# Gröbner bases in difference-differential modules and their applications*

October 24, 2005

**Meng Zhou**[a,1] **and Franz Winkler**[b]

[a]*Department of Mathematics, Beihang University, Beijing(100083), China*
[b]*RISC-Linz, J. Kepler University Linz, A-4040 Linz, Austria*

**Abstract**
In this paper we will extend the theory of Gröbner bases to difference-differential modules which were introduced by Levin(2000) as a generalization of modules over rings of differential operators. The main goal of this paper is to present and verify algorithms for constructing these Gröbner basis counterparts. To this aim we define the concept of "generalized term order" on $\mathbb{N}^m \times \mathbb{Z}^n$ and on difference-differential modules. The relation between the Gröbner bases and some characteristic sets in the modules is also considered. As applications, we can compute the difference-differential dimension polynomial of a difference-differential module and of a system of linear partial difference-differential equations via the Gröbner bases.

*Keywords:* Gröbner basis, generalized term order, difference-differential module, difference-differential dimension polynomial.

## 1 Introduction

The efficiency of the classical Gröbner basis method for the solution of problems by algorithmic way in polynomial ideal theory is well-known. The results of Buchberger(see Buchberger (1985)) on Gröbner bases in polynomial rings have been generalized by many authors to non-commutative case, especially to

*This work has been supported by the FWF project P16357-N04, while the first author spent a research year at RISC-Linz.

[1]Corresponding author.
*E-mail addresses:* zhoumeng1613@hotmail.com(M.Zhou), Franz.Winkler@risc.uni-linz.ac.at(F.Winkler).

modules over various rings of differential operators. Galligo (1985) first gave the Gröbner basis algorithm for the Weyl algebra $A_n$. Mora(1986) generalized the concept of Gröbner basis to non-commutative free algebras. Noumi (1988) and Takayama (1989) formulated the 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. It has been proved that the notion of Gröbner basis is a powerful tool to solve various problems of linear partial differential equations.

On the other hand, for some problems of linear difference-differential equations such as the dimension of the space of solutions and the computation of difference-differential dimension polynomials, the notion of Gröbner basis for the ring of difference-differential operators is essential. Gröbner bases in rings of differential operators are defined with respect to a term order on $\mathbb{N}^n \times \mathbb{N}^n$ or $\mathbb{N}^n$. This approach cannot be used for the ring of difference-differential operators, because for it we need to treat orders on $\mathbb{N}^m \times \mathbb{Z}^n$.Pauer and Unterkircher (1999) considered Gröbner bases in Laurent polynomial rings, but it is limited in commutative case. Levin(2000) introduced a characteristic set for free modules over rings of difference-differential operators. It is an analog of "Gröbner basis" connected with a specific "ordering" on $\mathbb{N}^m \times \mathbb{Z}^n$. But the ordering is not a term-ordering while the theory of Gröbner basis works for any term-ordering.

The main purpose of this paper is to give a new approach to the computation of Gröbner basis for an ideal of (or a module over) the ring of difference-differential operators. Our notion of Gröbner basis is based on generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$. In section 2 the generalized term order and its properties are discussed and some examples are presented. In section 3 we design carefully the reduction algorithm, the definition of the Gröbner basis and the S-polynomials, as well as the Buchberger algoriththm for the computation of the Gröbner bases. Section 4 is contributed to the relationship between the Gröbner bases and some characteristic sets in the modules. In section 5 we present a new appoach to compute difference-differential dimension polynomials associated with a module over the ring of difference-differential operators via the Gröbner bases.

Throughout the paper $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Z}_-$ and $\mathbb{Q}$ denotes the sets of all integers, all nonnegative integers, all nonpositive integers, and all rational numbers, respectively. By a ring we always mean an associative ring with a unit. By the module over a ring $A$ we mean a unitary left $A$-module.

DEFINITION 1.1. Let $R$ be a commutative noetherian ring, $\Delta = \{\delta_1, \cdots, \delta_m\}$ and $\sigma = \{\alpha_1, \cdots, \alpha_n\}$ be set of derivations and automorphisms of the ring $R$, respectively, such that $\beta(x) \in R$ and $\beta(\gamma(x)) = \gamma(\beta(x))$ hold for any $\beta, \gamma \in \Delta \bigcup \sigma$ and $x \in R$. Then $R$ is called a difference-differential ring with the basic set of derivations $\Delta$ and the basic set of automorphisms $\sigma$, or shortly a $\Delta$-$\sigma$-ring. If $R$ is a field, then it is called a $\Delta$-$\sigma$-field.

If $R$ is a $\Delta$-$\sigma$-ring, then $\Lambda$ will denote the commutative semigroup of elements of the form

$$\lambda = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n} \qquad (1.1)$$

where $(k_1, \cdots, k_m) \in \mathbb{N}^m$ and $(l_1, \cdots, l_n) \in \mathbb{Z}^n$. This semigroup contains the free commutative semigroup $\Theta$ generated by the set $\Delta$ and free commutative semigroup $\Gamma$ generated by the set $\sigma$. The subset $\{\alpha_1, \cdots, \alpha_n, \alpha_1^{-1}, \cdots, \alpha_n^{-1}\}$ of $\Lambda$ will be denoted by $\sigma^*$.

DEFINITION 1.2. Let $R$ be a $\Delta$-$\sigma$-ring and the semigroup $\Lambda$ be as above. 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 $a_\lambda$ are different from zero, is called a difference-differential operator (or shortly a $\Delta$-$\sigma$-operator) over $R$. Two $\Delta$-$\sigma$-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 $\Delta$-$\sigma$-operators over a $\Delta$-$\sigma$-ring $R$ is a ring with the following fundamental relations

$$\sum_{\lambda \in \Lambda} a_\lambda \lambda + \sum_{\lambda \in \Lambda} b_\lambda \lambda = \sum_{\lambda \in \Lambda} (a_\lambda + b_\lambda) \lambda,$$

$$a(\sum_{\lambda \in \Lambda} a_\lambda \lambda) = \sum_{\lambda \in \Lambda} (a a_\lambda) \lambda,$$

$$(\sum_{\lambda \in \Lambda} a_\lambda \lambda) \mu = \sum_{\lambda \in \Lambda} a_\lambda (\lambda \mu),$$

$$\delta a = a\delta + \delta(a), \qquad \tau a = \tau(a) \tau, \tag{1.3}$$

for all $a_\lambda, b_\lambda \in R$, $\lambda, \mu \in \Lambda$, $a \in R$, $\delta \in \Delta$, $\tau \in \sigma^*$. Note that the elements in $\Delta$ and $\sigma^*$ do not commute with the elements in $R$, and then the "terms" $\lambda \in \Lambda$ do not commute with the coefficients $a_\lambda \in R$.

DEFINITION 1.3. The ring of all $\Delta$-$\sigma$-operators over a $\Delta$-$\sigma$-ring $R$ is called the ring of difference-differential operators (or shortly the ring of $\Delta$-$\sigma$-operators) over $R$, it will be denoted by $D$. A left $D$-module $M$ is called a difference-differential module(or a $\Delta$-$\sigma$-module). If $M$ is finitely generated as a left $D$-module, then $M$ is called a finitely generated $\Delta$-$\sigma$-module.

When $\sigma = \emptyset$, $D$ will be the rings of differential operators $R[\delta_1, \cdots, \delta_m]$. If the coefficient ring $R$ is the polynomial ring over a field $K$, then $D$ will be Weyl algebra $A_m$. So $\Delta$-$\sigma$-module is a generalization of module over rings of differential operators. But in the ring of $\Delta$-$\sigma$-operators the "terms" are the form (1.1) and the index in $\alpha_1, \cdots, \alpha_n$ is $(l_1, \cdots, l_n) \in \mathbb{Z}^n$, the notion of "term order" is no longer valid. We need to generalize the concept of term order.

## 2 Generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$

Note that $\mathbb{Z}^n = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ is a group. We consider first some decomposition of $\mathbb{Z}^n$.

DEFINITION 2.1. If $\mathbb{Z}^n$ is a union of finitely many $\mathbb{Z}_j^{(n)}$:

$$\mathbb{Z}^n = \bigcup_{j=1}^{k} \mathbb{Z}_j^{(n)}$$

where $\mathbb{Z}_j^{(n)}$, $j = 1, \cdots, k$, satisfy following conditions:

(i) $(0, \cdots, 0) \in \mathbb{Z}_j^{(n)}$, and $\mathbb{Z}_j^{(n)}$ does not contain any pair of invertible elements $c = (c_1, \cdots, c_n) \neq 0$ and $c^{-1} = (-c_1, \cdots, -c_n)$,

(ii) $\mathbb{Z}_j^{(n)}$ is finitely generated sub-semigroup of $\mathbb{Z}^n$,

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

then $\{\mathbb{Z}_j^{(n)}, \ \ j = 1, \cdots, k\}$ is called an ortant decomposition of $\mathbb{Z}^n$ and $\mathbb{Z}_j^{(n)}$ is called the $j$-th ortant of the decomposition.

EXAMPLE 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 $\mathbb{N}$ or $\mathbb{Z}_-$. Then it is an ortant 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 ortant decomposition of $\mathbb{Z}^n$. □

EXAMPLE 2.2. Let $\mathbb{Z}_0^{(n)}$ be the sub-semigroup of $\mathbb{Z}^n$ generated by

$$\{(1, 0, \cdots, 0), (0, 1, 0, \cdots, 0), \cdots, (0, \cdots, 0, 1)\},$$

and $\mathbb{Z}_j^{(n)}$ be the sub-semigroup of $\mathbb{Z}^n$ generated by

$$\{(-1, \cdots, -1)\} \bigcup \{(1, 0, \cdots, 0), (0, 1, 0, \cdots, 0), \cdots, (0, \cdots, 0, 1)\}$$
$$\backslash \{(\underbrace{0, \cdots, 0, 1}_{j}, 0, \cdots, 0)\}, \qquad j = 1, 2, \cdots, n.$$

Then $\{\mathbb{Z}_0^{(n)}, \mathbb{Z}_1^{(n)}, \cdots, \mathbb{Z}_n^{(n)}\}$ is an ortant decomposition of $\mathbb{Z}^n$. For $n = 2$, we have

$$\mathbb{Z}_0^{(n)} = \{(a, b) | a \geq 0, b \geq 0, a, b \in \mathbb{Z}\},$$
$$\mathbb{Z}_1^{(n)} = \{(a, b) | a \leq 0, b \geq a, a, b \in \mathbb{Z}\},$$
$$\mathbb{Z}_2^{(n)} = \{(a, b) | b \leq 0, a \geq b, a, b \in \mathbb{Z}\}.$$

□

LEMMA 2.1. Let $\{\mathbb{Z}_j^{(n)}, \ \ j = 1, \cdots, k\}$ be an ortant decomposition of $\mathbb{Z}^n$. Then every ortant $\mathbb{Z}_j^{(n)}$ is isomorphic to $\mathbb{N}^n$ as a semigroup.

PROOF: By Definition 2.1.(ii), there are finite set of generators $\{a_1, \cdots, a_s\} \subseteq \mathbb{Z}_j^{(n)}$ which generate $\mathbb{Z}_j^{(n)}$ as a sub-semigroup of $\mathbb{Z}^n$. Because $\mathbb{Z}_j^{(n)}$ is in the free Abel-group $\mathbb{Z}^n$, we may choose $\{a_1, \cdots, a_s\}$ as free generators. By Definition 2.1.(iii), the group generated by $\mathbb{Z}_j^{(n)}$ is $\mathbb{Z}^n$. So $\{a_1, \cdots, a_s\}$ generate the group $\mathbb{Z}^n$. Note that $\mathbb{Z}^n$ is a free Abel-group with $n$-dimensional. There must be $n$ free generators $\{e'_1, \cdots, e'_n\} \subseteq \{a_1, \cdots, a_s\}$.Then $s = n$ and $\{e'_1, \cdots, e'_n\} =$

$\{a_1, \cdots, a_s\}$. Clearly $\{e'_1, \cdots, e'_n\}$ would generate a semigroup isomorphic to $\mathbb{N}^n$ and by Definition 2.1.(i) the semigroup would be the whole $\mathbb{Z}_j^{(n)}$. $\square$

DEFINITION 2.2. Let $\{\mathbb{Z}_j^{(n)}, \ \ j = 1, \cdots, k\}$ be an ortant decomposition of $\mathbb{Z}^n$. 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 $\mathbb{N}^m \times \mathbb{Z}^n$ are called similar elements, if the $n$-tuples $(l_1, \cdots, l_n)$ and $(s_1, \cdots, s_n)$ are in the same ortant $\mathbb{Z}_j^{(n)}$ of $\mathbb{Z}^n$. In this case we also say $a$ is similar to $b$.

