

Gröbner Bases in Difference-Differential Modules

Franz Winkler

RISC-Linz
J. Kepler University
Linz, Austria

This is joint work with M. Zhou of Beihang University in Beijing.

The work has been supported by the Austrian FWF project P16357-N04 and by the National Key Basic Research Project 2005CB321902 of China, while the first author spent a research year at RISC-Linz.

1. Introduction

- We extend the theory of Gröbner bases to difference-differential modules. The main purpose of this paper is to give a new approach to the computation of a Gröbner basis for an ideal in (or a module over) the ring of difference-differential operators.
- To this aim we introduce the concept of generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$ and on difference-differential modules.

Related work

- The theory of GB has been generalized by many authors to non-commutative domains, especially to modules over various rings of differential operators. Galligo (1985) first gave the Gröbner basis algorithm for the Weyl algebra $\mathcal{A}_n(K)$ of partial differential operators with coefficients in a polynomial ring over the field K .
- Mora (1986) generalized the concept of Gröbner basis to non-commutative free algebras.
- Kondrateva et al. (1998) described the Gröbner basis method for differential and difference modules.
- Noumi (1988) and Takayama (1998) formulated Gröbner bases in R_n , the ring of differential operators with rational function coefficients.
- Oaku and Shimoyama (1994) treated D_0 , the ring of differential operators with power series coefficients.

- Insa and Pauer (1998) presented a basic theory of Gröbner bases for differential operators with coefficients in a commutative Noetherian ring.
- Pauer and Unterkircher (1999) considered Gröbner bases in Laurent polynomial rings, but their approach is limited to the commutative case.
- Levin (2000) introduced characteristic sets for free modules over rings of difference-differential operators. Such characteristic sets depend on a specific order on $\mathbb{N}^m \times \mathbb{Z}^n$. But this order is not a term order in the sense of the theory of Gröbner bases.

Difference-differential modules

A ring is always an associative ring with 1. A module over a ring A is a unitary left A -module.

Def.1.1: Let R be a commutative Noetherian ring. Let $\Delta = \{\delta_1, \dots, \delta_m\}$ be a set of derivations on R and $\Sigma = \{\sigma_1, \dots, \sigma_n\}$ a set of automorphisms of R , such that $\alpha(x) \in R$ and $\alpha(\beta(x)) = \beta(\alpha(x))$ for any $\alpha, \beta \in \Delta \cup \Sigma$ and $x \in R$. Then R is called a *difference-differential ring* with the basic set of derivations Δ and the basic set of automorphisms Σ , or shortly a *Δ - Σ -ring*; if R is a field, then it is called a *Δ - Σ -field*.

Ex.1.1: Let $R = K[x_1, \dots, x_n]$ for a field K , $\delta_i = \partial/\partial x_i$ and σ_i the automorphism which maps x_i to $x_i - 1$. Then R is a Δ - Σ -ring for $\Delta = \{\delta_1, \dots, \delta_n\}$ and $\Sigma = \{\sigma_1, \dots, \sigma_n\}$.

Def.1.2: Let R be a Δ - Σ -ring and Λ be the free commutative semigroup of words over Δ and $\tilde{\Sigma}$ (containing the elements of Σ and their inverses).

Then an expression of the form

$$\sum_{\lambda \in \Lambda} a_{\lambda} \lambda, \quad (1.2)$$

where $a_{\lambda} \in R$ for all $\lambda \in \Lambda$ and only finitely many coefficients a_{λ} are different from zero, is called a *difference-differential operator* (or shortly a *Δ - Σ -operator*) over R .

Two Δ - Σ -operators $\sum_{\lambda \in \Lambda} a_{\lambda} \lambda$ and $\sum_{\lambda \in \Lambda} b_{\lambda} \lambda$ are equal if and only if $a_{\lambda} = b_{\lambda}$ for all $\lambda \in \Lambda$.

The set of all Δ - Σ -operators over a Δ - Σ -ring R is a ring with the following fundamental relations

$$\begin{aligned}
\sum_{\lambda \in \Lambda} a_\lambda \lambda + \sum_{\lambda \in \Lambda} b_\lambda \lambda &= \sum_{\lambda \in \Lambda} (a_\lambda + b_\lambda) \lambda, \\
a(\sum_{\lambda \in \Lambda} a_\lambda \lambda) &= \sum_{\lambda \in \Lambda} (aa_\lambda) \lambda, \\
(\sum_{\lambda \in \Lambda} a_\lambda \lambda) \mu &= \sum_{\lambda \in \Lambda} a_\lambda (\lambda \mu), \\
\delta a &= a\delta + \delta(a), & \sigma a &= \sigma(a)\sigma,
\end{aligned} \tag{1.3}$$

for all $a_\lambda, b_\lambda \in R$, $\lambda, \mu \in \Lambda$, $a \in R$, $\delta \in \Delta$, $\sigma \in \tilde{\Sigma}$. Note that the elements in Δ and $\tilde{\Sigma}$ do not commute with the elements in R , and therefore the terms $\lambda \in \Lambda$ do not commute with the coefficients $a_\lambda \in R$.

