On computing Gröbner bases in rings of differential operators with coefficients in a ring

September 14, 2005

Meng Zhou[a], **Franz Winkler**[b,1]
[a]Department of Applied Mathmatics, Beihang University, Beijing(100083), China.
(E-mail: Zhoumeng1613@hotmail.com)
[b]RISC-Linz, J. Kepler University Linz, A-4040 Linz, Austria.
(E-mail: Franz.Winkler@risc.uni-linz.ac.at)

abstract. Following the definition of Gröbner bases in rings of differential operators given by Insa and Pauer(1998), we discuss some computational properties of Gröbner bases arising when the coefficient set is a ring. First we give examples to show that the generalization of S-polynomials is necessary for computation of Gröbner bases. Then we prove that under certain conditions the G-S-polynomials can be reduced to be simpler than the original one. Especially for some simple case it is enough to consider S-polynomials in the computation of Gröbner bases. The algorithm for computation of Gröbner bases can thus be simplified. Last we discuss the elimination property of Gröbner bases in rings of differential operators and give some examples of solving PDE by elimination using Gröbner bases.

Keywords: Gröbner basis, rings of differential operators, generalized S-polynomials, elimination property.

1 Introduction

Let K be a field of characteristic zero, n a positive integer, $K(x_1, \cdots, x_n)$ the field of rational functions in n variables over K. Let $\frac{\partial}{\partial x_i} : K(x_1, \cdots, x_n) \longrightarrow K(x_1, \cdots, x_n)$ be the partial derivative by $x_i, 1 \leq i \leq n$.

Let R be a noetherian K-subalgebra of $K(x_1, \cdots, x_n)$ which is stable under $\frac{\partial}{\partial x_i}, 1 \leq i \leq n$. We denote by D_i the restriction of $\frac{\partial}{\partial x_i}$ to $R, 1 \leq i \leq n$. Let $A = R[D] = R[D_1, \cdots, D_n]$ be the R-subalgebra of $End_K(R)$ generated by $id_R = 1$ and $D_1, \cdots, D_n$. $R[D]$ is called "a ring of differential operators with coefficients in R"(Insa and Pauer(1998)). $R[D]$ are non-commutative K-algebras with fundamental relations

$$x_i x_j = x_j x_i, \quad D_i D_j = D_j D_i, \quad x_i D_j - D_j x_i = -\delta_{ij} \quad for \quad 1 \leq i, j \leq n,$$

[1]This work has been supported by the FWF project P16357-N04.

and $\quad rD_i - D_i r = -D_i(r) \qquad r \in R \qquad (1)$
where δ_{ij} is the Kronecker delta.

Then, the elements of $R[D]$ can be written uniquely as finite sums

$$\sum_{(i_1,\cdots,i_n)\in\mathbb{N}^n} r_{i_1,\cdots,i_n} D_1^{i_1}\cdots D_n^{i_n} \quad where \quad r_{i_1,\cdots,i_n}\in R$$

or shortly as $\quad \sum_{i\in\mathbb{N}^n} r_i D^i, \quad i=(i_1,\cdots,i_n), \quad r_i \in R. \qquad (2)$

By a ring of (linear partial) differential operators, one usually means one of the following three rings(cf. Björk (1979)):

(i) The Weyl algebra, or the ring of differential operators with polynomial coefficients

$$A_n = K[x_1,\cdots,x_n][D_1,\cdots,D_n], \tag{3}$$

where K is a field of characteristic 0;

(ii) The ring of differential operators with rational function coefficients

$$R_n = K(x_1,\cdots,x_n)[D_1,\cdots,D_n], \tag{4}$$

(iii) The ring of differential operators with convergent power series coefficients

$$D_0 = K\{x_1,\cdots,x_n\}[D_1,\cdots,D_n]. \tag{5}$$

We see that (3) and (4) are special examples of $R[D]$. And there are some other important examples for $R[D]$. For instance, the ring of differential operators with coefficients in a local ring R, $A = R[D_1,\cdots,D_n]$, where

$$R = K[x_1,\cdots,x_n]_M = \{\frac{f}{g}\in K(x_1,\cdots,x_n) \ \mid \ f\in K[x_1,\cdots,x_n], g\in M\}$$

and M is a subset of $K[x_1,\cdots,x_n]\backslash\{0\}$ closed under multiplication.

In rings of differential operators $R[D]$, the set of "terms" is $\{D^\alpha, \alpha\in\mathbb{N}^n\}$. Note that in this case the terms do not commute with the coefficients $r_i \in R$.

