AMS Special Session on Diff.Alg.&Rel.Topics, Stevens Inst. of Technology, Hoboken, NJ, 14–15 April 2007

Gröbner bases in difference-differential modules and their applications

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.

1. Introduction

- We extend the theory of Gröbner bases to difference-differential (d-d) 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. Such orders might also be of interest beyond the specific application to d-d modules.
- We show how Gröbner bases for d-d modules can be used for determining dimension polynomials for d-d modules.

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 $\Delta = \{\delta_1, \cdots, \delta_m\}$ be a set of derivations on R and $\Sigma = \{\sigma_1, \cdots, \sigma_n\}$ 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 $R = K[x_1, \ldots, x_n]$ 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 $\Delta = \{\delta_1, \ldots, \delta_n\}$ and $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$.

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

$$\sum_{\lambda \in \Lambda} a_\lambda \lambda, \tag{1.2}$$

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

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

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 $R[\delta_1, \cdots, \delta_m]$.

If the coefficient ring R is the polynomial ring in $x_1, \ldots, x_m$ 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 $\sigma_1, \cdots, \sigma_n$ is $(l_1, \cdots, l_n) \in \mathbb{Z}^n$. 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 $\mathbb{Z}^n_j$, i.e. $\mathbb{Z}^n = \bigcup_{j=1}^k \mathbb{Z}^n_j$, where $\mathbb{Z}^n_j$, $j = 1, \cdots, k$, satisfy the following conditions:

(i) $(0, \cdots, 0) \in \mathbb{Z}^n_j$, and $\mathbb{Z}^n_j$ does not contain any pair of invertible elements $c = (c_1, \cdots, c_n) \neq 0$ and $-c = (-c_1, \cdots, -c_n)$,

(ii) $\mathbb{Z}^n_j$ is isomorphic to $\mathbb{N}^n$ as a semigroup,

(iii) the group generated by $\mathbb{Z}^n_j$ is $\mathbb{Z}^n$.

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

Ex.2.1: Let $\{\mathbb{Z}_1^n, \cdots, \mathbb{Z}_{2^n}^n\}$ 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

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

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

Def.2.3: Let $\{\mathbb{Z}_j^n \mid j = 1, \cdots, k\}$ 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) $(0, \cdots, 0)$ 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 $\{\mathbb{Z}^n_j \mid j = 1, \cdots, 2^n\}$ be the canonical orthant decomposition of $\mathbb{Z}^n$ defined in Example 2.1. For every $a = (k_1, \cdots, k_m, l_1, \cdots, l_n) \in \mathbb{N}^m \times \mathbb{Z}^n$ let

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

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

Ex.2.3 (c): Let $\{\mathbb{Z}^{(n)}_j, \ \ j = 0, 1, \cdots, n\}$ be the orthant decomposition of $\mathbb{Z}^n$ defined in Example 2.2. For every element $a = (k_1, \cdots, k_m, l_1, \cdots, l_n) \in \mathbb{N}^m \times \mathbb{Z}^n$ let

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

For two elements $a = (k_1, \cdots, k_m, l_1, \cdots, l_n)$ and $b = (r_1, \cdots, r_m, s_1, \cdots, s_n)$ of $\mathbb{N}^m \times \mathbb{Z}^n$ define $a \prec b$ if and only if the $(1 + m + n)$-tuple $(\|a\|, k_1, \cdots, k_m, l_1, \cdots, l_n)$ is lexicographically smaller than $(\|b\|, r_1, \cdots, r_m, s_1, \cdots, s_n)$. 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 $E = \{e_1, \cdots, e_q\}$ is a set of generators of a module.

Def. 2.4: Let $\{\mathbb{Z}_j^n \mid j = 1, \cdots, k\}$ be an orthant decomposition of $\mathbb{Z}^n$. Let $E = \{e_1, \cdots, e_q\}$ 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) $(0, \cdots, 0, e_i)$ 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.

