A Note on Gröbner Bases of Ore Polynomials over a PID

Ziming Li*[1] and Yi Zhang †[2]

[1, 2]KLMM, AMSS, Chinese Academy of Sciences, Beijing
[2]Institute for Algebra, Johannes Kepler University, Linz

Abstract

We describe the notion of Gröbner bases and Buchberger's algorithm for Ore polynomials whose constant coefficients lie in a principal ideal domain. The note is based on Section 10.1 in the book *Gröbner Bases, A Computational Approach to Commutative Algebra* by T. Becker and V. Weispfenning. As we are dealing with noncommutative polynomials of certain type, tiny technical details are different from the usual commutative case in many places. So we proceed step by step and offer proofs for most of the statements. We also present a way to compute a basis of the saturation of a left ideal with respect to a constant in the last section.

1 Ore algebras

In this section, we define Ore algebras that we are concerned with.

Let R be a principal ideal domain and $n \in \mathbb{N}$. Let $R[x_1, \ldots, x_n]$ be the ring of usual commutative polynomials over R. For brevity, we denote this ring by $R[\mathbf{x}]$. For all $i = 1, \ldots, n$, let σ_i be an R-automorphism of $R[\mathbf{x}]$ with the following properties:

(i) $\sigma_i(x_i) = \gamma_i x_i + \tau_i$ for some $\gamma_i, \tau_i \in R$ with γ_i being a unit in R,

(ii) $\sigma_i(x_j) = x_j$ for $j \neq i$.

Let δ_i be a σ_i-derivation on $R[\mathbf{x}]$, *i.e.*, an R-linear map satisfying the following three properties:

(i) $\delta_i(fg) = \sigma_i(f)\delta_i(g) + \delta_i(f)g \quad \text{for} \quad f, g \in R[\mathbf{x}]$,

(ii) $\delta_i(x_i)$ is a linear polynomial in $R[x_i]$,

(iii) $\delta_i(x_j) = 0$ for all $j \neq i$.

*Supported by the NSFC grants (91118001, 60821002/F02) and a 973 project (2011CB302401). Email: zmli@mmrc.iss.ac.cn

†Supported by the Austrian Science Fund (FWF) grants Y464-N18, NSFC grants (91118001, 60821002/F02) and a 973 project (2011CB302401). Email: zhangy@amss.ac.cn

Then we have an Ore algebra

$$R[\mathbf{x}][\partial_1;\sigma_1,\delta_1]\cdots[\partial_n;\sigma_n,\delta_n]$$

of Ore polynomials [1], in which the addition is coefficient-wise and the multiplication is defined by associativity via the commutation rules

(i) $\partial_i p = \sigma_i(p)\partial_i + \delta_i(p)$ for $p \in R[\mathbf{x}]$, $1 \le i \le n$,

(ii) $\partial_i\partial_j = \partial_j\partial_i$ for $1 \le i, j \le n$.

The ring $R[\mathbf{x}][\partial_1;\sigma_1,\delta_1]\cdots[\partial_n;\sigma_n,\delta_n]$ is abbreviated as $R[\mathbf{x}][\boldsymbol{\partial}]$ when σ_i and δ_i are clear from the context.

2 Terms and monomials

By a *term*, we mean a product $x_1^{\alpha_1}\cdots x_n^{\alpha_n}\partial_1^{\beta_1}\cdots\partial_n^{\beta_n}$ with $\alpha_i, \beta_j \in \mathbb{N}$. For brevity, we set $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n)$ and $\boldsymbol{\beta} = (\beta_1,\ldots,\beta_n)$. Then we may denote a term as $\mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}}$. By a *monomial*, we mean a product at, where a is a nonzero element of R, and t a term. Set T to be the set of all terms, and M the set of all monomials. Let $P \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$. Since P is a sum of monomials, we denote the set of monomials in P by $\mathrm{M}(P)$. The set of corresponding terms is denoted by $\mathrm{T}(P)$.

Let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^n$, we write $\boldsymbol{\alpha} \le \boldsymbol{\beta}$ if $\alpha_i \le \beta_i$ for all $1 \le i \le n$. Let $as, bt \in M$ with $s = \mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}}, t = \mathbf{x}^{\mathbf{u}}\boldsymbol{\partial}^{\mathbf{v}} \in T$ and $a, b \in R$. We say that *as quasi-divides bt* if $a \mid b$ in R, $\boldsymbol{\alpha} \le \mathbf{u}$ and $\boldsymbol{\beta} \le \mathbf{v}$. In this case, we write $as \mid_q bt$. In other words, $s \mid t$ when we forget the commutation rules in $R[\mathbf{x}][\boldsymbol{\partial}]$.

Proposition 2.1. *Let S be a set of monomials in $R[\mathbf{x}][\boldsymbol{\partial}]$. Then S has a Dickson basis, i.e., there exists a finite subset N of S such that, for each $s \in S$, there exists $t \in N$ with $t \mid_q s$.*

Proof. We define the following map:

$$\begin{array}{cccc} \phi: & M & \longrightarrow & R \times \mathbb{N}^n \times \mathbb{N}^n \\ & a\mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} & \mapsto & (a, \boldsymbol{\alpha}, \boldsymbol{\beta}). \end{array}$$