DEFINITION 2.3. Let $\{\mathbb{Z}_j^{(n)}, \ \ j = 1, \cdots, k\}$ be an ortant decomposition of $\mathbb{Z}^n$. A total order $\prec$ on $\mathbb{N}^m \times \mathbb{Z}^n$ is called a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$ with respect to the decomposition, if the following conditions hold:

(i) $(0, \cdots, 0)$ is the smallest elements in $\mathbb{N}^m \times \mathbb{Z}^n$,

(ii)if $a \prec b$, then for any $c$ similar to $b$, $a+c \prec b+c$. Where $a, b, c \in \mathbb{N}^m \times \mathbb{Z}^n$.

EXAMPLE 2.3. Let $\{\mathbb{Z}_j^{(n)}, \ \ j = 1, \cdots, 2^n\}$ be the canonical ortant 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 $m+n+1$-tuple $(|a|, k_1, \cdots, k_m, l_1, \cdots, l_n)$ is smaller than $(|b|, r_1, \cdots, r_m, s_1, \cdots, s_n)$ relative to the lexicographic order on $\mathbb{N}^{m+1} \times \mathbb{Z}^n$. Then "$\prec$" is a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$.

In fact, obviously $(0, \cdots, 0)$ is the smallest elements in $\mathbb{N}^m \times \mathbb{Z}^n$. Now let $a \prec b$ and $c$ be similar to $b$. Then $|a| \le |b|$. We have

$$|a + c| \le |a| + |c| \le |b| + |c| = |b + c|. \tag{2.1}$$

The last equation holds because $c$ is similar to $b$. If $|a+c| < |b+c|$, then $a+c \prec b+c$. If $|a + c| = |b + c|$, then $|a| = |b|$ must hold by (2.1). So the $m + n$-tuple $(k_1, \cdots, k_m, l_1, \cdots, l_n)$ is lexicographically smaller than $(r_1, \cdots, r_m, s_1, \cdots, s_n)$. Because the lexicographic order on $\mathbb{N}^m \times \mathbb{Z}^n$ is a semi-group order, we also have $a + c \prec b + c$. $\square$

EXAMPLE 2.4. Let the ortant decomposition of $\mathbb{Z}^n$ be as in Example 2.3. For every $a = (k_1, \cdots, k_m, l_1, \cdots, l_n) \in \mathbb{N}^m \times \mathbb{Z}^n$ let

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

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 $m + 2n + 2$-tuple

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

is lexicographically smaller than

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

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

First,note that it is obvious that $(0, \cdots, 0)$ is the smallest elements. Then, let $a \prec b$ and $c = (u_1, \cdots, u_m, v_1, \cdots, v_n)$ be similar to $b$. Because $|a|_1 \le |b|_1$, so

$|a+c|_1 \leq |b+c|_1$. But $|a+c|_1 < |b+c|_1$ would imply $a+c \prec b+c$, we can soppose $|a+c|_1 = |b+c|_1$. This would imply $|a|_1 = |b|_1$ and then $|a|_2 \leq |b|_2$. A relation similar to (2.1) would give $|a+c|_2 \leq |b+c|_2$. In the "$<$" case $a+c \prec b+c$ would hold.

Now soppose $|a+c|_1 = |b+c|_1$, $|a+c|_2 = |b+c|_2$. Then $|a|_1 = |b|_1$, $|a|_2 = |b|_2$. Note that for $j = 1, \cdots, n$,

$$|l_j + v_j| \leq |l_j| + |v_j| \leq |s_j| + |v_j| = |s_j + v_j|.$$

So $(k_1, \cdots, k_m, |l_1|, \cdots, |l_n|, l_1, \cdots, l_n)$ is lexicographically smaller than $(r_1, \cdots, r_m, |s_1|, \cdots, |s_n|, s_1, \cdots, s_n)$, it would imply $a+c \prec b+c$. □

EXAMPLE 2.5. Let $\{\mathbb{Z}_j^{(n)},\ \ j = 0, 1, \cdots, n\}$ be the ortant decomposition of $\mathbb{Z}^n$ defined in Example 2.2. For every $a = (k_1, \cdots, k_m, l_1, \cdots, l_n) \in \mathbb{N}^m \times \mathbb{Z}^n$ 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 $m+n+1$-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 $\mathbb{N}^m \times \mathbb{Z}^n$.

To prove this, note that $\mathbb{Z}_j^{(n)} = \{(i_1, \cdots, i_n) \mid i_j \leq 0;\ i_k \geq i_j, k \neq j\}$, $j = 1, \cdots, n$. It would imply $min\{i_1, \cdots, i_n\} = i_j$ when $(i_1, \cdots, i_n) \in \mathbb{Z}_j^{(n)}$. Then for any $a, c \in \mathbb{N}^m \times \mathbb{Z}^n$ we have

$$\|a+c\| \leq \|a\| + \|c\|.$$

The equation holds if and only if that $a$ and $c$ are similar elements. Then it is easy to prove that the "$\prec$" is a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$ following the way as in Example 2.3. □

In order to investigate $\Delta$-$\sigma$-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.

DEFINITION 2.4. Let $\{\mathbb{Z}_j^{(n)},\ \ j = 1, \cdots, k\}$ be an ortant 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 $\mathbb{N}^m \times \mathbb{Z}^n \times E$ with respect to the decomposition, if the following conditions hold:

(i) $(0, \cdots, 0, e_i)$ is the smallest element in $\mathbb{N}^m \times \mathbb{Z}^n \times \{e_i\}$, $e_i \in E$,

(ii) if $(a, e_i) \prec (b, e_j)$, then for any $c$ similar to $b$, $(a+c, e_i) \prec (b+c, e_j)$. Where $a, b, c \in \mathbb{N}^m \times \mathbb{Z}^n$, $e_i, e_j \in E$.

There are many ways to extend a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$ to $\mathbb{N}^m \times \mathbb{Z}^n \times E$. (Of course it is possible to define it directly).

EXAMPLE 2.6. Let the ortant decomposition of $\mathbb{Z}^n$ and the generalized term order "$\prec$" on $\mathbb{N}^m \times \mathbb{Z}^n$ be as in Example 2.4. Given a order "$\prec'$" in $E = \{e_1, \cdots, e_q\}$, for two elements $(a, e_i) = (k_1, \cdots, k_m, l_1, \cdots, l_n, e_i)$ and $(b, e_j) = (r_1, \cdots, r_m, s_1, \cdots, s_n, e_j)$ of $\mathbb{N}^m \times \mathbb{Z}^n \times E$ define:

$$(a, e_i) \prec_1 (b, e_j) \Longleftrightarrow a \prec b \quad or \quad (a = b \ \ and \ \ e_i \prec' e_j);$$

$$(a, e_i) \prec_2 (b, e_j) \Longleftrightarrow e_i \prec' e_j \quad or \quad (e_i = e_j \quad and \quad a \prec b);$$

$$(a, e_i) \prec_3 (b, e_j) \Longleftrightarrow (|a|_1, |a|_2, e_i, k_1, \cdots, k_m, |l_1|, \cdots, |l_n|, l_1, \cdots, l_n)$$

$$< (|b|_1, |b|_2, e_j, r_1, \cdots, r_m, |s_1|, \cdots, |s_n|, s_1, \cdots, s_n) \text{ in lexicographic order.}$$

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

"$\prec_1$" is called TOP extension of "$\prec$" and "$\prec_2$" is called POT extension of "$\prec$". "$\prec_3$" is a generalized term order defined directly. □

LEMMA 2.2. Let $\{\mathbb{Z}_j^{(n)}, \quad j = 1, \cdots, k\}$ be an ortant decomposition of $\mathbb{Z}^n$ and "$\prec$" be a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$ with respect to the ortant decomposition. Then every strictly descending sequence in $\mathbb{N}^m \times \mathbb{Z}^n$ is finite. In particular, any subset of $\mathbb{N}^m \times \mathbb{Z}^n$ contains a smallest element.

PROOF. Let $a_1 \succ a_2 \succ a_3 \succ \cdots$ be a strictly descending sequence in $\mathbb{N}^m \times \mathbb{Z}^n$. Since there are finitely many ortants, without loss of generality we may assume that all $a_j$ are similar elements which are in $\mathbb{N}^m \times \mathbb{Z}_i^{(n)}$ for a fixed $i$. By Lemma 2.1, $\mathbb{N}^m \times \mathbb{Z}_i^{(n)}$ is isomophic to $\mathbb{N}^{m+n}$ as a semigroup. Define order $\prec_1$ on $\mathbb{N}^{m+n}$ as follows:

$$a \prec_1 b \Longleftrightarrow f^{-1}(a) \prec f^{-1}(b),$$

where $f$ is the isomophic map from $\mathbb{N}^m \times \mathbb{Z}_i^{(n)}$ to $\mathbb{N}^{m+n}$ and $\prec$ is the generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$. Since $\prec$ is a term order on $\mathbb{N}^m \times \mathbb{Z}_i^{(n)}$, it is easy to see $\prec_1$ is a term order on $\mathbb{N}^{m+n}$. Then the assertion of the Lemma follows from the well-order property of term order on $\mathbb{N}^{m+n}$. □

COROLLARY. Given an ortant decomposition of $\mathbb{Z}^n$ and a generalized term order "$\prec$" on $\mathbb{N}^m \times \mathbb{Z}^n \times E$, every strictly descending sequence in $\mathbb{N}^m \times \mathbb{Z}^n \times E$ is finite. In particular, any subset of $\mathbb{N}^m \times \mathbb{Z}^n \times E$ contains a smallest element.

PROOF. Let $a_1 \succ a_2 \succ a_3 \succ \cdots$ be a strictly descending sequence in $\mathbb{N}^m \times \mathbb{Z}^n \times E$. Since E is a finite set, we may suppose that all $a_j$ are in $\mathbb{N}^m \times \mathbb{Z}^n \times \{e_i\}$ for an $i$. Then Lemma 2.2 shows that the conclusion holds. □

# 3 Gröbner bases in finitely generated difference-differential-modules

Let $\{\mathbb{Z}_j^{(n)}, \quad j = 1, \cdots, k\}$ be an ortant decomposition of $\mathbb{Z}^n$ and "$\prec$" be a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n$ with respect to the ortant decomposition. Let $\Lambda$ be the semi-group introduced in Section 1 in which the elements are of the form (1.1). Since $\Lambda$ is isomorphic to $\mathbb{N}^m \times \mathbb{Z}^n$ as a semigroup, the "$\prec$" would define an order on $\Lambda$. we also call it a generalized term order on $\Lambda$.

Let $R$ be a $\Delta$-$\sigma$-field and $D$ be the ring of $\Delta$-$\sigma$-operators over $R$, 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 an $R$-vector space generated by the set of all elements of the form $\lambda e_i$ ($i = 1, \cdots, q$, where $\lambda \in \Lambda$). This set will be denoted by $\Lambda E$ and its elements will be called "terms" of $F$. In particular the elements of $\Lambda$ will be called "terms" of $D$. If "$\prec$" is a generalized term order on $\mathbb{N}^m \times \mathbb{Z}^n \times B$ then "$\prec$" would define a generalized term order on $\Lambda E$.

It is clear that 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 $a_i \in R$ $(i = 1, \cdots, d)$ and some distinct elements $\lambda_1 e_{j_1}, \cdots, \lambda_d e_{j_d} \in \Lambda E$.