Let $\prec$ be a term order on $\mathbb{N}^n$, i.e. $0=(0,\cdots,0)\prec s$ for all $s\in\mathbb{N}^n\backslash\{0\}$ and $s+u\prec t+u$ if $s\prec t$. For a differential operator $0\neq f=\sum_{i\in\mathbb{N}^n} r_i D^i$ define degree, leading coefficient and initial term as follows:

$deg(f) = max_\prec\{i \mid r_i \neq 0\}\in\mathbb{N}^n$

$lc(f) = r_{deg(f)}$

$in(f) = lc(f)D^{deg(f)}$

For a subset F of $R[D]$ define

$deg(F) = \{deg(f) \mid f\in F, f\neq 0\}$

$in(F) = \{in(f) \mid f\in F, f\neq 0\}$

Insa and Pauer(1998) proved the following result about division in $R[D]$.

Theorem 1 Let F be a finite subset of $R[D]\backslash\{0\}$ and let $g\in R[D]$. Then there is a $r\in R[D]$ and there is a family $(h_f)_{f\in F}$ in $R[D]$ such that

(i) $\quad g=\sum_{f\in F} h_f f + r,$

(ii) $\quad$ for all $f\in F, h_f = 0 \quad$ or $\quad deg(h_f f)\preceq deg(g),$

(iii) $\quad r=0 \ \ or \ \ lc(r)\notin {}_R\langle lc(f);\ deg(r)\in deg(f)+\mathbb{N}^n\rangle.$

An r satisfying the conditions in Theorem 1 is called a remainder of f after division by F.

An ideal in $R[D]$ always means a left-ideal of $R[D]$. For an ideal J in $R[D]$ a Gröbner basis of J is defined as follows.

Definition 1 Let J be an ideal in $R[D]$ and let G be a finite subset of $J\backslash\{0\}$, then G is called a Gröbner basis (or shortly GB) of J with respect to the term order "$\prec$" iff for all $f \in J$,

$$lc(f) \in \ _R\langle lc(g);\ g \in G,\ deg(f) \in deg(g) + \mathbb{N}^n \rangle.$$

Proposition 1 Let J be an ideal in $R[D]$, G be a Gröbner basis of J.

(i) If $f \in J$, then every remainder of f after division by G is 0.

(ii) $f \in J$ iff a remainder of f after division by G is 0.

Proof: (i) Let r be a remainder of f after division by G. Then by Theorem 1, $f = \sum_{g \in G} h_g g + r$ and

$$r = 0 \ \ or \ \ lc(r) \notin \ _R\langle lc(g);\ deg(r) \in deg(g) + \mathbb{N}^n \rangle.$$

Because $r \in J$ and G is a Gröbner basis of J, r must be 0 by Definition 1.

(ii) Let $f \in J$, r be a remainder of f after division by G. Then by (i) we see $r = 0$.

If a remainder r of f after division by G is 0, then

$$f = \sum_{g \in G} h_g g + r = \sum_{g \in G} h_g g,$$

therefore $f \in J$. $\square$

Corollary Let J be an ideal in $R[D]$ and let G be a finite subset of $J\backslash\{0\}$, then G is a Gröbner basis of J (with respect to the term order "$\prec$") iff for all $f \in J$, a remainder of f after division by G is 0.

Proof. If G is a Gröbner basis of J, then by Proposition 1 for all $f \in J$ a remainder of f after division by G is 0.

If there is a remainder of f after division by G is 0, then

$$f = \sum_{g \in G} h_g g + r = \sum_{g \in G} h_g g,$$

therefore $lc(f) = \sum c_i lc(g_i)$. This means

$$lc(f) \in \ _R\langle lc(g);\ g \in G,\ deg(f) \in deg(g) + \mathbb{N}^n \rangle.$$

So, by Definition 1, G is a Gröbner basis of J. $\square$

Insa and Pauer also describe Buchberger's algorithm for computing Gröbner bases in $R[D]$. Of course it is more complex than in A_n or R_n.

2 Computation of Gröbner bases in $R[D]$ and generalization of S-polynomials

We assume that we can solve linear equations over R, i.e. for all $r \in R$ and all finite subsets $S \subseteq R$, we can decide if r is an element of $_R\langle S \rangle$, and if yes we can compute a family $(d_s)_{s\in S}$ in R such that $r = \sum_{s\in S} d_s s$; for all finite subsets $S \subseteq R$ a finite system of generators of the R-module

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

can be computed.

Let J be the left ideal in $R[D]$ generated by a finite set of differential operators G, for $E \subseteq G$ let S_E be a finite set of generators of the R-module

$$\{(c_e)_{e\in E} \mid \sum_{e\in E} c_e lc(e) = 0\} \leq \ _R(R^E) \qquad (6)$$

Then for $s = (c_e)_{e\in E} \in S_E$,

$$f_s = \sum_{e\in E} c_e D^{m(E)-deg(e)} e \qquad (7)$$

is called the generalized S-polynomial(G-S-polynomial) with respect to s, where

$$m(E) = (max_{e\in E} deg(e)_1, \cdots, max_{e\in E} deg(e)_n) \in \mathbb{N}^n.$$

If $E = \{g, h\} \subseteq G$ includes only two elements, choose $c, d \in R$ such that

$$c \cdot lc(g) = d \cdot lc(h) = lcm(lc(g), lc(h)) \in R.$$

Then $S_E = \{(c, d)\}$ will be a set of generators of the R-module (6) and the G-S-polynomial with respect to (c, d) will be

$$f_{(c,d)} = cD^{m(\{g,h\})-deg(g)} g - dD^{m(\{g,h\})-deg(h)} h$$

It is called S-polynomial and denoted by $S(g, h)$.