Obviously, ϕ is a bijection. Moreover, the quasi-divisibility relation in M corresponds to the following quasi-order in $R \times \mathbb{N}^n \times \mathbb{N}^n$:

$$(a_1, \boldsymbol{\alpha}_1, \boldsymbol{\beta}_1) \prec' (a_2, \boldsymbol{\alpha}_2, \boldsymbol{\beta}_2) \quad \text{if and only if} \quad a_1 \mid a_2,\ \boldsymbol{\alpha}_1 \le \boldsymbol{\alpha}_2 \text{ and } \boldsymbol{\beta}_1 \le \boldsymbol{\beta}_2,$$

where $(a_1, \boldsymbol{\alpha}_1, \boldsymbol{\beta}_1), (a_2, \boldsymbol{\alpha}_2, \boldsymbol{\beta}_2) \in R \times \mathbb{N}^n \times \mathbb{N}^n$. By [2, Proposition 4.49], $\phi(S)$ has a Dickson basis N' with respect to $\prec'$. Then $\phi^{-1}(N')$ is a Dickson basis of S. □

3 Term order and monomial order

A *term order* $\prec$ is a linear order on T that satisfies the following conditions:

(i) $1 \preceq t$ for each $t \in T$;

(ii) $\mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} \prec \mathbf{x}^{\mathbf{a}}\boldsymbol{\partial}^{\mathbf{b}}$ implies $\mathbf{x}^{\boldsymbol{\alpha}+\mathbf{u}}\boldsymbol{\partial}^{\boldsymbol{\beta}+\mathbf{v}} \prec \mathbf{x}^{\mathbf{a}+\mathbf{u}}\boldsymbol{\partial}^{\mathbf{b}+\mathbf{v}}$ for each $(\mathbf{u},\mathbf{v}) \in \mathbb{N}^n \times \mathbb{N}^n$;

A term order induces a partial order on M as follows. For all $as, bt \in M$ with $s = \mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}}, t = \mathbf{x}^{\mathbf{u}}\boldsymbol{\partial}^{\mathbf{v}} \in T$ and $a, b \in R$,

$$as \prec bt \Longleftrightarrow s \prec t.$$

The induced order is called a *monomial order* on M.

Lemma 3.1. *Let $\prec$ be a monomial order on M. Then there is no strictly decreasing infinite sequence in M with respect to $\prec$.*

Proof. Suppose that

$$m_1, m_2, \ldots$$

is an infinite sequence in M with $m_i \succ m_{i+1}$ for all $i \in \mathbb{Z}^+$. By Proposition 2.1, there exist a finite number of monomials $m_{j_1}, \ldots, m_{j_k}$ such that, for all $i \in \mathbb{Z}^+$, there exists $\ell \in \{1, \ldots, k\}$ with $m_{j_\ell}|_q m_i$. Choose i to be greater than all the indices $j_1, \ldots, j_k$. Then m_{j_ℓ} cannot be higher than m_i, a contradiction. □

Let $\prec$ be a monomial order on M, and $P \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$. Then

$$P = c_1 t_1 + \cdots + c_\ell t_\ell,$$

where $c_1, \ldots, c_\ell \in R \setminus \{0\}$, and $t_1, \ldots, t_\ell$ are mutually distinct terms.

Assume that $t_1 \prec t_2 \prec \cdots \prec t_\ell$. Then t_ℓ, c_ℓ and $c_\ell t_\ell$ are called the *head term*, *head coefficient*, and *head monomial* of P, respectively. They are denoted by $\mathrm{HT}(P)$, $\mathrm{HC}(P)$ and $\mathrm{HM}(P)$, respectively.

Let $P, Q \in R[\mathbf{x}][\boldsymbol{\partial}]$. We say that $P, Q \in R[\mathbf{x}][\boldsymbol{\partial}]$ are *associated* to each other if there are unit elements $a, b \in R$ such that $aP = bQ$.

Proposition 3.2. *Let P and Q be two nonzero elements in $R[\mathbf{x}][\boldsymbol{\partial}]$. Then*

(i) $\mathrm{HT}(PQ) = \mathrm{HT}(\mathrm{HT}(P)\mathrm{HT}(Q))$*;*

(ii) $\mathrm{HC}(PQ)$ *and* $\mathrm{HC}(P)\mathrm{HC}(Q)$ *are associated;*

(iii) $\mathrm{HM}(PQ)$ *and* $\mathrm{HM}(\mathrm{HM}(P)\mathrm{HM}(Q))$ *are associated.*

Proof. Given $i \in \{1, \ldots, n\}$. By the definitions of σ_i, δ_i and the commutation rules in Section 1, we have

$$\partial_i x_i = \gamma_i(x_i \partial_i) + \tau_i \partial_i + a_i x_i + b_i,$$

where γ_i is a unit in R, and $\tau_i, a_i, b_i \in R$. Therefore, $\mathrm{HM}(\partial_i x_i) = \gamma_i x_i \partial_i$. A direct induction proves the proposition. □

The following corollary is a step-stone for generalizing usual polynomial reductions to the Ore case.

Corollary 3.3. *Let $m_1, m_2 \in M$. If $m_1 \mid_q m_2$, then there exists $m_3 \in M$, such that $m_2 = \mathrm{HM}(m_3 m_1)$.*

Proof. Let $m_1 = a\mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\beta}^{\boldsymbol{\beta}}, m_2 = b\mathbf{x}^{\mathbf{u}}\boldsymbol{\beta}^{\mathbf{v}}$ with $a, b \in R$, and $(\boldsymbol{\alpha}, \boldsymbol{\beta}), (\mathbf{u}, \mathbf{v}) \in \mathbb{N}^n \times \mathbb{N}^n$. Since $m_1 \mid_q m_2$, we have $a \mid b$, $\boldsymbol{\alpha} \leq \mathbf{u}$, $\boldsymbol{\beta} \leq \mathbf{v}$. Let $\mathbf{u}' = \mathbf{u} - \boldsymbol{\alpha}$, $\mathbf{v}' = \mathbf{v} - \boldsymbol{\beta}$. By item (iii) of the above proposition, there exists a unit γ in R, such that $\mathrm{HM}(\mathbf{x}^{\mathbf{u}'}\boldsymbol{\partial}^{\mathbf{v}'} m_1) = \gamma a \mathbf{x}^{\mathbf{u}}\boldsymbol{\beta}^{\mathbf{v}}$. Since $\gamma a \mid b$, there exists $c \in R$, such that $c\gamma a = b$. Let $m_3 = c\mathbf{x}^{\mathbf{u}'}\boldsymbol{\partial}^{\mathbf{v}'}$, then $m_2 = \mathrm{HM}(m_3 m_1)$. □

4 Reduction for Ore polynomials

In the sequel, we assume that $\prec$ is a term order on T.