If a term $\lambda e_j$ appears with nonzero coefficient in the form (3.1) of $f$, then it is called a term of $f$. If $(k_1, \cdots, k_m, l_1, \cdots, l_n)$ and $(r_1, \cdots, r_m, s_1, \cdots, s_n)$ are similar elements in $\mathbb{N}^m \times \mathbb{Z}^n$ then the two terms $\lambda_1 = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n}$ and $\lambda_2 = \delta_1^{r_1} \cdots \delta_m^{r_m} \alpha_1^{s_1} \cdots \alpha_n^{s_n}$ of $D$ are called similar. If $\lambda_1$,$\lambda_2 \in \Lambda$ are similar, then the two terms $u = \lambda_1 e_i$,$v = \lambda_2 e_j \in \Lambda E$ are called similar.

DEFINITION 3.1. Let $\lambda_1 = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n}$, $\lambda_2 = \delta_1^{r_1} \cdots \delta_m^{r_m} \alpha_1^{s_1} \cdots \alpha_n^{s_n}$ be two elements in $\Lambda$. If they are similar and $r_\nu \leq k_\nu$,$|s_\mu| \leq |l_\mu|$ for $\nu = 1, \cdots, m$, $\mu = 1, \cdots, n$, then $\lambda_1$ is called a multiple of $\lambda_2$ and it is donoted 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 it is denoted by $v|u$.

DEFINITION 3.2. Let "$\prec$" be a generalized term order on $\Lambda E$, $f \in F$ be of the form (3.1). Then

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

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

Note that in the case of that "$\prec$" is a generalized term order, in general the equation $\lambda lt(f) = lt(\lambda f)$ is not true unless the leading term $lt(f) = \eta e_i$ of $f$ is such that $\eta$ is similar to $\lambda$.

Now we are going to construct the division algorithm in the difference-differential module $F$. First we need some lemmas to describe the multiple properties in difference-differential modules. In what follows we always assume that an ortant decomposition of $\mathbb{Z}^n$ is given and a generalized term order is with respect to the decomposition.

DEFINITION 3.3. Let $\lambda$ be the form of (1.1). Then the subset $\Lambda_j$ of $\Lambda$

$$\Lambda_j = \{\lambda = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n} \ \mid \ (l_1, \cdots, l_n) \in \mathbb{Z}_j^{(n)}\},$$

where $\mathbb{Z}_j^{(n)}$ is the j-th ortant of the decomposition of $\mathbb{Z}^n$, is called $j$-th ortant of $\Lambda$. Let $F$ be a finitely generated free $D$-module and $\Lambda E$ be the set of terms of $F$. Then

$$\Lambda_j E = \{\lambda e_i \ \mid \ \lambda \in \Lambda_j, \ \ e_i \in E\}$$

is called $j$-th ortant of $\Lambda E$.

Obviously, two elements in $\Lambda$ or $\Lambda E$ are similar if and only if they are in same ortant. So from Definition 2.3., if "$\prec$" is a generalized term order on $\Lambda$ and $\xi \prec \lambda$, then $\eta\xi \prec \eta\lambda$ holds for any $\eta$ in the same ortant as $\lambda$.

LEMMA 3.1. Let $\lambda \in \Lambda$ and $a \in R$, "$\prec$" be a generalized term order on $\Lambda E \subseteq D$. Then

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

where $a' = \alpha(a)$ for an $\alpha \in \Gamma$(see (1.1)), and if $a \neq 0$ then $a' \neq 0$; $\xi \in D$ with $lt(\xi) \prec \lambda$ and all terms of $\xi$ are similar to $\lambda$.

PROOF. Let $\lambda = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n}$ as (1.1). Denote $\alpha_1^{l_1} \cdots \alpha_n^{l_n}$ by $\alpha$. Then by the fundamental relations (1.3) we have

$$\lambda a = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha(a)\alpha = \delta_1^{k_1} \cdots \delta_m^{k_m} a'\alpha = (a'\delta_1^{k_1} \cdots \delta_m^{k_m} + \delta)\alpha$$

$$= a'\delta_1^{k_1} \cdots \delta_m^{k_m} \alpha + \delta\alpha,$$

where $\delta \in R[\Delta]$, $a' = \alpha(a)$. Because $\alpha_j \in \sigma$, $j = 1, \cdots, n$, are invertible, we have $a' \neq 0$ if $a \neq 0$.

If $lt(\delta) = \delta_1^{k_1'} \cdots \delta_m^{k_m'}$, then it is obvious that $(k_1, \cdots, k_m) \in \{(k_1', \cdots, k_m') + \mathbb{N}^m\}$ from (1.3). This means that $lt(\delta) \prec \delta_1^{k_1} \cdots \delta_m^{k_m}$. Furthermore, it is easy to show that all terms of $\xi = \delta\alpha$ are similar to $\lambda$. Since $\delta_1^{k_1} \cdots \delta_m^{k_m}$ is in every ortant of $\Lambda$, it is follows that $lt(\xi) = lt(\delta\alpha) \prec \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha = \lambda$. □

In general $lt(\lambda f) = \lambda lt(f)$ is not true. But we have the following Lemma.

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

(i) If $\lambda \in \Lambda$, then $lt(\lambda f) = max_{\prec}\{\lambda \cdot u_i\}$ where $u_i$ are terms of $f$ and then $lt(\lambda f) = \lambda \cdot u$ for an unique term $u$ of $f$.

(ii) If $lt(f) \in \Lambda_j e$ then for any $\lambda \in \Lambda_j$

$$lt(\lambda f) = \lambda \cdot lt(f) \in \Lambda_j E$$

PROOF. (i)Suppose that $f = \sum_{i=1}^{d} a_i \lambda_i e_{j_i}$ as (3.1) and $\lambda \in \Lambda$, then by Lemma 3.1 we have

$$\lambda f = \sum_{i=1}^{d} \lambda a_i \lambda_i e_{j_i} = \sum_{i=1}^{d} (a_i'\lambda + \xi_i)\lambda_i e_{j_i} \tag{3.2}$$

where $\xi_i \in D$ with $lt(\xi_i) \prec \lambda$. Note that $\xi_i = \delta_i\alpha$ in the proof of Lemma 3.1, where $\delta_i \in R[\Delta]$, $\alpha \in \Gamma$. So every term of $\xi_i$ is the form of $\sigma_i\alpha$ with $\sigma_i \in \Theta$(see(1.1)) and $\alpha = \alpha_1^{l_1} \cdots \alpha_n^{l_n}$ such that $\lambda = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n}$ as in the proof of Lemma 3.1. It is follows that

$$\sigma_i\alpha \cdot \lambda_i e_{j_i} \prec \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha \cdot \lambda_i e_{j_i} = \lambda\lambda_i e_{j_i} \tag{3.3}$$

So $lt(\lambda f) \in \{\lambda \cdot \lambda_i e_{j_i}\}$. If $\lambda \cdot \lambda_i e_{j_i} = \lambda \cdot \lambda_i' e_{j_i}'$ then $e_{j_i} = e_{j_i}'$ and $\lambda_i = \lambda_i'$. Therefore $lt(\lambda f) = max_{\prec}\{\lambda \cdot \lambda_i e_{j_i} | i = 1, \cdots, d\} = \lambda \cdot u$ for an unique term $u$ of $f$.

(ii) Suppose that $f$ is as above and $lt(f) = \lambda_1 e_{j_1} \in \Lambda_j E$. If $\lambda \in \Lambda_j$, then in (3.2) we have $\lambda_i e_{j_i} \prec \lambda_1 e_{j_1}$. Then $\lambda$ similar to $\lambda_1$ implys

$$\lambda\lambda_i e_{j_i} \prec \lambda\lambda_1 e_{j_1} \tag{3.4}$$

From (3.3) and (3.4) we conclude that $lt(\lambda f) = \lambda \cdot lt(f) \in \Lambda_j E$. □

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 an unique term $u_j$ of $f$ such that

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

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

PROOF. Let $f$ be the form of (3.1) and then $\{\lambda_i e_{j_i} | i = 1, \cdots, d\}$ be the set of terms of $f$. Let $\lambda_i = \delta^{s_i}\alpha^{t_i}$, $s_i \in \mathbb{N}^m$ and $t_i \in \mathbb{Z}^n$. By Definition 2.1.(iii), the group generated by $\mathbb{Z}_j^{(n)}$ is $\mathbb{Z}^n$. Therefore there exist $u_i,\ v_i \in \mathbb{Z}_j^{(n)}$ such that $u_i - v_i = t_i$. This means that $\alpha^{v_i}\lambda_i = \delta^{s_i}\alpha^{u_i} \in \Lambda_j$. Put $\zeta_i = \alpha^{v_i}$ and $\lambda = \prod_{i=1}^d \zeta_i$, then $\lambda \cdot \lambda_i \in \Lambda_j$ holds for all $i = 1, \cdots, d$. Now we have

$$\lambda f = \sum_{i=1}^{d} \lambda \cdot a_i \lambda_i e_{j_i} = \sum_{i=1}^{d} (a_i' \lambda + \xi_i) \lambda_i e_{j_i}$$

from Lemma 3.1. Because there is no $\delta$ factor in $\lambda$, so $\xi_i = 0$ from the proof of Lemma 3.1. Then all terms of $\lambda f$ are in $\Lambda_j E$ and $lt(\lambda f) \in \Lambda_j E$.

By Lemma 3.2 (i), we may suppose that there are terms $u,\ v$ of $f$ such that $lt(\lambda f) = \lambda u \in \Lambda_j E$, $lt(\eta f) = \eta v \in \Lambda_j E$. For $\lambda,\ \eta \in \Lambda$ the above proof shows there is $\zeta \in \Lambda_j$ such that $\zeta\lambda,\ \zeta\eta \in \Lambda_j$. Then $\lambda v \prec \lambda u$, $\eta u \prec \eta v$ imply $\zeta\lambda v \prec \zeta\lambda u$, $\zeta\eta u \prec \zeta\eta v$ because $\zeta \in \Lambda_j$. Furthmore, this would imply $(\zeta\eta)\zeta\lambda v \prec (\zeta\eta)\zeta\lambda u$, $(\zeta\lambda)\zeta\eta u \prec (\zeta\lambda)\zeta\eta v$ because $\zeta\lambda,\ \zeta\eta \in \Lambda_j$. Then $\zeta\eta\zeta\lambda v = \zeta\eta\zeta\lambda u$ and then $u = v$.

Denote the term $u = v$ of $f$ by $lt_j(f)$, then for any $\lambda \in \Lambda$ such that $lt(\lambda f) \in \Lambda_j E$, $lt(\lambda f) = \lambda \cdot lt_j(f)$. □

If $h \in D,\ f \in F$,then $hf = \sum_{i,k} a_{i,k}\lambda_i u_k$ for some $\lambda_i \in \Lambda$ and $u_k \in \Lambda E$ and some of which are possibly not terms of $h$ and $f$. It would be believed that $lt(hf) \prec \lambda_i u_k$ maybe occur for some $\lambda_i$ and $u_k$ in $hf$. The following Proposition asserts this case will not appear.

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

PROOF. Let $h = \sum_{i\in I} b_i\lambda_i$ where $I$ is a finite set and $\lambda_i,\ i \in I$, are distinct elements in $\Lambda$. Then

$$hf = \sum_{i\in I} b_i \lambda_i f$$

By Lemma 3.2 (i), there is an unique term $u_{k_i}$ of $f$ such that $lt(\lambda_i f) = \lambda_i u_{k_i} \succeq \lambda_i u$ for all terms $u$ of $f$. Since $lt(\lambda_i f) = \lambda_i u_{k_i}$, $i \in I$, are distinct, we have

$$lt(hf) \in \{\lambda_i u_{k_i}\}_{i\in I} = \{lt(\lambda_i f)\}_{i\in I}.$$

In fact, if $lt(\lambda_{i_1} f) = lt(\lambda_{i_2} f)$ then they must be in a same $\Lambda_j E$. It is follows from Lemma 3.3 that there is an unique term $lt_j(f)$ of $f$ such that

$$lt(\lambda_{i_1} f) = \lambda_{i_1} lt_j(f) = lt(\lambda_{i_2} f) = \lambda_{i_2} lt_j(f) \in \Lambda_j E.$$

Therefore $\lambda_{i_1} = \lambda_{i_2}$. This means that there is a unique $i$ such that

$$lt(hf) = lt(\lambda_i f) = \lambda_i u_{k_i} \tag{3.5}$$

Denote $\lambda_i$ by $\lambda$, $u_{k_i}$ by $u$, we have

$$lt(hf) = \lambda u \succeq \lambda_i \cdot u_k$$

for all terms $\lambda_i$ of $h$ and all trems $u_k$ of $f$. □

THEOREM 3.1. Let $\Sigma = \{f_1, \cdots, f_p\} \subseteq F \backslash \{0\}$, $g \in F$. Then

$$g = h_1 f_1 + \cdots + h_p f_p + r \tag{3.6}$$

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

(i) $h_i = 0$ or $lt(h_i f_i) \preceq lt(g)$, $i = 1, \cdots, p$; (By Proposition 3.1 this means that $\lambda u \preceq lt(g)$ for all terms $\lambda$ of $h_i$ and all terms $u$ of $f_i$.)

