Groebner-Shirshov Bases in Some Noncommutative Algebras

by

Xiangui Zhao

A thesis submitted to the Faculty of Graduate Studies of

The University of Manitoba

in partial fulfilment of the requirements of the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

University of Manitoba

Winnipeg

Abstract

Gröbner-Shirshov bases, introduced independently by Shirshov in 1962 and Buchberger in 1965, are powerful computational tools in mathematics, science, engineering, and computer science. This thesis focuses on the theories, algorithms, and applications of Gröbner-Shirshov bases for two classes of noncommutative algebras: differential difference algebras and skew solvable polynomial rings.

This thesis consists of three manuscripts (Chapters 2–4), an introductory chapter (Chapter 1) and a concluding chapter (Chapter 5).

In Chapter 1, we introduce the background and the goals of the thesis.

In Chapter 2, we investigate the Gelfand-Kirillov dimension of differential difference algebras. We find lower and upper bounds of the Gelfand-Kirillov dimension of a differential difference algebra under some conditions. We also give examples to demonstrate that our bounds are sharp.

In Chapter 3, we generalize the Gröbner-Shirshov basis theory to differential difference algebras with respect to any left admissible ordering and develop the Gröbner-Shirshov basis theory of finitely generated free modules over differential difference algebras. By using the theory we develop, we present an algorithm to compute the Gelfand-Kirillov dimensions of finitely generated modules over differential difference algebras.

In Chapter 4, we first define skew solvable polynomial rings, which are generalizations of solvable polynomial algebras and (skew) PBW extensions. Then

we present a signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings over fields. Our algorithm can detect redundant reductions and therefore it is more efficient than the traditional Buchberger algorithm.

Finally, in Chapter 5, we summarize our results and propose possible future work.

Co-authorship Statement

Chapters 2–4 consist of three manuscripts co-authored with Yang Zhang (the thesis advisor of the candidate):

1. *Gelfand-Kirillov dimension of differential difference algebras*, LMS Journal of Computation and Mathematics **17** (1) (2014), 485–495.

2. *Gelfand-Kirillov dimension of modules over differential difference algebras*, accepted by Algebra Colloquium.

3. *A signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings.*

Contributions of the advisor and the candidate to the manuscripts: In all cases, the advisor helped to propose the problems, supervised the development of the research, and revised the manuscripts. The candidate figured out the key ideas, and did the majority of the research and writing of each manuscript independently with useful discussion with the advisor.

Acknowledgements

First and foremost, I would like to express the deepest appreciation to my supervisor, Professor Yang Zhang, who has supported me throughout my thesis study with his knowledge, patience, and encouragement. Without his guidance and persistent help this thesis would not have been possible.

I would also like to thank my committee members, Professor Guenter Krause, Professor Tommy Kucera, Professor R. Padmanabhan, and Professor Jun Cai, for their training, challenging and encouragement.

In addition, I wish to thank the financial support from the University of Manitoba and the Government of Manitoba via Manitoba Graduate Scholarship, and from the National Sciences and Engineering Research Council via Professors Yang Zhang and Guenter Krause.

Finally, I would like to thank the London Mathematical Society and World Scientific Publishing Company for giving their permission for our manuscripts to be included in the thesis.

This thesis is dedicated to my parents, for their endless love, support and encouragement.

Contents

Chapter 1

Introduction

1.1 Gröbner-Shirshov Bases

The theory of Gröbner-Shirshov bases was introduced independently by A.I. Shirshov [51] for Lie algebras in 1962, and by B. Buchberger [11] for commutative algebras in 1965[1]. It turns out that Gröbner-Shirshov bases are powerful computational tools and are quite useful to give algebraic structures which are applicable to a wide range of problems in mathematics, science, engineering and computer science.

The basic idea behind the theory of Gröbner-Shirshov bases can be described as a generalization of the theory of greatest common divisors (gcd) of univariate polynomials over a field. We explain this by taking a Gröbner-Shirshov basis of a commutative polynomial algebra as an example. Let k be a field and $k[x]$ be the polynomial algebra over k in a single variable x. Any ideal I of $k[x]$ is generated by a single element. The ideal I generated by $\{f_1, \ldots, f_n\} \subseteq k[x]$ for some $n \in \mathbb{N}$, is also generated by $d = \gcd(f_1, \ldots, f_n) \in k[x]$, where $\gcd(f_1, \ldots, f_n)$ stands for the greatest common divisor of $f_1, \ldots, f_n$ and it can be computed by the Euclidean

[1]W. Gröbner was the Ph.D. thesis advisor of Buchberger. In commutative polynomial algebras, instead of Gröbner-Shirshov basis, the term Gröbner basis is commonly used.

Algorithm. Then an element $f \in k[x]$ belongs to I if and only if f is a multiple of d, i.e., the remainder of the division of f by d is zero. Gröbner-Shirshov bases in multivariate polynomial algebras $k[x_1, \ldots, x_m]$ ($m \in \mathbb{N}$) are analogues of greatest common divisors in the following sense. Given a finite set $F \subseteq k[x_1, \ldots, x_m]$, the Buchberger algorithm [11] computes a new (finite) set $G \subseteq k[x_1, \ldots, x_m]$, called a Gröbner-Shirshov basis, which generates the same ideal as F does and a polynomial $f \in k[x_1, \ldots, x_m]$ belongs to the ideal generated by F if and only if the remainder of the *(multivariate) division*[2] of f by polynomials in G is zero.