Def.1.3: The ring of all Δ - Σ -operators over a Δ - Σ -ring R is called the *ring of difference-differential operators* (or shortly the *ring of Δ - Σ -operators*) over R . It will be denoted by D .

A left D -module M is called a *difference-differential module* (or a *Δ - Σ -module*). If M is finitely generated as a left D -module, then M is called a finitely generated Δ - Σ -module.

When $\Sigma = \emptyset$, D will be the ring of differential operators $R[\delta_1, \dots, \delta_m]$.

If the coefficient ring R is the polynomial ring in x_1, \dots, x_m over a field K and $\delta_i = \partial/\partial x_i$ for $1 \leq i \leq m$, then D will be the Weyl algebra $\mathcal{A}_m(K)$. So Δ - Σ -modules are generalizations of modules over rings of differential operators.

But in the ring of Δ - Σ -operators the terms are of the form (1.1) and the exponent in $\sigma_1, \dots, \sigma_n$ is $(l_1, \dots, l_n) \in \mathbb{Z}^n$. The notion of term order, as commonly used in Gröbner basis theory, is no longer valid. We need to generalize the concept of term order.

2. Generalized term order

Def.2.1: Let \mathbb{Z}^n be the union of finitely many subsets \mathbb{Z}_j^n , i.e. $\mathbb{Z}^n = \bigcup_{j=1}^k \mathbb{Z}_j^n$, where \mathbb{Z}_j^n , $j = 1, \dots, k$, satisfy the following conditions:

- (i) $(0, \dots, 0) \in \mathbb{Z}_j^n$, and \mathbb{Z}_j^n does not contain any pair of invertible elements $c = (c_1, \dots, c_n) \neq 0$ and $-c = (-c_1, \dots, -c_n)$,
- (ii) \mathbb{Z}_j^n is isomorphic to \mathbb{N}^n as a semigroup,
- (iii) the group generated by \mathbb{Z}_j^n is \mathbb{Z}^n .

Then $\{\mathbb{Z}_j^n \mid j = 1, \dots, k\}$ is called an *orthant decomposition* of \mathbb{Z}^n and \mathbb{Z}_j^n is called the *j-th orthant* of the decomposition.

Ex.2.1: Let $\{\mathbb{Z}_1^n, \dots, \mathbb{Z}_{2^n}^n\}$ be all distinct Cartesian products of n sets each of which is either \mathbb{Z}_+ or \mathbb{Z}_- . Then this is an orthant decomposition of \mathbb{Z}^n . The set of generators of \mathbb{Z}_j^n as a semigroup is

$$\{(c_1, 0, \dots, 0), (0, c_2, 0, \dots, 0), \dots, (0, \dots, 0, c_n)\},$$

where c_j is either 1 or -1 , $j = 1, \dots, n$. We call this decomposition the *canonical orthant decomposition* of \mathbb{Z}^n .

Ex.2.2: The decomposition $\mathbb{Z}^2 = \mathbb{Z}_0^2 \cup \mathbb{Z}_1^2 \cup \mathbb{Z}_2^2$, where

$$\mathbb{Z}_0^2 = \{(a, b) | a \geq 0, b \geq 0, a, b \in \mathbb{Z}\},$$

$$\mathbb{Z}_1^2 = \{(a, b) | a \leq 0, b \geq a, a, b \in \mathbb{Z}\},$$

$$\mathbb{Z}_2^2 = \{(a, b) | b \leq 0, a \geq b, a, b \in \mathbb{Z}\},$$

is an orthant decomposition of \mathbb{Z}^2 .

Def.2.2: Let $\{\mathbb{Z}_j^n \mid j = 1, \dots, k\}$ be an orthant decomposition of \mathbb{Z}^n . Then $a = (k_1, \dots, k_m, l_1, \dots, l_n)$ and $b = (r_1, \dots, r_m, s_1, \dots, s_n)$ of $\mathbb{N}^m \times \mathbb{Z}^n$ are called *similar* elements, if the n -tuples (l_1, \dots, l_n) and (s_1, \dots, s_n) are in the same orthant \mathbb{Z}_j^n of \mathbb{Z}^n .

Def.2.3: Let $\{\mathbb{Z}_j^n \mid j = 1, \dots, k\}$ be an orthant decomposition of \mathbb{Z}^n . A total order \prec on $\mathbb{N}^m \times \mathbb{Z}^n$ is called a *generalized term order* on $\mathbb{N}^m \times \mathbb{Z}^n$ w.r.t. the decomposition, if the following conditions hold:

- (i) $(0, \dots, 0)$ is the smallest element in $\mathbb{N}^m \times \mathbb{Z}^n$,
- (ii) if $a \prec b$, then $a + c \prec b + c$ for any c similar to b .

