Gröbner Bases with Coefficients in Rings

Franz Pauer

Institut für Mathematik
Universität Innsbruck

Austria

2008-07-27

Gröbner bases over rings: History

Gröbner bases in **commutative polynomial rings** with coefficients in rings:
Two approaches
(Example: $I :=< 2x, 3y >\leq \mathbb{Z}[x, y]$)

1. Simultaneous reduction by several polynomials:
   Trinks(1978): Gröbner bases in polynomial rings over a noetherian commutative ring;
   Pauer, Pfeifhofer (1988)
   Jacobson, Löfwall (1991);
   Adams, Loustaunau (1994): textbook;
   ...
   Gröbnerbasis of I: $\{2x, 3y\}$,
   $1 = (-1)\cdot 2 + 3$; $xy = (-1)y(2x) + x(3y)$.

2. Separate reduction by polynomials:
   Buchberger(1984); Kandri-Rody, Kapur (1988); Möller (1988); ...
   Gröbnerbasis of I: $\{2x, 3y, xy\}$, since xy is neither a multiple (in $\mathbb{Z}[x, y]$) of $2x$ nor of $3y$.

Gröbner bases in **(non-commutative) rings of differential operators:**
Galligo (1985), Castro (1987): Weyl-algebra
Insa, Pauer (1998): approach of Trinks; improvements by Winkler, Zhou (2005).

Important difference between the commutative and the non-commutative case:
ideals generated by monomials are "easy" in the commutative case (each finite set of monomials is a Gröbner basis of the ideal generated by it), but not in the non-commutative case.

Example: $\{y_1\frac{\partial}{\partial y_2}, y_2\frac{\partial}{\partial y_1}\}$ and $\{\frac{\partial}{\partial y_1}, \frac{\partial}{\partial y_2}\}$ generate the same left-ideal in the Weyl-algebra $K[y_1, y_2][\frac{\partial}{\partial y_1}, \frac{\partial}{\partial y_2}]$!

The Coefficient Ring

R ... (left-)noetherian associative ring with unity such that we can solve linear equations over R, i.e.

- for all $z \in R$ and for all finite subsets $S \subseteq R$, we can decide, whether z is an element of the left-ideal in R generated by S and - if yes - we can compute a family $(d_s)_{s \in S}$ in R such that $z = \sum_{s \in S} d_s s$,
  and

- for all finite subsets $S \subseteq R$ we can compute a finite system of generators of the R-module

$$\{(c_s)_{s \in S} \in R^S \mid \sum_{s \in S} c_s s = 0\}$$

  of its syzygies.

Examples for R:

- $\mathbb{Z}$
- $\mathbb{Z}_k$, where $k \in \mathbb{N}$
- polynomial rings with coefficients in a field (over which we can solve linear equations)
- $\{\frac{p}{q} \,|\, p, q \in K[y_1, \ldots, y_n], q(a) \neq 0\} \subseteq$ $\subseteq K(y_1, \ldots, y_n)$, where $a \in K^n$
- Weyl-algebras over fields
- ...

Rings with Gröbner bases over R

$<$ ... term order on $\mathbb{N}^n$
A ... (left-)noetherian associative ring with unity containing R as a subring.
We assume that there are $x_1, \ldots, x_n \in A$ such that

- A is a free (left-)R-module and the family $(x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n})_{\alpha \in \mathbb{N}^n}$ is an R-basis of the R-module A,

- For all $\alpha \in \mathbb{N}^n$ and $f, g \in A$ such that $f \cdot g \neq 0$:
  $deg(f \cdot g) \leq deg(f) + deg(g)$,
  $deg(x^\alpha g) = \alpha + deg(g)$,
  $lc(x^\alpha g) = lc(g)$.

  (For $f := \sum_{\beta \in \mathbb{N}^n} c_\beta x^\beta$ we define
  $deg(f) := max_<\{\beta |\ c_\beta \neq 0\} \in \mathbb{N}^n$,
  $lc(f) := c_{deg(f)}$,
  $lm(f) := lc(f) x^{deg(f)}$).

Examples for A:

- commutative polynomial rings $R[x_1, \ldots, x_n]$ over the ring R
  Example: $R = \mathbb{Z}_6$, $f := \bar{3}x + \bar{1}$, $g := \bar{2}$, $f \cdot g = \bar{2}$, $deg(f \cdot g) = 0 < 1 = deg(f) + deg(g)$.

