a and $\dim_{\mathbb{K}} A_d < \infty$.

Let \prec_e be an elimination ordering

Here, we have $\dim_{\mathbb{K}} A_\alpha = \infty$ but the "homogeneous part" of any $a \in A$ with respect to \prec_e is exactly the leading term $\text{lc}(a)$ $\text{lm}(a)$.

However:

$\text{Gr } I \subset \text{Gr } A$ is a Gröbner basis does not imply $I \subset A$ is a Gröbner basis, while the converse is true.

Normal Form

Definition

Let \mathcal{G} denote the set of all finite and ordered subsets $G \subset A^r$.

A map $\text{NF} : A^r \times \mathcal{G} \rightarrow A^r$, $(f, G) \mapsto \text{NF}(f|G)$, is called a **(left) normal form** on A^r if, for all $f \in A^r$, $G \in \mathcal{G}$,

- 1 $\text{NF}(0 | G) = 0$,
- 2 $\text{NF}(f|G) \neq 0 \Rightarrow \text{Im}(\text{NF}(f|G)) \notin L(G)$,
- 3 $f - \text{NF}(f|G) \in {}_A\langle G \rangle$.

Let $G = \{g_1, \dots, g_s\} \in \mathcal{G}$. A representation $f = \sum_{i=1}^s a_i g_i$, $a_i \in A$ of $f \in {}_A\langle G \rangle$, satisfying $\text{Im}(a_i g_i) \preceq \text{Im}(f)$ for all $1 \leq i \leq s$ such that $a_i g_i \neq 0$ is called a **standard left representation** of f with respect to G .

Left Buchberger's Criterion

Definition

Let $f, g \in A^r$ with $\text{lm}(f) = x^\alpha e_i$ and $\text{lm}(g) = x^\beta e_j$. Set $\gamma = \mu(\alpha, \beta)$, $\gamma_i := \max(\alpha_i, \beta_i)$ and define the **left s-polynomial** of (f, g) to be

$$\text{LeftSpoly}(f, g) := x^{\gamma-\alpha}f - \frac{\text{lc}(x^{\gamma-\alpha}f)}{\text{lc}(x^{\gamma-\beta}g)}x^{\gamma-\beta}g \text{ if } i = j \text{ and } 0 \text{ otherwise.}$$

Theorem

Let $I \subset A^r$ be a left submodule and $G = \{g_1, \dots, g_s\}$, $g_i \in I$.
Let $\text{LeftNF}(\cdot|G)$ be a left normal form on A^r w.r.t G .

Then the following are equivalent:

- 1 G is a left Gröbner basis of I ,
- 2 $\text{LeftNF}(f|G) = 0$ for all $f \in I$,
- 3 each $f \in I$ has a left standard representation with respect to G ,
- 4 $\text{LeftNF}(\text{LeftSpoly}(g_i, g_j)|G) = 0$ for $1 \leq i, j \leq s$.

Criteria for detecting useless critical pairs

Generalized Product Criterion

Let A be a G -algebra of Lie type (that is, all $c_{ij} = 1$). Let $f, g \in A$. Suppose that $\text{Im}(f)$ and $\text{Im}(g)$ have no common factors, then $\text{spoly}(f, g) \rightarrow_{\{f, g\}} [g, f]$, where $[g, f] := gf - fg$ is the Lie bracket.

Chain Criterion

If (f_i, f_j) , (f_i, f_k) and (f_j, f_k) are in the set of pairs P and $x^{\alpha_j} \mid \text{lcm}(x^{\alpha_i}, x^{\alpha_k})$, then we can delete (f_i, f_k) from P .

The Chain Criterion can be proved with the Schreyer's construction of the first syzygy module of a given module, which generalizes to the case of G -algebras.

Gröbner basics

Gröbner Basics are ...

...the most important and fundamental applications of Gröbner Bases.

- Ideal (resp. module) membership problem (NF, REDUCE)
- Intersection with subrings (elimination of variables) (ELIMINATE)
- Intersection of ideals (resp. submodules) (INTERSECT)
- Quotient and saturation of ideals (QUOT)
- Kernel of a module homomorphism (MODULO)
- Kernel of a ring homomorphism (NCPREIMAGE.LIB)
- Algebraic relations between pairwise commuting polynomials
- Hilbert polynomial of graded ideals and modules

Anomalies With Elimination

Contrast to Commutative Case

In terminology, we rather use "intersection with subalgebras" instead of "elimination of variables", since the latter may have no sense.

Let $A = \mathbb{K}\langle x_1, \dots, x_n \mid \{x_j x_i = c_{ij} x_i x_j + d_{ij}\}_{1 \leq i < j \leq n} \rangle$ be a G -algebra.