Ex.2.3: (a) Let $\{\mathbb{Z}_j^n \mid j = 1, \dots, 2^n\}$ be the canonical orthant decomposition of \mathbb{Z}^n defined in Example 2.1. For every $a = (k_1, \dots, k_m, l_1, \dots, l_n) \in \mathbb{N}^m \times \mathbb{Z}^n$ let

$$|a| = k_1 + \dots + k_m + |l_1| + \dots + |l_n|.$$

For two elements $a = (k_1, \dots, k_m, l_1, \dots, l_n)$ and $b = (r_1, \dots, r_m, s_1, \dots, s_n)$ of $\mathbb{N}^m \times \mathbb{Z}^n$ define $a \prec b$ if and only if the $(1 + m + n)$ -tuple $(|a|, k_1, \dots, k_m, l_1, \dots, l_n)$ is smaller than $(|b|, r_1, \dots, r_m, s_1, \dots, s_n)$ w.r.t. the lexicographic order on $\mathbb{N}^{m+1} \times \mathbb{Z}^n$. Then " \prec " is a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$.

(b) Let the orthant decomposition of \mathbb{Z}^n be as in Example 2.1. For every $a = (k_1, \dots, k_m, l_1, \dots, l_n) \in \mathbb{N}^m \times \mathbb{Z}^n$ let

$$|a|_1 = \sum_{j=1}^m k_j, \quad |a|_2 = \sum_{j=1}^n |l_j|.$$

For two elements $a = (k_1, \dots, k_m, l_1, \dots, l_n)$ and $b = (r_1, \dots, r_m, s_1, \dots, s_n)$ of $\mathbb{N}^m \times \mathbb{Z}^n$ define $a \prec b$ if and only if the $(2 + m + 2n)$ -tuple

$$(|a|_1, |a|_2, k_1, \dots, k_m, |l_1|, \dots, |l_n|, l_1, \dots, l_n)$$

is lexicographically smaller than

$$(|b|_1, |b|_2, r_1, \dots, r_m, |s_1|, \dots, |s_n|, s_1, \dots, s_n).$$

Then " \prec " is a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$.

(c) Let $\{\mathbb{Z}_j^{(n)}, j = 0, 1, \dots, n\}$ be the orthant decomposition of \mathbb{Z}^n defined in Example 2.2. For every element $a = (k_1, \dots, k_m, l_1, \dots, l_n) \in \mathbb{N}^m \times \mathbb{Z}^n$ let

$$\|a\| = -\min\{0, l_1, \dots, l_n\} .$$

For two elements $a = (k_1, \dots, k_m, l_1, \dots, l_n)$ and $b = (r_1, \dots, r_m, s_1, \dots, s_n)$ of $\mathbb{N}^m \times \mathbb{Z}^n$ define $a \prec b$ if and only if the $(1 + m + n)$ -tuple $(\|a\|, k_1, \dots, k_m, l_1, \dots, l_n)$ is lexicographically smaller than $(\|b\|, r_1, \dots, r_m, s_1, \dots, s_n)$. Then " \prec " is a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$.

In order to investigate Δ - Σ -modules, we need to extend the notion of generalized term order to $\mathbb{N}^m \times \mathbb{Z}^n \times E$, where $E = \{e_1, \dots, e_q\}$ is a set of generators of a module.

Def. 2.4: Let $\{\mathbb{Z}_j^n \mid j = 1, \dots, k\}$ be an orthant decomposition of \mathbb{Z}^n . Let $E = \{e_1, \dots, e_q\}$ be a set of q distinct elements. A total order \prec on $\mathbb{N}^m \times \mathbb{Z}^n \times E$ is called a *generalized term order* on $\mathbb{N}^m \times \mathbb{Z}^n \times E$ w.r.t. the decomposition, if the following conditions hold:

- (i) $(0, \dots, 0, e_i)$ is the smallest element in $\mathbb{N}^m \times \mathbb{Z}^n \times \{e_i\}$ for any $e_i \in E$,
- (ii) if $(a, e_i) \prec (b, e_j)$, then $(a + c, e_i) \prec (b + c, e_j)$ for any c similar to b .

Ex.2.4: Let the orthant decomposition of \mathbb{Z}^n and the generalized term order " \prec " on $\mathbb{N}^m \times \mathbb{Z}^n$ be as in Example 2.3(b). Given an order " \prec_E " on $E = \{e_1, \dots, e_q\}$, for two elements

$$\begin{aligned} (a, e_i) &= (k_1, \dots, k_m, l_1, \dots, l_n, e_i) & \text{and} \\ (b, e_j) &= (r_1, \dots, r_m, s_1, \dots, s_n, e_j) \end{aligned}$$

of $\mathbb{N}^m \times \mathbb{Z}^n \times E$ define:

$$\begin{aligned} (a, e_i) \prec_1 (b, e_j) &\iff a \prec b \quad \text{or} \quad (a = b \quad \text{and} \quad e_i \prec_E e_j); \\ (a, e_i) \prec_2 (b, e_j) &\iff e_i \prec_E e_j \quad \text{or} \quad (e_i = e_j \quad \text{and} \quad a \prec b); \\ (a, e_i) \prec_3 (b, e_j) &\iff \\ &(|a|_1, |a|_2, e_i, k_1, \dots, k_m, |l_1|, \dots, |l_n|, l_1, \dots, l_n) \\ &< (|b|_1, |b|_2, e_j, r_1, \dots, r_m, |s_1|, \dots, |s_n|, s_1, \dots, s_n) \\ &\text{in lexicographic order.} \end{aligned}$$

Then " \prec_1 ", " \prec_2 ", " \prec_3 " are generalized term orders on $\mathbb{N}^m \times \mathbb{Z}^n \times E$.