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

PROOF. The elements $h_1, \cdots, h_p \in D$ and $r \in F$ can be computed as follows:

First set $r = g$ and $h_i = 0$, $i = 1, \cdots, p$.

While $r \neq 0$ and $lt(r)$ is a multiple of $lt(\lambda_i f_i)$ for a element $\lambda_i \in \Lambda$, suppose $lt(\lambda_i f_i) \in \Lambda_j E$, then there exists a element $\eta \in \Lambda_j$ such that

$$lt(r) = \eta \cdot lt(\lambda_i f_i).$$

By Lemma 3.2.(ii), $lt(\eta \cdot \lambda_i f_i) = \eta \cdot lt(\lambda_i f_i) = lt(r)$. Then

$$\eta \cdot \lambda_i f_i = c_i \eta \cdot lt(\lambda_i f_i) + \xi_i$$

$$c_i \eta \cdot lt(\lambda_i f_i) = \eta \cdot \lambda_i f_i - \xi_i$$

where $c_i = lc(\eta \cdot \lambda_i f_i)$ and $lt(\xi_i) \prec \eta \cdot lt(\lambda_i f_i)$. Therefore

$$r = lc(r)lt(r) + \cdots = lc(r)\eta \cdot lt(\lambda_i f_i) + \cdots = \frac{lc(r)}{c_i}(\eta \lambda_i f_i - \xi_i).$$

Put $b_i = \frac{lc(r)}{c_i}$ and $r_i = \frac{lc(r)}{c_i} \cdot (-\xi_i)$. Then

$$r = b_i \eta \lambda_i f_i + r_i.$$

Now we may replace $r$ by $r_i$ and $h_i$ by $h_i + b_i \eta \lambda_i$. Since in each step we have

$$lt(r_i) \prec lt(\eta \cdot \lambda_i f_i) \preceq lt(r) \preceq lt(g),$$

by the Corollary of Lemma 2.2, the algorithm above terminates after finitely many steps. This completes the proof. □

DEFINITION 3.4. Let $\{f_1, \cdots, f_p\} \subseteq F \backslash \{0\}$, $g \in F$. Suppose that the equation (3.6) hold and satisfy the conditions (i), (ii) in Theorem 3.1. If $r \neq g$ we say $g$ can be reduced by $\{f_1, \cdots, f_p\}$ to $r$. In this case we have $lt(r) \prec lt(g)$ by the proof of Theorem 3.1. In the case of $r = g$ and $h_i = 0$, $i = 1, \cdots, p$, we say that $g$ is reduced with respect to $\{f_1, \cdots, f_p\}$.

The following example illustrates the reason for the condition (ii) in Theorem 3.1.

EXAMPLE 3.1. Let $R = \mathbb{Q}(x_1, x_2)$, $D = R[\delta_1, \delta_2, \alpha, \alpha^{-1}]$. Where $\delta_1$, $\delta_2$ are the partial derivative by $x_1$, $x_2$ respectively, and $\alpha$ is an automorphism of $R$. Choose generalized term order on $\mathbb{N}^2 \times \mathbb{Z}$ as in Example 2.3, i.e.

$$u = \delta_1^{k_1}\delta_2^{k_2}\alpha^l \prec v = \delta_1^{r_1}\delta_2^{r_2}\alpha^s$$

$$\Longleftrightarrow (\|u\|, k_1, k_2, l) < (\|v\|, r_1, r_2, s) \ \ \textit{in lexicographic order.}$$

Where $\|u\| = k_1 + k_2 + |l|$.

Let $g = \delta_1\alpha^{-2} + \delta_2\alpha^2$, $f = \delta_1\alpha^{-1} + \alpha$. 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 $lt(r_1) = \delta_2\alpha^2$ is not any multiple of $lt(f) = \delta_1\alpha^{-1}$, we can find $\lambda = \delta_2\alpha$ such that $lt(r_1) = lt(\lambda f) = lt(\delta_1\delta_2 + \delta_2\alpha^2)$. 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. Then $g$ is reduced by $f$ to $r_2$. □

DEFINITION 3.5. Let $W$ be a submodule of the finitely generated free $D$-module $F$ and $\prec$ be a generalized term order on $\Lambda E$. $G = \{g_1, \cdots, g_p\} \in W\backslash\{0\}$. Then $G$ is called a Gröbner basis of $W$ (with respect to the generalized term order $\prec$) if and only if for any $f \in W\backslash\{0\}$, $lt(f)$ is a multiple of $lt(\lambda g_j)$ for some $\lambda \in \Lambda$, $g_j \in G$. If every element of $G$ is reduced with respect to other element of $G$, then $G$ is called a reduced Gröbner basis of $W$.

Remark: In classical case we can have $\lambda \cdot lt(g_j) = lt(\lambda g_j)$, but not in our case.

PROPOSITION 3.2. Let $G$ be a finite subset of $W\backslash\{0\}$. 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 with respect to $G$ if and only if $f = 0$.

PROOF. (i) If $G$ is a Gröbner basis of $W$, $f \in W$, then from Theorem 3.1 $f$ can be reduced by $G$ to $r$ with $lt(r)$ is not a multiple of any $lt(\lambda g)$, $\lambda \in \Lambda$, $g \in G$. If $r \neq 0$ then $r \in W$ therefore $lt(r)$ must be a multiple of $lt(\lambda g)$ for a $g \in G$, a contradiction.

If every $f \in W$ can be reduced by $G$ to 0, then $f = \sum_{g\in G} h_g g$. By Proposition 3.1, there is a $g \in G$ such that $lt(f) = max_{g\in G}\{lt(h_g g)\} = \lambda u$ for a term of $h_g$ and a term of $g$. Then $lt(f) = lt(\lambda g)$. By Difinition 3.4 $G$ is a Gröbner basis of $W$.

(ii) and (iii). It is obvious from Theorem 3.1 and Difinition 3.4. □

EXAMPLE 3.2. 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 Gröbner basis of $W$. In fact, $0 \neq f \in W$ implies $f = hg$ for a $0 \neq h \in D$. By Proposition 3.1, $lt(f) = \lambda u = max_{\prec}\{\lambda_i u_k\}$ for a term $\lambda$ of $h$ and a term $u$ of $g$. Then $lt(f) = lt(\lambda g)$. By Definition 3.4, $G$ is a Gröbner basis of $W$.

Below we will consider the Buchberger's algorithm for computing a Gröbner basis of a submodule $W$ of $F$.

DEFINITION 3.6. Let $F$ be a finitely generated free $D$-module and $f,\ g \in F\backslash\{0\}$. For every $\Lambda_j$ let $V(j, f, g)$ be a finite system of generators of the $R[\Lambda_j]$-module ${}_{R[\Lambda_j]}\langle lt(\lambda f) \in \Lambda_j E \mid \lambda \in \Lambda\rangle \bigcap_{R[\Lambda_j]}\langle lt(\eta g) \in \Lambda_j E \mid \eta \in \Lambda\rangle$. 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 computation of $V(j, f, g)$ is involved in the generalized term order on $\Lambda e$. Pauer and Unterkircher(1999) researched $V(j, f, g)$ in commutative Laurent polynomial rings and gave algorithm for some important cases. Their results are still valid for difference-differential modules.

EXAMPLE 3.3. Let $F = D = R[\delta_1, \delta_2, \alpha_1, \alpha_1^{-1}, \alpha_2, \alpha_2^{-1}]$ and $R = \mathbb{Q}(x_1, x_2)$. Where $\delta_1,\ \delta_2$ are the partial derivative by $x_1,\ x_2$ respectively, and $\alpha_1,\ \alpha_2$ are two automorphism of $R$. Choose the generalized term order on $\mathbb{N}^2 \times \mathbb{Z}^2$ as in Example 2.5, i.e.

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

$$\Longleftrightarrow (\|u\|, k_1, k_2, l_1, l_2) < (\|v\|, r_1, r_2, s_1, s_2) \ \ \textit{in lexicographic order.}$$

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

Let $f = \alpha_1^{-2} - \delta_2$, $g = \delta_1 + \alpha_2^4$. Note that the ortants of $\Lambda$ are $\Lambda_0, \Lambda_1, \Lambda_2$ which described in Example 2.2 for $n = 2$. It is easy to see that

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

and

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

Then $V(0, f, g) = \{v_0\} = \{\delta_1\delta_2\alpha_1^2\}$ and by Definition 3.5,

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

Similarly we have

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

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

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

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

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

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

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

□

For the proof of theorem 3.2 we need the following lemmas.

LEMMA 3.4. Let $\{r_1, \cdots, r_l\} \subseteq F$ and $\{a_1, \cdots, a_l\} \subseteq R$. If $\sum_{j=1}^{l} a_j = 0$ , then

$$\sum_{j=1}^{l} a_j r_j = \sum_{i,k} b_{i,k}(r_i - r_k)$$

for some $1 \leq i,\ k \leq l$.

PROOF. It is easy to see that

$$\sum_{j=1}^{l} a_j r_j = a_1(r_1 - r_2) + (a_1 + a_2)(r_2 - r_3) + (a_1 + a_2 + a_3)(r_3 - r_4)$$

$$+ \cdots + (a_1 + a_2 + \cdots + a_{l-1})(r_{l-1} - r_l) + (a_1 + a_2 + \cdots + a_l)r_l.$$

Since $a_1 + a_2 + \cdots + a_l = 0$ it follows that

$$\sum_{j=1}^{l} a_j r_j = \sum_{i,k} b_{i,k}(r_i - r_k)$$

for some $1 \leq i,\ k \leq l$. □

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 $v \in V(j, g_i, g_k)$ which is defined in Definition 3.6, such that $u = \zeta v$. Therefore if $G$ is a finite subset of $F\backslash\{0\}$ and the S-polynomials $S(j, g_i, g_k, v)$ 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 $g \in G$.

PROOF. Suppose $V(j, g_i, g_k) = \{v_1, \cdots, v_l\}$. Then

$$u = \sum_{\mu} p_\mu v_\mu$$

where $p_\mu \in R[\Lambda_j]$. Since $p_\mu = \sum_\nu a_{\mu\nu}\lambda_{\mu\nu}$, where $a_{\mu\nu} \in R$ and $\lambda_{\mu\nu} \in \Lambda_j$, it follows that

$$u = \sum_{\mu,\nu} a_{\mu\nu}(\lambda_{\mu\nu}v_\mu)$$

Note that $u$ and $\lambda_{\mu\nu}v_\mu$ are terms in $\Lambda_j E$ and we can rewrite the right of the equation such that the terms $\lambda_{\mu\nu}v_\mu$ are distinct. Then we see that there is an unique $a_{\mu\nu} = 1$ and others are zero. Then $u = \zeta v$ for a $\zeta \in \Lambda_j$ and $v \in V(j, g_i, g_k)$.

Now if $S(j, g_i, g_k, v)$ can be reduced to 0 by $G$ then

$$S(j, g_i, g_k, v) = \sum_{g\in G} h'_g g$$

and $lt(h'_g g) \preceq lt(S(j, g_i, g_k, v)) \prec v$ for $g \in G$. Therefore

$$\zeta S(j, g_i, g_k, v) = \sum_{g\in G}(\zeta h'_g)g = \sum_{g\in G} h_g g$$

where $h_g = \zeta h'_g$. By Lemma 3.2 (i), $lt(\zeta h'_g g) = \zeta w$ for a term $w$ of $h'_g g$. Then $lt(h_g g) = lt(\zeta h'_g g) = \zeta w$. Therefore $w \preceq lt(h'_g g) \prec v$ and $\zeta \in \Lambda_j$ imply that $\zeta w \prec \zeta v = u$. □

THEOREM 3.2. (Generalized Buchberger Theorem) Let $F$ be a free $D$-module and $\prec$ be a generalized term order on $\Lambda E$, $G$ 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 $\Lambda_j$, 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 $G$.

