Non–commutative Computations with 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

16.02.2006, Linz

Origins Of Non-commutativity

Let C be some algebra of functions (C^∞ etc).
For any function $f \in C$, we introduce an operator

$$F : C \to C,\ F(t) = f \cdot t.$$

We call f a **representative** of F. $\forall f, g \in C$ we have $F \circ G = G \circ F$.

Definition

A map $\partial : C \to C$ is called a **differential** if ∂ is C–linear and $\forall f, g \in C$, $\partial(fg) = \partial(f)g + f\partial(g)$.

In particular, $\partial_i = \frac{\partial}{\partial t_i}$ on C are differentials.

News

Bad news: operators F and ∂_i do not commute.
Good news: $\partial_j \circ \partial_i = \partial_i \circ \partial_j$ and there is a relation between F and ∂_i.

Non–commutative Relations

Lemma

For any differential ∂ and $f \in C$, $\quad \partial \circ F = F \circ \partial + \partial(f)$.

Proof.

$\forall\ h \in C$, we have the following:

$$(\partial \circ F)(h) = \partial(f \cdot h) = f \cdot \partial(h) + \partial(f) \cdot h =$$

$$= (F \circ \partial)(h) + \partial(f) \cdot (h) = (F \circ \partial + \partial(f))(h).$$

Example

Let $C = \mathbb{K}[t_1, \ldots, t_n]$ and $\partial_i = \frac{\partial}{\partial t_i}$. Then there is a n–th Weyl algebra
$\mathbb{K}\langle t_1, \ldots, t_n, \partial_1, \ldots, \partial_n \mid \{t_j t_i = t_i t_j, \partial_j \partial_i = \partial_i \partial_j,$
$\partial_k t_k = t_k \partial_k + 1\} \cup \{\partial_j t_i = t_i \partial_j\}_{i \neq j}\rangle$,
an algebra of linear differentional operators with polynomial coefficients.

More Non–commutative Relations

Shift Algebra

For small $\triangle t \in \mathbb{R}$, we define a shift operator

$$\sigma_t : C \to C,\ \sigma_t(f(t)) = f(t + \triangle t).$$

Then, since $\sigma_t(f \cdot g) = \sigma_t(f) \cdot \sigma_t(g)$, we define a real shift algebra $\mathbb{K}(\triangle x)\langle x, \sigma_x \mid \sigma_x x = x\sigma_x + \triangle x \sigma_x \rangle$.

The Center of an Algebra

For a $\mathbb{K}$–algebra A, we define the center of A to be

$$Z(A) = \{a \in A \mid a \cdot b = b \cdot a\, \forall b \in A\}.$$

It is a subalgebra of A, containing constants of $\mathbb{K}$.

q–Calculus and Non–commutative Relations

Let k be a field of char 0 and $\mathbb{K} = k(q)$.

q–dilation operator

$D_q : C \to C, \quad D_q(f(x)) = f(qx)$:

$$\mathbb{K}(q)\langle x, D_q \mid D_q \cdot x = q \cdot x \cdot D_q \rangle.$$

Continuous q–difference Operator

$\Delta_q : C \to C, \quad \Delta_q(f(x)) = f(qx) - f(x)$:

$$\mathbb{K}(q)\langle x, \Delta_q \mid \Delta_q \cdot x = q \cdot x \cdot \Delta_q + (q-1) \cdot x \rangle.$$

q–differential Operator

$\partial_q : C \to C, \ \partial_q(f(x)) = \frac{f(qx)-f(x)}{(q-1)x}$:

$$\mathbb{K}(q)\langle x, \partial_q \mid \partial_q \cdot x = q \cdot x \cdot \partial_q + 1 \rangle.$$

Some Preliminaries

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

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

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
   $\mathrm{lm}(f) = x^\alpha$, the **leading monomial** of f
   $\mathrm{lc}(f) = c$, the **leading coefficient** of f

Computational Objects

Suppose we are given the following data

1. a field $\mathbb{K}$ and a commutative ring $R = \mathbb{K}[x_1, \ldots, x_n]$,
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

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

The Construction

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

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

PBW Bases and G–algebras

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

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

Theorem

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

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

Easy Check $NDC_{ijk} = x_k(x_j x_i) - (x_k x_j)x_i$.

Definition

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

Setting up G–algebras

After initializing a commutative ring R with the ordering $\prec$, one defines C_{ij} and D_{ij} and finally calls `ncalgebra(C,D);`

```
ring R = 0,(x,y,z),Dp;
int  N = nvars(R);
matrix C[3][3];
C[1,2] = ...; C[1,3] = ...; C[2,3] = ...;
matrix D[N][N];
D[1,3] = ...;
ncalgebra(C,D);
```

Frequently Happening Errors

- matrix is smaller in size than $n \times n$;
- matrix C contain zeros in its upper part;
- the ordering condition is not satisfied.

Gel'fand–Kirillov dimension

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

A degree filtration

Consider the vector space $V = \mathbb{K}x_1 \oplus \ldots \oplus \mathbb{K}x_m$.
Set $V_0 = \mathbb{K}$, $V_1 = \mathbb{K} \oplus V$ and $V_{n+1} = V_n \oplus V^{n+1}$.
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

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

$$\mathrm{GKdim}(M) \;=\; \lim_{n\to\infty} \sup \log_n(\dim_{\mathbb{K}} H_n)$$

Implementation: GKDIM.LIB, function `GKdim`. Uses Gröbner basis.