Lemma 2.1: Let $\{\mathbb{Z}_j^n \mid j = 1, \dots, k\}$ be an orthant decomposition of \mathbb{Z}^n and " \prec " be a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$ with respect to the orthant decomposition.

- (a) Every strictly descending sequence in $\mathbb{N}^m \times \mathbb{Z}^n$ is finite. In particular, every subset of $\mathbb{N}^m \times \mathbb{Z}^n$ contains a smallest element.
- (b) Every strictly descending sequence in $\mathbb{N}^m \times \mathbb{Z}^n \times E$ is finite. In particular, every subset of $\mathbb{N}^m \times \mathbb{Z}^n \times E$ contains a smallest element.

3. Gröbner bases in finitely generated difference-differential modules

Let K be a Δ - Σ -field and D be the ring of Δ - Σ -operators over K , and let F be a finitely generated free D -module (i.e. a finitely generated free difference-differential-module) with a set of free generators $E = \{e_1, \dots, e_q\}$. Then F can be considered as a K -vector space generated by the set of all elements of the form λe_i , where $\lambda \in \Lambda$ and $i = 1, \dots, q$. This set will be denoted by ΛE and its elements will be called “terms” of F . If “ \prec ” is a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n \times E$ then “ \prec ” obviously induces an order on ΛE , which we also call a generalized term order.

Every element $f \in F$ has a unique representation as a linear combination of terms

$$f = a_1 \lambda_1 e_{j_1} + \dots + a_d \lambda_d e_{j_d} \quad (3.1)$$

for some nonzero elements $a_i \in K$ ($i = 1, \dots, d$) and some distinct elements $\lambda_1 e_{j_1}, \dots, \lambda_d e_{j_d} \in \Lambda E$.

Reduction in difference-differential modules

Def.3.1: Let

$$\lambda_1 = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n} \quad \text{and} \quad \lambda_2 = \delta_1^{r_1} \cdots \delta_m^{r_m} \alpha_1^{s_1} \cdots \alpha_n^{s_n}$$

be two elements in Λ . If they are similar and $r_\mu \leq k_\mu$, $|s_\nu| \leq |l_\nu|$ for $\mu = 1, \dots, m$, $\nu = 1, \dots, n$, then λ_1 is called a *multiple* of λ_2 and this relation is denoted by $\lambda_2 | \lambda_1$. If $\lambda_2 | \lambda_1$ and $i = j$ then $u = \lambda_1 e_i$ is called a *multiple* of $v = \lambda_2 e_j$ and this relation is denoted by $v | u$.

Def. 3.2: Let \prec be a generalized term order on ΛE , $f \in F$ be of the form (3.1). Then

$$\text{lt}(f) = \max_{\prec} \{\lambda_i e_{j_i} | i = 1, \dots, d\}$$

is called the *leading term* of f . If $\lambda_i e_{j_i} = \text{lt}(f)$, then a_i is called the *leading coefficient* of f , denoted by $\text{lc}(f)$.

Lemma 3.1: Let $\lambda \in \Lambda$, $a \in K$, and \prec be a generalized term order on $\Lambda \subseteq D$. Then

$$\lambda a = a'\lambda + \xi,$$

where $a' = \sigma(a)$ for some $\sigma \in \Sigma^*$. If $a \neq 0$ then also $a' \neq 0$. Furthermore, $\xi \in D$ with $\text{lt}(\xi) \prec \lambda$ and all terms of ξ are similar to λ .

Lemma 3.2: Let F be a finitely generated free D -module and $0 \neq f \in F$. Then the following hold:

- (i) If $\lambda \in \Lambda$, then $\text{lt}(\lambda f) = \lambda \cdot u$ for a unique term u of f .
- (ii) If $\text{lt}(f) \in \Lambda_j E$ then for any $\lambda \in \Lambda_j$

$$\text{lt}(\lambda f) = \lambda \cdot \text{lt}(f) \in \Lambda_j E.$$

Lemma 3.3: Let F be a finitely generated free D -module and $0 \neq f \in F$. Then for each j , there exists some $\lambda \in \Lambda$ and a unique term u_j of f such that

$$\text{lt}(\lambda f) = \lambda \cdot u_j \in \Lambda_j E.$$

We will write $lt_j(f)$ for this term u_j .

Proposition 3.1: Let $0 \neq f \in F$, $0 \neq h \in D$. Then $\text{lt}(hf) = \max_{\prec} \{\lambda_i u_k\}$ where λ_i are terms of h and u_k are terms of f . Therefore $\text{lt}(hf) = \lambda \cdot u$ for a unique term λ of h and a unique term u of f .

