SCIENCE CHINA
Mathematics

• ARTICLES •

June 2011 Vol. 54 No. 6: 1077–1087
doi: 10.1007/s11425-011-4176-y

On computing Gröbner bases in rings of differential operators

MA XiaoDong, SUN Yao & WANG DingKang*

KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China*
Email: maxiaodong@amss.ac.cn, sunyao@amss.ac.cn, dwang@mmrc.iss.ac.cn

Received May 28, 2010; accepted September 17, 2010; published online February 21, 2011

Abstract Insa and Pauer presented a basic theory of Gröbner basis for differential operators with coefficients in a commutative ring in 1998, and a criterion was proposed to determine if a set of differential operators is a Gröbner basis. In this paper, we will give a new criterion such that Insa and Pauer's criterion could be concluded as a special case and one could compute the Gröbner basis more efficiently by this new criterion.

Keywords Gröbner basis, rings of differential operators

MSC(2000): 13B25, 13N10, 13P10

Citation: Ma X D, Sun Y, Wang D K. On computing Gröbner bases in rings of differential operators. Sci China Math, 2011, 54(6): 1077–1087, doi: 10.1007/s11425-011-4176-y

1 Introduction

Many investigations have been done on Gröbner basis in rings of differential operators [1,2,4,6,8], but the coefficients are in fields (of rational functions), rings of power series, or rings of polynomials over a field. For example, Mora gave an introduction to commutative and non-commutative Gröbner bases, which includes Gröbner bases for Wely algebra [7]. As in Insa and Pauer's paper [5], the rings of coefficients in this paper are general commutative rings, which is the main difference from other existing works.

In Insa and Pauer's paper, the results of Buchberger on Gröbner basis in polynomial rings have been extended to the theory of Gröbner basis for differential operators. A criterion was presented to determine if a set of differential operators is a Gröbner basis, and a basic method for computing the Gröbner basis was also proposed. Pauer generalized the theory to a class of rings which includes rings of differential operators with coefficients in Noetherian rings [9].

For computing the Gröbner basis of a set of differential operators, instead of computing the generators of the syzygy module generated by their initials, Insa and pauer's method needs to compute the generators of many syzygy modules generated by their leading coefficients. Thus, Insa and pauer's method leads to many unnecessary computations. In order to improve the efficiency, Zhou and Winkler proposed some techniques to reduce the computations on the syzygies [10].

In this paper, a new criterion is proposed for computing Gröbner basis in the ring of differential operators with coefficients in a general commutative ring.

The new criterion is based on the following simple fact: Let f, g be two differential operators, then

$$fg = gf + h,$$

*Corresponding author

where fg and gf have the same degree, but h has less degree than fg or gf. The above equation implies that even though the multiplication in the rings of differential operators is not commutative, the products fg and gf still have the same initial. According to this fact, it suffices to consider the generators of the syzygy module in a commutative ring which is deduced from the ring of differential operators. With these generators, a new criterion is proposed to determine if a set of differential operators is a Gröbner basis. This new result generalizes original Insa-Pauer Theorem such that their theorem can be concluded as a special case of the new theorem. Furthermore, the results of this paper can be extended naturally to the rings that preserve the same fact.

Then the proposed criterion also leads to an efficient method for computing Gröbner bases in the rings of differential operators. This new method computes fewer s-polynomials than those in Insa and Pauer's method as well as Zhou and Winkler's improved version. So it is not surprising that this new method will have better efficiency than others.

This paper is organized as follow. Section 2 includes some preliminaries of the Gröbner basis in the rings of differential operators. Insa-Pauer Theorem comes in Section 3. In Section 4, the new criterion is presented in detail. And some algorithmic problems are discussed in Section 5. Section 6 is the conclusion.

2 Gröbner basis in rings of differential operators

Let K be a field of characteristic zero, $\mathbb{N}$ the set of non-negative integers, $n \in \mathbb{N}$ a positive integer and $K[X] := K[x_1, \ldots, x_n]$ (resp. $K(X) := K(x_1, \ldots, x_n)$) the ring of polynomials (resp. the field of rational functions) in n variables over K. Let $\frac{\partial}{\partial x_i} : K(X) \longrightarrow K(X)$ be the partial derivative by x_i for $1 \leqslant i \leqslant n$.

Let $\mathcal{R}$ be a Noetherian K-subalgebra of $K(X)$ which is stable by $\frac{\partial}{\partial x_i}$ for $1 \leqslant i \leqslant n$, i.e. $\frac{\partial}{\partial x_i}(r) \in \mathcal{R}$ for all $r \in \mathcal{R}$. Important examples for $\mathcal{R}$ are $K[X]$, $K(X)$ and $K[X]_M := \{\frac{f}{g} \in K(X) \mid f \in K[X], g \in M\}$ where M is a subset of $K[X] \setminus \{0\}$ closed under multiplication.

Assume the linear equations over $\mathcal{R}$ can be solved, i.e.,

(1) for all $g \in \mathcal{R}$ and all finite subsets $F \subset \mathcal{R}$, it is possible to decide whether g is an element of ${}_{\mathcal{R}}\langle F \rangle$, and if yes, it is available to obtain a family $(d_f)_{f \in F}$ in $\mathcal{R}$ such that $g = \sum_{f \in F} d_f f$;

(2) for all finite subsets $F \subset \mathcal{R}$, a finite system of generators of the $\mathcal{R}$-module

$$\left\{ (s_f)_{f \in F} \,\middle|\, \sum_{f \in F} s_f f = 0, s_f \in \mathcal{R} \right\}$$

can be computed.

The partial differential operator D_i is defined as the restriction of $\frac{\partial}{\partial x_i}$ to $\mathcal{R}$ for $1 \leqslant i \leqslant n$. Let $\mathcal{A} := \mathcal{R}[D] = \mathcal{R}[D_1, \ldots, D_n]$ be the $\mathcal{R}$-subalgebra of $\mathrm{End}_k(\mathcal{R})$ generated by $\mathrm{id}_{\mathcal{R}} = 1$ and $D_1, \ldots, D_n$, where $\mathrm{End}_K(\mathcal{R})$ denotes the R-algebra of endomorphisms of the additive group of R which vanish at elements of K. Then the ring $\mathcal{A}$ is "a ring of differential operators with coefficients in $\mathcal{R}$", while the elements of $\mathcal{A}$ are called "differential operators with coefficients in $\mathcal{R}$" [5]. It is well known that $\mathcal{A}$ is a left-Noetherian associative $\mathcal{R}$-algebra, so the ideals in $\mathcal{A}$ always refer to the left-ideals of $\mathcal{A}$ in this paper.