Lemma 2.1: Let $\{\mathbb{Z}^n_j \mid j = 1, \cdots, k\}$ 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 $E = \{e_1, \cdots, e_q\}$. 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 $i = 1, \ldots, q$. 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

$$f = a_1\lambda_1 e_{j_1} + \cdots + a_d\lambda_d e_{j_d} \tag{3.1}$$

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

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 $\mu = 1, \cdots, m$, $\nu = 1, \cdots, n$, 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

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

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 $\mathrm{lt}(\xi) \prec \lambda$ 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 $\mathrm{lt}(\lambda f) = \lambda \cdot u$ for a unique term u of f.

(ii) If $\mathrm{lt}(f) \in \Lambda_j E$ then for any $\lambda \in \Lambda_j$

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

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

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

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 $\mathrm{lt}(hf) = \max_{\prec}\{\lambda_i u_k\}$ where λ_i are terms of h and u_k are terms of f. Therefore $\mathrm{lt}(hf) = \lambda \cdot u$ 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 $f_1, \cdots, f_p \in F \setminus \{0\}$. Then every $g \in F$ can be represented as

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

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

(i) $h_i = 0$ or $\mathrm{lt}(h_i f_i) \preceq \mathrm{lt}(g)$ for $i = 1, \cdots, p$,

(ii) $r = 0$ or $\mathrm{lt}(r)$ is not a multiple of any $\mathrm{lt}(\lambda f_i)$ for $\lambda \in \Lambda$, $i = 1, \cdots, p$.

Def.3.4: Let $f_1, \ldots, f_p \in F \setminus \{0\}$, $g \in F$. 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 $\{f_1, \cdots, f_p\}$ to r. In this case we have $\mathrm{lt}(r) \prec \mathrm{lt}(g)$ by the proof of Theorem 3.1. In the case of $r = g$ and $h_i = 0$ for $i = 1, \cdots, p$, we say that g *is reduced* w.r.t. $\{f_1, \cdots, f_p\}$.

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.

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

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 $\mathrm{lt}(r_1)=\delta_2\alpha^2$ is not any multiple of $\mathrm{lt}(f)=\delta_1\alpha^{-1}$, we can find $\lambda=\delta_2\alpha$ such that $\mathrm{lt}(r_1)=\mathrm{lt}(\lambda f)=\mathrm{lt}(\delta_1\delta_2+\delta_2\alpha^2)$. 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 $G = \{g_1, \cdots, g_p\} \subseteq W\backslash\{0\}$. Then G is called a *Gröbner basis* of W (w.r.t. the generalized term order $\prec$) if and only if for every $f \in W \setminus \{0\}$, $\mathrm{lt}(f)$ is a multiple of $\mathrm{lt}(\lambda g_j)$ 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

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

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

$$S(j, f, g, v) = \frac{v}{lt_j(f)} \frac{f}{lc_j(f)} - \frac{v}{lt_j(g)} \frac{g}{lc_j(g)}$$

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.

$$u = \delta_1^{k_1}\delta_2^{k_2}\alpha_1^{l_1}\alpha_2^{l_2} \ \prec \ v = \delta_1^{r_1}\delta_2^{r_2}\alpha_1^{s_1}\alpha_2^{s_2}$$
$$\Longleftrightarrow (\|u\|, k_1, k_2, l_1, l_2) \ <_{lex} \ (\|v\|, r_1, r_2, s_1, s_2),$$

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

$$\{\lambda \in \Lambda \mid \mathrm{lt}(\lambda f) \in \Lambda_0\} = \Lambda_0\alpha_1^2\ , \quad \{\eta \in \Lambda \mid \mathrm{lt}(\eta g) \in \Lambda_0\} = \Lambda_0,$$
$$\{\mathrm{lt}(\lambda f) \in \Lambda_0 \mid \lambda \in \Lambda\} = \Lambda_0\delta_2\alpha_1^2, \quad \{\mathrm{lt}(\eta g) \in \Lambda_0 \mid \eta \in \Lambda\} = \Lambda_0\delta_1.$$