Definition 4.1. *Let $F, G, P \in R[\mathbf{x}][\boldsymbol{\partial}]$ with $FP \neq 0$, and let $\mathcal{P}$ be a subset of $R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$. Then we say*

(i) F reduces to G modulo P by eliminating m *(notation $F \underset{P,m}{\longrightarrow} G$), if there exists $m \in \mathrm{M}(F)$ with $\mathrm{HM}(P) \mid_q m$, and $G = F - m'P$, where m' is a monomial such that $\mathrm{HM}(m'P) = m$;*

(ii) F reduces to G modulo P *(notation $F \underset{P}{\longrightarrow} G$), if $F \underset{P,m}{\longrightarrow} G$ for some m in $\mathrm{M}(F)$;*

(iii) F reduces to G modulo $\mathcal{P}$ *(notation $F \underset{\mathcal{P}}{\longrightarrow} G$), if $F \underset{P}{\longrightarrow} G$ for some $P \in \mathcal{P}$;*

(iv) F *is* reducible modulo P *if there exists $G \in R[\mathbf{x}][\boldsymbol{\partial}]$ such that $F \underset{P}{\longrightarrow} G$;*

(v) F *is* reducible modulo $\mathcal{P}$ *if there exists $G \in R[\mathbf{x}][\boldsymbol{\partial}]$ such that $F \underset{\mathcal{P}}{\longrightarrow} G$.*

Remark 4.2. *The existence of m' in item (i) of the above definition is guaranteed by Corollary 3.3.*

If F is not reducible modulo P (modulo $\mathcal{P}$), then we say F is *in normal form modulo P (modulo $\mathcal{P}$). A normal form of F modulo $\mathcal{P}$* is an element $G \in R[\mathbf{x}][\boldsymbol{\partial}]$ that is in normal form modulo $\mathcal{P}$ and satisties

$$F \overset{*}{\underset{\mathcal{P}}{\longrightarrow}} G,$$

where $\overset{*}{\underset{\mathcal{P}}{\longrightarrow}}$ is the reflexive-transitive closure [2, Definition 4.71] of $\underset{\mathcal{P}}{\longrightarrow}$. We call

$$F \underset{P,m}{\longrightarrow} G$$

a *top-reduction* of F if $m = \mathrm{HM}(F)$; whenever a top-reduction of F exists (with $P \in \mathcal{P}$), we say that F is *top-reducible modulo P (modulo $\mathcal{P}$).*

Algorithm 4.1. *Given $F \in R[\mathbf{x}][\boldsymbol{\partial}]$, $\mathcal{P} \subset R[\mathbf{x}][\boldsymbol{\partial}]$ compute a normal form of F modulo $\mathcal{P}$.*

```
G ← 0
L ← F
while L ≠ 0 do
 | while L is top-reducible modulo 𝒫 do
 |  | S ← L − m′P for some P ∈ 𝒫, m′ ∈ T with HM(m′P) = HM(L)
 |  | L ← S
 | end
 | G ← G + HM(L)
 | L ← L − HM(L)
end
```

The correctness of the above algorithm is evident.

Proof of the termination of Algorithm 4.1: Suppose Algorithm 4.1 does not terminate. Let $\{L_i\}_{i\in\mathbb{N}}$ be the operators in the order that they are evaluated to L. Then, $L_0 = F$. Moreover, the valuation of L_{i+1} has two cases (i) $L_{i+1} = L_i - m'P$, for some $P \in \mathcal{P}, m' \in T$ with $\mathrm{HM}(m'P) = \mathrm{HM}(L_i)$; (ii) $L_{i+1} = L_i - \mathrm{HM}(L_i)$, here $i \in \mathbb{N}$. Therefore, we have $\mathrm{HT}(L_{i+1}) \prec \mathrm{HT}(L_i)$, for all $i \in \mathbb{N}$, i.e., $\{\mathrm{HT}(L_i)\}_{i\in\mathbb{N}}$ is a strictly decreasing sequence with respect to $\prec$, a contradiction to Lemma 3.1.

5 Definition of Gröbner bases

As a matter of notation, let S be a subset of $R[\mathbf{x}][\boldsymbol{\partial}]$, we denote the left ideal generated by S in $R[\mathbf{x}][\boldsymbol{\partial}]$ as $R[\mathbf{x}][\boldsymbol{\partial}] \cdot S$. The set of head monomials of elements in S is denoted by $\mathrm{HM}(S)$.

Definition 5.1. *A finite set $\mathcal{G} \subset R[\mathbf{x}][\boldsymbol{\partial}]$ is called a* Gröbner basis *if it has the property that, for each $u \in \mathrm{HM}(R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G})$, there exists $v \in \mathrm{HM}(\mathcal{G})$, such that $v \mid_q u$. If I is a left ideal of $R[\mathbf{x}][\boldsymbol{\partial}]$, then a* Gröbner basis of I *is a Gröbner basis that generates the left ideal I.*

Remark 5.2. *Note that $\mathcal{G} \subset R[\mathbf{x}][\boldsymbol{\partial}]$ is a Gröbner basis if and only if, for each $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} \setminus \{0\}$, F is top-reducible modulo $\mathcal{G}$.*

Proposition 5.1. *Let I be a left ideal of $R[\mathbf{x}][\boldsymbol{\partial}]$. Then I has a Gröbner basis.*

Proof. By Proposition 2.1, there exists a finite set T of $\mathrm{HM}(I)$ such that, for all $s \in \mathrm{HM}(I)$, there exists $t \in T$ with $t \mid_q s$.