The following proposition generalizes Buchberger's Theory to $R[D]$ with coefficients in a commutative noetherian ring R.

Proposition 2 (Insa and Pauer (1998)). Let J be an ideal in $R[D]$. Then G is a Gröbner basis of $J \iff$ for all $E \subseteq G$ and for all $s = (c_e)_{e\in E} \in S_E$ a remainder of f_s after division by G is zero.

If R is a PID, then G is a Gröbner basis of $J \iff$ for all $\{g, h\} \in G$ a remainder of $S(g, h)$ after division by G is zero.

Therefore, the Buchberger's algorithm is: if there is a remainder r of f_s after division by G is not zero, replace G by $G \bigcup \{r\}$.

But in the paper of Insa and Pauer, all examples for GB computation involve S-polynomials only, even when R is not a PID. There is no example to show that G-S-polynomials are necessary for GB computation. The next example shows, even if R is a commutative domain, when G includes at least three elements G-S-polynomials will be necessary for GB computation.

Example 1 Let $R = \mathbb{Q}[x_1, \cdots x_6]$ and $A = R[D_1, \cdots D_6]$, J be the left ideal of A generated by $G = \{f_1, f_2, f_3\}$, where $f_1 = x_1D_4 + 1$, $f_2 = x_2D_5$, $f_3 = (x_1 + x_2)D_6$. Let $\prec$ be the graded lexicographic order with $(1, 0, \cdots, 0) \prec (0, 1, \cdots, 0) \prec (0, \cdots, 0, 1)$.

Now all S-polynomials $S(g,h)$ in G reduce to 0 by G:

$$S(f_1,f_2) = x_2D_5f_1 - x_1D_4f_2 = x_2D_5(x_1D_4+1) - x_1D_4x_2D_5 = x_2D_5 = 0(modG)$$

$$S(f_1,f_3) = (x_1+x_2)D_6f_1 - x_1D_4f_3 = (x_1+x_2)D_6(x_1D_4+1) - x_1D_4(x_1+x_2)D_6$$
$$= (x_1+x_2)D_6 = 0(modG)$$

$$S(f_2,f_3) = (x_1+x_2)D_6f_2 - x_2D_5f_3 = (x_1+x_2)D_6x_2D_5 - x_2D_5(x_1+x_2)D_6 = 0$$

But consider $E = G \subseteq G$,

$$\{(c_e)_{e\in E} \mid \sum_{e\in E} c_e lc(e) = 0\} = \{(c_1,c_2,c_3) \mid c_1x_1 + c_2x_2 + c_3(x_1+x_2) = 0\}$$

and $s = (1,1,-1) \in S_E$. Then there is a G-S-polynomial
$f_s = c_1D_5D_6f_1 + c_2D_4D_6f_2 + c_3D_4D_5f_3$
$= D_5D_6(x_1D_4+1) + D_4D_6(x_2D_5) - D_4D_5[(x_1+x_2)D_6] = D_5D_6$

Because the remainder of f_s after division by G is not zero, G is not a GB of J. In order to get a GB of J, denote f_s by f_4, we must replace G by $G_1 = \{f_1,f_2,f_3,f_4\}$ and then compute G-S-polynomials for all $E \subseteq G_1$ and for all $s = (c_e)_{e\in E} \in S_E$.

But as we will demonstrate afterwards, we can conclude that G_1 is a GB of J by the fact that $S(f_i,f_4)$ $(i = 1,2,3)$ are zero after division by G_1. $\square$

If $G = \{g,h\}$ include only two elements and R is a commutative domain then most examples of computing GB in $R[D]$ show that we can get a GB by computing S-polynomials only. But we find an example in which that is not the case.

Example 2 Let $R = \mathbb{Q}[x_1,x_2,x_3]$ and $A = R[D_1,D_2,D_3]$, J be the left ideal of A generated by $G = \{f_1,f_2\}$, where $f_1 = x_1D_3^2 + x_2D_3 + x_2$, $f_2 = x_2D_3^2 + x_1D_3 + x_1$. Let $\prec$ be the graded lexicographic order with $(1,0,0) \prec (0,1,0) \prec (0,0,1)$. Compute S-polynomials:

$$f_3 = S(f_1,f_2) = (x_2^2 - x_1^2)D_3 + (x_2^2 - x_1^2)$$

$$f_4 = S(f_1,f_3) = (x_2^2 - x_1^2)(x_2 - x_1)D_3 + (x_2^2 - x_1^2)x_2$$

$$f_5 = S(f_2,f_3) = (x_2^2 - x_1^2)(x_1 - x_2)D_3 + (x_2^2 - x_1^2)x_1$$

$$f_6 = S(f_4,f_5) = (x_2^2 - x_1^2)(x_1 + x_2)$$

$$f_7 = S(f_3,f_4) = (x_2^2 - x_1^2)x_1$$

$$f_8 = S(f_3,f_5) = (x_2^2 - x_1^2)x_2$$

Let $G_1 = \{f_1,f_2,f_3,f_7,f_8\}$, then all $S(f_i,f_j)$ in G_1 is zero after division by G_1:

$$S(f_1,f_2) = f_3 = 0(modG_1)$$

$$S(f_1,f_3) = f_4 = (f_8 - f_7)D_3 + f_8 = 0(modG_1)$$

$$S(f_1,f_7) = (x_2^2 - x_1^2)x_2D_3 + (x_2^2 - x_1^2)x_2 = f_8(D_3+1) = 0(modG_1)$$

$$S(f_1,f_8) = (x_2^2 - x_1^2)x_2^2D_3 + (x_2^2 - x_1^2)x_2^2 = f_8x_2(D_3+1) = 0(modG_1)$$

$$S(f_2,f_3) = f_5 = (f_7 - f_8)D_3 + f_7 = 0(modG_1)$$

$$S(f_2,f_7)=(x_2^2-x_1^2)x_1^2D_3+(x_2^2-x_1^2)x_1^2=f_7x_1(D_3+1)=0(modG_1)$$
$$S(f_2,f_8)=(x_2^2-x_1^2)x_1D_3+(x_2^2-x_1^2)x_1=f_7(D_3+1)=0(modG_1)$$
$$S(f_3,f_7)=f_7=0(modG_1)$$
$$S(f_3,f_8)=f_8=0(modG_1)$$
$$S(f_7,f_8)=0$$

But G_1 is not a GB of J because there is a G-S-polynomial f_s that is not reduced to zero by G_1. Choose $E=\{f_1,f_2,f_3\}\subseteq G_1$, then

$$\{(c_e)_{e\in E}\mid\sum_{e\in E}c_elc(e)=0\}=\{(c_1,c_2,c_3)\mid c_1lc(f_1)+c_2lc(f_2)+c_3lc(f_3)=0\}$$
$$=\{(c_1,c_2,c_3)\mid c_1x_1+c_2x_2+c_3(x_2^2-x_1^2)=0\}$$

and $s=(c_1,c_2,c_3)=(x_1,-x_2,1)\in S_E$.

Then

$f_s=x_1f_1-x_2f_2+D_3f_3$

$=x_1(x_1D_3^2+x_2D_3+x_2)-x_2(x_2D_3^2+x_1D_3+x_1)+D_3[((x_2^2-x_1^2)D_3+(x_2^2-x_1^2)]$

$=(x_2^2-x_1^2)D_3$

f_s may be reduced to $g=(x_2^2-x_1^2)$ by G_1 because that $f_s=f_3-(x_2^2-x_1^2)$. Now g can't be reduced to zero by G_1.

Let $G_2=\{f_1,f_2,g\}$. For $E=G_2$, the set S_E of generators of the R-module $\{(c_1,c_2,c_3)\mid c_1x_1+c_2x_2+c_3(x_2^2-x_1^2)=0\}$ is (cf. F. Winkler(1996))

$$S_E=\{(x_1,-x_2,1),(0,x_2^2-x_1^2,-x_2),(x_2^2-x_1^2,0,-x_1)\}$$

It is easy to check all G-S-polynomials f_s in G_2 are zero after divided by G_2. Therefore the GB of J is $G_2=\{f_1,f_2,g\}$ but it can't be computed with S-polynomials only. □

Generally we need to compute G-S-polynomials f_s for all $E\subseteq G$ and for all $s\in S_E$ in order to get a GB of J generated by G. And in the process if we replace G by $G_1=G\bigcup\{r\}$, we must repeat the procedure for G_1. If we can get the GB by computing S-polynomials only in some conditions then the procedure would be simplified. Now we consider in what conditions we can do so.

Let R be a commutative domain(not necessarily a PID), $A=R[D_1,\cdots,D_n]$, J the ideal in A generated by G which is a finite subset of $J\backslash\{0\}$. For $E=\{f_1,\cdots,f_k\}\subseteq G$,

$$\{(c_e)_{e\in E}\mid\sum_{e\in E}c_elc(e)=0\}=\{(c_1,\cdots,c_k)\mid\sum_{j=1}^{k}c_jlc(f_j)=0\}$$

is the set of solutions of the equation

$$c_1lc(f_1)+\cdots+c_klc(f_k)=0.$$

Denote $s_j=lc(f_j)$, so the equation becomes

$$c_1s_1+\cdots+c_ks_k=0. \tag{8}$$

LetS_E be the finite set of generators of the solutions of (8).