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

$$\{\lambda \in \Lambda \mid \mathrm{lt}(\lambda f) \in \Lambda_1\} = \Lambda_1\alpha_1\ , \quad \{\eta \in \Lambda \mid \mathrm{lt}(\eta g) \in \Lambda_1\} = \Lambda_1,$$
$$\{\mathrm{lt}(\lambda f) \in \Lambda_1 \mid \lambda \in \Lambda\} = \Lambda_1\alpha_1^{-1}, \quad \{\mathrm{lt}(\eta g) \in \Lambda_1 \mid \eta \in \Lambda\} = \Lambda_1\delta_1.$$

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,

$$\{\lambda \in \Lambda \mid \mathrm{lt}(\lambda f) \in \Lambda_2\} = \Lambda_2\alpha_1^2, \quad \{\eta \in \Lambda \mid \mathrm{lt}(\eta g) \in \Lambda_2\} = \Lambda_2\alpha_2^{-1},$$
$$\{\mathrm{lt}(\lambda f) \in \Lambda_2 \mid \lambda \in \Lambda\} = \Lambda_2\delta_2\alpha_1^2, \quad \{\mathrm{lt}(\eta g) \in \Lambda_2 \mid \eta \in \Lambda\} = \Lambda_2\delta_1\alpha_2^{-1}.$$

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

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

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 $F \backslash \{0\}$ 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 $F\backslash\{0\}$ and W be the submodule in F generated by G. For each Λ_j and $f, g \in F\backslash\{0\}$ 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: $G = \{g_1, \cdots, g_\mu\}$, a set of generators of W
Output: $G' = \{g'_1, \cdots, g'_\nu\}$, 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

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

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

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

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

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

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

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

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.

4. Computing d-d dimension polynomials

Let R be a Δ-Σ-field,
D the ring of Δ-Σ-operators over R,
M a finitely generated Δ-Σ-module (i.e. a finitely generated difference-differential-module),
F a finitely generated free Δ-Σ-module.

For $\lambda \in \Lambda$ of the form $\lambda = \delta_1^{k_1} \cdots \delta_m^{k_m} \sigma_1^{l_1} \cdots \sigma_n^{l_n}$ let

$$|\lambda| \ = \ k_1 + \cdots + k_m + |l_1| + \cdots + |l_n| \ .$$

Also, for $w = \lambda e_i \in \Lambda E$ of a term of F, let

$$|w| \ = |\lambda| \ .$$

If $u = \sum_{\lambda \in \Lambda} a_\lambda \lambda \in D$, then

$$|u| \ = \ \max\{|\lambda| \mid a_\lambda \neq 0\} \ .$$

We may consider D as a filtered ring with the filtration $(D_\mu)_{\mu \in \mathbb{Z}}$ such that $D_\mu = \{u \in D \mid |u| \leq \mu\}$ for any $\mu \in \mathbb{N}$ and $D_\mu = 0$ for $\mu < 0$. It is clear that $\bigcup \{D_\mu \mid \mu \in \mathbb{Z}\} = D$, $D_\mu \subseteq D_{\mu+1}$ for any $\mu \in \mathbb{Z}$ and $D_\nu D_\mu = D_{\mu+\nu}$ for any $\mu, \nu \in \mathbb{Z}$.

Def. 4.1. Let R be a Δ-Σ-field and M be a Δ-Σ-module. A sequence $(M_\mu)_{\mu\in\mathbb{Z}}$ of R-vector subspaces of the module M is called a filtration of M if the following three conditions hold:

(i) $M_\mu \subseteq M_{\mu+1}$ for all $\mu \in \mathbb{Z}$ and $M_\mu = 0$ for all sufficiently small $\mu \in \mathbb{Z}$.

(ii) $\bigcup\{M_\mu \mid \mu \in \mathbb{Z}\} = M$.