$\mathcal{A}$ is a non-commutative K-algebra with fundamental relations:

$$x_i x_j = x_j x_i, \quad D_i D_j = D_j D_i \quad \text{for } 1 \leqslant i, j \leqslant n,$$

and

$$D_i r - r D_i = D_i(r), \quad r \in \mathcal{R}.$$

For a simple example, let $\mathcal{A} = (k[x_1, x_2])[D_1, D_2]$, then

$$x_1 x_2 = x_2 x_1, \quad D_1 D_2 = D_2 D_1 \quad \text{and} \quad D_1 x_1 x_2 - x_1 x_2 D_1 = D_1(x_1 x_2) = x_2.$$

And for any $f \in \mathcal{A}$, f can be written uniquely as a finite sum

$$f = \sum_{\alpha \in \mathbb{N}^n} r_\alpha D^\alpha, \quad \text{where } r_\alpha \in \mathcal{R}.$$

Let $\prec$ be an admissible order on $\mathbb{N}^n$, i.e. a total order on $\mathbb{N}^n$ such that $0 \in \mathbb{N}^n$ is the smallest element and $\alpha \prec \beta$ implies $\alpha+\gamma \prec \beta+\gamma$ for all $\alpha, \beta, \gamma \in \mathbb{N}^n$. Then for a differential operator $0 \neq f = \sum_{\alpha \in \mathbb{N}^n} r_\alpha D^\alpha \in \mathcal{A}$, the degree, leading coefficient and initial are defined as

$$\begin{aligned}
&\deg(f) := \max\nolimits_{\prec}\{\alpha \mid r_\alpha \neq 0\} \in \mathbb{N}^n, \\
&\mathrm{lc}(f) := r_{\deg(f)}, \\
&\mathrm{init}(f) := \mathrm{lc}(f) D^{\deg(f)}.
\end{aligned}$$

If F is a subset of $\mathcal{A}$, we define

$$\begin{aligned}
&\deg(F) := \{\deg(f) \mid f \in F, f \neq 0\}, \\
&\mathrm{init}(F) := \{\mathrm{init}(f) \mid f \in F, f \neq 0\}.
\end{aligned}$$

It is easy to check that $\mathcal{A}$ has the following properties. Let $f, g, h \in \mathcal{A}$:

Associativity:

$$(fg)h = f(gh).$$

Distributivity:

$$f(g+h) = fg + fh \quad \text{and} \quad (f+g)h = fh + gh.$$

There is another property about $\mathcal{A}$ which will be used frequently in this paper. Let $\mathrm{init}(f) = r_f D^{\alpha_f}$ and $\mathrm{init}(g) = r_g D^{\alpha_g}$, $r_f, r_g \in \mathcal{R}$, then

$$\deg(fg) = \deg(f) + \deg(g), \quad \mathrm{lc}(fg) = \mathrm{lc}(f)\mathrm{lc}(g) \quad \text{and} \quad \mathrm{init}(fg) = r_f r_g D^{\alpha_f} D^{\alpha_g}.$$

Therefore, $\mathcal{A}$ also has a **Quasi-Commutativity:**

$$\deg(fg - gf) \prec \deg(fg) = \deg(gf).$$

Then the Gröbner basis in the rings of differential operators with coefficients in $\mathcal{R}$ is defined as the following.

Definition 2.1. *Let $\mathcal{J}$ be an ideal in $\mathcal{A}$ and G a finite subset of $\mathcal{J} \setminus \{0\}$. Then G is a Gröbner basis of $\mathcal{J}$ w.r.t. $\prec$ iff for all $f \in \mathcal{J}$,*

$$\mathrm{lc}(f) \in {}_{\mathcal{R}}\langle \mathrm{lc}(g) \mid g \in G, \deg(f) \in \deg(g) + \mathbb{N}^n \rangle.$$

Example 2.2. If $\mathcal{J} = {}_{\mathcal{A}}\langle f \rangle \subset \mathcal{A}$ and $f \neq 0$, then $\{f\}$ is a Gröbner basis of $\mathcal{J}$.

3 Insa-Pauer Theorem

In order to compute the Gröbner basis, a division (or reduction) in $\mathcal{A}$ is necessary. In theory, there may exist various kinds of divisions in $\mathcal{A}$. The following division is the one presented by Insa and Pauer in [5].

Proposition 3.1 (Division in $\mathcal{A}$). *Let F be a finite subset of $\mathcal{A} \setminus \{0\}$ and $g \in \mathcal{A}$. Then there exist a differential operator $r \in \mathcal{A}$ and a family $(h_f)_{f \in F}$ in $\mathcal{A}$ such that*

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

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

(iii) *$r = 0$ or $\mathrm{lc}(r) \notin {}_{\mathcal{R}}\langle \mathrm{lc}(f) \mid \deg(r) \in \deg(f) + \mathbb{N}^n \rangle$.*

This definition of division in $\mathcal{A}$ is also used in the new theorem presented in the next section. Based on this division, a Gröbner basis in $\mathcal{A}$ has the following property [5].

Proposition 3.2. *Let $\mathcal{J}$ be an ideal in $\mathcal{A}$, G a Gröbner basis of $\mathcal{J}$ and $f \in \mathcal{A}$. Then $f \in \mathcal{J}$ iff a remainder of f after division by G is zero.*

Then the next theorem proposed by Insa and Pauer provides a criterion for checking if a set of differential operators is a Gröbner basis.