By the definition of T, it corresponds to a finite set $\mathcal{G} \subset I$ such that, for each $t \in T$, there exists $P \in \mathcal{G}$ with $\mathrm{HM}(P) = t$. Since $R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} \subset I$, we have that $\mathcal{G}$ is a Gröbner basis by Definition 5.1.

Next, we prove that $\mathcal{G}$ generates I. For each $P \in I$, we have that $P \xrightarrow[\mathcal{G}]{*} Q$ by Algorithm 4.1 such that Q is a normal form of P modulo $\mathcal{G}$. So

$$Q = P - \sum_{G \in \mathcal{G}} V_G G$$

for some $V_G \in R[\mathbf{x}][\boldsymbol{\partial}]$. Thus, $Q \in I$. If Q is nonzero, then Q is top-reducible modulo $\mathcal{G}$, a contradiction. Consequently, $Q = 0$. □

6 Standard representations of Ore polynomials

Let $F \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$. *A standard representation* of F with respect to a finite set $\mathcal{P}$ of $R[\mathbf{x}][\boldsymbol{\partial}]$ is a representation

$$F = \sum_{P \in \mathcal{P}} V_P P,$$

where $V_P \in R[\mathbf{x}][\boldsymbol{\partial}]$, such that $\mathrm{HT}(V_P P) \preceq \mathrm{HT}(F)$ or $V_P = 0$ for each $P \in \mathcal{P}$.

Lemma 6.1. *Let $\mathcal{P}$ be a finite set of $R[\mathbf{x}][\boldsymbol{\partial}]$, $F \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$, and assume that $F \xrightarrow[\mathcal{P}]{*} 0$. Then F has a standard representation with respect to $\mathcal{P}$.*

Proof. Suppose that $F \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$ such that $F \xrightarrow[\mathcal{P}]{*} 0$, but F does not have a standard representation. We may assume that F is minimal with this property in terms of the length [2, page 174] of the reduction chain. Since $F \xrightarrow[\mathcal{P}]{*} 0$, there exits $H \in R[\mathbf{x}][\boldsymbol{\partial}]$ with $F \xrightarrow[G]{} H$ for some $G \in \mathcal{P}$, say $H = F - mG$, where m is a monomial on $R[\mathbf{x}][\boldsymbol{\partial}]$. If $H = 0$, then $F = mG$ is a standard representation of F, a contradiction. Otherwise, H has a stardard representation

$$H = \sum_{i=1}^{k} V_i P_i$$

w.r.t. $\mathcal{P}$ by the minimality of F. Using the fact that $\mathrm{HT}(mG)$ is a term in F, it follows that

$$F = mG + \sum_{i=1}^{k} V_i P_i$$

is a stardard representation of F with respect to $\mathcal{P}$, a contradiction. □

Assume that $\mathcal{G}$ is a Gröbner basis of a left ideal I of $R[\mathbf{x}][\boldsymbol{\partial}]$. By the argument in Proposition 5.1, for each element $F \in I$, we have that $F \xrightarrow[\mathcal{G}]{*} 0$. Thus, F has a standard representation with respect to $\mathcal{G}$ by the above lemma. However, the converse is not true. The next lemma shows that if we add one more condition then it can be a criterion for Gröbner bases.

To this end, we need one more notation. For $s, t \in T$ with $s = \mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}}$ and $t = \mathbf{x}^{\mathbf{u}}\boldsymbol{\partial}^{\mathbf{v}}$, we define the quasi least common multiple of s and t to be $\mathbf{x}^{\mathbf{e}}\partial^{\mathbf{f}}$, where $e_i = \max(\alpha_i, u_i), f_i = \max(\beta_i, v_i)$ for $1 \le i \le n$, and denote it by $\mathrm{qlcm}(s,t)$. In other words, $\mathrm{qlcm}(s,t)$ is the least common multiple of s and t when they are treated as commutative terms.

Lemma 6.2. *Assume that $\mathcal{G}$ is a finite subset of $R[\mathbf{x}][\boldsymbol{\partial}]$ satisfying the following two conditions.*

(i) For all $G_1, G_2 \in \mathcal{G}$ there exists $H \in \mathcal{G}$ with

$$\mathrm{HT}(H) \mid_q \mathrm{qlcm}(\mathrm{HT}(G_1), \mathrm{HT}(G_2)) \quad \text{and} \quad \mathrm{HC}(H) \mid \gcd(\mathrm{HC}(G_1), \mathrm{HC}(G_2)).$$

(ii) Every $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G}$ has a standard representation w.r.t. $\mathcal{G}$.

Then $\mathcal{G}$ is a Gröbner basis.