PROOF. If $G$ is a Gröbner basis of $W$, since $S(j, g_i, g_k, v)$ is a element of $W$, then it follows from Proposition 3.2 that $S(j, g_i, g_k, v)$ can be reduced to 0 by $G$.

Now let $G$ be a finite subset of $F\backslash\{0\}$ and $W$ be the submodule in $F$ generated by $G$. Suppose that for all $\Lambda_j$, for all $v \in V(j, g_i, g_k)$ and for all $g_i,\ g_k \in G$, the S-polynomials $S(j, g_i, g_k, v)$ can be reduced to 0 by $G$. We have to show for any $f \in W\backslash\{0\}$, there is an $\lambda \in \Lambda$, $g \in G$ such that $lt(f) = lt(\lambda g)$.

Since $W$ is generated by $G$, we have

$$f = \sum_{g\in G} h_g g$$

for some $\{h_g\}_{g\in G} \subseteq D$.

Let $u = max_\prec\{lt(h_g g) \mid g \in G\}$. We may choose the family $\{h_g \mid g \in G\}$ such that $u$ is minimal, i.e. if $f = \sum_{g\in G} h'_g g$ then $u \preceq max_\prec\{lt(h'_g g) \mid g \in G\}$. Note that $u \succeq \lambda g$ for all terms $\lambda$ of $h_g$ and all $g \in G$ by Proposition 3.1.

If $lt(f) = u = lt(h_g g)$ for some $g \in G$, then it is follows from equation (3.5) that there is a term $\lambda$ of $h_g$ such that $lt(f) = lt(\lambda g)$. Therefore the proof would be completed. Hence it remains to show that $lt(f) \prec u$ cannot hold.

Suppose $lt(f) \prec u$ and let $B = \{g \mid lt(h_g g) = u \succ lt(f)\}$. Then by equation (3.5) in the proof of Proposition 3.1, there is an unique term $\lambda_g$ of $h_g$, $g \in B$, such that $u = lt(\lambda_g g) \succ lt(\eta_g g)$ for any terms $\eta_g \neq \lambda_g$ of $h_g$. Let $c_g$ be the coefficient of $h_g$ at $\lambda_g$. We have

$$f = \sum_{g\in B} h_g g + \sum_{g\notin B} h_g g = \sum_{g\in B} c_g\lambda_g g + \sum_{g\in B}(h_g - c_g\lambda_g)g + \sum_{g\notin B} h_g g, \qquad (3.7)$$

where all terms appearing in the last two sums are $\prec u$.

From Lemma 3.2 (i), suppose $v_g$ is the term of $g$ such that $u = lt(\lambda_g g) = \lambda_g v_g \succ \lambda_g v$ for any terms $v \neq v_g$ of $g$. Let $d_g$ be the coefficient of $g$ at $v_g$. Then by Lemma 3.1,

$$\sum_{g\in B} c_g\lambda_g g = \sum_{g\in B} c_g\lambda_g d_g(\frac{g}{d_g}) = \sum_{g\in B} c_g(d'_g\lambda_g + \xi_g)(\frac{g}{d_g})$$

$$= \sum_{g\in B} c_g d'_g\lambda_g(\frac{g}{d_g}) + \sum_{g\in B} c_g\xi_g(\frac{g}{d_g}) \qquad (3.8)$$

for some elements $d'_g \in R$ and $\xi_g \in D$ with all terms appear in the last sum are $\prec u$.

Note that $u$ appear only in

$$\sum_{g\in B} c_g d'_g\lambda_g(\frac{g}{d_g}) = \sum_{g\in B} c_g d'_g\lambda_g v_g + \sum_{g\in B} c_g d'_g\lambda_g(\frac{g}{d_g} - v_g)$$

$$= (\sum_{g\in B} c_g d'_g)u + \sum_{g\in B} c_g d'_g\lambda_g(\frac{g}{d_g} - v_g)$$

and all terms appearing in the last sum are $\prec u$. Since $lt(f) \prec u$ it follows that $\sum_{g\in B} c_g d'_g = 0$. Denote $\lambda_g(\frac{g}{d_g})$ by $r_g$, then by Lemma 3.4,

$$\sum_{g\in B} c_g d'_g\lambda_g(\frac{g}{d_g}) = \sum_{g\in B}(c_g d'_g)r_g = \sum_{i,k} b_{i,k}(r_{g_i} - r_{g_k}) \qquad (3.9)$$

for some $g_i,\ g_k \in B$.

Since

$$r_{g_i} - r_{g_k} = \lambda_{g_i}(\frac{g_i}{d_{g_i}}) - \lambda_{g_k}(\frac{g_k}{d_{g_k}})$$

and $\lambda_{g_i}v_{g_i} = \lambda_{g_k}v_{g_k} = u \in \Lambda_j E$ for an $\Lambda_j$, it follows from Lemma 3.3 that $v_{g_i} = lt_j(g_i),\ v_{g_k} = lt_j(g_k),\ d_{g_i} = lc_j(g_i),\ d_{g_k} = lc_j(g_k),\ \lambda_{g_i} = \frac{u}{lt_j(g_i)},\ \lambda_{g_k} = \frac{u}{lt_j(g_k)}$ and then

$$r_{g_i} - r_{g_k} = \frac{u}{lt_j(g_i)}\frac{g_i}{lc_j(g_i)} - \frac{u}{lt_k(g_k)}\frac{g_k}{lc_j(g_k)}$$

with $lt(r_{g_i} - r_{g_k}) \prec u$.

Note that for all $\Lambda_j$, for all $v \in$ and for all $g_i,\ g_k \in G$, the S-polynomials $S(j, g_i, g_k, v)$ can be reduced to 0 by $G$. Then by Lemma 3.5, we have

$$r_{g_i} - r_{g_k} = \sum_{g\in G} p_g g \qquad (3.10)$$

with $lt(p_g g) \prec u$.

Substitute the first sum in the right of (3.7) by (3.8), and substitute the first sum in the right of (3.8) by (3.9), then substitute $r_{g_i} - r_{g_k}$ in the right of (3.9) by

(3.10), we get another form of $f = \sum_{g\in G} h'_g g$ and $u \succ max_{\prec}\{lt(h'_g g) \mid g \in G\}$, which is a contradiction to the minimality of $u$. This completes the proof of the theorem. □

EXAMPLE 3.4. If $W$ is a submodule of $F$ generated by a finite set $G$ and every $g, g \in G$, include only one term, then $G$ is a Gröbner basis of $W$. In fact in this case all $S$-polynomials $S(j, g_i, g_k, v) = 0$. By Theorem 3.2 this implies that $G$ is a Gröbner basis of $W$.

THEOREM 3.3. (Buchberger's Algorithm) Let $F$ be a free $D$-module and $\prec$ be a generalized term order on $\Lambda E$, $G$ be a finite subset of $F\backslash\{0\}$ and $W$ be the submodule in $F$ generated by $G$. For each $\Lambda_j$ 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:** $G = \{g_1, \cdots, g_\mu\}$ which is a set of generators of $W$
**output:** $G' = \{g'_1, \cdots, g'_\nu\}$ which is a Gröbner basis of $W$
**Begin**
$G_0 := G$
**While** there exist $f, g \in G_i$ and $v \in V(j, f, g)$ such that $S(j, f, g, v)$ reduced to $r \neq 0$ by $G_i$
**Do** $G_{i+1} := G_i \bigcup \{r\}$
**If** $G_{i+1} = G_i$ **then** $G_{i+1} = G'$
**End**

PROOF. By Theorem 3.2 we only have to show that there is an $i \in \mathbb{N}$ such that $G_{i+1} = G_i$. Suppose there is no such $i \in \mathbb{N}$. Since in every step of the algorithm we get $r$ such that $lt(r)$ is not a multiple of any $lt(\lambda g),\ \lambda \in \Lambda,\ g \in G_i$, if $lt(r) \in \Lambda_j E$ then $R_j^{(i)} =_{R[\Lambda_j]} \langle lt(\lambda g) \in \Lambda_j E \mid \lambda \in \Lambda,\ g \in G_i\rangle \subset R_j^{(i+1)} =_{R[\Lambda_j]} \langle lt(\lambda g) \in \Lambda_j E \mid \lambda \in \Lambda,\ g \in G_{i+1}\rangle$ as $R[\Lambda_j]$-submodule of $\bigoplus_{e\in E} R[\Lambda_j]e$. Therefore for all $i \in \mathbb{N}$ there is an $m \in \mathbb{N}$ such that $R_j^{(i)} \subsetneq R_j^{(i+m)}$. Since $R[\Lambda_j]$ is noetherian this is not possible. □

EXAMPLE 3.5. Let $F$ and the generalized term order on $\Lambda$ 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 $W$ which generated by $G$. To prove this, we must show all $S$-polynomials of $G$ reduced to 0 by $G$.

Following the method described in Example 3.3, we have

$$V(0, g_1, g_2) = \{\alpha_1^2\alpha_2^4\} \quad V(1, g_1, g_2) = \{\alpha_1^{-1}\alpha_2^3\} \quad V(2, g_1, g_2) = \{\alpha_1\alpha_2^{-1}\}$$

$$S(0, g_1, g_2, \alpha_1^2\alpha_2^4) = \alpha_1^2 g_1 - \alpha_2^4 g_2 = \alpha_1^2 + \alpha_2^4 = g_1 + g_2$$

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

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

and

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

$$S(0, g_1, g_3, \alpha_1^2\alpha_2^4) = \alpha_1^2 g_1 - g_3 = \alpha_1^2 - 1 = g_2$$

$$S(1, g_1, g_3, \alpha_1^{-1}\alpha_2^3) = \alpha_1^{-1}\alpha_2^{-1}g_1 - \alpha_1^{-1}\alpha_2^3 g_3 = \alpha_1^{-1}\alpha_2^{-1} - \alpha_1\alpha_2^7$$
$$= (\alpha_1^{-1}\alpha_2^{-1})g_3 - \alpha_1\alpha_2^3 g_1$$

Note that the right of this equation satisfies the condition in Theorem 3.1 (i), i.e. $lt(h_i g_i) \preceq lt(S)$.

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

and

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

$$S(0, g_2, g_3, \alpha_1^2\alpha_2^4) = \alpha_2^4 g_2 - g_3 = -\alpha_2^4 - 1 = -g_1$$
$$S(1, g_2, g_3, \alpha_1^{-1}) = \alpha_1^{-1}g_2 - \alpha_1^{-1}g_3 = \alpha_1\alpha_2^4 + \alpha_1 = \alpha_1 g_1$$
$$S(2, g_2, g_3, \alpha_1\alpha_2^{-1}) = \alpha_1^{-1}\alpha_2^{-1}g_2 - \alpha_1\alpha_2^{-1}g_3 = -\alpha_1^{-1}\alpha_2^{-1} - \alpha_1^3\alpha_2^3$$
$$= \alpha_1^{-1}\alpha_2^{-1}g_3 + \alpha_1\alpha_2^3 g_2$$

The right of this equation also satisfies the condition in Theorem 3.1 (i).

Then, by Theorem 3.2, $G$ is a Gröbner basis of $W$. □

# 4 Characteristic sets and reduced Gröbner bases of difference-differential-modules

The notion of characteristic set is introduced first in differential algebra by Ritt (1950)(see Kolchin (1973) also). Then Levin (2000) introduced it to difference-differential modules with respect to a special order. In this section we introduce the concept of characteristic set of difference-differential-modules in a similar manner as that of Levin. But our characteristic set is with respect to any generalized term order on $\Lambda E$ and the proof of many results are differ. Then we prove that a characteristic set is a reduced Gröbner basis which defined by Definition 3.5. Also we consider some interest results about reduced Gröbner bases of difference-differential-modules.

DEFINITION 4.1. Let $F$ be a free $D$-module and $\prec$ be a generalized term order on $\Lambda E$, $G$ be a subset of $F\backslash\{0\}$. If every element of $G$ is reduced with respect to other elements of $G$, then $G$ is called autoreduced.