Theorem 3.3 (Insa-Pauer Theorem). *Let G be a finite subset of $\mathcal{A}\setminus\{0\}$ and $\mathcal{J}$ the ideal in $\mathcal{A}$ generated by G. For $E \subset G$, let S_E be a finite set of generators of the $\mathcal{R}$-module*

$$\mathrm{Syz}_{\mathcal{R}}(E) := \left\{ (s_e)_{e\in E} \,\middle|\, \sum_{e\in E} s_e \mathrm{lc}(e) = 0 \right\} \subset {}_{\mathcal{R}}(\mathcal{R}^{|E|}),$$

where $|E|$ is the cardinality of the set E. Then the following assertions are equivalent:

(i) *G is a Gröbner basis of $\mathcal{J}$.*

(ii) *For all $E \subset G$ and for all $(s_e)_{e\in E} \in S_E$, a remainder of*

$$\mathrm{SPoly}(E, (s_e)_{e\in E}) := \sum_{e\in E} s_e D^{m(E)-\deg(e)} e$$

after division by G is zero, where $m(E)$ is the least common multiple of the degrees of polynomials in E, i.e.,

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

According to this theorem, one is able to compute the Gröbner basis of ${}_{\mathcal{A}}\langle F\rangle$ for any subset $F \subset \mathcal{A}$. All needed to do is to check the remainder of $\sum_{e\in E} s_e D^{m(E)-\deg(e)} e$ after division by F is zero or not for all $E \subset F$. If there does exist a remainder r which is not zero, then expand F to $F' := F \cup \{r\}$ and repeat the process for F'. The procedure terminates exactly when all the remainders are zero. The terminality of this algorithm can be proved in a similar way as the general Gröbner basis algorithm.

During the above computing process, in order to seek non-zero remainders w.r.t. the subsets of F, one needs to compute the generators of $Syz(E)$ for all $E \subset F$, which is really expensive. In view of this, Zhou and Winkler proposed some techniques to avoid some unnecessary computations [10]. In their paper, they show that if the elements in E have some special properties, then instead of computing the generators of $Syz(E)$, it suffices to calculate the generators of $Syz(E')$ for some $E' \subset E$. Since the new theorem in this paper generalizes Insa-Pauer Theorem in a different way from Zhou and Winkler, the details of their method are omitted here. Interesting readers can refer to [10].

4 The new theorem for Gröbner basis in rings of differential operators

The differential operator

$$\mathrm{SPoly}(E, (s_e)_{e\in E}) = \sum_{e\in E} s_e D^{m(E)-\deg(e)} e$$

in (ii) of Insa-Pauer Theorem is denoted as a "generalized s-polynomial" w.r.t. the subset $E \subset G$ in [10], as it plays the same role as the general s-polynomials.

However, this generalized s-polynomial in Insa-Pauer Theorem is constructed quite strangely, since it is not created by the syzygies of $\mathrm{init}(G)$ in the traditional way but results from the set S_E, which is a set of generators of $\{(s_e)_{e\in E} \mid \sum_{e\in E} s_e \mathrm{lc}(e) = 0\}$. With a further study, one will find the reason easily. That is, the syzygy of $\mathrm{init}(G)$ is extremely difficult to define and even harder to compute, as $\mathcal{A}$ is a non-commutative ring. This explains why Insa and Pauer concentrate on the syzygy of $\mathrm{lc}(E)$ in $\mathcal{R}$ instead.

At this point, it is natural to ask: **do we really need the syzygy of init(G)?** The answer is **NO!**

By revisiting the proof of Insa-Pauer Theorem carefully, in order to show G is a Gröbner basis, it suffices to consider the differential operators which are generated by G and possibly have new initials. What we need to do is to eliminate the present initials of G and to try to create all possible new initials in ${}_{\mathcal{A}}\langle G\rangle$. Fortunately, the syzygy of $\mathrm{init}(G)$ is not the only one that could do this job, since the ring $\mathcal{A}$ has the Quasi-Commutativity.

With these considerations in mind, let us introduce a commutative ring $\mathcal{B}$ deduced from the Quasi-Commutative ring $\mathcal{A}$.

Let $\mathcal{B} := \mathcal{R}[Y] = \mathcal{R}[y_1, \ldots, y_n]$ generated by $\mathrm{id}_{\mathcal{R}} = 1$ and $y_1, \ldots, y_n$. $\mathcal{B}$ is a commutative K-algebra with fundamental relations:

$$x_i x_j = x_j x_i, \quad y_i y_j = y_j y_i \quad \text{and} \quad x_i y_j = y_j x_i \quad \text{for } 1 \leqslant i, j \leqslant n.$$

For any $f \in \mathcal{B}$, f can also be written uniquely as a finite sum $f = \sum_{\alpha \in \mathbb{N}^n} r_\alpha Y^\alpha$, where $r_\alpha \in \mathcal{R}$. Similarly, the degree, the leading coefficient and the initial are defined as: $\deg(f) := \max_{\prec}\{\alpha \mid r_\alpha \neq 0\} \in \mathbb{N}^n$, $\mathrm{lc}(f) := r_{\deg(f)}$ and $\mathrm{init}(f) := \mathrm{lc}(f) Y^{\deg(f)}$ respectively.

Since Y commutes with X and the linear equations over $\mathcal{R}$ are solvable, it is easy to check that the linear equations over $\mathcal{B}$ can be solved as well, which means the generators of

$$\mathrm{Syz}_{\mathcal{B}}(F) := \left\{ (s_f)_{f \in F} \,\middle|\, \sum_{f \in F} s_f \mathrm{init}(f) = 0, s_f \in \mathcal{B} \right\}$$

can be computed, where $F \subset \mathcal{B} \setminus \{0\}$.