Now we are ready to introduce the concept of “reduction”, which is central in the theory of Gröbner bases.

Theorem 3.1: Let $f_1, \dots, f_p \in F \setminus \{0\}$. Then every $g \in F$ can be represented as

$$g = h_1 f_1 + \dots + h_p f_p + r \tag{3.2}$$

for some elements $h_1, \dots, h_p \in D$ and $r \in F$ such that

- (i) $h_i = 0$ or $\text{lt}(h_i f_i) \preceq \text{lt}(g)$ for $i = 1, \dots, p$,
- (ii) $r = 0$ or $\text{lt}(r)$ is not a multiple of any $\text{lt}(\lambda f_i)$ for $\lambda \in \Lambda$, $i = 1, \dots, p$.

Def.3.4: Let $f_1, \dots, f_p \in F \setminus \{0\}$, $g \in F$. Suppose that equation (3.2) in Theorem 3.1 holds and the conditions (i), (ii) are satisfied. If $r \neq g$ we say g can be *reduced* by $\{f_1, \dots, f_p\}$ to r . In this case we have $\text{lt}(r) \prec \text{lt}(g)$ by the proof of Theorem 3.1. In the case of $r = g$ and $h_i = 0$ for $i = 1, \dots, p$, we say that g is *reduced* w.r.t. $\{f_1, \dots, f_p\}$.

Note that we are using the notion of reduction as head-reduction.

Ex.3.1: Let $K = \mathbb{Q}(x_1, x_2)$, $D = K[\delta_1, \delta_2, \alpha, \alpha^{-1}]$, where δ_1, δ_2 are the partial derivatives w.r.t. x_1, x_2 , respectively, and α is an automorphism of K . So D is the $\{\delta_1, \delta_2\} - \{\alpha\}$ -ring over the coefficient field $\mathbb{Q}(x_1, x_2)$. Choose the generalized term order on $\mathbb{N}^2 \times \mathbb{Z}$ as in Example 2.3 (a), i.e.

$$u = \delta_1^{k_1} \delta_2^{k_2} \alpha^l \prec v = \delta_1^{r_1} \delta_2^{r_2} \alpha^s \iff (\|u\|, k_1, k_2, l) <_{lex} (\|v\|, r_1, r_2, s),$$

where $\|u\| = k_1 + k_2 + |l|$. Let

$$g = \delta_1 \alpha^{-2} + \delta_2 \alpha^2, \quad f = \delta_1 \alpha^{-1} + \alpha.$$

Then

$$g = \delta_1 \alpha^{-2} + \delta_2 \alpha^2 = \alpha^{-1}(\delta_1 \alpha^{-1} + \alpha) + (\delta_2 \alpha^2 - 1) = \alpha^{-1} f + r_1.$$

Although $\text{lt}(r_1) = \delta_2 \alpha^2$ is not any multiple of $\text{lt}(f) = \delta_1 \alpha^{-1}$, we can find $\lambda = \delta_2 \alpha$ such that $\text{lt}(r_1) = \text{lt}(\lambda f) = \text{lt}(\delta_1 \delta_2 + \delta_2 \alpha^2)$. Therefore

$$g = \alpha^{-1} f + \delta_2 \alpha f + (-\delta_1 \delta_2 - 1) = (\alpha^{-1} + \delta_2 \alpha) f + r_2$$

Now r_2 satisfies the condition (ii) in Theorem 3.1. So g is reduced by f to r_2 .

Gröbner bases

Def. 3.5: Let W be a submodule of the finitely generated free D -module F and \prec be a generalized term order on ΛE . Let $G = \{g_1, \dots, g_p\} \subseteq W \setminus \{0\}$. Then G is called a *Gröbner basis* of W (w.r.t. the generalized term order \prec) if and only if for every $f \in W \setminus \{0\}$, $\text{lt}(f)$ is a multiple of $\text{lt}(\lambda g_j)$ for some $\lambda \in \Lambda$, $g_j \in G$. If every element of G is reduced with respect to the other elements of G , then G is called a *reduced Gröbner basis* of W .

Proposition 3.2: Let G be a finite subset of $W \setminus \{0\}$. The following assertions hold:

- (i) G is a Gröbner basis of W if and only if every $f \in W$ can be reduced by G to 0. So a Gröbner basis of W generates the D -module W .
- (ii) If G is a Gröbner basis of W , $f \in F$, then $f \in W$ if and only if f can be reduced by G to 0.
- (iii) If G is a Gröbner basis of W , then $f \in W$ is reduced w.r.t. G if and only if $f = 0$.

Def. 3.6: Let F be a finitely generated free D -module and $f, g \in F \setminus \{0\}$. For every Λ_j let $V(j, f, g)$ be a finite system of generators of the $K[\Lambda_j]$ -module

$$\begin{aligned} & {}_{K[\Lambda_j]} \langle \text{lt}(\lambda f) \mid \text{lt}(\lambda f) \in \Lambda_j E, \lambda \in \Lambda \rangle \cap \\ & {}_{K[\Lambda_j]} \langle \text{lt}(\eta g) \mid \text{lt}(\eta g) \in \Lambda_j E, \eta \in \Lambda \rangle. \end{aligned}$$

Then for every generator $v \in V(j, f, g)$,

$$S(j, f, g, v) = \frac{v}{\text{lt}_j(f)} \frac{f}{\text{lc}_j(f)} - \frac{v}{\text{lt}_j(g)} \frac{g}{\text{lc}_j(g)}$$

is called an *S-polynomial* of f and g with respect to j and v .