(iii) $D_\nu M_\mu \subseteq M_{\mu+\nu}$ for any $\mu \in \mathbb{Z}, \nu \in \mathbb{N}$.

If every R-vector space M_μ is finitely generated and there exist numbers $\mu_0 \in \mathbb{Z}$ such that $D_\nu M_\mu = M_{\mu+\nu}$ for all $\mu \geq \mu_0$, $\nu \in \mathbb{N}$, then the filtration $(M_\mu)_{\mu\in\mathbb{Z}}$ is called an excellent filtration of M.

Example 4.1: Let M be a finitely generated Δ-Σ-module(i.e. a left D-module) with generators $h_1, \cdots, h_q$. If

$$M_\mu = D_\mu h_1 + \cdots + D_\mu h_q$$

for any $\mu \in \mathbb{Z}$, then $(M_\mu)_{\mu\in\mathbb{Z}}$ is an excellent filtration of M. $\square$

Def. 4.2: A polynomial $f(t_1, \cdots, t_p)$ in p variables $t_1, \cdots, t_p$ with rational coefficients is called numerical if $f(t_1, \cdots, t_p) \in \mathbb{Z}$ for all sufficiently large $(r_1, \cdots, r_p) \in \mathbb{Z}^p$, i.e. there exists a n-tuple $(s_1, \cdots, s_p) \in \mathbb{Z}^p$ such that $f(r_1, \cdots, r_p) \in \mathbb{Z}$ for all integers $r_1, \cdots, r_p \in \mathbb{Z}$ with $r_i \geq s_i$ $(1 \leq i \leq p)$.

Theorem 4.1. (Levin (2000)) Let A be a subset of $\mathbb{N}^m \times \mathbb{Z}^n$. Choose the canonical orthant decomposition of $\mathbb{Z}^n$ (see Example 2.1). Let $\unlhd$ be the partial order on $\mathbb{N}^m \times \mathbb{Z}^n$ such that

$$(k_1, \cdots, k_m, l_1, \cdots, l_n) \unlhd (r_1, \cdots, r_m, s_1, \cdots, s_n)$$

if and only if $(l_1, \cdots, l_n)$ and $(s_1, \cdots, s_n)$ belong to a same orthant and

$$(r_1, \cdots, r_m, |s_1|, \cdots, |s_n|) \in \{(k_1, \cdots, k_m, |l_1|, \cdots, |l_n|) + \mathbb{N}^{m+n}\}.$$

Furthermore, let

$$W_A = \{w \in \mathbb{N}^m \times \mathbb{Z}^n \mid \forall a \in A : a \not\trianglelefteq w\}$$

and

$$\begin{aligned} W_A[\mu] \ = \ \{&(k_1, \cdots, k_m, l_1, \cdots, l_n) \in W_A \mid \\ &k_1 + \cdots + k_m + |l_1| + \cdots + |l_n| \leq \mu\}. \end{aligned}$$

Then there exists a numerical polynomial $\phi_A(t)$ with the following properties.

(i) $\phi_A(\mu) = Card\ W_A[\mu]$ for all sufficiently large $\mu \in \mathbb{N}$.
(ii) $deg\ \phi_A \leq m + n$, and if $A = \emptyset$ then $deg\ \phi_A = m + n$.
(iii)$\phi_A(t) = 0$ if and only if $(0, \cdots, 0) \in A$. $\square$

Definition 4.3: The numerical polynomial $\phi(t)$ is called difference-differential dimension polynomial in one variable t associated with M,if

(i) $deg(\phi(t)) \leq m+n$ and

(ii)$\phi(\mu) = dim_R M_\mu$ for all sufficiently large $\mu \in \mathbb{N}$.