PROPOSITION 4.1. If $G$ is an autoreduced subset of $F$, then $G$ must be a finite set.

PROOF. Let $G$ be an autoreduced set of $F$. Suppose $G$ is infinite. Then the set $V = \{lt(g) \mid g \in G\}$ is infinite and it does not contain two equal elements. Since $V \subseteq \Lambda E$, there exists an $\Lambda_j$ and a $e_i \in E$ such that $V' \subseteq \Lambda_j e_i$ for an infinite subset $V'$ of $V$. By Definition 3.3, $\Lambda_j$ is correspondent to $\mathbb{Z}_j^{(n)}$ and by Definition 2.1, $\mathbb{Z}_j^{(n)}$ is a finitely generated semigroup. Then there is a finite set $\Sigma = \{\sigma_1, \cdots, \sigma_n\}$ such that $\{\delta_1, \cdots, \delta_m, \sigma_1, \cdots, \sigma_n\}$ is a set of free generators of $\Lambda_j$ as a semigroup. Choose an element $u_1 = \lambda e_i \in V'$ and suppose

$\lambda = \delta_1^{k_1} \cdots \delta_m^{k_m} \sigma_1^{l_1} \cdots \sigma_n^{l_n}$. Then there must be an element $u_2 = \eta e_i \in V'$, $\eta = \delta_1^{r_1} \cdots \delta_m^{r_m} \sigma_1^{s_1} \cdots \sigma_n^{s_n}$, such that

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

This is because, in the set $\Lambda_j$ of terms we can use Dickson's Lemma as in normal polynomial rings and the Dickson's Lemma says in an infinite set of terms $V'$, there must be a finite subset $\{u_1, \cdots, u_l\}$ such that any $u \in V'$ can be divided exactly by a $u_i$, $i = 1, \cdots, l$. So if no such element $u_2 = \eta e_i \in V'$, $V'$ would be a finite set. Therefore $u_2 = \eta e_i = \zeta \lambda e_i = \zeta u_1$ for a $\zeta \in \Lambda_j$. This means that there is a $lt(g_2) = \zeta \cdot lt(g_1)$ and $lt(g_1) \in \Lambda_j e_i$. By Lemma 3.2 (ii) we have $lt(g_2) = lt(\zeta g_1)$. This is a contradiction with the fact that $G$ is an autoreduced set. □

PROPOSITION 4.2. Let $G \subseteq F$ and $W$ be the submodule of $F$ generated by $G$. Then there exists a subset $G'$ of $F$ such that $G'$ is autoreduced and $G'$ generates $W$.

PROOF. By the following algorithm an autoreduced subset $G'$ of $F$ can be computed from $G$:

**Input:** $G = \{g_1, \cdots, g_\mu\}$
**output:** $G' = \{g'_1, \cdots, g'_\nu\}$ which is autoreduced
**Begin**
$G_0 := G$
**While** there exist $g \in G_i$ such that $g$ can be reduced to $r$ by $G_i \backslash \{g\}$
**Do**
  If $r \neq 0$ then $G_{i+1} := G_i \backslash \{g\} \bigcup \{r\}$
  If $r = 0$ then $G_{i+1} := G_i \backslash \{g\}$
**If** $G_{i+1} = G_i$ **then** $G_{i+1} = G'$
**End**

Since in every step $lt(r) \prec lt(g)$ from Definition 3.4, it is easy to show that there is an $i \in \mathbb{N}$ such that $G_{i+1} = G_i$. In fact if such $i$ do not exist, then there is series $\{r_i | i \in \mathbb{N}\}$ such that $lt(r_{i+1} \prec lt(r_i)$ which is a contradiction with the Corollary of Lemma 2.2.

It is obvious that $G'$ generates the submodule $W$ if $G$ is a set of generators of $W$. □

DEFINITION 4.2. Let $G = \{g_1, \cdots, g_\mu\}$, $G' = \{g'_1, \cdots, g'_\nu\}$ be two autoreduced set of $F$. An autoreduced set $G$ is said to have lower rank than $G'$ if one of the following two case holds:

(i) There exists $k \in \mathbb{N}$ such that $k \leq min\{\mu, \nu\}$, $lt(g_i) = lt(g'_i)$ for $i = 1, \cdots, k-1$ and $lt(g_k) \prec lt(g'_k)$.

(ii) $\mu \geq \nu$ and $lt(g_i) = lt(g'_i)$ for $i = 1, \cdots, \nu$.

If $\mu = \nu$ and $lt(g_i) = lt(g'_i)$ for $i = 1, \cdots, \nu$, then $G$ is said to have same rank as $G'$.

Obviously, the rank of an autoreduced set $G$ is involved to the range of elements of $G$. In what follows, when consider an autoreduced set $G = \{g_1, \cdots, g_\mu\}$, we always mean that $lt(g_1) \prec lt(g_2) \prec \cdots \prec lt(g_\mu)$.

THEOREM 4.1. In every nonempty set of autoreduced subsets of $F$ there exists an autoreduced subset of lowest rank.

PROOF. Let $\Omega = \{G_i \mid i \in I\}$ be an nonempty set of autoreduced subsets of $F$. Suppose $G_i = \{g_1^{(i)}, \cdots, g_{r_i}^{(i)}\}$. Let $u_k = min_{\prec}\{lt(g_k^{(i)})\}_{i\in I}$. Define by induction an infinite descending chain of subsets of $\Omega$ as follows: $\Omega_0 = \Omega$, $\Omega_1 = \{G_i \in \Omega_0 \mid r_i \geq 1, lt(g_1^{(i)}) = u_1\}$, $\cdots$, $\Omega_k = \{G_i \in \Omega_{k-1} \mid r_i \geq k, lt(g_k^{(i)}) = u_k\}$. If $\Omega_k$ were nonempty for all $k \in \mathbb{N}$, then there is a infinite set $V = \{u_k \mid k \in \mathbb{N}\}$. Similar to the proof of Proposition 4.1, there exist a $\Lambda_j$, an $e_l$ and $u_{k_1}, u_{k_2} \in \Lambda_j e_l$, $k_1 > k_2$, such that $u_{k_1} = \lambda u_{k_2}$ for an $\lambda \in \Lambda_j$. Since $k_1 > k_2$ it follows that $\Omega_{k_1} \subseteq \Omega_{k_2}$, and this implys that if $G_i \in \Omega_{k_1}$ then $G_i \in \Omega_{k_2}$. Choose a such $G_i$, then by Lemma 3.2 (ii), we have $lt(g_{k_1}^{(i)}) = lt(\lambda g_{k_2}^{(i)})$, this would contradict that $G_i$ is an autoreduced subset. □

DEFINITION 4.3. Let $F$ be a free $D$-module and $\prec$ be a generalized term order on $\Lambda E$, $W$ be a submodule of $F$. Then an autoreduced subset of $W$ of lowest rank is called a characteristic set of $W$.

THEOREM 4.2. Let $G$ be a characteristic set of $W$. The following assertions hold:

(i) $f \in F$, then $f \in W$ if and only if $f$ can be reduced by $G$ to 0.
(ii) $G$ generates the $D$-module $W$.
(iii) $f \in W$ is reduced with respect to $G$ if and only if $f = 0$.

PROOF. (i) Obviously if $f$ can be reduced by $G$ to 0, then $f \in W$. Suppose that $G = \{g_1, \cdots, g_\mu\}$ and $0 \neq f \in W$ is reduced with respect to $G$. Then $lt(f) \neq lt(g_1)$ by Theorem 3.1. If $lt(f) \prec lt(g_1)$ then $\{f\}$ would be an autoreduced subset of $W$ of lower rank than $G$ by Definition 4.2, this is not possible.

Suppose that $lt(f) \succ lt(g_1)$. Put $G' = \{g \in G \mid lt(g) \prec lt(f)\} \bigcup \{f\}$. Then $G'$ would be an autoreduced subset of $W$ of lower rank than $G$. This would contradict that $G$ is a characteristic set.

(ii) Let $0 \neq f \in W$. Then By Theorem 3.1 we have $f = \sum_{g\in G} h_g g + r$ and $r$ is reduced with respect to $G$. This implies $r = 0$ with (i).

(iii) It follows from (i). □

COROLLARY. Let $G$ be a characteristic set of $W$. Then $G$ is a Gröbner basis of $W$. Furthmore, $G$ is a reduced Gröbner basis of $W$. So there exist reduced Gröbner bases in $W$.

PROOF. It follows from Proposition 3.2 (iii) and Theorem 4.2. □

If $G$ is a Gröbner basis of $W$, then the autoreduced algorithm in Proposition 4.2 gives an autoreduced subset $G'$ from $G$. Unfortunately, in our case $G'$ may be not a Gröbner basis of $W$, unlike usual cases.

EXAMPLE 4.1. Let $W$ and $G = \{g_1, g_2, g_3\} = \{\alpha_2^4 + 1, \alpha_1^2 - 1, \alpha_1^2\alpha_2^4 + 1\}$ as in Example 3.5. Then $G$ is a Gröbner basis of $W$. But $G$ is not an autoreduced subset of $W$. Infact we have $g_3 = \alpha_1^2 g_1 - g_2$. So the autoreduced subset from $G$

is $G' = \{g_1, g_2\} = \{\alpha_2^4+1, \alpha_1^2-1\}$. $G'$ is not a Gröbner basis of $W$ because there are $S$-polynomials of $G'$ which don't reduced to 0 by $G'$ (see Example 3.5):

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

So $r$ can be reduced to 0 by $g_3$ but $r$ can not be reduced to 0 by $g_1$, $g_2$. Even though $r = (\alpha_1^{-1}\alpha_2^{-1})g_3 = (\alpha_1^{-1}\alpha_2^{-1})(\alpha_1^2 g_1 - g_2) = \alpha_1\alpha_2^{-1}g_1 - \alpha_1^{-1}\alpha_2^{-1}g_2$, the leading term $lt(\alpha_1\alpha_2^{-1}g_1) = lt(\alpha_1^{-1}\alpha_2^{-1}g_2) = \alpha_1\alpha_2^{-1}$ is larger than $lt(r) = \alpha_1^{-1}\alpha_2^{-1}$. In fact $\alpha_1\alpha_2^{-1}g_1 - \alpha_1^{-1}\alpha_2^{-1}g_2$ is just an $S$-polynomial $S(2, g_1, g_2, \alpha_1\alpha_2^{-1})$. (see Example 3.5). It may be seen also that $lt(r)$ is not any multiple of $lt(\lambda g_i)$, $i = 1, 2$, $\lambda \in \Lambda$. So by Theorem 3.1, $r$ is reduced with respect to $G'$. □

In usual commutative algebra, if $G = \{g_1, \cdots, g_\mu\}$ is a Gröbner basis of $W$, then $G_1 = \{\lambda_1 g_1, \cdots, \lambda_\mu g_\mu\}$ may be not a Gröbner basis of $W$. But in our case we have the following assertion.

PROPOSITION 4.3. Let $F$ be a free $D$-module and $\prec$ be a generalized term order on $\Lambda E$, $W$ be a submodule of $F$. If $G = \{g_1, \cdots, g_\mu\}$ is a Gröbner basis of $W$, then $G_1 = \{g_1', \cdots, g_\mu'\}$ also is a Gröbner basis of $W$, where $g_i' = \lambda_i g_i$ and $\lambda_i$, $i = 1, \cdots, \mu$, are invertible elements in $\Lambda$ (i.e. $\lambda_i \in \Gamma$, see (1.1)).

PROOF. Since $G$ is a Gröbner basis of $W$, by Definition 3.5, for any $f \in W\backslash\{0\}$, there is an $\lambda \in \Lambda$ such that $lt(f) = lt(\lambda g_i)$ for some $i$. It follows that $lt(f) = lt(\lambda g_i) = lt((\lambda\lambda_i^{-1})g_i')$ for some $i$. This means that $G_1$ is a Gröbner basis of $W$ by Definition 3.5. □

Example 4.1 shows, even $G$ is a Gröbner basis of $W$, the autoreduced subset $G'$ from $G$ is not a Gröbner basis of $W$ generally. Note that $G'$ and $G$ generate the same module $W$. We may get a Gröbner basis $G''$ again with Buchberger's algorithm from $G'$.