The $K[\Lambda_j]$ -module considered in Definition 3.6 is a “monomial module”, i.e. it is generated by elements containing only one term. Such a module always has a finite “monomial basis”, i.e. every basis element contains only one term. In the following we assume that $V(j, f, g)$ is such a finite monomial basis.

The computation of $V(j, f, g)$ involves the generalized term order on ΛE . Pauer and Unterkircher (1999) have investigated $V(j, f, g)$ for commutative Laurent polynomial rings and have given algorithms for some important cases. Their results are still valid for difference-differential modules.

Ex. 3.3: Let $F = D = K[\delta_1, \delta_2, \alpha_1, \alpha_1^{-1}, \alpha_2, \alpha_2^{-1}]$ and $K = \mathbb{Q}(x_1, x_2)$, where δ_1, δ_2 are the partial derivatives w.r.t. x_1 and x_2 , respectively, and α_1, α_2 are two automorphism on K . Choose the generalized term order on $\mathbb{N}^2 \times \mathbb{Z}^2$ as in Example 2.3(c), i.e.

$$u = \delta_1^{k_1} \delta_2^{k_2} \alpha_1^{l_1} \alpha_2^{l_2} \prec v = \delta_1^{r_1} \delta_2^{r_2} \alpha_1^{s_1} \alpha_2^{s_2}$$

$$\iff (\|u\|, k_1, k_2, l_1, l_2) <_{lex} (\|v\|, r_1, r_2, s_1, s_2),$$

where $\|u\| = -\min(0, l_1, l_2)$.

Let

$$f = \alpha_1^{-2} - \delta_2, \quad g = \delta_1 + \alpha_2^4.$$

Note that the orthants of Λ are $\Lambda_0, \Lambda_1, \Lambda_2$ as described in Example 2.2 for $n = 2$. One can see that

$$\{\lambda \in \Lambda \mid \text{lt}(\lambda f) \in \Lambda_0\} = \Lambda_0 \alpha_1^2, \quad \{\eta \in \Lambda \mid \text{lt}(\eta g) \in \Lambda_0\} = \Lambda_0$$

and

$$\{\text{lt}(\lambda f) \in \Lambda_0 \mid \lambda \in \Lambda\} = \Lambda_0 \delta_2 \alpha_1^2,$$

$$\{\text{lt}(\eta g) \in \Lambda_0 \mid \eta \in \Lambda\} = \Lambda_0 \delta_1.$$

Then $V(0, f, g) = \{v_0\} = \{\delta_1 \delta_2 \alpha_1^2\}$ and by Definition 3.6,

$$S(0, f, g, v_0) = \delta_1 \alpha_1^2 f + \delta_2 \alpha_1^2 g = \delta_1 + \delta_2 \alpha_1^2 \alpha_2^4.$$

Similarly we have

$$\{\lambda \in \Lambda \mid \text{lt}(\lambda f) \in \Lambda_1\} = \Lambda_1 \alpha_1, \quad \{\eta \in \Lambda \mid \text{lt}(\eta g) \in \Lambda_1\} = \Lambda_1$$

and

$$\{\text{lt}(\lambda f) \in \Lambda_1 \mid \lambda \in \Lambda\} = \Lambda_1 \alpha_1^{-1},$$

$$\{\text{lt}(\eta g) \in \Lambda_1 \mid \eta \in \Lambda\} = \Lambda_1 \delta_1.$$

Then $V(1, f, g) = \{v_1\} = \{\delta_1 \alpha_1^{-1}\}$ and

$$S(1, f, g, v_1) = \delta_1 \alpha_1 f - \alpha_1^{-1} g = -\delta_1 \delta_2 \alpha_1 - \alpha_1^{-1} \alpha_2^4.$$

Finally,

$$\begin{aligned}\{\lambda \in \Lambda \mid \text{lt}(\lambda f) \in \Lambda_2\} &= \Lambda_2 \alpha_1^2, \\ \{\eta \in \Lambda \mid \text{lt}(\eta g) \in \Lambda_2\} &= \Lambda_2 \alpha_2^{-1}, \\ \{\text{lt}(\lambda f) \in \Lambda_2 \mid \lambda \in \Lambda\} &= \Lambda_2 \delta_2 \alpha_1^2, \\ \{\text{lt}(\eta g) \in \Lambda_2 \mid \eta \in \Lambda\} &= \Lambda_2 \delta_1 \alpha_2^{-1}.\end{aligned}$$

Then $V(2, f, g) = \{v_2\} = \{\delta_1 \delta_2 \alpha_1 \alpha_2^{-1}\}$ and

$$S(2, f, g, v_2) = \delta_1 \alpha_1 \alpha_2^{-1} f + \delta_2 \alpha_1 \alpha_2^{-1} g = \delta_1 \alpha_1^{-1} \alpha_2^{-2} + \delta_2 \alpha_1 \alpha_2^3.$$

For the proof of the Generalized Buchberger Theorem we need the following lemmas.