Proof. It suffices to prove that for all $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} \setminus \{0\}$, F is top-reducible modulo $\mathcal{G}$. By (ii), we have

$$F = \sum_{i=1}^{k} V_i G_i$$

is a standard representation of F with respect to $\mathcal{G}$. Let $N \subset \{1, \ldots, k\}$ be the set of indices with the property that $\mathrm{HT}(F) = \mathrm{HT}(V_i G_i)$. Then

$$\mathrm{HM}(F) = \sum_{i \in N} \mathrm{HM}(V_i G_i),$$

and thus

$$\mathrm{qlcm}\{\mathrm{HT}(G_i) \mid i \in N\} \mid_q \mathrm{HT}(F) \quad \text{and} \quad \gcd\{\mathrm{HC}(G_i) \mid i \in N\} \mid \mathrm{HC}(F).$$

Note that the second divisibility relies on the fact that the two head coefficients $\mathrm{HC}(V_i G_i)$ and $\mathrm{HC}(V_i)\mathrm{HC}(G_i)$ are associated, which is stated in Proposition 3.2. By (i) and a straightforward induction on the cardinality of N, there exists $H \in \mathcal{G}$ such that $\mathrm{HT}(H)$ quasi-divides the above quasi lcm, and $\mathrm{HC}(H)$ divides the gcd. We have

$$\mathrm{HM}(H) \mid_q \mathrm{HM}(F),$$

and thus F is top-reducible modulo $\mathcal{G}$. □

Remark 6.1. *When R is a field, the first condition in the above lemma is trivial, because the gcd of head coefficients is always one, and, therefore, H can be chosen to be either G_1 or G_2.*

7 Buchberger's criterion

Definition 7.1. *For $i = 1, 2$, we let $G_i \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$ with $\mathrm{HC}(G_i) = a_i$ and $\mathrm{HT}(G_i) = t_i$. Moreover, let*

$$b_i a_i = \mathrm{lcm}(a_1, a_2) \text{ with } b_i \in R \quad \text{and} \quad \mathrm{HT}(s_i t_i) = \mathrm{lcm}(t_1, t_2) \text{ with } s_i \in T.$$

By Proposition 3.2, there exists an invertible element $r_i \in R$ such that $\mathrm{HC}(s_i G_i) = r_i a_i$. Then the S-polynomial *of G_1 and G_2 is defined as*

$$\mathrm{spol}(G_1, G_2) = b_1 r_1^{-1} s_1 G_1 - b_2 r_2^{-1} s_2 G_2$$

Now let $c_1, c_2 \in R$ such that $\gcd(a_1, a_2) = c_1 a_1 + c_2 a_2$. Then we define the G-polynomial *of G_1 and G_2 with respect to c_1 and c_2 as*

$$\mathrm{gpol}_{(c_1,c_2)}(G_1, G_2) = c_1 r_1^{-1} s_1 G_1 + c_2 r_2^{-1} s_2 G_2.$$

Strictly speaking, S-polynomials are only defined up to unit factors. As usual, there will be no harm in speaking of the S-polynomial. Nevertheless, the G-polynomial of $G_1, G_2 \in R[\mathbf{x}][\boldsymbol{\partial}]$ depends heavily on the choice of c_1 and c_2. We will from now on assume that for each pair $a_1, a_2 \in R \setminus \{0\}$, an arbitrary but fixed choice of a pair $c_1, c_2 \in R$ has been made such that $c_1 a_1 + c_2 a_2 = \gcd(a_1, a_2)$, and that G-polynomials are formed using this choice. The subscript (c_1, c_2) may then be suppressed.

Note that condition (i) of Lemma 6.2 is equivalent to the G-polynomial of G_1 and G_2 being top-reducible modulo $\mathcal{G}$.

Theorem 7.1. *Let $\mathcal{G}$ be a finite subset of $R[\mathbf{x}][\boldsymbol{\partial}]$. Assume that for all elements $G_1, G_2 \in \mathcal{G}$, $\mathrm{spol}(G_1, G_2)$ either equals zero or has a standard representation with respect to $\mathcal{G}$, and $\mathrm{gpol}(G_1, G_2)$ is top-reducible modulo $\mathcal{G}$. Then every nonzero polynomial $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G}$ has a standard representation.*

Proof. Suppose that $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} \setminus \{0\}$ does not have a standard representation with respect to $\mathcal{G}$. Let

$$F = \sum_{i=1}^{k} V_i G_i \tag{1}$$

with $V_i \in R[\mathbf{x}][\boldsymbol{\partial}]$ and $G_i \in \mathcal{G}$, $i = 1, \ldots, k$. We may assume that

$$s = \max\{\mathrm{HT}(V_i G_i) \mid 1 \leq i \leq k\}$$

is minimal among all such representations of F. Then $\mathrm{HT}(F) \prec s$. For a contradiction, we will produce a representation

$$F = \sum_{i=1}^{k'} V_i' G_i'$$

of the same kind such that $s' = \max\{\mathrm{HT}(V_i' G_i') \mid 1 \leq i \leq k'\} \prec s$. We proceed by induction on the number n_s of indices i with $s = \mathrm{HT}(V_i G_i)$.

First, $n_s = 1$ is impossible because $\mathrm{HT}(F) = s$ in this case. Let $n_s = 2$, without loss of generality, we may assume that $\mathrm{HT}(V_1 G_1) = \mathrm{HT}(V_2 G_2) = s$. This means that

$$s = \mathrm{HT}(t_1 \cdot \mathrm{HT}(G_1)) = \mathrm{HT}(t_2 \cdot \mathrm{HT}(G_2))$$

for some $t_1, t_2 \in T$. So $\mathrm{qlcm}(\mathrm{HT}(G_1), \mathrm{HT}(G_2))$ quasi-divides s, say

$$s = \mathrm{HT}(u \cdot \mathrm{qlcm}(\mathrm{HT}(G_1), \mathrm{HT}(G_2)))$$

with $u \in T$. Since $n_s = 2$, we have $\mathrm{HM}(V_1 G_1) + \mathrm{HM}(V_2 G_2) = 0$, and so

$$a_1 \cdot \mathrm{HC}(G_1) = -a_2 \cdot \mathrm{HC}(G_2)$$

for some $a_1, a_2 \in R \setminus \{0\}$. Moreover, a_i and $\mathrm{HC}(V_i)$ are associated for $i = 1, 2$. It follows that there exists $a \in R \setminus \{0\}$ with