Lemma 1 For $E = \{f_1, \cdots, f_k\} \subseteq G$, if some $s_j = lc(f_j)$ is invertible in R, then all G-S-polynomials corresponding to S_E can be simplified to S-polynomials.

Proof: If some s_j is invertible in R, say s_k is invertible, then the equation (8) will be

$$c_k = -\sum_{i=1}^{k-1} c_i \cdot (\frac{s_i}{s_k})$$

Then $\xi_i = (\underbrace{0, \cdots, 1}_{i}, 0, \cdots, -\frac{s_i}{s_k}), \quad i = 1, \cdots, k-1$, will be generators of the solutions. The corresponding G-S-polynomials are:

$$f_{\xi_i} = \sum_{e \in E} c_e D^{m(E)-deg(e)} e = D^{m(E)-deg(f_i)} f_i + (-s_i) D^{m(E)-deg(f_k)} f_k$$

Note that for S-polynomials

$$S(f_i, f_k) = D^{m(\{f_i,f_k\})-deg(f_i)} f_i + (-s_i) D^{m((\{f_i,f_k\})-deg(f_k)} f_k$$

we have

$$f_{\xi_i} = D^{\alpha} S(f_i, f_k) + h_i f_k$$

for some $\alpha \in \mathbb{N}^n$, $h_i \in R[D]$. If $S(f_i, f_k)$ is zero after divided by G, then f_{ξ_i} is zero after divided by G. $\square$

Definition 2 Let $E_1 = \{f_1, \cdots, f_s\} \subseteq G$, $E_2 = \{g_1, \cdots, g_t\} \subseteq G$. Then G-S-polynomials corresponding to S_{E_1} (or S_{E_2}) are said to be of grade s (or t). If $s < t$, then G-S-polynomials corresponding to S_{E_1} are said to be of lower grade than G-S-polynomials corresponding to S_{E_2}.

Lemma 2 For $E = \{f_1, \cdots, f_k\} \subseteq G$, if some s_i can be divided exactly by s_j $(j \neq i)$ in R, then all G-S-polynomials corresponding to S_E can be simplified to G-S-polynomials of lower grade.

Proof: If some s_i can be divided exactly by s_j $(j \neq i)$ in R, say $s_k = h_k s_{k-1}$, then the equation (8) will be

$$c_1 s_1 + \cdots + (c_{k-1} + c_k h_k) s_{k-1} = 0 \tag{9}$$

Denote $c'_{k-1} = c_{k-1} + c_k h_k$, the equation (9) will be

$$c_1 s_1 + \cdots + c'_{k-1} s_{k-1} = 0 \tag{10}$$

If $\beta_i = (c_1^{(i)}, \cdots, c_{k-1}^{(i)})$ are the generators of solutions of (10), then
$\xi_i = (c_1^{(i)}, \cdots, c_{k-1}^{(i)}, 0)$ and $\alpha = (0, \cdots, 0, -h_k, 1)$
will be the generators of solutions of (9).

In fact, if $c = (c_1, \cdots, c_k)$ is a solution of (9), put $c'_{k-1} = c_{k-1} + c_k h_k$, then $(c_1, \cdots, c_{k-2}, c'_{k-1})$ is a solution of (10). So $(c_1, \cdots, c_{k-2}, c'_{k-1}) = \sum k_i \beta_i$ and $(c_1, \cdots, c_{k-2}, c'_{k-1}, 0) = \sum k_i \xi_i$. Because
$(c_1, \cdots, c_{k-2}, c'_{k-1}, 0) + c_k \alpha = (c_1, \cdots, c_{k-2}, c_{k-1} + c_k h_k, 0) + (0, \cdots, 0, -c_k h_k, c_k)$ $= c$, we get that $c = \sum k_i \xi_i - c_k \alpha$. This means $\{\xi_i, \alpha\}$ are the generators of solutions of (9).

The G-S-polynomials corresponding to α can be simplified to S-polynomials $S(f_{k-1}, f_k)$, and the G-S-polynomials corresponding to ξ_i can be simplified to G-S-polynomials of lower grade. $\square$

With Lemma 1 and Lemma 2 we get the following proposition.

Proposition 3 Let $G = \{f_1, \cdots, f_m\}$ and J be the left ideal of $R[D]$ generated by G.

(a) If all S-polynomials $S(f_i, f_j)$ are reduced to zero by G, then for $E = \{g_1, \cdots, g_k\} \subseteq G$ with some $lc(g_j)$ invertible, all of G-S-polynomials corresponding to E will be reduced to zero by G.

(b) If all G-S-polynomials with grade k are reduced to zero by G, then for $E = \{g_1, \cdots, g_k, g_{k+1}\} \subseteq G$ with some $lc(g_j)$ divided exactly by another $lc(g_i)$, all of G-S-polynomials corresponding to E will be reduced to zero by G. $\square$

The following corollary improves the result of Insa and Pauer (see Proposition 1).

