PLURAL, a Non–commutative Extension of SINGULAR: Past, Present and Future

Viktor Levandovskyy

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

International Congress on Mathematical Software 2006

3.09.2006, Castro Urdiales

What is PLURAL?

What is PLURAL?

PLURAL is the kernel extension of SINGULAR,
providing a wide range of symbolic algoritms with non–commutative polynomial algebras (*GR*–algebras).

- Gröbner bases, Gröbner basics, non–commutative Gröbner basics
- more advanced algorithms for non–commutative algebras,

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

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

Towards *GR*–algebras

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 $D = \{d_{ij}\} \subset R, \quad 1 \leq i < j \leq n$

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

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

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 $\{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}\}$ if and only if

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

Definition

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

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* $\operatorname{GKdim}(A) = n + \operatorname{GKdim}(\mathbb{K})$,
- *the global homological dimension* $\operatorname{gl.dim}(A) \leq n$,
- *the Krull dimension* $Kr.dim(A) \leq n$,
- *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

Mora, Apel, Kandri–Rody and Weispfenning, ...

- 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
- many 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

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 $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$ have no common factors, then $\mathrm{spoly}(f, g) \rightarrow_{\{f,g\}} [g, f]$, 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 $x^{\alpha_j} \mid \mathrm{lcm}(x^{\alpha_i}, x^{\alpha_k})$, 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.

Left, right and twosided structures

It suffices to have implemented

- left Gröbner bases
- functionality for opposite algebras $\mathcal{A}^{op}$
- functionality for enveloping algebras $\mathcal{A}^{env} = \mathcal{A} \otimes_{\mathbb{K}} \mathcal{A}^{op}$
- mapping $\mathcal{A} \to \mathcal{A}^{op} \to \mathcal{A}$

Then

1. for a finite set $F \subset \mathcal{A}$, $\quad RGB_{\mathcal{A}}(F) = \left(LGB_{\mathcal{A}^{op}}(F^{op})\right)^{op}$
2. the two–sided Gröbner can be computed, for instance, with the algorithm by Manuel and Maria Garcia Roman in $\mathcal{A}^{env}$.

Gröbner Trinity

With essentially the same algorithm, we can compute

1. GB left Gröbner basis G of a module M
2. SYZ left Gröbner basis of the 1st syzygy module of M
3. LIFT the transformation matrix between two bases G and M

The algorithm for Gröbner Trinity must be able to compute ...

- with submodules of free modules
  - accept monomial module orderings as input
  - distinguish preferred module components
- within factor algebras
- with extra weights for the ordering / module generators
- and to use the information on Hilbert polynomial

Gröbner basis engine

...is an (implementation of an) algorithm,
designed to compute the Gröbner Trinity and
having the prescribed functionality.

Gröbner basis engine(s) behind SINGULAR's `std` command

- Gröbner bases (non–negatively graded orderings)
- standard bases (local and mixed orderings)
- PLURAL (left Gröbner bases for non–negatively graded orderings over *GR*–algebras)

Potential Gröbner basis engines

`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

Gröbner basics

Buchberger, Sturmfels, ...
GBasics are the most important and fundamental applications of Gröbner Bases.

Universal Gröbner Basics

- 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

Admissible Subalgebras

Let $A = \mathbb{K}\langle x_1, \ldots, x_n \mid \{x_j x_i = c_{ij} x_i x_j + d_{ij}\}_{1 \le i < j \le n}\rangle$ 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 $r + 1 \le i < j \le n$
and $A_r \subsetneq A$ 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 $f \in A$, $\operatorname{lm}(f) \in B$ implies $f \in B$.