Lemma 3.4: Let $f_1, \dots, f_l \in F$ and $a_1, \dots, a_l \in K$. If $\sum_{j=1}^l a_j = 0$, then

$$\sum_{j=1}^l a_j r_j = \sum_{j=1}^{l-1} b_j (f_j - f_{j+1})$$

for some $b_j \in R$.

Lemma 3.5: Let $g_i, g_k \in F$ and $lt(\lambda g_i) = lt(\eta g_k) = u \in \Lambda_j E$, where $\lambda, \eta \in \Lambda$. Then there exists $\zeta \in \Lambda_j$ and $v \in V(j, g_i, g_k)$, such that $u = \zeta v$. Therefore if G is a finite subset of $F \setminus \{0\}$ and the S-polynomial $S(j, g_i, g_k, v)$ can be reduced to 0 by G then

$$\zeta S(j, g_i, g_k, v) = \frac{u}{lt_j(g_i)} \frac{g_i}{lc_j(g_i)} - \frac{u}{lt_j(g_k)} \frac{g_k}{lc_j(g_k)} = \sum_{g \in G} h_g g$$

with $lt(h_g g) \prec u$ for $g \in G$.

Theorem 3.2 (Generalized Buchberger Theorem) Let F be a free D -module and \prec be a generalized term order on ΛE , G be a finite subset of $F \setminus \{0\}$ and W be the submodule in F generated by G . Then G is a Gröbner basis of W if and only if for all Λ_j , for all $g_i, g_k \in G$ and for all $v \in V(j, g_i, g_k)$, the S-polynomials $S(j, g_i, g_k, v)$ can be reduced to 0 by G .

Theorem 3.3 (Buchberger Algorithm) Let F be a free D -module and \prec be a generalized term order on ΛE , G be a finite subset of $F \setminus \{0\}$ and W be the submodule in F generated by G . For each Λ_j and $f, g \in F \setminus \{0\}$ let $V(j, f, g)$ and $S(j, f, g, v)$ be as in Definition 3.6. Then by the following algorithm a Gröbner basis of W can be computed:

Input: $G = \{g_1, \dots, g_\mu\}$, a set of generators of W

Output: $G' = \{g'_1, \dots, g'_\nu\}$, a Gröbner basis of W

Begin

$G_0 := G$

While $\exists f, g \in G_i, v \in V(j, f, g)$ s.t.
 $S(j, f, g, v)$ reduces to $r \neq 0$ by G_i

Do $G_{i+1} := G_i \cup \{r\}$

If $G_{i+1} = G_i$ **then** $G_{i+1} = G'$

End

Ex. 3.5: Let F and the generalized term order on Λ be as in Example 3.3. Let $G = \{g_1, g_2, g_3\} = \{\alpha_2^4 + 1, \alpha_1^2 - 1, \alpha_1^2\alpha_2^4 + 1\}$. Then G is a Gröbner basis of the submodule W generated by G . To prove this, we must show that all S -polynomials of G can be reduced to 0 by G .

Following the method described in Example 3.3, we have $V(0, g_1, g_2) = \{\alpha_1^2\alpha_2^4\}$, $V(1, g_1, g_2) = \{\alpha_1^{-1}\alpha_2^3\}$, $V(2, g_1, g_2) = \{\alpha_1\alpha_2^{-1}\}$. So

$$\begin{aligned} S(0, g_1, g_2, \alpha_1^2\alpha_2^4) &= \alpha_1^2g_1 - \alpha_2^4g_2 = \alpha_1^2 + \alpha_2^4 = g_1 + g_2, \\ S(1, g_1, g_2, \alpha_1^{-1}\alpha_2^3) &= \alpha_1^{-1}\alpha_2^{-1}g_1 + \alpha_1^{-1}\alpha_2^3g_2 = \\ &\quad \alpha_1^{-1}\alpha_2^{-1} + \alpha_1\alpha_2^3 = (\alpha_1^{-1}\alpha_2^{-1})g_3, \\ S(2, g_1, g_2, \alpha_1\alpha_2^{-1}) &= \alpha_1\alpha_2^{-1}g_1 - \alpha_1^{-1}\alpha_2^{-1}g_2 = \\ &\quad \alpha_1^{-1}\alpha_2^{-1} + \alpha_1\alpha_2^3 = (\alpha_1^{-1}\alpha_2^{-1})g_3. \end{aligned}$$