- rings of differential operators with coefficients in certain rings R:
  $K(y) := K(y_1, \ldots, y_n)$ field of rational functions over a field K,
  $\frac{\partial}{\partial y_i}$: $K(y) \to K(y)$ partial derivative by y_i,
  R noetherian K-subalgebra of $K(y_1, \ldots, y_n)$ which is stable by $\frac{\partial}{\partial y_i}$, $1 \leq i \leq n$,
  D_i restriction of $\frac{\partial}{\partial y_i}$ to $R, 1 \leq i \leq n$.
  $A := R[D] := R[D_1, \ldots, D_n]$ subring of $End_K(R)$ generated by $R \cdot id_R = R$ and $x_1 := D_1, \ldots, x_n := D_n$.
  If $R = K[y]$, then A is the Weyl-Algebra.

Gröbner bases in A

I ... left-ideal in A
$\alpha \in \mathbb{N}^n$

$lc(\alpha, I) :=_R < lc(f); f \in I, deg(f) = \alpha >$
(left-ideal in R)

I and $<$ yield a family of left-ideals in R:

$$(lc(\alpha, I))_{\alpha \in deg(I)}$$

A *Gröbner basis of* I allows to have this family under control:

G ... finite subset of $I \setminus \{0\}$
G is a Gröbner basis of I (with respect to $<$) iff for all $\alpha \in \mathbb{N}^n$ the ideal $lc(\alpha, I)$ is generated by

$$\{lc(g);\ g \in G,\ deg(g) \in \alpha - \mathbb{N}^n\}.$$

If A is commutative: G Gröbner basis of I iff the ideal $< lc(f); f \in I \setminus \{0\} >$ is generated by $\{lc(g);\ g \in G\}$. Not true in the non-commutative case!

Division in A

F ... finite subset of $A \setminus \{0\}$
$g \in A$

Division with remainder of g by F:
there are $r \in A$ and a family $(h_f)_{f \in F}$ in A such that

- $g = \sum_{f \in F} h_f f + r$ (r is "a remainder of g after division by F"),

- for all $f \in F$, $h_f = 0$ or
  $deg(h_f) + deg(f) \leq deg(g)$,

- $r = 0$ or $lc(r) \notin_R < lc(f)$; $f \in F$ and
  $deg(f) \in deg(r) - \mathbb{N}^n >$.

Computation of $r \in A$, $(h_f)_{f\in F}$:

First set $r := g$ and $h_f := 0$ $(f \in F)$.

While $r \neq 0$ and $lc(r) \in$
$\in_R < lc(f);\ f \in F$ and $deg(f) \in deg(r) - \mathbb{N}^n >$
do the following:

Let $F' := \{f \in F \mid deg(r) \in deg(f) + \mathbb{N}^n\}$, compute a family $(c_f)_{f\in F'}$ in R such that

$$\sum_{f\in F'} c_f lc(f) = lc(r).$$

Replace

$$r \quad \text{by} \quad r - \sum_{f\in F'} c_f x^{deg(r)-deg(f)} f$$

and

$$h_f \quad \text{by} \quad h_f + c_f x^{deg(r)-deg(f)} f, \quad f \in F'.$$

Example:
$R := \{\frac{p}{q} \mid p, q \in \mathbb{Q}[y_1, y_2],\ q(0,0) \neq 0\}$
$A = R[D_1, D_2]$, $<$ such that $(1,0) > (0,1)$,
$f_1 := y_2 D_1 + 1, f_2 := y_1 D_2$,
$g := (y_1 + y_2) D_1 D_2 + y_1 y_2 D_2$,

Division of g by $\{f_1, f_2\}$ yields:
$r := g - (D_2 f_1 + D_1 f_2) = -D_1 + (y_1 y_2 - 2) D_2$
and $h_1 := D_2, \quad h_2 := D_1$,
$lc(r) = -1 \notin_R < lc(f_1) > = < y_2 >$

Ideal-membership in A:
G Gröbner basis of I, $f \in A$.
$f \in I$ iff a remainder of f after division by g is zero.

Buchberger algorithm in A:

G ... finite subset of $A \setminus \{0\}$
I ... left-ideal generated by G
For any non-empty subset $E \subseteq G$ let S_E be a finite set of generators of the R-module

$$\{(c_e)_{e\in E} | \sum_{e\in E} c_e \cdot lc(e) = 0\} \leq {}_R(R^E)$$

of syzygies of the family $(lc(e))_{e\in E}$. Then

- G Gröbner basis of I iff for all $E \subseteq G$ and for all $(c_e)_{e\in E} \in S_E$ a remainder of

  $$\sum_{e\in E} c_e x^{m(E)-deg(e)} e$$

  after division by G is zero.
  ($m(E) \in \mathbb{N}^n$ is the componentwise maximum of $(deg(e))_{e\in E}$).