Consider a subalgebra A_r , generated by $\{x_{r+1}, \dots, x_n\}$.

We say that such A_r is an *admissible subalgebra*, if d_{ij} are polynomials in x_{r+1}, \dots, x_n for $r+1 \leq i < j \leq n$ and $A_r \subsetneq A$ is closed in itself w. r. t. the multiplication and it is a G -algebra.

Definition (Elimination ordering)

Let A and A_r be as before and $B := \mathbb{K}\langle x_1, \dots, x_r \mid \dots \rangle \subset A$

An ordering \prec on A is an **elimination ordering** for x_1, \dots, x_r

if for any $f \in A$, $\text{Im}(f) \in B$ implies $f \in B$.

Anomalies With Elimination: Conclusion

”Elimination of variables x_1, \dots, x_r from an ideal I ”

means the intersection $I \cap A_r$ with an admissible subalgebra A_r .

In contrast to the commutative case:

- not every subset of variables determines an admissible subalgebra
- there can be no admissible elimination ordering \prec_{A_r}

Example

Consider the algebra $A = \mathbb{K}\langle a, b \mid ba = ab + b^2 \rangle$. It is a G -algebra with respect to any well-ordering, such that $b^2 \prec ab$, that is $b \prec a$. Any elimination ordering for b must satisfy $b \succ a$, hence A is not a G -algebra w.r.t. any elimination ordering for b .

The Gröbner basis of a two-sided ideal, generated by $b^2 - ba + ab$ in $\mathbb{K}\langle a, b \rangle$ is infinite and equals to $\{ba^{n-1}b - \frac{1}{n}(ba^n - a^n b) \mid n \geq 1\}$.

Non-commutative Gröbner basics

For the noncommutative PBW world, we need even more:

- Gel'fand–Kirillov dimension of a module (GKDIM.LIB)
- Two–sided Gröbner basis of a bimodule (`twostd`)
- Central Character Decomposition of a module (NCDECOMP.LIB)
- Preimage of a module under algebra morphism
- One–dimensional representations
- Ext and Tor modules for centralizing bimodules (NCHOMOLOG.LIB)
- Maximal two–sided ideal in a left ideal (NCANN.LIB in work)
- Check whether a module is simple
- Center of an algebra and centralizers of polynomials
- Operations with opposite and enveloping algebras

Gröbner basis engine

Left Gröbner basis of a left module $M \subset A^r$

- for any admissible (monomial module) well-ordering
- completely reduced Gröbner basis
- generalized criteria, different selection strategies
- **quite fast in general**

With essentially one computation we can get

- Gröbner basis of a left module (also over a factor-algebra), `std`
- Gröbner basis of the left syzygy module, `syz`
- the transition matrix between two bases, `lift`

Gröbner basis engine(s)

`slimgb` — Slim Gröbner basis

- implemented by M. Brickenstein
- uses t -representation and generalized t -Chain Criterion
- "exchanging" normal form
- selection strategy prefers "shorter" polynomials
- performs simultaneous reductions of a group of polys by a poly
- controls the size of coefficients

`janet` — Janet involutive basis

- implemented by D. Yanovich, following the ideas of V. P. Gerdt
- an enhanced implementation is planned

Extended Gröbner basis engine

- Left Gröbner basis of a two-sided ideal T

- ▶ needed e.g. for constructing factor algebras
- ▶ fast algorithm (and a faster one is planned)
- ▶ idea: completion of right action
- ▶ generalization to bimodules under development

- Left Gröbner basis of a syzygy module of M

- ▶ Gröbner basis-driven algorithm
- ▶ free resolutions (normal and minimized)
- ▶ (potential) Schreyer and La Scala algorithms
- ▶ Betti numbers (in graded case)

Implementation in PLURAL

What is PLURAL?

- PLURAL is the kernel extension of SINGULAR
- PLURAL is distributed with SINGULAR (from version 3-0-0 on)
- freely distributable under GNU Public License
- available for most hardware and software platforms

PLURAL as a Gröbner engine

- implementation of all the Gröbner basics available
- `slimgb` is available for Plural (and it is fast!)
- `janet` is available for two-sided input
- non-commutative Gröbner basics:
 - ▶ as kernel functions (`twostd`, `opposite` etc)
 - ▶ as libraries (`NCDECOMP.LIB`, `NCTOOLS.LIB`, `NCPREIMAGE.LIB` etc)

Preimage in commutative subalgebra

Definition

Let $\mathcal{A} = A/T_A$ and $\mathcal{B} = B/T_B$ be GR-algebras and $\Psi : \mathcal{A} \rightarrow \mathcal{B}$ be a map, such that $\Psi(T_A) \subseteq T_B$.