$$a \cdot \mathrm{lcm}(\mathrm{HC}(G_1), \mathrm{HC}(G_2)) = a_1 \cdot \mathrm{HC}(G_1) = -a_2 \cdot \mathrm{HC}(G_2)$$

and it is straightforward to see that

$$V_1 G_1 + V_2 G_2 = au \cdot \mathrm{spol}(G_1, G_2) + W,$$

where $W \in R[\mathbf{x}][\boldsymbol{\partial}]$ with $\mathrm{HT}(W) \prec s$. By assumption, $\mathrm{spol}(G_1, G_2) = 0$, or else it has a standard representation

$$\mathrm{spol}(G_1, G_2) = \sum_{i=1}^{k''} V_i'' G_i''.$$

with respect to $\mathcal{G}$. Substituting $V_1 G_1 + V_2 G_2$ into (1), we obtain a representation

$$F = \sum_{i=3}^{k} V_i G_i + au \sum_{i=1}^{k''} V_i'' G_i'' + W, \tag{2}$$

where the second sum is missing if the S-polynomial was zero. The maximum of the head terms occuring in the first sum is less than s by our assumption $n_s = 2$; the maximum s'' of the head terms in the second sum (if any) satisfies

$$s'' \prec \mathrm{HT}(u \cdot \mathrm{qlcm}(\mathrm{HT}(G_1), \mathrm{HT}(G_2))) = s.$$

Together, we see that the maximum s' of the head terms in the representation (2) satisfies $s' \prec s$, which means that (2) is the s'-representation that we were looking for.

Now let $n_s > 2$. Without loss of generality, we may again assume that

$$\mathrm{HT}(V_1G_1) = \mathrm{HT}(V_2G_2) = s.$$

Moreover, we have

$$\mathrm{HC}(V_1G_1) = a_1 \cdot \mathrm{HC}(G_1) \quad \text{and} \quad \mathrm{HC}(V_2G_2) = a_2 \cdot \mathrm{HC}(G_2) \tag{3}$$

where, as before, a_1 and a_2 are associated to the head coefficients of V_1 and V_2, respectively. Top-reducibility of $\mathrm{gpol}(G_1, G_2)$ modulo $\mathcal{G}$ means that there exists an element $H \in \mathcal{G}$ with

$$\mathrm{HT}(H) \mid_q \mathrm{lcm}(\mathrm{HT}(G_1), \mathrm{HT}(G_2)) \quad \text{and} \quad \mathrm{HC}(H) \mid \gcd(\mathrm{HC}(G_1), \mathrm{HC}(G_2)).$$

Since s quasi-divides both $\mathrm{HT}(G_1)$ and $\mathrm{HT}(G_2)$, we may conclude that $\mathrm{HT}(H)$ divides s, and (3) shows that

$$\mathrm{HC}(H) \mid \mathrm{HC}(V_1G_1) \quad \text{and} \quad \mathrm{HC}(H) \mid \mathrm{HC}(V_2G_2).$$

We can thus find a term $v \in T$, and $b_1, b_2 \in R$ such that

$$\mathrm{HM}(V_1G_1) = \mathrm{HM}(b_1v \cdot \mathrm{HM}(H)) \quad \text{and} \quad \mathrm{HM}(V_2G_2) = \mathrm{HM}(b_2v \cdot \mathrm{HM}(H)). \tag{4}$$

We can now modify our representation (1) as follows:

$$F = (V_1G_1 - b_1vH) + (V_2G_2 - b_2vH) + \left((b_1 + b_2)vH + \sum_{i=3}^{k} V_iG_i \right).$$

Equation (4) tells us that the head terms of sums in the first bracket and second one are less than s. The number of summands with head term s in the third bracket is less or equal to $1 + (n_s - 2) = n_s - 1$. By the induction hypothesis, we have

$$F = \sum_{i=1}^{k'} V_i'G_i'$$

with $s' = \max\{\mathrm{HT}(V_i'G_i') \mid 1 \leq i \leq k'\} \prec s$. □

The next corollary is Buchberger's criterion for Ore polynomials, which reads exactly the same as that in commutative case.

Corollary 7.2. *Let $\mathcal{G}$ be a finite subset of $R[\mathbf{x}][\boldsymbol{\partial}]$, and assume that for all elements $G_1, G_2 \in \mathcal{G}$,*

$$\mathrm{spol}(G_1, G_2) \xrightarrow[\mathcal{G}]{*} 0$$

and $\mathrm{gpol}(G_1, G_2)$ *is top-reducible modulo $\mathcal{G}$. Then $\mathcal{G}$ is a Gröbner basis.*

Proof. By Lemma 6.1, all nonzero S-polynomials have standard representations. By the above theorem, it follows that every $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} \setminus \{0\}$ has a standard representation with respect to $\mathcal{G}$. As we have mentioned before, top-reducibility of $\mathrm{gpol}(G_1, G_2)$ modulo $\mathcal{G}$ means that condition (i) of Lemma 6.2 is satisfied. Hence, the lemma applies, and thus $\mathcal{G}$ is a Gröbner basis. □

8 Buchberger's algorithm

The following algorithm for the computation of Gröbner bases is a fairly obvious imitation of the Buchberger algorithm. It enlarges the input set by non-zero normal forms of S-polynomials and G-polynomials until all S-polynomials reduce to zero and all G-polynomial are top-reducible.