Constructive Elimination Lemma

"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 $\prec_{A_r}$ on A

Lemma

Let A be a G–algebra, generated by $\{x_1, \ldots, x_n\}$ and $I \subset A$ be an ideal. Suppose, that the following conditions are satisfied:

- *$\{x_{r+1}, \ldots, x_n\}$ generate an essential subalgebra B,*
- *$\exists$ an admissible elimination ordering $\prec_B$ for $x_1, \ldots, x_r$ on A.*

Then, if S is a left Gröbner basis of I with respect to $\prec_B$, we have $S \cap B$ is a left Gröbner basis of $I \cap B$.

Anomalies With Elimination: Example

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 $\mathbb{K}\langle a, b \rangle$ w.r.t. an ordering $b \succ a$ 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 basics:

- Gel'fand–Kirillov dimension of a module (GKDIM.LIB)
- Two–sided Gröbner basis of a bimodule (e.g. `twostd`)
- Annihilator of finite dimensional module
- Preimage of one–sided ideal under algebra morphism
- Finite dimensional representations
- Graded Betti numbers (for graded modules over graded algebras)
- Left and right kernel of the presentation of a module
- Central Character Decomposition of a module (NCDECOMP.LIB)

Very Important

- Ext and Tor modules for centralizing bimodules (NCHOMOLOG.LIB)
- Hochschild cohomology for modules

Non-commutative Gröbner basics in PLURAL

Unrelated to Gröbner Bases, but Essential Functions

Center of an algebra and centralizers of polynomials
Operations with opposite and enveloping algebras

PLURAL as a Gröbner engine

- implementation of all the universal Gröbner basics available
- `slimgb` is available for Plural
- `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)

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 $Z_0 = \{c_1, \ldots, c_r\}$, 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 $Z_p = \{z_1, \ldots, z_n\}$.

Similar phenomenon arises in quantum algebras, when $\exists m : \; q^m = 1$.

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 (e.g. via elimination)

Example ($\mathfrak{g} = \mathfrak{sl}_2$)

$Z_0 = \{c\} = \{4ef + h^2 - 2h\}$, $Z_p = \{z_1, z_2, z_3\} = \{e^p, f^p, h^p - h\}$.
Let $F_p = F_p(c, z_1, z_2, z_3)$ be the dependence in the case char $\mathbb{K} = p$.
$F_5 = c^2(c+1)(c+2)^2 + z_1 z_2 - z_3^2$
$F_7 = c^2(c+1)(c-1)^2(c-3)^2 + 3z_1 z_2 - z_3^2$
$F_{11} = c^2(c+1)(c+3)^2(c-3)^2(c-2)^2(c-4)^2 + 7z_1 z_2 - z_3^2$
...
$F_{29} = (c+1)(c-6)^2(c+8)^2(c-4)^2(c+14)^2(c-8)^2 c^2(c-3)^2(c-12)^2(c-5)^2(c+6)^2(c+5)^2(c+2)^2(c+10)^2(c+7)^2 + 25z_1 z_2 - z_3^2$
Each dependency polynomial determines a singularity of the type A_1.

Challenge: Ann F^s for different F

Let char $\mathbb{K} = 0$ and $F \in \mathbb{K}[x_1, \ldots, x_n]$.

Problem Formulation

Compute the ideal Ann $F^s \in \mathbb{K}\langle x_1, \ldots, x_n, \partial_1, \ldots, \partial_n \mid \partial_i x_j = x_j \partial_i + \delta_{ij} \rangle$ (n–th Weyl algebra).
Both algorithms available (OT, BM) use two complicated eliminations.

- polynomial singularities
- very hard: Reiffen curves $x^p + y^q + xy^{q-1}$, $q \geq p + 1 \geq 5$
- generic and non–generic hyperplane arrangements
- further examples by F. Castro and J.-M. Ucha

Systems: KAN/SM1, RISA-ASIR, MACAULAY2, SINGULAR:PLURAL.