Corollary Let $G = \{f_1, \cdots, f_m\} \subseteq R[D]$ and J be the left ideal of $R[D]$ generated by G. Then G is a Gröbner basis of $J \Longleftrightarrow$ any G-S-polynomials with lower grade than k ($k \leq m$) are reduced to zero by G and in any k elements of G there is an $lc(f)$ divided exactly by another $lc(f)$. $\square$

Especially, if in $G = \{f_1, \cdots, f_m\}$ all $S(f_i, f_j)$ are reduced to zero by G, and for any three elements $\{f_i, f_j, f_k\} \subseteq G$ there is an $lc(f)$ divided exactly by another $lc(f)$, then G is a Gröbner basis of J.

The algorithm to compute GB of J in $R[D]$ will be simplified. The following proposition improves the result of Insa and Pauer (Prop. 4 of [5]).

Proposition 4 Let J be an ideal in $R[D]$ given by a finite set G of generators. In the following way we compute in finitely many steps a Gröbner basis of J: While there are a subset $E \subseteq G$ and a family $s = (c_e)_{e \in E} \in S_E$ such that the remainder r of G-S-polynomials f_s after divided by G is zero, replace G by $G \bigcup \{r\}$. And in the procedure we ignore those subsets E in which there is an $lc(f)$ divided exactly by another $lc(f)$. $\square$

Example 3 Let $R = \{\frac{f}{g} \in K(x_1, x_2) \mid f, g \in K[x_1, x_2], g(0,0) \neq 0\}$ and $A = R[D_1, D_2]$, J be the left ideal of A generated by $G = \{x_1 D_2, x_2 D_1\}$. Let $\prec$ be the graded lexicographic order with $(1,0) \prec (0,1)$. Example 5 in Insa and Pauer(1998) compute the GB of J with S-polynomials only and get

$$G' = \{x_1 D_2, x_2 D_1, x_2 D_2 - x_1 D_1, x_1^2 D_1, x_1 D_1^2 + 2D_1\}$$

in which all S-polynomials $S(f_i, f_j)$ are reduced to zero by G'.
Now for any three elements $\{f_i, f_j, f_k\}$ in G', there is an $lc(f)$ divided exactly by another $lc(f)$. So by the Corollary of Proposition 3 or Proposition 4, we ignore all G-S-polynomials with higher grade than 2 and then G' is a Gröbner basis of J. $\square$

Example 4 In Example 1 we get

$$G_1 = \{f_1, f_2, f_3, f_4\} = \{x_1 D_4 + 1, x_2 D_5, (x_1 + x_2) D_6, D_5 D_6\}$$

with all $S(f_i, f_j)$ are zero after divided by G_1. Because $lc(f_4) = 1$ is invertible we ignore any $E \subseteq G_1$ which include f_4 when we compute G-S-polynomials. So the only G-S-polynomial f_s we need to consider is that corresponding to $E = \{f_1, f_2, f_3\}$. But we already compute $f_s = f_4$ in Example 1. This means f_s is reduced to zero by G_1. By Proposition 2 G_1 is a Gröbner basis of J. $\square$

Note that in Example 2, we get

$$G_1 = \{f_1, f_2, f_3, f_7, f_8\} = \{x_1 D_3^2 + x_2 D_3 + x_2,\ x_2 D_3^2 + x_1 D_3 + x_1,$$

$$(x_2^2 - x_1^2)D_3 + (x_2^2 - x_1^2),\ (x_2^2 - x_1^2)x_1,\ (x_2^2 - x_1^2)x_2\}$$

with all $S(f_i, f_j)$ are zero after divided by G_1. But G_1 is not a Gröbner basis of J.

This is because, if we choose 3 elements $\{f_1, f_2, f_3\} \subseteq G_1$, then

$$\{lc(f_1), lc(f_2), lc(f_3)\} = \{x_1, x_2, (x_2^2 - x_1^2)\}.$$

None of the three is divided exactly by another and we need to compute the corresponding G-S-polynomials.

3 Elimination properties of Gröbner bases in rings of differential operators $R[D]$

Let $R[Y]$ be a ring of differential operators, $Y = \{y_1, \cdots, y_m\}$ and $\{y_1, \cdots, y_m\}$ denotes $\{x_1, \cdots, x_n, D_1, \cdots, D_n\}$ or $\{D_1, \cdots, D_n\}$. Denote by Y_k the first k elements of Y. If I is an ideal in $R[Y]$, then it is known that $I_k = I \bigcap R[Y_k]$ is an ideal of $R[Y_k]$, which is called the k-th elimination ideal of I.

In commutative polynomial algebras, the elimination ideal I_k of I can be easily obtained if one has a Gröbner basis of I with respect to a term ordering having the "elimination" property.