Algorithm 8.1. *Given a finite subset $\mathcal{P} \subset R[\mathbf{x}][\boldsymbol{\partial}]$, compute a finite subset $\mathcal{G} \subset R[\mathbf{x}][\boldsymbol{\partial}]$ such that $\mathcal{G}$ is a Gröbner basis in $R[\mathbf{x}][\boldsymbol{\partial}]$ and $R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{P} = R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G}$.*

```
G ← P
B ← {{P1, P2} | P1, P2 ∈ G, P1 ≠ P2}
D ← ∅
C ← B
while B ≠ ∅ do
    while C ≠ ∅ do
        select {P1, P2} from C
        C ← C \ {{P1, P2}}
        if there does not exist G ∈ G with HT(G) | lcm(HT(P1), HT(P2)),
        HC(G) | HC(P1) and HC(G) | HC(P2) then
            H ← gpol(P1, P2)
            H0 ← a normal form of H modulo G
            D ← D ∪ {{G, H0} | G ∈ G}
            G ← G ∪ {H0}
        end
    end
    select {P1, P2} from B
    B ← B \ {{P1, P2}}
    H ← spol(P1, P2)
    H0 ← a normal form of H modulo G
    if H0 ≠ 0 then
        D ← D ∪ {{G, H0} | G ∈ G}
        G ← G ∪ {H0}
        B ← B ∪ D; C ← D; D ← ∅
    end
end
```

Theorem 8.2. *Let R be a computable PID [2, Definition 10.13] and assume that the term order $\prec$ is decidable [2, page 178]. Then the above algorithm computes, for every finite subset $\mathcal{P}$ of $R[\mathbf{x}][\boldsymbol{\partial}]$, a Gröbner basis $\mathcal{G}$ in $R[\mathbf{x}][\boldsymbol{\partial}]$ such that $R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} = R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{P}$.*

Proof. We first prove the termination of the above algorithm. Suppose that the algorithm does not terminate for input $\mathcal{P}$. Then there are infinitely many polynomials to be added to $\mathcal{G}$. Assume that they are added sequently as H_1, H_2, $\ldots$,. Then, we have an infinite sequence

$$\mathrm{HM}(H_1), \mathrm{HM}(H_2), \ldots.$$

Since each H_i is in normal form modulo the $\mathcal{G}$ to which it will be added. It follows that

$$\mathrm{HM}(H_i) \nmid_q \mathrm{HM}(H_j)$$

for all $j > i$. By Proposition 2.1, there exists a finite set

$$D = \{\mathrm{HM}(H_{i_1}), \ldots, \mathrm{HM}(H_{i_\ell}\}$$

such that, for all $j \in \mathbb{Z}^+$, there exists $m \in D$ with $m \mid_q \mathrm{HM}(H_j)$. But this is impossible when j is greater than i_1, ..., i_ℓ, a contradiction.

When the algorithm terminates, both B and C are empty. It follows that all the S-polynomials formed by elements in $\mathcal{G}$ reduces to zero modulo $\mathcal{G}$ and all the G-polynomials formed by elements in $\mathcal{G}$ are top-reducible. By Corollary 7.2, $\mathcal{G}$ is a Gröbner basis. It is evident that $R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{P} = R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G}$. □

.

9 Elimination ideals

Let I be a left ideal in $R[\mathbf{x}][\boldsymbol{\partial}]$ and $\{U_1, \ldots, U_r\} \subset \{x_1, \ldots, x_n, \partial_1, \ldots, \partial_n\}$. We denote $\{U_1, \ldots, U_r\}$ and $\{x_1, \ldots, x_n, \partial_1, \ldots, \partial_n\}$ as $\{\mathbf{U}\}$ and $\{\mathbf{x}, \boldsymbol{\partial}\}$, respectively. It is evident to see that $I \cap R[\mathbf{U}]$ is a left ideal of the ring $R[\mathbf{U}]$. This ideal is called the *elimination ideal* of I with respect to $\{\mathbf{U}\}$, or $\mathbf{U}$ for short, and we will denote it by $I_{\mathbf{U}}$. As a matter of notation, we write $\mathrm{T}(\{\mathbf{U}\})$ or $\mathrm{T}(\mathbf{U})$ as the set of terms with respect to $\mathbf{U}$. Assume that a term order $\prec$ on T is given and $\{\mathbf{U}\} \subset \{\mathbf{x}, \boldsymbol{\partial}\}$. We write $\{\mathbf{U}\} \prec \{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\}$ if for each $s \in \mathrm{T}(\mathbf{U})$ and $1 \neq t \in \mathrm{T}(\{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\})$, $s \prec t$. We can always find a decidable term order $\prec$ on T satisfying $\{\mathbf{U}\} \prec \{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\}$: just take for $\prec$ a lexicographical order where every variable in $\{\mathbf{U}\}$ is less than every one in $\{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\}$.

Lemma 9.1. *Assume that $\{\mathbf{U}\} \subset \{\mathbf{x}, \boldsymbol{\partial}\}$ and $\prec$ is a term order that satisfies $\{\mathbf{U}\} \prec \{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\}$. Then the following claims hold:*

(i) If $s \in \mathrm{T}$ and $t \in \mathrm{T}(\mathbf{U})$ with $s \prec t$, then $s \in \mathrm{T}(\mathbf{U})$.

(ii) If $F \in R[\mathbf{U}]$ and $P, G \in R[\mathbf{x}][\boldsymbol{\partial}]$ with $F \underset{P}{\longrightarrow} G$, then $P, G \in R[\mathbf{U}]$.

(iii) If $F \in R[\mathbf{U}]$ and $\mathcal{G} \subset R[\mathbf{x}][\boldsymbol{\partial}]$, then every normal form of F modulo $\mathcal{G}$ lies in $R[\mathbf{U}]$.

Proof. (i) Assume for a contradiction that $s \notin \mathrm{T}(\mathbf{U})$. Then s can be divided by some $1 \neq v \in \mathrm{T}(\{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\})$. We obtain $s \prec t \prec v$, a contradiction.