With a little care, the only difference between $\mathcal{B}$ and $\mathcal{A}$ is that $\mathcal{B}$ is commutative and $\mathcal{A}$ is not. The following map bridges the two rings easily. Let σ be a map from $\mathcal{B}$ to $\mathcal{A}$ such that for any $\sum_{\alpha \in \mathbb{N}^n} r_\alpha Y^\alpha \in \mathcal{B}$ where $r_\alpha \in \mathcal{R}$,

$$\sigma\left(\sum_{\alpha \in \mathbb{N}^n} r_\alpha Y^\alpha \right) = \sum_{\alpha \in \mathbb{N}^n} r_\alpha D^\alpha \in \mathcal{A}.$$

By the definition of σ, the following properties hold for all $f, g \in \mathcal{B}$:

$$\begin{aligned}
&\deg(f) = \deg(\sigma(f)), \\
&\mathrm{lc}(f) = \mathrm{lc}(\sigma(f)), \\
&\sigma(\mathrm{init}(f)) = \mathrm{init}(\sigma(f)), \\
&\deg(fg) = \deg(\sigma(fg)) = \deg(\sigma(f)\sigma(g)), \\
&\mathrm{lc}(fg) = \mathrm{lc}(\sigma(fg)) = \mathrm{lc}(\sigma(f)\sigma(g)), \\
&\sigma(\mathrm{init}(fg)) = \mathrm{init}(\sigma(fg)) = \mathrm{init}(\sigma(f)\sigma(g)).
\end{aligned}$$

But remark that

$$\sigma(fg) \neq \sigma(f)\sigma(g).$$

It is also very easy to check that σ is an **$\mathcal{R}$-homomorphism**, i.e. for $f, g \in \mathcal{B}$ and $r \in \mathcal{R}$,

$$\sigma(rf + g) = r\sigma(f) + \sigma(g).$$

All the above properties will be used frequently in the proof of the new theorem.

Before presenting the new theorem, let us study some properties of the ring $\mathcal{B}$ first. These properties will be used in the proof of the new theorem as well. We start with the following definition.

Definition 4.1. *An element $(s_f)_{f \in F} \in \mathrm{Syz}_{\mathcal{B}}(F)$ is* **homogeneous of degree** α*, where $\alpha \in \mathbb{N}^n$, provided that*

$$(s_f)_{f \in F} = (c_f Y^{\alpha_f})_{f \in F},$$

where $c_f \in \mathcal{R}$ and $\alpha_f + \deg(f) = \alpha$ whenever $c_f \neq 0$.

The following two lemmas are well known. For details, please see [3].

Lemma 4.2. $\mathrm{Syz}_{\mathcal{B}}(F)$ *has a set of homogeneous generators, i.e. there exists a finite set $C_F \subset S(F)$ such that each element of C_F is homogeneous and* $\mathrm{Syz}_{\mathcal{B}}(F) = {}_{\mathcal{B}}\langle C_F \rangle$.

Lemma 4.3. *Let C_F be a set of homogeneous generators of* $\mathrm{Syz}_{\mathcal{B}}(F)$*. If $(s_f)_{f \in F} \in \mathrm{Syz}_{\mathcal{B}}(F)$ is homogeneous of degree α, then there exists a family $(r_{\bar{s}})_{\bar{s} \in C_F}$, where $r_{\bar{s}} \in \mathcal{B}$, such that*

$$(s_f)_{f \in F} = \sum_{\bar{s} \in C_F} r_{\bar{s}} \bar{s},$$

and $r_{\bar{s}}\bar{s}$ is homogeneous of degree α for all $\bar{s} \in C_F$.

The following example illustrates the above lemma.

Example 4.4. Let $\mathcal{R} = \mathbb{Q}[x_1, \dots, x_6]$, $\mathcal{A} = \mathcal{R}[D_1, \dots, D_6]$ and J the left ideal of $\mathcal{A}$ generated by $F = \{f_1, f_2, f_3\}$, 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 lexicographical order with $D_1 \prec \cdots \prec D_6$.

Here, the ring $\mathcal{B} = \mathcal{R}[y_1, \dots, y_6]$ is the corresponding commutative ring w.r.t. $\mathcal{A}$. The set

$$C_F = \{\bar{s}_1, \bar{s}_2, \bar{s}_3, \bar{s}_4\} \subset \mathcal{B}^3$$

generates $\mathrm{Syz}_{\mathcal{B}}(F)$, and C_F is also a set of homogeneous generators of $\mathrm{Syz}_{\mathcal{B}}(F)$, where $\bar{s}_1 = (y_5y_6, y_4y_6, -y_4y_5)$, $\bar{s}_2 = ((x_1 + x_2)y_6, 0, -x_1y_4)$, $\bar{s}_3 = (x_2y_5, -x_1y_4, 0)$, $\bar{s}_4 = (0, (x_1 + x_2)y_6, -x_2y_5)$.

Given $((x_1 - x_2)y_5y_6, 2x_1y_4y_6, -x_1y_4y_5) \in \mathrm{Syz}_{\mathcal{B}}(F)$ which is homogeneous of degree 3, there exist $r_1 = -x_2$, $r_2 = y_5$, $r_3 = -y_6$ and $r_4 = y_4$ such that

$$((x_1 - x_2)y_5y_6, 2x_1y_4y_6, -x_1y_4y_5) = r_1\bar{s}_1 + r_2\bar{s}_2 + r_3\bar{s}_3 + r_4\bar{s}_4,$$

and $r_i\bar{s}_i$ is homogeneous of degree 3 for $i = 1, 2, 3, 4$.

Now, it is time to present the new theorem.

Theorem 4.5 (Main theorem). *Let G be a finite subset of $\mathcal{A} \setminus \{0\}$ and $\mathcal{J}$ the ideal in $\mathcal{A}$ generated by G. For each $g \in G$, assume* $\mathrm{init}(g) = c_gD^{\alpha_g}$*, where $c_g \in \mathcal{R}$ and $\alpha_g \in \mathbb{N}^n$. Let C_G be a set of homogeneous generators of* $\mathrm{Syz}_{\mathcal{B}}(H_G)$*, where $H_G = \{c_gY^{\alpha_g} \mid g \in G\} \subset \mathcal{B}$ and C_G is called a set of commutative syzygy generators of* $\mathrm{init}(G)$ *for short. Then the following assertions are equivalent*:

(i) *G is a Gröbner basis of $\mathcal{J}$.*

(ii) *For all $(s_g)_{g\in G} \in C_G$ where $s_g \in \mathcal{B}$ and hence $\sigma(s_g) \in \mathcal{A}$, a remainder of*

$$\mathrm{CSPoly}((s_g)_{g\in G}) := \sum_{g\in G} \sigma(s_g)g$$

after division by G is zero.

Proof. (i) $\Rightarrow$ (ii): It follows from Proposition 3.2.