Let the **ideal of obstructions** of Ψ be $O_\Psi := \mathcal{B}\langle\{o_{ij} \mid 1 \leq i < j \leq n\}\rangle$, where the **obstruction polynomial** $o_{ij} := \Psi(\bar{x}_j\bar{x}_i) - \Psi(\bar{x}_j)\Psi(\bar{x}_i)$.

Fact

$\Psi \in \text{Mor}(\mathcal{A}, \mathcal{B}) \Leftrightarrow O_\Psi = \langle 0 \rangle$.

Theorem

Let $\mathcal{A} = \mathbb{K}[y_1, \dots, y_m]/T_A$, \mathcal{B} be a GR-algebra, $\Phi \in \text{Mor}(\mathcal{A}, \mathcal{B})$ and $\mathcal{J} \subset \mathcal{B}$ be a left ideal. Let $I_\Phi = \langle\{y_i - \Phi(y_i) \mid 1 \leq i \leq m\}\rangle \subset \mathcal{A} \otimes_{\mathbb{K}} \mathcal{B}$ be a left ideal. Then $\Phi^{-1}(\mathcal{J}) = (I_\Phi + \mathcal{J}) \cap \mathcal{A}$.

Centers in char p . Preliminaries

Let \mathbb{K} be a field, and \mathfrak{g} be a simple Lie algebra of dimension n and of rank r over \mathbb{K} . Consider $A = U(\mathfrak{g})$.

char $\mathbb{K} = 0$

The center of A is generated by the elements $Z_0 = \{c_1, \dots, c_r\}$, which are algebraically independent.

char $\mathbb{K} = p$

Z_0 are again central, but there are more central elements:

- for every positive root α of \mathfrak{g} , $\{x_\alpha^p, x_{-\alpha}^p\}$ are central,
- for every simple root, $h_\alpha^p - h$ is central.

We denote the set of p -adic central elements by $Z_p = \{z_1, \dots, z_n\}$.

Challenge: Central Dependence in char p

Problem Formulation

The set of all central elements $Z := Z_0 \cup Z_p$ is algebraically dependent. Compute the ideal of dependencies!

Example ($g = s[2]$)

$$Z_0 = \{c\} = \{4ef + h^2 - 2h\}, \quad Z_p = \{z_1, z_2, z_3\} = \{e^p, f^p, h^p - h\}.$$

Let $F_p = F_p(c, z_1, z_2, z_3)$ be the dependence in the case $\text{char } \mathbb{K} = p$.

$$F_5 = c^2(c+1)(c+2)^2 + z_1z_2 - z_3^2$$

$$F_7 = c^2(c+1)(c-1)^2(c-3)^2 + 3z_1z_2 - z_3^2$$

$$F_{11} = c^2(c+1)(c+3)^2(c-3)^2(c-2)^2(c-4)^2 + 7z_1z_2 - z_3^2$$

...

$$F_{29} = (c+1)(c-6)^2(c+8)^2(c-4)^2(c+14)^2(c-8)^2c^2(c-3)^2(c-12)^2(c-5)^2(c+6)^2(c+5)^2(c+2)^2(c+10)^2(c+7)^2 + 25z_1z_2 - z_3^2$$

Each dependency polynomial determines a singularity of the type A_1 .

Combined Computations

Commutative Libraries, using Plural

- SHEAFCOH.LIB
computation of the cohomology of coherent sheaves
- CONTROL.LIB
algebraic analysis tools for System and Control Theory

Many Plural libs use commutative functionality of Singular (like NCDECOMP.LIB)

Announcement

The newest addition to SINGULAR:PLURAL is the library DMOD.LIB, containing algorithms of algebraic D -Module Theory. A joint work of V. Levandovskyy (RISC) and J. M. Morales (Sevilla)

Perspectives

Gröbner bases for more non-commutative algebras

- tensor product of commutative local algebras with certain non-commutative algebras (e.g. with exterior algebras for the computation of direct image sheaves)
- different localizations of G -algebras
 - localization at some "coordinate" ideal of commutative variables (producing e.g. local Weyl algebras $\mathbb{K}[x] \langle D \mid Dx = xD + 1 \rangle$)
 - ⇒ local orderings and the generalization of **standard basis** algorithm, Gröbner basics and homological algebra
 - localization as field of fractions of commutative variables (producing e.g. rational Weyl algebras $\mathbb{K}(x) \langle D \mid Dx = xD + 1 \rangle$), including **Ore Algebras** (F. Chyzak, B. Salvy)
 - ⇒ global orderings and a generalization **Gröbner basis** algorithm. However, conceptually new problems arise, Gröbner basics require rethinking and distinct theoretical treatment

Thank you !



Please visit the SINGULAR homepage

• <http://www.singular.uni-kl.de/>