Choose the canonical orthant decomposition on $\mathbb{Z}^n$ as in Example 2.1 and define the generalized term order "$\prec$" on ΛE of the terms of F as follows(see Example 2.3(a)):

If $u = \delta_1^{k_1} \cdots \delta_m^{k_m} \sigma_1^{l_1} \cdots \sigma_n^{l_n} e_i$ and $v = \delta_1^{r_1} \cdots \delta_m^{r_m} \sigma_1^{s_1} \cdots \sigma_n^{s_n} e_j$, then

$$
\begin{aligned}
u \prec v \iff & (|u|, e_i, k_1, \cdots, k_m, |l_1|, \cdots, |l_n|, l_1, \cdots, l_n) \\
& <_{\text{lex}} \\
& (|v|, e_j, r_1, \cdots, r_m, |s_1|, \cdots, |s_n|, s_1, \cdots, s_n) \ .
\end{aligned}
$$

Theorem 4.2: Let R be a Δ-Σ-field, D the ring of Δ-Σ-operators over R and M be a finitely generated Δ-Σ-module with generators $h_1, \cdots, h_q$. Let F be a free Δ-Σ-module with a basis $e_1, \cdots, e_q$ and $\pi: F \longrightarrow M$ the natural Δ-Σ-epimorphism of F onto M (i.e. $\pi(e_i) = h_i$ for $i = 1, \cdots, q$).

Let M_μ be the vector space over R as in Example 4.1. Suppose $G = \{g_1, \cdots, g_d\}$ is a Gröbner basis of $N = ker\ \pi$ with respect to the generalized term order "$\prec$" defined above, U_μ is the set of all terms $w \in \Lambda E$ such that $|w| \leq \mu$ and $w \neq lt(\lambda g_i)$, $\lambda \in \Lambda$, $i = 1, \cdots, d$. Then $\pi(U_\mu)$ is a basis of the R-vector space M_μ.

By Theorem 4.2 the difference-differential dimension polynomial $\phi(t)$ (with $\phi(\mu)$ the dimension of M_μ as an R-vector space) can be computed by difference-differential Gröbner bases.

Theorem 4.3: Let R be a Δ-Σ-field, D the ring of Δ-Σ-operators over R and M be a finitely generated Δ-Σ-module, and $(M_\mu)_{\mu\in\mathbb{Z}}$ an excellent filtration of M. If $G = \{g_1, \cdots, g_d\}$ is a Gröbner basis of $N = ker\ \pi$ as in Theorem 4.2, then the difference-differential dimension polynomial $\phi(t)$ such that $deg(\phi(t)) \le m + n$ and $\phi(\mu) = dim_R M_\mu$ for all sufficiently large $\mu \in \mathbb{N}$ can be computed as

$$\begin{aligned}\phi(\mu) &= Card(U_\mu)\\ &= Card\{w \in \Lambda E \mid ord\ w \le \mu;\ w \ne lt(\lambda g_i), \lambda \in \Lambda, g_i \in G\}\end{aligned}$$

Example 4.2: Let R be a difference-differential field whose basic sets Δ and Σ consist of a single derivation operator δ and a single automorphism σ, respectively. Furthermore, let D be the ring of Δ-Σ-operators over R and $M = Dh$ be a cyclic Δ-Σ-module whose generator h satisfies the defining equation

$$(\delta^a\sigma^b + \delta^a\sigma^{-b} + \delta^{a+b})h = 0$$

where $a, b \in \mathbb{N}$. In other words, M is isomorphic to the factor module of a free Δ-Σ-module F with a free generator e by its Δ-Σ-submodule $N = D(\delta^a\sigma^b+\delta^a\sigma^{-b}+\delta^{a+b})e$. Let the generalized term order $\prec$ on ΛE be the same as in Theorem 4.3. Then

$$\{g\} \ = \ \{(\delta^a\sigma^b + \delta^a\sigma^{-b} + \delta^{a+b})e\}$$

is a difference-differential Gröbner basis of N(If W is generated by one element $g \in F\backslash\{0\}$, then any finite subset G of $W\backslash\{0\}$ containing g is a difference-differential Gröbner basis of W).
Since $lt(g) = (\delta^{a+b})e$ belongs to any orthant of ΛE, it follows that $lt(\lambda g) = \lambda(\delta^{a+b})e$ for any $\lambda \in \Lambda$. Then by Theorem 4.3,

$$\begin{aligned} dim_R M_t &= Card(U_t) \\ &= Card\{u \in \Lambda \mid ord\ u \le t; u \ne \lambda\delta^{a+b}, \lambda \in \Lambda\}. \end{aligned}$$