Furthermore, $V(0, g_1, g_3) = \{\alpha_1^2\alpha_2^4\}$, $V(1, g_1, g_3) = \{\alpha_1^{-1}\alpha_2^3\}$, $V(2, g_1, g_3) = \{\alpha_2^{-1}\}$. So

$$\begin{aligned} S(0, g_1, g_3, \alpha_1^2\alpha_2^4) &= \alpha_1^2g_1 - g_3 = \alpha_1^2 - 1 = g_2, \\ S(1, g_1, g_3, \alpha_1^{-1}\alpha_2^3) &= \alpha_1^{-1}\alpha_2^{-1}g_1 - \alpha_1^{-1}\alpha_2^3g_3 = \\ &\quad \alpha_1^{-1}\alpha_2^{-1} - \alpha_1\alpha_2^7 = \\ &\quad (\alpha_1^{-1}\alpha_2^{-1})g_3 - \alpha_1\alpha_2^3g_1, \end{aligned}$$

(note that the r.h.s. of this equation satisfies the condition in Theorem 3.1 (i), i.e. $\text{lt}(h_i g_i) \preceq \text{lt}(S)$)

$$S(2, g_1, g_3, \alpha_2^{-1}) = \alpha_2^{-1}g_1 - \alpha_2^{-1}g_3 = \alpha_2^3 - \alpha_1^2\alpha_2^3 = -\alpha_2^3g_2.$$

Finally, $V(0, g_2, g_3) = \{\alpha_1^2 \alpha_2^4\}$, $V(1, g_2, g_3) = \{\alpha_1^{-1}\}$,
 $V(2, g_2, g_3) = \{\alpha_1 \alpha_2^{-1}\}$. So

$$\begin{aligned}
S(0, g_2, g_3, \alpha_1^2 \alpha_2^4) &= \alpha_2^4 g_2 - g_3 = -\alpha_2^4 - 1 = -g_1, \\
S(1, g_2, g_3, \alpha_1^{-1}) &= \alpha_1^{-1} g_2 - \alpha_1^{-1} g_3 = \alpha_1 \alpha_2^4 + \alpha_1 = \\
&\quad \alpha_1 g_1, \\
S(2, g_2, g_3, \alpha_1 \alpha_2^{-1}) &= \alpha_1^{-1} \alpha_2^{-1} g_2 - \alpha_1 \alpha_2^{-1} g_3 = \\
&\quad -\alpha_1^{-1} \alpha_2^{-1} - \alpha_1^3 \alpha_2^3 = \\
&\quad \alpha_1^{-1} \alpha_2^{-1} g_3 + \alpha_1 \alpha_2^3 g_2.
\end{aligned}$$

The r.h.s. of this equation also satisfies the condition in Theorem 3.1 (i). So, by Theorem 3.2, G is a Gröbner basis of W .

References

- [1] T. Becker, V. Weispfenning. *Gröbner bases. A Computational Approach to Commutative Algebra*. Springer-Verlag, New York (1993).
- [2] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem null-dimensionalen Polynomideal*. Ph.D. dissertation, Univ. Innsbruck, Austria (1965).
- [3] B. Buchberger. Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *J. Symb. Comp.* 41/3-4, 475–511 (2006).
- [4] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms*, 2nd ed. Springer-Verlag (1997)
- [5] A. Galligo. Some algorithmic questions on ideals of differential operators. *Proc. EUROCAL'85*, B.F. Caviness (ed.), LNCS 204, 413-421, Springer-Verlag, Berlin (1985).
- [6] M. Insa, F. Pauer. Gröbner bases in rings of differential operators. In *Gröbner Bases and Applications*, B. Buchberger and F. Winkler (eds.), 367-380, Cambridge University Press (1998).
- [7] M.V. Kondrateva, A.B. Levin, A.V. Mikhalev and E.V. Pankratev. *Differential and Difference Dimension Polynomials*. Kluwer Acad. Publ., Dordrecht (1998).

- [8] A.B. Levin. Reduced Gröbner bases, free difference-differential modules and difference-differential dimension polynomials. *J. Symb. Comput.* 30/4, 357-382 (2000).
- [9] T. Mora. Gröbner bases for non-commutative polynomial rings. In *Proc. AA ECC-3*, J. Calmet (ed.), LNCS 229, 353-362, Springer-Verlag (1986).
- [10] M. Noumi. Wronskian determinants and the Gröbner representation of linear differential equations. In *Algebraic Analysis*, M. Kashiwara, T. Kawai (eds.), 549-569, Academic Press, Boston (1988).
- [11] T. Oaku, T. Shimoyama. A Gröbner basis method for modules over rings of differential operators. *J. Symb. Comput.* 18/3, 223-248 (1994).
- [12] F. Pauer, A. Unterkircher. Gröbner bases for ideals in Laurent polynomial rings and their applications to systems of difference equations. *AA ECC 9*, 271-291 (1999).
- [13] N. Takayama. Gröbner basis and the problem of contiguous relations. *Japan J. Appl. Math.* 6, 147-160 (1989).
- [14] F. Winkler. *Polynomial Algorithms in Computer Algebra*. Springer-Verlag, Wien New York (1996).
- [15] M. Zhou, F. Winkler. Gröbner bases in difference-differential modules and their applications. Techn.Rep. 05-14, RISC, J.Kepler Univ. Linz, Austria (2005).