Definition 3 Let $R[Y]$ be a ring of differential operators and "$\prec$" be a term order on $\langle Y \rangle = \{Y^\alpha \mid \alpha \in \mathbb{N}^m\}$ (this is equivalent to a term order on $\mathbb{N}^m$). If for every $s, t \in \langle Y \rangle$, $s < t$ and $t \in \langle Y_k \rangle$ implies $s \in \langle Y_k \rangle$, then the term order is called an elimination term order at the position k. (This is equivalent to: If for every $\alpha = (\alpha_1, \cdots, \alpha_m), \beta = (\beta_1, \cdots, \beta_m) \in \mathbb{N}^m$, $\alpha < \beta$ and $\beta_i = 0$ for all $i > k$ implies $\alpha_i = 0$ for all $i > k$, then the term order is called an elimination term order at the position k.)

It is well known (cf.[1]), a term order is an elimination term order on $\langle Y \rangle$ at the position k iff for all $s \in \langle Y_k \rangle$, $s < y_j$ when $j > k$.

In commutative polynomial algebras, lexicographic order is an elimination order, but degree-lexicographic order is not an elimination order. It is easy to see this is also true for rings of differential operators.

Definition 4 Let G be a Gröbner basis of an ideal I in $R[Y]$. If for each $g_i \in G$,

$$lc(g_i) \notin \ _R\langle lc(g_j) \mid g_j \in G, j \neq i, deg(g_i) \in deg(g_j) + \mathbb{N}^m \rangle,$$

then G is called a reduced Gröbner basis of I.

The following proposition discribes the elimination property of Gröbner bases in $R[Y]$.

Proposition 5 Let I be an ideal in a ring of differential operators $R[Y]$, G be a Gröbner basis of I with respect to an elimination term order "$\prec$" at the position k. Then the following holds:

(i) For each $f \in R[Y_k]$ and $g \in R[Y]$, if

$$deg(f) \in deg(g) + \mathbb{N}^m,$$

then $g \in R[Y_k]$.

(ii) $G_k = G \bigcap R[Y_k]$ is a Gröbner basis of $I_k = I \bigcap R[Y_k]$ with respect to the restriction of "$\prec$" onto $\langle Y_k \rangle$.

(iii) If G is reduced, then G_k is reduced.

Proof: (i) Since $deg(f) \in deg(g) + \mathbb{N}^m$, we have that the leading term if g is in $\langle Y_k \rangle$. But $\prec$ is an elimination ordering, so $g \in R[Y_k]$.

(ii) Let $f \in I_k = I \bigcap R[Y_k]$. Then $f \in I$ and since G is a Gröbner basis for I there exist $g_1, \cdots, g_s \in G$ such that

$$lc(f) \in \ _R\langle lc(g_j) \mid 1 \leq j \leq s \rangle$$

and $\qquad deg(f) \in deg(g_j) + \mathbb{N}^m, \quad 1 \leq j \leq s.$

By (i) this means that $g_j \in R[Y_k]$ for all $1 \leq j \leq s$, so

$$lc(f) \in \ _R\langle lc(g) \mid g \in G_k, deg(f) \in deg(g) + \mathbb{N}^m \rangle.$$

By Definition 1, $G_k = G \bigcap R[Y_k]$ is a Gröbner basis for I_k.

(iii) The conclusion is obvious. □

Note that the definition of Gröbner bases in $A = R[D_1, \cdots, D_n]$ is a generalization of the definition of Gröbner bases in the Weyl algebra

$$A_n = K[x_1, \cdots, x_n][D_1, \cdots, D_n]$$

and also of the definition of Gröbner bases in

$$R_n = K(x_1, \cdots, x_n)[D_1, \cdots, D_n].$$

Therefore, if Proposition 5 hold for $A = R[D_1, \cdots, D_n]$, then the elimination property holds in rings of differential operators A_n, R_n and $R[D]$, if we choose some elimination term order and get a Gröbner basis of an ideal I.

Now we give some simple examples for applying the elimination property of Gröbner bases to systems of linear differential equations.

Example 5 $\quad \begin{cases} 2xy'' = 0 \\ y''' + x^2 y' - xy = 0 \end{cases}$

This system of linear ordinary differential equations can be written as

$$\begin{cases} (2xD^2)y = 0 \\ (D^3 + x^2 D - x)y = 0 \end{cases}$$

where D is the differential operator $\frac{\partial}{\partial x}$. Put $f_1 = 2xD^2$, $f_2 = D^3 + x^2 D - x$, then $f_1, f_2 \in K[x][D]$, the Weyl algebra with one variable. Note that $K[x]$ is a PID, we compute a Gröbner basis of $I = \langle f_1, f_2 \rangle$ by S-polynomials with respect to lexicographic order:

$$S(f_1, f_2) = \frac{1}{2} D f_1 - x f_2 = D^2 - x^3 D + x^2 = f_3,$$

then $\qquad f_2 = (D - x^3) f_3 + (x^4 + 3)(x^2 D - x).$

So we can reduce f_2 to $\bar{f}_2 = (x^4 + 3)(x^2 D - x)$.