Therefore,

$$\begin{aligned} dim_R M_t &= Card\{\delta^c\sigma^d \mid c \in \mathbb{N},\ d \in \mathbb{Z},\ c + |d| \le t, \\ &\qquad\qquad (c, |d|) \notin \{(a+b, 0) + \mathbb{N}^2\}\} \\ &= Card\{\delta^c\sigma^d \mid c \in \mathbb{N}, d \in \mathbb{Z}, c + |d| \le t\} \\ &\quad - Card\{\delta^c\sigma^d \mid c \in \mathbb{N}, d \in \mathbb{Z}, c + |d| \le t - (a+b)\} \\ &= [(t+2)(t+1) - (t+1)] \\ &\quad -[\ (t-a-b+2)(t-a-b+1) - (t-a-b+1)] \\ &= 2(a+b)t + (a+b)(2-a-b)\ . \end{aligned}$$

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 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.
- dimension polynomials of d-d modules as generalizations of Hilbert polynomials are introduced and studied in Mikhalev and Pankratev (1989).

References

[1] G. Carrà Ferro. Gröbner bases and differential algebra. *LNCS* 356, 129–140, Springer-Verlag (1989).

[2] 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).

[3] 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).

[4] M.V. Kondrateva, A.B. Levin, A.V. Mikhalev and E.V. Pankratev. *Differential and Difference Dimension Polynomials*. Kluwer Acad. Publ., Dordrecht (1998).

[5] A.B. Levin. Reduced Gröbner bases, free difference-differential modules and difference-differential dimension polynomials. *J. Symb. Comput.* 30/4, 357-382 (2000).

[6] A.V. Mikhalev, E.V. Pankratev. *Computer Algebra, Computations in Differential and Difference Algebra.* (in Russian) Moscow State Univ. Press, Moscow (1989).

[7] T. Mora. Gröbner bases for non-commutative polynomial rings. In *Proc. AAECC-3*, J. Calmet (ed.), LNCS 229, 353-362, Springer-Verlag (1986).

[8] M. Noumi. Wronskian determinants and the Gröbner representation of linear differential equations. In *Algebraic Anal-*

ysis, M. Kashiwara, T. Kawai (eds.), 549-569, Academic Press, Boston (1988).

[9] T. Oaku, T. Shimoyama. A Gröbner basis method for modules over rings of differential operators. *J. Symb. Comput.* 18/3, 223-248 (1994).

[10] F. Pauer, A. Unterkircher. Gröbner bases for ideals in Laurent polynomial rings and their applications to systems of difference equations. *AAECC* 9, 271-291 (1999).

[11] F. Pauer, S. Zampieri. Gröbner bases with respect to generalized term orders and their applications to the modelling problem. *J. Symbolic Comp.* 21, 155–168 (1996).

[12] N. Takayama. Gröbner basis and the problem of contiguous relations. *Japan J. Appl. Math.* 6, 147-160 (1989).

[13] F. Winkler. *Polynomial Algorithms in Computer Algebra.* Springer-Verlag, Wien New York (1996).

[14] M. Zhou, F. Winkler. Gröbner bases in difference-differential modules and their applications. Techn.Rep. 05-14, RISC, J.Kepler Univ. Linz, Austria (2005).

[15] M. Zhou, F. Winkler. Gröbner bases in difference-differential modules. *Proc. ISSAC 2007*, 353–360 (2006).