EXAMPLE 4.2. Let $W$ and $G$, $G'$ be as in Example 4.1. Put

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

and $G'' = \{g_1, g_2, r\}$. Since $G = \{g_1, g_2, g_3\}$ is a Gröbner basis of $W$ and $r = (\alpha_1^{-1}\alpha_2^{-1})g_3$, it follows that $G''$ is a Gröbner basis of $W$ by Proposition 4.3. It is easy to check that $G''$ is an autoreduced subset of $W$. So $G''$ is a reduced Gröbner basis of $W$. □

In usual commutative algebra, if reduced Gröbner bases $G = \{g_1, \cdots, g_\mu\}$ with $lc(g_i) = 1$, $i = 1, \cdots, \mu$, then it exists uniquely. But in our $D$-module's case this is not true, while the Corollary of Theorem 4.2 asserts reduced Gröbner bases exist. For example, if $W$ generated by only one element $f$, then $G = \{f\}$ is a reduced Gröbner basis (see Example 3.2) of $W$. By Proposition 4.3, $G' = \{\lambda f\}$ also is a reduced Gröbner basis of $W$ if $\lambda$ belong to the free semigroup $\Gamma$ generated by the set $\Sigma = \{\alpha_1, \cdots, \alpha_n\}$(see(1.1)).

# 5 Applications to difference-differential dimension polynomials

Let $R$ be a $\Delta$-$\sigma$-field, $D$ the ring of $\Delta$-$\sigma$-operators over $R$, $M$ a finitely generated $\Delta$-$\sigma$-module(i.e. a finitely generated difference-differential-module), $F$ a finitely generated free $\Delta$-$\sigma$-module. And we will keep the notation and conventions of the preceding sections.

For $\lambda \in \Lambda$ of the form (1.1), let $ord\lambda = k_1 + \cdots + k_m + |l_1| + \cdots + |l_n|$. Also, for $w = \lambda e_i \in \Lambda E$ of a term of $F$, let $ord\ w = ord\lambda$. If $u = \sum_{\lambda\in\Lambda} a_\lambda \lambda \in D$, then $ord\ u = max\{ord\lambda \mid a_\lambda \neq 0\}$.

We may consider $D$ as a filtered ring with the filtration $(D_\mu)_{\mu\in\mathbb{Z}}$ such that $D_\mu = \{u \in D \mid ord\ u \leq \mu\}$ 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 $\mu, \nu \in \mathbb{Z}$.

DEFINITION 5.1. Let $R$ be a $\Delta$-$\sigma$-field and $M$ be a $\Delta$-$\sigma$-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 $M_\mu$ 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 5.1. Let $M$ be a finitely generated $\Delta$-$\sigma$-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 $M$. $\square$

DEFINITION 5.2. Let $R$ be a $\Delta$-$\sigma$-field, $M$ and $N$ be two $\Delta$-$\sigma$-modules over $R$. A homomorphism of $R$-modules $f : M \longrightarrow N$ is called a $\Delta$-$\sigma$-homomorphism (or difference-differential homomorphism), if $f(\beta x) = \beta f(x)$ for any $x \in M$, $\beta \in \Delta \bigcup \sigma^*$. Surjective (respectively, injective or bijective) $\Delta$-$\sigma$-homomorphism is called a $\Delta$-$\sigma$-epimorphism (respectively, $\Delta$-$\sigma$-monomorphism or $\Delta$-$\sigma$-isomorphism).

Choose the canonical ortant decomposition on $\mathbb{Z}^n$ as in Example 2.1 and define the generalized term order "$\prec$" on $\Lambda E$ of the terms of $F$ as follows(see Example 2.6):

If $u = \delta_1^{k_1} \cdots \delta_m^{k_m} \alpha_1^{l_1} \cdots \alpha_n^{l_n} e_i$ and $v = \delta_1^{r_1} \cdots \delta_m^{r_m} \alpha_1^{s_1} \cdots \alpha_n^{s_n} e_j$, then

$$u \prec v \Longleftrightarrow (ord\ u, e_i, k_1, \cdots, k_m, |l_1|, \cdots, |l_n|, l_1, \cdots, l_n)$$

$$< (ord\ v, e_j, r_1, \cdots, r_m, |s_1|, \cdots, |s_n|, s_1, \cdots, s_n) \ \ \textit{in lexicographic order.}$$

THEOREM 5.1. Let $R$ be a $\Delta$-$\sigma$-field, $D$ the ring of $\Delta$-$\sigma$-operators over $R$ and $M$ be a finitely generated $\Delta$-$\sigma$-module with generators $h_1, \cdots, h_q$. Let $F$

be a free $\Delta$-$\sigma$-module with a basis $e_1, \cdots, e_q$ and $\pi : F \longrightarrow M$ the natural $\Delta$-$\sigma$-epimorphism of $F$ onto $M$ (i.e. $\pi(e_i) = h_i$ for $i = 1, \cdots, q$).

Let $M_\mu$ be the vector $R$-space as in Example 5.1. 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, $U_\mu$ is the set of all terms $w \in \Lambda E$ such that $ord\ w \leq \mu$ 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 $M_\mu$.

PROOF. First, we need to show that the set $\pi(U_\mu)$ generates the $R$-vector space $M_\mu$. Since $M_\mu = D_\mu h_1 + \cdots + D_\mu h_q$, it is enough to show that every element $\lambda h_i$ ($i = 1, \cdots, q$, $\lambda \in \Lambda$, $ord\ \lambda \leq \mu$), that does not belong to $\pi(U_\mu)$, can be written as a finite linear combination of elements of $\pi(U_\mu)$ with coefficients from $R$. Since $\lambda h_i \notin \pi(U_\mu)$ implies $\lambda e_i \notin U_\mu$, whence $\lambda e_i = lt(\lambda' g_j)$ for some $\lambda' \in \Lambda$, $g_j \in G$. Therefore

$$\lambda' g_j = a_j \lambda e_i + \sum_\nu a_\nu \lambda_\nu e_\nu$$

where $a_j \neq 0$ and $a_\nu \neq 0$ for finitely many $a_\nu$. Obviously, $\lambda_\nu e_\nu \prec \lambda e_i$ and then $ord\ \lambda_\nu \leq \mu$. Note that $G \subseteq N = ker(\pi)$, we have $0 = \pi(g_j)$ and

$$0 = \lambda' \pi(g_j) = \pi(\lambda' g_j) = a_j \pi(\lambda e_i) + \sum_\nu a_\nu \pi(\lambda_\nu e_\nu) = a_j \lambda h_i + \sum_\nu a_\nu \lambda_\nu h_\nu.$$

So that $\lambda h_i$ is a finite linear combination with coefficients from $R$ of some elements of the form $\lambda_\nu h_\nu$ ($1 \leq \nu \leq q$) such that $ord\ \lambda_\nu \leq \mu$ and $\lambda_\nu e_\nu \prec \lambda e_i$. Thus, we can apply the induction on $\lambda e_j$ ($\lambda \in \Lambda$, $1 \leq j \leq q$) with respect to the order "$\prec$" and obtain that every element $\lambda h_i$ ($ord\ \lambda \leq \mu$, $1 \leq i \leq q$) can be written as a finite linear combination of elements of $\pi(U_\mu)$ with coefficients from $R$.

Now, let us prove that the set $\pi(U_\mu)$ is linearly independent over $R$. Suppose that $\sum_{i=1}^{l} a_i \pi(u_i) = 0$ for some $u_1, \cdots, u_l \in U_\mu$, $a_1, \cdots, a_l \in R$. Then $h = \sum_{i=1}^{l} a_i u_i \in N$ and $lt(h) \neq lt(\lambda g_i)$, $\lambda \in \Lambda$, $i = 1, \cdots, d$, by the definition of $U_\mu$. Since $G$ is a Gröbner basis of $N$ it is follows from Proposition 3.2 (iii) that $h = 0$. Therefore $a_1 = \cdots = a_l = 0$. This completes the proof of the theorem. □

From Theorem 5.1 the dimention of $M_\mu$ as an $R$-vector space can be computed by Gröbner bases of difference-differential modules.

DEFINITION 5.3. 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 $r_i \geq s_i$ ($1 \leq i \leq p$).

The following theorem proved in Levin (2000) generalize the Kondrateva result on the numerical polynomials associated with subsets of $\mathbb{N}^m$ (Kondrateva,1992) to the numerical polynomials associated with subsets of $\mathbb{N}^m \times \mathbb{Z}^n$.

THEOREM 5.2. 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 $\trianglelefteq$ be the partial order on

$\mathbb{N}^m \times \mathbb{Z}^n$ such that $(k_1, \cdots, k_m, l_1, \cdots, l_n) \trianglelefteq (r_1, \cdots, r_m, s_1, \cdots, s_n)$ if and only if $(l_1, \cdots, l_n)$ and $(s_1, \cdots, s_n)$ belong to a same ortant and

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

Furthemore, let

$$W_A = \{w \in \mathbb{N}^m \times \mathbb{Z}^n \mid \textit{there is no element } a \in A \textit{ such that } a \trianglelefteq w\}$$

and

$$W_A[r, s] = \{(k_1, \cdots, k_m, l_1, \cdots, l_n) \in W_A \mid k_1 + \cdots + k_m \leq r, |l_1| + \cdots + |l_n| \leq s\}.$$

Then there exists a numerical polynomial $\psi_A(t_1, t_2)$ in two variables $t_1$ and $t_2$ with the following properties.

(i) $\psi_A(r, s) = Card\ W_A[r, s]$ for all sufficiently large $(r, s) \in \mathbb{N}^2$.

(ii) $deg\ \psi_A \leq m + n$, $deg_{t_1}\psi_A \leq m$, and $deg_{t_2}\psi_A \leq n$.

(iii)If $A = \emptyset$, then $deg\ \psi_A = m + n$. In this case,

$$\psi_A(t_1, t_2) = \binom{t_1 + m}{m} \sum_{i=0}^{n} (-1)^{n-i} 2^i \binom{n}{i} \binom{t_2 + i}{i}.$$

(iv)$\psi_A(t_1, t_2) = 0$ if and only if $(0, \cdots, 0) \in A$. □

In Levin (2000) the author used Theorem 5.2 to prove the existence of difference-differential dimension polynomial $\psi(t_1, t_2)$ in two variables $t_1, t_2$ of the difference-differential module $M$ by means of characteristic set with respect to a special reduction. But the approach of characteristic set is not valid for the one-variable case. However, our approach of Gröbner bases in difference-differential modules can deal with the difference-differential dimension polynomials in one variable effectively.

The analog of Theorem 5.2 for the existence of numerical polynomial $\phi_A(t)$ in one variable $t$ associated with the subset $A$ of $\mathbb{N}^m \times \mathbb{Z}^n$ can be obtained in the same way as that used in the proof of Theorem 5.2.(see Levin 2000). We state it as follows.

COROLLARY. Let $A$, $\trianglelefteq$ and $W_A$ be the same as in the conditions of Theorem 5.2. Let

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

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 $(0, \cdots, 0) \in A$. □

Now we may use the approach of Gröbner bases of difference-differential modules to establish the existence of dimension polynomial in difference-differential modules. We give a definition after the following theorem.

THEOREM 5.3. Let $R$ be a $\Delta$-$\sigma$-field, $D$ the ring of $\Delta$-$\sigma$-operators over $R$ and $M$ be a finitely generated $\Delta$-$\sigma$-module, and $(M_\mu)_{\mu \in \mathbb{Z}}$ an excellent filtration of $M$.