Applications

- Systems and Control Theory (VL, E. Zerz et. al.)
  - CONTROL.LIB, NCONTROL.LIB, RATCONTROL.LIB
  - algebraic analysis tools for System and Control Theory
  - In progress: non–commutative polynomial algebras (NCONTROL.LIB)
- Algebraic Geometry (W. Decker, C. Lossen and G. Pfister)
  - SHEAFCOH.LIB
  - computation of the cohomology of coherent sheaves
  - In progress: direct image sheaves (F. - O. Schreyer)
- D–Module Theory (VL and J. Morales)
  - DMOD.LIB
  - Ann F^s algorithms: OT (Oaku and Takayama), BM (Briançon and Maisonobe)

Applications In Progress

- Homological algebra in *GR*–algebras (with G. Pfister)
  - NCHOMOLOG.LIB
  - Ext and Tor modules for centralizing bimodules
  - Hochschild cohomology for modules
- Clifford Algebras (VL, V. Kisil et. al.)
  - CLIFFORD.LIB
  - basic algorithms and techniques of the theory of Clifford algebras
- Annihilator of a left module (VL)
  - NCANN.LIB
  - the original algorithm of VL for $\mathrm{Ann}(M)$ for M with $\dim_{\mathbb{K}} M = \infty$
  - the algorithm terminates for holonomic modules, i.e. for a module M, such that $\mathrm{GKdim}(M) = 2 \cdot \mathrm{GKdim}(\mathrm{Ann}(M))$
  - high complexity, a lot of tricks and improvements needed

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. Gröbner basics require distinct theoretical treatment!

Software from RISC Linz

Algorithmic Combinatorics Group, Prof. Peter Paule

- most of the software are packages for MATHEMATICA
- created by P. Paule, A. Riese, C. Schneider, M. Kauers, K. Wegschaider, S. Gerhold, M. Schorn, F. Caruso, C. Mallinger, B. Zimmermann, C. Koutschan, T. Bayer, C. Weixlbaumer et al.

The Software is freely available for non–commercial use

`www.risc.uni-linz.ac.at/research/combinat/software/`

Symbolic Summation

Hypergeometric Summation

- FASTZEIL, Gosper's and Zeilberger's algorithms
- ZEILBERGER, Gosper and Zeilberger alg's for MAXIMA
- MULTISUM, proving hypergeometric multi-sum identities

q–Hypergeometric Summation

- QZEIL, *q*–analogues of Gosper and Zeilberger alg's
- BIBASIC TELESCOPE, generalized Gosper's algorithm to bibasic hypergeometric summation
- QMULTISUM, proving *q*–hypergeometric multi-sum identities

Symbolic Summation in Difference Fields

- SIGMA, discovering and proving multi-sum identities

More Software from RISC Linz

Sequences and Power Series

- ENGEL, q–Engel Expansion
- GENERATINGFUNCTIONS, manipulations with univariate holonomic functions and sequences
- RLANGGFUN, inverse Schützenberger methodology in MAPLE

Partition Analysis, Permutation Groups

- OMEGA, Partition Analysis
- PERMGROUP, permutation groups, group actions, Polya theory

Difference/Differential Equations

- DIFFTOOLS, solving linear difference eq's with poly coeffs
- ORESYS, uncoupling systems of linear Ore operator equations
- RATDIFF, rat. solutions of lin. difference eq's after van Hoeij
- SUMCRACKER, identities and inequalities, including summations

Thank you for your attention! ¡Muchas gracias por su atención!

SINGULAR PLURAL

Please visit the SINGULAR homepage

- http://www.singular.uni-kl.de/

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 $j(M) = \min\{i \mid \operatorname{Ext}^i_A(M, A) \neq 0\}$, 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 $N \subseteq \operatorname{Ext}^i_A(M, A)$ the inequality $j(N) \geq i$ holds.
3. A is called an **Auslander regular** algebra, if it is Noetherian with $\operatorname{gl.dim}(A) < \infty$ and the Auslander condition holds.
4. A is called a **Cohen–Macaulay** algebra, if for every fin. gen. nonzero A–module M, $j(M) + \operatorname{GKdim}(M) = \operatorname{GKdim}(A) < \infty$.