Factor–algebras

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.

Two–sided Gröbner Bases

A set of generators *F* is called a two–sided Gröbner basis,
if it is a left and a right Gröbner basis at the same time.

Implementation: command `twostd`.

Note

- there are algebras without nontrivial two–sided ideals (Weyl)
- a two–sided ideal is usually bigger than the left ideal, built on the same generating set

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 $\alpha_i \leq \beta_i \; \forall i = 1 \ldots n$. 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 $c \in \mathbb{K} \setminus \{0\}$, $p \in \mathrm{Mon}(A)$ and $r \in A$ such that $\mathrm{lm}(r) \prec x^\alpha$ 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 $\mathrm{lm}(g) \mid \mathrm{lm}(f)$.

Normal Form

Definition

Let $\mathcal{G}$ denote the set of all finite and ordered subsets $G \subset A^r$.
A map $\text{NF} : A^r \times \mathcal{G} \to A^r,\ (f, G) \mapsto \text{NF}(f|G)$, is called a **(left) normal form** on A^r if, for all $f \in A^r$, $G \in \mathcal{G}$,

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

Let $G = \{g_1, \ldots, g_s\} \in \mathcal{G}$. A representation $f = \sum_{i=1}^{s} a_i g_i,\ \ a_i \in A$ of $f \in {}_A\langle G\rangle$, satisfying $\text{lm}(a_i g_i) \preceq \text{lm}(f)$ 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 $\mathrm{lm}(f) = x^\alpha e_i$ and $\mathrm{lm}(g) = x^\beta e_j$. Set $\gamma = \mu(\alpha, \beta)$, $\gamma_i := \max(\alpha_i, \beta_i)$ and define the **left s–polynomial** of (f, g) to be $\mathrm{LeftSpoly}(f, g) := x^{\gamma-\alpha} f - \frac{\mathrm{lc}(x^{\gamma-\alpha} f)}{\mathrm{lc}(x^{\gamma-\beta} g)} x^{\gamma-\beta} g$ if $i = j$ and 0 otherwise.

Theorem

Let $I \subset A^r$ be a left submodule and $G = \{g_1, \ldots, g_s\}$, $g_i \in I$.
Let $\mathrm{LeftNF}(\cdot|G)$ 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. $\mathrm{LeftNF}(f|G) = 0$ for all $f \in I$,
3. each $f \in I$ has a left standard representation with respect to G,
4. $\mathrm{LeftNF}\big(\mathrm{LeftSpoly}(g_i, g_j)|G\big) = 0$ for $1 \leq i, j \leq s$.

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 $A = \mathbb{K}\langle x_1, \ldots, x_n \mid \{x_j x_i = c_{ij} x_i x_j + d_{ij}\}_{1 \leq i < j \leq n}\rangle$ be a G–algebra.
Consider a subalgebra A_r, generated by $\{x_{r+1}, \ldots, x_n\}$.
We say that such A_r is an *admissible subalgebra*, if d_{ij} are polynomials in $x_{r+1}, \ldots, x_n$ 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 $B := \mathbb{K}\langle x_1, \ldots, x_r \mid \ldots\rangle \subset A$
An ordering $\prec$ on A is an **elimination ordering for** $x_1, \ldots, x_r$
if for any $f \in A$, $\text{lm}(f) \in B$ implies $f \in B$.

Anomalies With Elimination: Conclusion

"Elimination of variables $x_1, \ldots, x_r$ 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

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)

Surprize

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).

Functionality: an algorithm ANNFS

- Oaku–Takayama approach (ANNFSOT command)
- Brianson–Maisonobe approach (ANNFSBM command)
- a so–called Bernstein polynomial is computed within both approaches

Constructively: two bigger rings are constructed and two eliminations are applied in a sequence.
Complexity of such computations is high!

D–modules

What's Behind

Let $R = \mathbb{K}[x_1, \ldots, x_n]$ and $f \in R$. We are interested in $R[f^{-s}] = \mathbb{K}[x_1, \ldots, x_n, \frac{1}{f^s}]$ as an R–module for $s \in \mathbb{N}$.
On the one hand, $R[f^{-s}] \cong R[y]/\langle yf^s - 1\rangle$.
On the other hand, $R[f^{-s}]$ is a D–module, where D is the n–th Weyl algebra $\mathbb{K}\langle x_1, \ldots, x_n, \partial_1, \ldots, \partial_n \mid \{\partial_j x_i = x_i \partial_j + \delta_{ij}\}\rangle$.
The algorithm ANNFS computes a D–module structure on $R[f^{-s}]$, that is a left ideal $I \subset D$, such that $R[f^{-s}] \cong D/I$.

Especially interesting are cases when f is irreducible singular, reducibly singular or when f is a hyperplane arrangement.

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 $\mathbb{K}[x]_{\langle x \rangle}\langle D \mid Dx = xD + 1 \rangle$)

$\Rightarrow$ 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)

$\Rightarrow$ 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/