(ii) $\Rightarrow$ (i): Let $h \in \mathcal{J}$. It suffices to show

$$\mathrm{lc}(h) \in {}_{\mathcal{R}}\langle \mathrm{lc}(g) \mid g \in G, \deg(h) \in \deg(g) + \mathbb{N}^n\rangle.$$

For a family $(f_g)_{g\in G}$ in $\mathcal{A}$, define

$$\delta((f_g)_{g\in G}) := \max_{\prec}\{\deg(f_g) + \deg(g) \mid g \in G\}.$$

Since $h \in \mathcal{J}$, there exists a family $(h_g)_{g\in G}$ in $\mathcal{A}$ such that $h = \sum_{g\in G} h_gg$. Choose $(h_g)_{g\in G}$ such that

$$\delta := \delta((h_g)_{g\in G}) \text{ is minimal,}$$

which implies that if $(h'_g)_{g\in G}$ such that $h = \sum_{g\in G} h'_gg$, then $\delta \preceq \delta((h'_g)_{g\in G})$.

Let $E := \{g \in G \mid \deg(h_g) + \deg(g) = \delta\} \subset G$.

Case 1. $\deg(h) = \delta$. Then

$$\mathrm{init}(h) = \sum_{g\in E} \mathrm{init}(h_gg) \quad \text{and} \quad \mathrm{lc}(h) = \sum_{g\in E} \mathrm{lc}(h_g)\mathrm{lc}(g) \in {}_{\mathcal{R}}\langle \mathrm{lc}(g) \mid g \in E\rangle.$$

If $g \in E$, then $\deg(h) = \delta = \deg(h_g) + \deg(g)$ and hence $\deg(h) \in \deg(g) + \mathbb{N}^n$. Therefore, $\mathrm{lc}(h) \in {}_{\mathcal{R}}\langle \mathrm{lc}(g) \mid g \in G, \deg(h) \in \deg(g) + \mathbb{N}^n\rangle$.

Case 2. $\deg(h) \prec \delta$. Then

$$\sum_{g\in E} \mathrm{init}(h_gg) = 0, \text{ which implies } \sum_{g\in E} \mathrm{lc}(h_g)\mathrm{lc}(g) = 0.$$

Combined with the fact that $\deg(h_g) + \deg(g) = \delta$ for $g \in E$, it follows

$$0 = \sum_{g \in E} \mathrm{lc}(h_g)\mathrm{lc}(g)Y^{\delta} = \sum_{g \in E} \mathrm{lc}(h_g)Y^{\deg(h_g)}\mathrm{lc}(g)Y^{\deg(g)} \in \mathcal{B}.$$

Denote

$$t_g := \begin{cases} \mathrm{lc}(h_g)Y^{\deg(h_g)}, & g \in E, \\ 0, & g \in G \setminus E. \end{cases}$$

Notice that

$$\sigma(t_g) := \begin{cases} \mathrm{init}(h_g), & g \in E, \\ 0, & g \in G \setminus E. \end{cases}$$

Then $(t_g)_{g \in G}$ is a homogeneous element of $\mathrm{Syz}_{\mathcal{B}}(H_G)$ with degree δ. Since C_G is a set of homogeneous generators of $\mathrm{Syz}_{\mathcal{B}}(H_G)$, by Lemma 4.3, there exists a family $(r_{\bar{s}})_{\bar{s} \in C_G}$ where $r_{\bar{s}} \in \mathcal{B}$, such that $(t_g)_{g \in G} = \sum_{\bar{s} \in C_G} r_{\bar{s}}\bar{s}$ and $r_{\bar{s}}\bar{s}$ is homogeneous of degree δ, i.e. for $\forall g \in G$,

$$t_g = \sum_{\bar{s} \in C_G} r_{\bar{s}} s_g, \quad \text{where } \bar{s} = (s_g)_{g \in G},$$

and for $\forall\, g \in G$, $\forall\, \bar{s} \in C_G$,

$$\deg(r_{\bar{s}}) + \deg(s_g) + \deg(g) = \delta \text{ whenever } r_{\bar{s}} s_g \neq 0.$$

Remark that all $t_g, r_{\bar{s}}, s_g \in \mathcal{B}$.

Now

$$\begin{aligned} h &= \sum_{g \in G} h_g g = \sum_{g \in E} h_g g + \sum_{g \in G \setminus E} h_g g \\ &= \Bigg(\sum_{g \in E} h_g g - \sum_{g \in G} \sum_{\bar{s} \in C_G} \sigma(r_{\bar{s}})\sigma(s_g) g \Bigg) + \sum_{g \in G} \sum_{\bar{s} \in C_G} \sigma(r_{\bar{s}})\sigma(s_g) g + \sum_{g \in G \setminus E} h_g g. \end{aligned} \tag{1}$$

For the **FIRST** sum in (1),

$$\begin{aligned} \sum_{g \in E} h_g g - \sum_{g \in G} \sum_{\bar{s} \in C_G} \sigma(r_{\bar{s}})\sigma(s_g) g &= \sum_{g \in E} \mathrm{init}(h_g) g - \sum_{g \in G} \sum_{\bar{s} \in C_G} \sigma(r_{\bar{s}})\sigma(s_g) g + \sum_{g \in E} (h_g - \mathrm{init}(h_g)) g \\ &= \sum_{g \in G} \sigma(t_g) g - \sum_{g \in G} \sum_{\bar{s} \in C_G} \sigma(r_{\bar{s}})\sigma(s_g) g + \sum_{g \in E} (h_g - \mathrm{init}(h_g)) g \\ &= \sum_{g \in G} \Bigg(\sigma(t_g) - \sum_{\bar{s} \in C_G} \sigma(r_{\bar{s}})\sigma(s_g) \Bigg) g + \sum_{g \in E} (h_g - \mathrm{init}(h_g)) g \\ &= \sum_{g \in G} \sum_{\bar{s} \in C_G} (\sigma(r_{\bar{s}} s_g) - \sigma(r_{\bar{s}})\sigma(s_g)) g + \sum_{g \in E} (h_g - \mathrm{init}(h_g)) g. \end{aligned} \tag{2}$$