- We can compute in finitely many steps a Gröbner basis of I as follows: While there are a subset $E \subseteq G$ and a family

$(c_e)_{e\in E} \in S_E$ such that the remainder r of

$$\sum_{e\in E} c_g x^{m(E)-deg(e)} e$$

after division by G is not zero, replace G by $G \cup \{r\}$.

Examples

1. $\{\bar{2}, \bar{3}x + \bar{1}\}$ and $\{\bar{2}, x + \bar{1}\}$ are Gröbner bases of the ideal generated by $\bar{3}x + \bar{1}$ in $\mathbb{Z}_6[x]$.

2. $\{D_1, D_2\}$ is a Gröbner basis of $< y_1 D_2, y_2 D_1 >$ in $\mathbb{Q}[y_1, y_2][D_1, D_2]$.

Reduced Gröbner bases

Additional data for the coefficient ring R:

- for any ideal Q in R select a finite system of generators $Gen(Q)$ of Q and

- for any ideal Q of R and any coset $z+Q \subseteq R$ select $r(z,Q) \in z+Q$ such that $r(0,Q) = 0 \in 0+Q$.

I ... left-ideal in A
$\alpha \in \mathbb{N}^n$

$lc(\alpha - \mathbb{N}^n, I) :=_R < lc(f); f \in I,$
$\deg(f) \in \alpha - \mathbb{N}^n, deg(f) \neq \alpha >$
(left-ideal in R, subset of $lc(\alpha, I)$)

$$Gen(\alpha, I) :=$$

$$= \{r(h, lc(\alpha - \mathbb{N}^n, I)) \,|\, h \in Gen(lc(\alpha, I))\} \setminus \{0\}\,.$$

A Gröbner basis G of I is a *reduced Gröbner basis* (with respect to $<$) iff

- for all $\alpha \in deg(I)$ the map
  $\{g \in G \,|\, deg(g) = \alpha\} \to Gen(\alpha, I)$,
  $g \mapsto lc(g)$,
  is bijective and

- for all $g := \sum_{\beta \in \mathbb{N}^n} c_{\beta,g} x^\beta \in G$ and all $\alpha \in \mathbb{N}^n$ with $\alpha \neq deg(g)$ and $c_{\alpha,g} \neq 0$ we have $c_{\alpha,g} = r(c_{\alpha,g}, lc(\alpha, I))$.

Every left-ideal in A has a unique reduced Gröbner basis.

References

Adams, W., Loustaunau, P., *An Introduction to Gröbner Bases*, American Mathematical Society, Providence, 1994

Buchberger, B., *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math. 4 (1970), 374-383

Buchberger, B., *A critical pair / completion algorithm for finitely generated ideals in rings*, In: Börger, E. et al.(eds.), *Logic and Machines: Decision Problems and Complexity*, Springer Lecture Notes in Computer Science 171 (1984), 137-155

Castro, F., *Calculs effectifs pour les ideaux d'opérateurs differentiels*, In: Aroca, J. et. al (eds.), Géométrie algébrique et applications. Vol. III, 1-20, Hermann, Paris 1987

Galligo, A., *Some algorithmic questions on ideals of differential operators*, Springer Lecture Notes in Computer Science 204 (1985), 413-421

Insa, M., Pauer, F., *Gröbner Bases in Rings of Differential Operators*, in: B. Buchberger, F. Winkler (eds.): Gröbner Bases and Applications. Cambridge University Press, Cambridge, 1998, 367 - 380

Kandri-Rody, A., Kapur, D., *Computing a Gröbner Basis of a Polynomial Ideal over a Euclidean Domain*, J. Symbolic Computation 6 (1988), 37-58

Levandowskyy, V., *Non-commutative Computer Algebra for polynomial algebras: Gröbner bases, applications and implementation*, Dissertation, Universität Kaiserslautern, 2005

Möller, H., *On the construction of Gröbner bases using syzygies*, J. Symbolic Computation 6 (1988), 345-359

Pauer, F., Pfeifhofer, M., *The Theory of Gröbner Bases*, L'Enseignement Mathématique 34 (1988), 215-232

Pauer, F., *Gröbner bases with coefficients in rings*, J. Symbolic Computation 42 (2007), 1003-1011

Trinks, W.,*Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen*, J. Number Theory 10 (1978), 475-488

Winkler, F., Zhou, M., *On computing Gröbner bases in rings of differential operators with coefficients in a ring*, Technical report no. 05-04 in RISC Report Series, University of Linz, 2005