Then there exists a numerical polynomial $\phi(t)$ such that $deg(\phi(t)) \leq m+n$ and $\phi(\mu) = dim_R M_\mu$ for all sufficiently large $\mu \in \mathbb{N}$. Furthemore, $\phi(t)$ can be written as $\phi(t) = \frac{2^n a}{(m+n)!} t^{m+n} + o(t^{m+n})$, $a \in \mathbb{Z}$ and $o(t^{m+n})$ denotes a polynomial from $\mathbb{Q}[t]$ whose degree is less than $m+n$, and the integers $d = deg\phi(t)$, $a$, and $\Delta^d \phi(t)$ do not depend on the choice of a system of generators of the module $M$. ($\Delta^d \phi(t)$ denotes the $d$-th finite difference of $\phi(t)$: $\Delta\phi(t) = \phi(t+1) - \phi(t)$, $\Delta^2\phi(t) = \Delta(\Delta\phi(t))$, etc. )

PROOF. Since $(M_\mu)_{\mu\in\mathbb{Z}}$ is an excellent filtration of $M$ it follows that every $M_\mu$ is a finitely generated $R$-vector space and $D_\nu M_\mu = M_{\mu+\nu}$ for $\mu \geq \mu_0$, $\nu \geq 0$. Let $h_1, \cdots, h_q$ be a basis of the $R$-vector space $M_{\mu_0}$. Then the elements $h_1, \cdots, h_q$ generate $M$ as a left $D$-module and $M_\mu = \sum_{i=1}^q D_{\mu-\mu_0} h_i$ for all $\mu \geq \mu_0$. Without loss of generality we can assume that $\mu_0 = 0$.(If $\phi(t)$ is a numerical polynomial with the desired properties that corresponds to the case $\mu_0 = 0$ then $\phi(t-\mu_0)$ is the one for arbitrary $\mu_0 \in \mathbb{Z}$.) Thus we may suppose that $M = \sum_{i=1}^q Dh_i$ and $M_\mu = \sum_{i=1}^q D_\mu h_i$ for all $\mu \in \mathbb{Z}$.

Let $F$ be a free $\Delta$-$\sigma$-module with a basis $e_1, \cdots, e_q$. Let $\pi: F \longrightarrow M$, $N = ker\ \pi$ and $U_\mu(\mu \in \mathbb{N})$ be the same as in the conditions of Theorem 5.1. Furthemore, let "$\prec$" be the generalized term order on $\Lambda E$ of the terms of $F$ and $G = \{g_1, \cdots, g_d\}$ be the Gröbner basis of $N$ as in Theorem 5.1. By Theorem 5.1, for any $\mu \in \mathbb{N}$, $\pi(U_\mu)$ is a basis of the $R$-vector space $M_\mu$. Note that in the second part of the proof of Theorem 5.1 it was shown that the restriction of $\pi$ on $U_\mu$ is bijective, we have $dim_R M_\mu = Card\ \pi(U_\mu) = Card(U_\mu)$.

Note that $U_\mu = \{w \in \Lambda E \mid ord\ w \leq \mu;\ w \neq lt(\lambda g_i), \lambda \in \Lambda, g_i \in G\}$. Let $V_i^{(j)}$ be a finite set of generators of the $R[\Lambda_j]$-module ${}_{R[\Lambda_j]}\langle lt(\lambda g_i) \in \Lambda_j E \mid \lambda \in \Lambda\rangle$. Let $V = \bigcup_{i,j} V_i^{(j)}$. Then $U_\mu = \{w \in \Lambda E \mid ord\ w \leq \mu;\ w$ is not a multiple of any element $v \in V\}$.

Let $V_{e_i} = \{v \in V \mid v = \lambda e_i, \lambda \in \Lambda\}$ and $U_\mu^{(i)} = \{w \in \Lambda e_i \mid ord\ w \leq \mu;\ w$ is not a multiple of any element $v \in V_{e_i}\}$, $i = 1, \cdots, q$. Then $Card(U_\mu) = \sum_{i=1}^q Card(U_\mu^{(i)})$.

By the Corollory of Theorem 5.2, there exists a numerical polynomial $\phi_i(t)$ such that $deg(\phi_i(t)) \leq m+n$ and $\phi_i(\mu) = Card(U_\mu^{(i)})$, $i = 1, \cdots, q$, for all sufficiently large $\mu \in \mathbb{N}$. Therefore $\phi(t) = \sum_{i=1}^q \phi_i(t)$ satisfies that $deg(\phi(t)) \leq m+n$ and $\phi(\mu) = Card(U_\mu) = dim_R M_\mu$ for all sufficiently large $\mu \in \mathbb{N}$.

The last conclusion of the theorem is well known properties of the dimention polynomial $\phi(t)$ satisfied that $deg(\phi(t)) \leq m+n$ and $\phi(\mu) = dim_R M_\mu$ for all sufficiently large $\mu \in \mathbb{N}$.(see Kondrateva 1999.) □

DEFINITION 5.4. The numerical polynomial $\phi(t)$ in Theorem 5.3 is called difference-differential dimension polynomial in one variable $t$ associated with $M$ .

The difference-differential dimension polynomial is treated as characteristics of the system of defining equations on the generators of $M$ and determines "strength"(see Kondrateva 1999 and Levin 2000) of the system of difference-differential equations.

In Mikhalev and Pankratev (1989) the authors proved existence of difference-differential dimension polynomials $\phi(t)$ associated with $M$ by classical Gröbner basis methods of computation of Hilbert polynomials. The proof is based on the fact that the ring of $\Delta$-$\sigma$-operators over the $\Delta$-$\sigma$-field $R$ is isomorphic to the factor ring of the ring of generalized polynomials $R[x_1, \cdots, x_{m+2n}]$ (where $x_i a = a x_i + \delta_i(a)$ $(1 \le i \le m)$, $x_{m+j} a = \alpha_j(a) x_{m+j}$ and $x_{m+n+j} a = \alpha_j^{-1}(a) x_{m+n+j}$ $(1 \le j \le n)$ for any $a \in R$) by the ideal $I$ generated by the polynomials $x_{m+j} x_{m+n+j} - 1$ $(1 \le j \le n)$. Now we present an alternate direct and algorithmic approach of Gröbner bases on difference-differential modules to compute the difference-differential dimension polynomials. The following example shows that the computation of difference-differential dimension polynomials associated with $M$ is rather simple by the method described in Theorem 5.3.

EXAMPLE 5.2. Let $R$ be a difference-differential field whose basic sets $\Delta$ and $\sigma$ consist of a single derivation operator $\delta$ and a single automorphism $\alpha$, respectively. Furthemore, let $D$ be the ring of $\Delta$-$\sigma$-operators over $R$ and $M = Dh$ be a cyclic $\Delta$-$\sigma$-module whose generator $h$ satisfies the defining equation

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

In other words, $M$ is isomorphic to the factor module of a free $\Delta$-$\sigma$-module $F$ with a free generator $e$ by its $\Delta$-$\sigma$-submodule $N = D(\delta^a \alpha^b + \delta^a \alpha^{-b} + \delta^{a+b})e$. Let the generalized term order $\prec$ on $\Lambda E$ is the same as in Theorem 5.3. Then $\{g = (\delta^a \alpha^b + \delta^a \alpha^{-b} + \delta^{a+b})e\}$ is a Gröbner basis of $N$(see Example 3.2). since $lt(g) = (\delta^{a+b})e$ belong to any ortant of $\Lambda E$(see Definition 3.3), it follows from Lemma 3.2 (ii) that $lt(\lambda g) = \lambda(\delta^{a+b})e$ for any $\lambda \in \Lambda$. Then by Theorem 5.3,

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

Therefore,

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

The result coinside with that was shown in Kondrateva (1999) and Levin (2000). □

EXAMPLE 5.3. Let $M$ be the $\Delta$-$\sigma$-module same as in Example 5.2. But the generalized term order $\prec$ on $\Lambda E$ is defined as follows:

$$\delta^k \alpha^l e \prec \delta^r \alpha^s e \Longleftrightarrow (k + |l|, |l|, k, l) < (r + |s|, |s|, r, s) \ \ \textit{in lexicographic order.}$$

Note that Theorem 5.1 and 5.3 still valid for "$\prec$". Denote $\{\delta^k \alpha^l \mid l \ge 0\}$ by $\Lambda_1$ and $\{\delta^k \alpha^l \mid l \le 0\}$ by $\Lambda_2$. Since $lt(g) = \delta^a \alpha^b e \in \Lambda_1$ and $lt(\alpha^{-1} g) = \delta^a \alpha^{-(b+1)} e \in \Lambda_2$ it follows that

$$\{lt(\lambda g) \in \Lambda_1 \mid \lambda \in \Lambda\} = \Lambda_1 \delta^a \alpha^b e \qquad \{lt(\eta g) \in \Lambda_2 \mid \eta \in \Lambda\} = \Lambda_2 \delta^a \alpha^{-(b+1)} e.$$

Therefore

$$dim_R M_t = Card\{\delta^c \alpha^d \mid c, d \in \mathbb{N}, c + d \le t, (c, d) \notin \{(a, b) + \mathbb{N}^2\}\} +$$

$$+Card\{\delta^c\alpha^d \mid c\in\mathbb{N}, d\in\mathbb{Z}, d<0, c+|d|\leq t, (c,-d)\notin\{(a,b+1)+\mathbb{N}^2\}\}$$

$$=[\frac{1}{2}(t+1)(t+2)-\frac{1}{2}(t-a-b+1)(t-a-b+2)]+$$

$$+[\frac{1}{2}t(t+1)-\frac{1}{2}(t-a-b)(t-a-b+1)]$$

$$=2(a+b)t+(a+b)(2-a-b).$$

□

## References


Apel, J. (1995). A Gröbner approach to involutive bases. *J. Symb. Comput.*, **19**, 441-457.

Becker, T., Weispfenning, V. (1993). *Gröbner bases. A Computational Approach to Commutative Algebra.* New York, Spinger-Verlag.

Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In *Multidimensional Systems Theory*, pp. 184-232. D. Reidel.

Carra Ferro, G. (1989). *Gröbner bases and Differential Algebra.* LNCS, **356**, pp.129-140.

Carra Ferro, G. (1997). Differential Gröbner bases in one variable and in the partial case. Algorithms and software for symbolic analysis of nonlinear systems. *Math. Comput. Modelling*, **25**, 1-10.

Cohn, R. M. (1965). *Difference Algebra.* New York, Interscience.

Galligo, A. (1985). Some algorithmic questions on ideals of differential operators. *Springer Lec. Notes Comp. Sci.*, **204**, 413-421.

Insa, M., Pauer, F. (1998). Gröbner bases in rings of differential operators. In *Gröbner Bases and Applications*, pp. 367-380. New York, Cambridge University Press.

Kolchin, E. R. (1964). The notion of dimension in the theory of algebraic differential equations, *Bull. Am. Math. soc.*,**70**, 570-573.

Kolchin, E. R. (1973).*Differential Algebra and Algebraic Groups.* New York, Academic Press.

Kondrateva, M. V., Levin, A. B., Mikhalev, A. V., Pankratev, E. V. (1992). Computation of dimension polynomials. *Int. J. Algebra Comput.*,**2**, 117-137.

Kondrateva, M. V., Levin, A. B., Mikhalev, A. V., Pankratev, E. V. (1999). *Differential and Difference Dimension Polynomials.* Dordrecht, Kluwer Academic Publishers.

Levin, A. B., Mikhalev, A. V.(1987). Differential dimension polynomial and the strength of a system of differential equations. In *Computable Ivariants in the Theory of Algebraic Systems. Collection of Papers*, pp. 58-66. Novosibirsk. In Russian.

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

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

Mora, T.(1986). Gröbner bases for non-commutative polynimial rings. *Springer Lec. Notes Comp. Sci.*, **229**, 353-362.

Noumi, M. (1988). Wronskima determinants and the Gröbner representation of linear differential equation. In *Algebraic Analysis*, pp. 549-569. Boston, Academic Press.

Nordbeck, P.(1998). On some basic applications of Gröbner bases in noncommutative polynomial rings. In *Gröbner Bases and Applications*, pp.463-472. New York, Cambridge University Press.

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

Pauer, F., Zampieri, S. (1996). Gröbner bases with respect to generlized term orders and their applications to the modelling problem. *J. Symb. Comput.*,

**21**, 155-168.

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

Ritt, J. F. (1950). *Differential Algebra.* New York, American Math. Society.

Sit, W.(1975). Well-odering of certain numerical polynomials. *Trans. Am. Math. Soc.*, **212**,37-45.

Stanley, R.(1997). *Enumerative Combinatorics*, Volume I, New York, Cambridge University Press.

Yakayama, N. (1989). Gröbner basis and the problem of contiguous relstions. *Japan J. Appl. Math.*, **6**, 147-160.