Since $\mathrm{init}(\sigma(r_{\bar{s}} s_g)) = \mathrm{init}(\sigma(r_{\bar{s}})\sigma(s_g))$, then for $\forall g \in G$, $\forall \bar{s} \in C_G$,

$$\deg((\sigma(r_{\bar{s}} s_g) - \sigma(r_{\bar{s}})\sigma(s_g)) g) \prec \deg(\sigma(r_{\bar{s}})\sigma(s_g) g) = \deg(r_{\bar{s}}) + \deg(s_g) + \deg(g) = \delta,$$

whenever $r_{\bar{s}} s_g \neq 0$. In case of $r_{\bar{s}} s_g = 0$ and $\sigma(r_{\bar{s}})\sigma(s_g) \neq 0$, $\mathrm{lc}(r_{\bar{s}} s_g) = 0$ implies $\mathrm{lc}(\sigma(r_{\bar{s}})\sigma(s_g)) = 0$, so the above inequation holds as well. Besides, clearly for $\forall g \in E$,

$$\deg((h_g - \mathrm{init}(h_g)) g) \prec \deg(h_g g) = \delta.$$

For the **SECOND** sum in (1),

$$\sum_{g \in G} \sum_{\bar{s} \in C_G} \sigma(r_{\bar{s}})\sigma(s_g) g = \sum_{\bar{s} \in C_G} \sigma(r_{\bar{s}}) \Bigg(\sum_{g \in G} \sigma(s_g) g \Bigg).$$

For each $\bar{s} = (s_g)_{g\in G} \in C_G$, assume that $\bar{s}$ is homogeneous of degree $\beta_{\bar{s}}$, then $\beta_{\bar{s}} = \deg(\sigma(s_g)) + \deg(g)$ whenever $\sigma(s_g) \neq 0$, and consider

$$\begin{aligned}\sum_{g\in G} \sigma(s_g)g &= \sum_{g\in G} \mathrm{init}(\sigma(s_g)g) + \sum_{g\in G}(\sigma(s_g)g - \mathrm{init}(\sigma(s_g)g)) \\ &= \sum_{g\in G} \mathrm{lc}(\sigma(s_g))\mathrm{lc}(g)D^{\beta_{\bar{s}}} + \sum_{g\in G}(\sigma(s_g)g - \mathrm{init}(\sigma(s_g)g)).\end{aligned}$$

By the definition of C_G and $\bar{s}$ is a homogeneous element of $\mathrm{Syz}_{\mathcal{B}}(H_G)$ with degree $\beta_{\bar{s}}$, then

$$0 = \sum_{g\in G} s_g c_g Y^{\alpha_g} = \sum_{g\in G} \mathrm{lc}(s_g) c_g Y^{\beta_{\bar{s}}}, \quad \text{where } \mathrm{init}(g) = c_g D^{\alpha_g}.$$

Notice that $\mathrm{lc}(\sigma(s_g)) = \mathrm{lc}(s_g)$, which implies that

$$\sum_{g\in G} \mathrm{lc}(\sigma(s_g))\mathrm{lc}(g)D^{\beta_{\bar{s}}} = 0.$$

Combined with the fact that $\deg(\sigma(s_g)g - \mathrm{init}(\sigma(s_g)g)) \prec \beta_{\bar{s}}$, the following inequation holds:

$$\deg\bigg(\sum_{g\in G} \sigma(s_g)g\bigg) \prec \beta_{\bar{s}}.$$

By (ii) a remainder of $\sum_{g\in G} \sigma(s_g)g$ after division by G is zero, i.e. there exist families $(f_g(\bar{s}))_{g\in G}$ in $\mathcal{A}$, such that

$$\sum_{g\in G} \sigma(s_g)g = \sum_{g\in G} f_g(\bar{s})g,$$

and $\deg(f_g(\bar{s})g) \preceq \deg(\sum_{g\in G} \sigma(s_g)g) \prec \beta_{\bar{s}}$. So the second sum in (1) turns out to be

$$\begin{aligned}\sum_{g\in G}\sum_{\bar{s}\in C_G} \sigma(r_{\bar{s}})\sigma(s_g)g &= \sum_{\bar{s}\in C_G} \sigma(r_{\bar{s}})\bigg(\sum_{g\in G}\sigma(s_g)g\bigg) = \sum_{\bar{s}\in C_G} \sigma(r_{\bar{s}})\bigg(\sum_{g\in G} f_g(\bar{s})g\bigg) \\ &= \sum_{g\in G}\sum_{\bar{s}\in C_G} \sigma(r_{\bar{s}})f_g(\bar{s})g \end{aligned} \tag{3}$$

and for $\forall g \in G$, $\forall \bar{s} \in C_G$,

$$\deg(\sigma(r_{\bar{s}})f_g(\bar{s})g) \prec \deg(\sigma(r_{\bar{s}})) + \beta_{\bar{s}} = \delta \text{ whenever } r_{\bar{s}} \neq 0.$$

For the **THIRD** sum in (1), by the definition of E, it is obvious that $\deg(h_g g) \prec \delta$ for $g \in G \setminus E$.

Based on the expressions in (2) and (3), let

$$h'_g := \begin{cases} \displaystyle\sum_{\bar{s}\in C_G} (\sigma(r_{\bar{s}}s_g) - \sigma(r_{\bar{s}})\sigma(s_g) + \sigma(r_{\bar{s}})f_g(\bar{s})) + (h_g - \mathrm{init}(h_g)), & g \in E, \\ \displaystyle\sum_{\bar{s}\in C_G} (\sigma(r_{\bar{s}}s_g) - \sigma(r_{\bar{s}})\sigma(s_g) + \sigma(r_{\bar{s}})f_g(\bar{s})) + h_g, & g \in G \setminus E. \end{cases}$$

Then it is easy to verify that $h = \sum_{g\in G} h'_g g$ and $\delta((h'_g)_{g\in G}) \prec \delta$, which is a contradiction to the minimality of δ. Hence Case 2 never occurs.

To sum up, the theorem is proved. □

The above theorem provides a more fundamental criterion than Insa-Pauer Theorem, since it suffices to consider the "s-polynomials" constructed from a set of commutative syzygy generators of $\mathrm{init}(G)$. As we will see in the next section, Insa-Pauer Theorem only provides a method for computing the set C_G. Thus the new theorem is more essential and Insa-Pauer Theorem can be concluded as a simple corollary.