$$S(f_1, f_3) = \frac{1}{2} f_1 - x f_3 = x^4 D - x^3 = x^2 (x^2 D - x) = f_4.$$

Now $\bar{f}_2 = (x^4+3)(x^2D-x) = x^2f_4 + 3(x^2D-x)$, we can reduce $\bar{f}_2$ to $\bar{\bar{f}}_2 = x^2D-x$, then $f_3 = -x\bar{\bar{f}}_2 + D^2$, so we can reduce f_3 to $\bar{f}_3 = D^2$.

$$S(\bar{\bar{f}}_2, \bar{f}_3) = D\bar{\bar{f}}_2 - x^2\bar{f}_3 = x^2D^2 + 2xD - xD - 1 - x^2D^2 = xD - 1 = f_5.$$

Note that $f_4 = x^3f_5,\ \bar{\bar{f}}_2 = xf_5,\ f_1 = 2x\bar{f}_3$, and $S(\bar{f}_3, f_5) = 0$, we see that $\{D^2, xD-1\}$ is a Gröbner basis of $I = \langle f_1, f_2\rangle$. The system of linear differential equations can be reduced to:

$$\begin{cases} y'' = 0 \\ xy' - y = 0 \end{cases}$$

Then it is easy to see that $y = cx, \quad c \in \mathbb{C}$, is the general solution of the system. □

Möller and Mora(1986) have shown how to generalize the theory of Gröbner bases to commutative polynomial modules. In fact, this generalization also works in $R[Y]$ modules. Here we just show an example.

Example 6 $\begin{cases} xy_1'' + y_2'' = 0 \\ x^2y_1' + xy_2' = 0 \end{cases}$

where y_1 and y_2 are the two unknown functions in x.

Put $f_1 = (xD^2, D^2) = xD^2e_1 + D^2e_2, \quad f_2 = (x^2D, xD) = x^2De_1 + xDe_2$, where $D = \partial_x,\ f_1, f_2 \in [R[D]]^2$, the free $R[D]$-module with dimension 2 and $e_1 = (1,0), e_2 = (0,1)$ is the standard basis of the module. The order will be POT extension of lexicographic order:

$$(i, e_j) \prec (k, e_l) \Longleftrightarrow j \prec l \quad or \quad [j = l \quad and \quad i \prec k].$$

Then

$$S(f_1, f_2) = xf_1 - Df_2 = x(xD^2, D^2) - D(x^2D, xD) = (-2xD, -D) = f_3$$

$$S(f_1, f_3) = f_1 + \frac{1}{2}Df_3 = (xD^2, D^2) + \frac{1}{2}D(-2xD, -D) = (-D, \frac{1}{2}D^2) = f_4$$

$$S(f_2, f_3) = f_2 + \frac{1}{2}xf_3 = (x^2D, xD) + (-x^2D, -\frac{1}{2}xD) = (0, \frac{1}{2}xD) = f_5$$

Note that $f_3 = 2xf_4 - 2Df_5,\ f_2 = -x^2f_4 + (xD+1)f_5$. Now it is easy to verify that $\{f_1, f_4, f_5\}$ is a Gröbner basis of $N = \langle f_1, f_2\rangle$. The system can be reduced to:

$$\begin{cases} xy_1'' + y_2'' = 0 \\ 2y_1' - y_2'' = 0 \\ xy_2' = 0 \end{cases}$$

Then $y_1 = c_1, y_2 = c_2$ is the solution of the system. □

References

1. Borges, M. A., Borges, Mijail: Gröbner bases property on elimination ideal in the non-commutative case. In: B. Buchberger, F. Winkler(eds.): Gröbner bases and applications. Cambridge University Press 1998
2. Björk, J: Rings of differential operators. Amsterdam: North-Holland 1979
3. Buchberger, B.: Gröbner bases: An algorithmic method in polynomial ideal theory. In: N. K. Bose(ed.):Multidimensional systems theory. Dordrecht: Reidel Publishing Company 1985
4. Galligo, A.: Some algorithmic questions on ideals of differential operators. In: B. F. Caviness(ed.): Proc. EUROCAL'85, LNCS 204. Berlin: Springer 1985
5. Insa, M., Pauer, F.:(1998). Gröbner bases in rings of differential operators. In: B. Buchberger, F. Winkler(eds.): Gröbner bases and applications. Cambridge University Press 1998
6. Levin, A.: Reduced Gröbner bases, free difference-differential modules and difference-differential dimension polynomials. J.Symbolic Computation (30/4), 357-382 (2000)
7. Mora, F.: Gröbner bases for non-commutative polynomial rings. In: J. Calmet(ed.): Proc. AAECC-3, LNCS 229. Berlin: Springer 1986
8. Möller, H. M. and Mora, F.: New constructive methods in classical ideal thoery. J. of Algebra (100), 138-178 (1986)

9 Oaku, T., Shimoyama, T.: A Gröbner basis method for modules over rings of differential operators. J. Symbolic Computation (18/3), 223-248 (1994)

10 Winkler, F.: Polynomial algorithms in computer algebra, Wien New York: Springer-Verlag 1996