(ii) Since $\mathrm{HT}(P)$ divides some $t \in \mathrm{T}(F)$, we must have $\mathrm{HT}(P) \in \mathrm{T}(\mathbf{U})$ and thus $\mathrm{T}(P) \subset \mathrm{T}(\mathbf{U})$ by (i), *i.e.*, $P \in R[\mathbf{U}]$. It follows from the definition of reduction that $G \in R[\mathbf{U}]$. Claim (iii) can be derived from (ii) by induction on the length of reduction chains. □

The next proposition provides a way to compute elimination ideals.

Proposition 9.2. *Let I be a left ideal of $R[\mathbf{x}][\boldsymbol{\partial}]$ and $\{\mathbf{U}\} \subset \{\mathbf{x}, \boldsymbol{\partial}\}$. Assume that $\prec$ is a term order that satisfies $\{\mathbf{U}\} \prec \{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\}$, and $\mathcal{G}$ is Gröbner basis of I with respect to $\prec$. Then $\mathcal{G} \cap R[\mathbf{U}]$ is a Gröbner basis of the elimination ideal $I_{\mathbf{U}}$.*

Proof. Set $\mathcal{G}' = \mathcal{G} \cap R[\mathbf{U}]$. We show that every $0 \neq F \in I_{\mathbf{U}}$ is reducible modulo $\mathcal{G}'$. Let $0 \neq F \in I_{\mathbf{U}}$. Then $F \in I$, and thus F is reducible modulo $\mathcal{G}$, say $F \underset{G}{\longrightarrow} H$ with $G \in \mathcal{G}$. By Lemma 9.1 (ii), $G \in \mathcal{G}'$, and thus F is reducible modulo $\mathcal{G}'$. □

10 Saturation with respect to a constant

Let I be a left ideal in $R[\mathbf{x}][\boldsymbol{\partial}]$, and $c \in R$. The saturation of I with respect to c is defined to be

$$I : c^\infty = \left\{ P \in R[\mathbf{x}][\boldsymbol{\partial}] \mid c^i P \in I \text{ for some } i \in \mathbb{N} \right\}.$$

Since c is a constant with respect to σ_i and δ_i, c is in the center of $R[\mathbf{x}][\boldsymbol{\partial}]$. It follows that the saturation $I : c^\infty$ is a left ideal A basis of the saturation ideal can be computed in the same way as in the commutative case.

To this end, we need to introduce some new indeterminates. Let σ_y be the identity map of $R[\mathbf{x}, y]$, where y is a new indeterminate. Let δ_y be the σ_y-derivation that maps everything in $R[\mathbf{x}, y]$ to zero. Then one can extend the ring $R[\mathbf{x}][\boldsymbol{\partial}]$ to $R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$. Moreover, $R[y][\partial_y]$ lies in the center of the extended ring. For $r \in R$, one can define an evaluation map

$$\begin{array}{cccc} \phi_r : & R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y] & \longrightarrow & R[\mathbf{x}][\boldsymbol{\partial}] \\ & \sum_{i=0}^{\ell} \sum_{j=0}^{m} f_{ij} y^i \partial_y^j & \mapsto & \sum_{i=0}^{\ell} f_{i0} r^i, \end{array}$$

where $f_{ij} \in R[\mathbf{x}][\boldsymbol{\partial}]$. Since $R[y][\partial_y]$ is contained in the center of $R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$, the map ϕ_r is a ring homomorphism.

Proposition 10.1. *Let I be a left ideal of $R[\mathbf{x}][\boldsymbol{\partial}]$ and c be a non-zero element in R. Assume that J is a left ideal*

$$R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y] \cdot (I \cup \{1 - cy\}),$$

Then $I : c^\infty = J \cap R[\mathbf{x}][\boldsymbol{\partial}]$.

Proof. Let $J_{\mathbf{x},\boldsymbol{\partial}} = J \cap R[\mathbf{x}][\boldsymbol{\partial}]$. If $G \in J_{\mathbf{x},\boldsymbol{\partial}}$, then

$$G = Q_1 P + Q_2 (1 - cy) \tag{5}$$

with $Q_1, Q_2 \in R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$ and $P \in I$. Temporarily passing to the extended ring $Q_R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$ of $R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$, we may apply the evaluation homomorphism $\phi_{1/c}$ to (5) and then multiply the resulted equation by c^d, where $d = \deg_y(Q_1)$. We thus obtain $c^d G = QP$ with Q being in $R[\mathbf{x}][\boldsymbol{\partial}]$. Consequently, $J_{\mathbf{x},\boldsymbol{\partial}} \subset I : c^\infty$.

Conversely, let $G \in I : c^\infty$, say $c^d G \in I$. Then $G \in R[\mathbf{x}][\boldsymbol{\partial}]$ and $c^d G \in J$. Since $1 - cy$ belongs to J,

$$1 - (cy)^d = (1 + cy + (cy)^2 + \cdots + (cy)^{d-1})(1 - cy) \in J$$

Since y and c commute with every element of $R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$,

$$\left(1 - (cy)^d\right) G = G \left(1 - (cy)^d\right) \in J.$$

Again, $(cy)^d G = y^d (c^d G) \in J$ because $c^d G \in J$. It follows that

$$G = \left(1 - (cy)^d\right) G + (cy)^d G \in J.$$

Thus, $G \in J_{\mathbf{x},\boldsymbol{\partial}}$. □

By the above proposition, a Gröbner basis of $I : c^\infty$ with $c \in R$ can be computed by elimination given in the previous section.

References

[1] F. Chyzak and B. Salvy. Non-commutative elimination in Ore algebras proves multivariate identities. *J. Symb. Comput.* , 26:187–227, 1998.

[2] T. Becker and V. Weispfenning. *Gröbner Bases, A Computational Approach to Commutative Algebra.* Springer-Verlag, New York, USA, 1993.