In fact, the main theorem extends much more generally.

Theorem 4.6. *The main theorem is true for all rings with the quasi-commutative property.*

Proof. In the proof of the main theorem, only the quasi-commutative property is used. □

Similar to Insa and Pauer's approach, one can also develop an algorithm for computing Gröbner basis of ${}_{\mathcal{A}}\langle F\rangle$ for any given $F\subset\mathcal{A}$ based on the main theorem. According to Theorem 4.5, it suffices to compute **one** set of commutative syzygy generators of $\mathrm{init}(F)$ in the commutative ring $\mathcal{B}$, instead of computing the generators of $\mathrm{Syz}_{\mathcal{R}}(E)$ for **all** subsets $E\subset F$. Clearly, Insa and Pauer's method leads to more computations than needed. To illustrate this, let us see the following example from [10].

Example 4.7. Let $\mathcal{R}=\mathbb{Q}[x_1,\dots,x_6]$, $\mathcal{A}=\mathcal{R}[D_1,\dots,D_6]$ and J the left ideal of $\mathcal{A}$ generated by $F=\{f_1,f_2,f_3,f_4\}$, where $f_1=x_1D_4+1, f_2=x_2D_5, f_3=(x_1+x_2)D_6, f_4=D_5D_6$. Let $\prec$ be the graded lexicographical order with $D_1\prec\cdots\prec D_6$.

By Insa-Pauer Theorem, in order to compute a Gröbner basis for ${}_{\mathcal{A}}\langle F\rangle$, one needs to consider the following 12 "generalized s-polynomials" (duplicated cases are omitted):

$$\begin{aligned}
&\mathrm{SPoly}(\{f_1,f_2\},(x_2,-x_1))=x_2D_5f_1-x_1D_4f_2,\\
&\mathrm{SPoly}(\{f_1,f_3\},(x_1+x_2,-x_1))=(x_1+x_2)D_6f_1-x_1D_4f_3,\\
&\mathrm{SPoly}(\{f_1,f_4\},(1,-x_1))=D_5D_6f_1-x_1D_4f_4,\\
&\mathrm{SPoly}(\{f_2,f_3\},(x_1+x_2,-x_2))=(x_1+x_2)D_6f_2-x_2D_5f_3,\\
&\mathrm{SPoly}(\{f_2,f_4\},(1,-x_2))=D_6f_2-x_2f_4,\\
&\mathrm{SPoly}(\{f_3,f_4\},(1,-(x_1+x_2)))=D_5f_3-(x_1+x_2)f_4,\\
&\mathrm{SPoly}(\{f_1,f_2,f_3\},(x_2,-x_1,0))=x_2D_5D_6f_1-x_1D_4D_6f_2,\\
&\mathrm{SPoly}(\{f_1,f_2,f_3\},(1,1,-1))=D_5D_6f_1+D_4D_6f_2-D_4D_5f_3,\\
&\mathrm{SPoly}(\{f_1,f_2,f_4\},(0,1,-x_2))=D_4D_6f_2-x_2D_4f_4,\\
&\mathrm{SPoly}(\{f_1,f_3,f_4\},(x_1+x_2,-x_1,0))=(x_1+x_2)D_5D_6f_1-x_1D_4D_5f_4,\\
&\mathrm{SPoly}(\{f_1,f_3,f_4\},(1,-1,x_2))=D_5D_6f_1-D_4D_5f_3+x_2D_4f_4,\\
&\mathrm{SPoly}(\{f_2,f_3,f_4\},(1,-1,x_1))=D_6f_2-D_5f_3+x_1f_4.
\end{aligned}$$

By Zhou and Winkler's trick, $\mathrm{SPoly}(\{f_1,f_2,f_4\},(0,1,-x_2))$, $\mathrm{SPoly}(\{f_1,f_3,f_4\},(x_1+x_2,-x_1,0))$, $\mathrm{SPoly}(\{f_1,f_3,f_4\},(1,-1,x_2))$ and $\mathrm{SPoly}(\{f_2,f_3,f_4\},(1,-1,x_1))$ can be removed.

However, according to the new theorem, $\mathcal{B}=\mathcal{R}[y_1,\dots,y_6]$ and $H_F=\{x_1y_4,x_2y_5,(x_1+x_2)y_6,y_5y_6\}$. Then

$$\begin{aligned}
C_F=\{\bar{s}_1,\bar{s}_2,\bar{s}_3,\bar{s}_4,\bar{s}_5\}=\{&(x_2y_5,-x_1y_4,0,0),((x_1+x_2)y_6,0,-x_1y_4,0),\\
&(y_5y_6,0,0,-x_1y_4),(0,y_6,0,-x_2),(0,0,y_5,-(x_1+x_2))\},
\end{aligned}$$

is a set of commutative syzygy generators of $\mathrm{init}(F)$. Therefore, in the new method, it suffices to consider:

$$\begin{aligned}
&\mathrm{CSPoly}(\bar{s}_1)=x_2D_5f_1-x_1D_4f_2,\\
&\mathrm{CSPoly}(\bar{s}_2)=(x_1+x_2)D_6f_1-x_1D_4f_3,\\
&\mathrm{CSPoly}(\bar{s}_3)=D_5D_6f_1-x_1D_4f_4,\\
&\mathrm{CSPoly}(\bar{s}_4)=D_6f_2-x_2f_4,\\
&\mathrm{CSPoly}(\bar{s}_5)=D_5f_3-(x_1+x_2)f_4.
\end{aligned}$$

No matter in either Insa and Pauer's method or Zhou and Winkler's improved version, one has to compute the remainders of $\mathrm{SPoly}(\{f_2,f_3\},(x_1+x_2,-x_2))$ and $\mathrm{SPoly}(\{f_1,f_2,f_3\},(1,1,-1))$ all the time, which are not needed any more in the new method. Therefore, the new method avoids all these unnecessary computations and hence has better efficiency.

To finish this example, it is easy to check that all the remainders of $\mathrm{CSPoly}(\bar{s}_i)$ after division by F are zero. So F itself is a Gröbner basis for ${}_{\mathcal{A}}\langle F\rangle$.

Let us see another example from [10].

Example 4.8. Let $\mathcal{R} = \mathbb{Q}[x_1, x_2, x_3]$, $\mathcal{A} = \mathcal{R}[D_1, D_2, D_3]$ and J the left ideal of $\mathcal{A}$ generated by $F = \{f_1, f_2\}$, 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 lexicographical order with $D_1 \prec D_2 \prec D_3$.

The Gröbner basis of the left ideal J is $G = \{f_1, f_2, p, q\}$, where $p = qD_3 + q$ and $q = x_2^2 - x_1^2$. However, to check whether G is a Gröbner basis, we have to deal with 10 distinct "generalized s-polynomials" according to Insa-Pauer Theorem. By using our method, only 3 "CSPolys" are necessary to handle, which is much fewer.

5 On Computing C_G over $\mathcal{R}[Y]$

So far, as shown by the main Theorem 4.5, in order to check if a set of differential operators G is a Gröbner basis for ${}_{\mathcal{A}}\langle G\rangle$, it only needs to consider the "s-polynomials" deduced by C_G, which is a set of commutative syzygy generators of $\mathrm{init}(G)$. Now, the last question is **how to compute the set C_G over $\mathcal{R}[Y]$?**

By the definition of C_G, it is a set of homogeneous generators of $\mathrm{Syz}_{\mathcal{B}}(H_G)$ which is a syzygy module of monomials in $\mathcal{B} = \mathcal{R}[Y]$. In fact, Insa-Pauer Theorem implies a natural method to compute it. That is, the set

$$\{(s_eY^{m(E)-\deg(e)})_{e\in E} \mid (s_e)_{e\in E} \in S_E, E \subset G\},$$

where S_E is a set of generators of $\mathrm{Syz}_{\mathcal{R}}(E) = \{(s_e)_{e\in E} \mid \sum_{e\in E} s_e\mathrm{lc}(e) = 0, s_e \in \mathcal{R}\}$ and $m(E) = (\max_{e\in E}\deg(e)_1, \ldots, \max_{e\in E}\deg(e)_n) \in \mathbb{N}^n$, extends to a set of generators of $\mathrm{Syz}_{\mathcal{B}}(H_G)$ naturally. But Example 4.7 shows this set is not minimal in general.

Since $\mathcal{B} = \mathcal{R}[Y]$ is a commutative ring, there are many sophisticated results to compute the syzygy of monomials in $\mathcal{B}$, such as the techniques in [1]. Also Zhou and Winkler's trick can be exploited for this purpose. Here, we only mention two special cases.

(i) $\mathcal{R}$ is a field:

When $\mathcal{R}$ is a field, the following set

$$\{(\mathrm{lc}(g)Y^{m(f,g)-\deg(f)}, -\mathrm{lc}(f)Y^{m(f,g)-\deg(g)}) \mid f, g \in G\}$$

extends to a set of generators of $\mathrm{Syz}_{\mathcal{B}}(H_G)$.

(ii) $\mathcal{R}$ is the polynomial ring $K[X]$:

Since the variables X commute with Y, C_G can be obtained by computing the generators of $\mathrm{Syz}_{\mathcal{B}}(H_G)$ in the polynomial ring $K[X, Y]$. Notice that $H_G = \{c_gY^{\alpha_g} \mid g \in G\} \subset K[X, Y]$. We can obtain a finite set of generators for $\{(s_g)_{g\in G} \mid \sum_{g\in G} s_gc_gY^{\alpha_g} = 0, s_g \in K[X, Y]\}$ in the polynomial ring $K[X, Y]$ and denote it by S. It is straightforward to check that S is also a set of generators for $\mathrm{Syz}_{\mathcal{B}}(H_G)$ when considered in $K[X][Y]$. Then the collection of all homogeneous parts of S is a set of homogeneous generators for $\mathrm{Syz}_{\mathcal{B}}(H_G)$, since $\mathrm{Syz}_{\mathcal{B}}(H_G)$ itself is a graded syzygy module in $(K[X][Y])^{|H_G|}$.

We should also notice that the s-polynomial of two polynomials f and g may be no more *one* polynomial but *several* polynomials when the coefficient ring R has a special structure.

6 Conclusion

In this paper, a new theorem which determines if a set of differential operators is a Gröbner basis in the ring of differential operators is proposed. This new theorem is so essential that Insa-Pauer Theorem can be considered as a direct corollary. Furthermore, based on the new theorem, a new method for computing Gröbner basis in rings of differential operators is deduced. The new method avoids many unnecessary computations naturally and hence has better efficiency than other well-known methods.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 10971217, 60821002/F02) and NC Special Project. The authors cordially thank Professor Ziming Li for his helpful suggestions and we also thank the anonymous referees for their careful reading and helpful comments.

References

1 Adams W, Loustaunau P. An Introduction to Gröbner Bases. Providence: American Mathematical Society, 1994
2 Björk J. Rings of Differential Operators. Amsterdam-Oxford-New York: North-Holland Pub Co, 1979
3 Cox D, Little J, O'Shea D. Ideals, Varieties and Algorithms. Second Edition. New York: Springer, 1996
4 Galligo A. Some algorithmic questions on ideals of differential operators. In: Lecture Notes in Computer Science, vol. 204. New York: Springer, 1985, 413–421
5 Insa M, Pauer F. Gröbner bases in rings of differential operators. In: Buchberger B, Winkler F, eds. Gröbner Bases and Applications. Cambridge: Cambridge University Press, 1998
6 Mora F. Gröbner bases for non-commutative polynomial rings. In: Calmet J, ed. Proc. AAECC-3, LNCS, vol. 229. New York: Springer, 1986, 353–362
7 Mora T. An introduction to commutative and noncommutative Gröbner bases. Theoret Comput Sci, 1994, 134: 131–173
8 Oaku T, Shimoyama T. A Gröbner basis method for modules over rings of differential operators. J Symbol Comput, 1994, 3: 223–248
9 Pauer F. Gröbner bases with coefficients in rings. J Symbol Comput, 2007, 42: 1003–1011
10 Zhou M, Winkler F. On computing Gröbner bases in rings of differential operators with coefficients in a ring. Math Comput Sci, 2007, 1: 211–223