The fundamental insight and contribution of Gröbner-Shirshov basis theory for commutative polynomial algebras are that every polynomial system can be transformed, by an algorithm, into a finite Gröbner-Shirshov basis. Buchberger's algorithm [11] is the first one to compute Gröbner-Shirshov bases in commutative polynomial algebras. The basic idea of the Buchberger algorithm is as follows. Let $F \subseteq k[x_1, \ldots, x_m]$ be a finite set. Compute the *S-polynomial* of any pair of polynomials from F, and calculate its remainder by multivariate division with respect to F. Add all nonzero remainders (if exist) to F and denote the resulting set by F_1. Now compute remainders (with respect to F_1) of S-polynomials of pairs of polynomials from F_1. If any nonzero remainder exists, add them all to F_1 and denote the resulting set by F_2. Repeat the above process and we get a chain of subsets of $k[x_1, \ldots, x_m]$:

$$F = F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots .$$

It is shown that the above chain has a finite length, say it terminates with F_l for some $l \in \mathbb{N}$. Thus the algorithm terminates after finitely many steps and F_l is a Gröbner-Shirshov basis of the ideal generated by F.

The Buchberger algorithm has been implemented in most computer algebra

[2]The appropriate concept of multivariate division with remainder is a central aspect of the theory. The definition, properties, and algorithm of multivariate division can be found in standard textbooks of Gröbner-Shirshov bases, e.g., [2, 1, 19].

systems, e.g., Maple, Mathematica, Magma, Singular and Macaulay 2. However, Buchberger's algorithm is not efficient, mainly due to the fact that in each loop it has to calculate a remainder of the S-polynomial for every pair of elements from the input set. Furthermore, the strategies of selection used during the computation, for example, the choices of monomial ordering and critical pair, can also be optimized. There have been extensive efforts in improving the efficiency of Buchberger's algorithm in commutative polynomial algebras. Some improvements are concerned with selection strategies, for example, the algorithms proposed by Giovini et al. [32], Gerdt and Blinkov [30], and Faugère [22]. Some are concerned with the detection of superfluous reduction, i.e., the reduction of S-polynomials with zero remainder[3], for instance, the algorithms in Buchberger [12] and Faugère [23]. Among the most efficient algorithms are signature-based algorithms, which aim to detect superfluous reductions of S-polynomials. The first signature-based algorithm F5 was proposed by Faugère [23] in 2002. Since then, several variants of F5 have been presented, for example, the F5C algorithm by Eder and Perry [21] and F5 with extended criteria by Hashemi and Ars [34]. Other signature-based algorithms include incremental algorithms G2V and GVW by Gao et al. [26, 27], XL type algorithms by Courtois et al. [18] and Ding et al. [20].

Noncommutative (associative) Gröbner-Shirshov bases and nonassociative Gröbner-Shirshov bases have also been widely investigated, for example, the Gröbner-Shirshov basis theories for free Lie algebras [51] (which implies the Gröbner-Shirshov basis theory of free associative algebras, see also [4, 49]), Weyl algebras [25], solvable polynomial algebras [38], rings of differential operators [37, 54, 44], G-algebras [41], skew polynomial rings [17], differential difference algebras [45], PBW algebras [14, 31], σ-PBW extensions [24], dialgebras [7], metabelian Lie algebras [16], L-algebras [6], semirings [8], and tensor

[3]The reduction of those S-polynomial is redundant since it gives no contribution to the final Gröbner-Shirshov basis.

product of free Lie algebras [5]. More algebraic structures which admit Gröbner-Shirshov basis theory can be found in the survey article [9].

In contrast to the commutative case, an ideal of a noncommutative algebra does not necessarily have a finite Gröbner-Shirshov basis. If it does have a Gröbner-Shirshov basis, we can still use (the noncommutative analogue of) Buchberger's algorithm to compute it. However, owing to the noncommutativity, it is difficult to detect and reject redundant computations effectively. Only recently, a signature-based algorithm was presented by Sun et al. [52] to compute Gröbner-Shirshov bases in solvable polynomial algebras.

This thesis focuses on the theories, algorithms, and applications of Gröbner-Shirshov bases in two classes of noncommutative algebras: differential difference algebras and skew solvable polynomial rings, which will be defined in Section 1.2.

1.2 Differential Difference Algebras and Skew Solvable Polynomial Algebras

In this section, we introduce the concepts of differential difference algebras and skew solvable polynomial rings, which are studied in this thesis.

Let k be a field. We assume that all algebras and rings in question are unital and associative unless otherwise stated.

1.2.1 Differential Difference Algebras

Given a k-algebra A, denote the set of k-algebra automorphisms of A by $\mathrm{Aut}(A)$. If $\sigma \in \mathrm{Aut}(A)$, then a mapping δ on A is called a *σ-derivation* provided that, for any $a, b \in A$ and $c \in k$, $\delta(ca+b) = c\delta(a)+\delta(b)$ and $\delta(ab) = \sigma(a)\delta(b)+\delta(a)b$. Particularly, if $\sigma = \mathrm{id}$ then δ is called a *derivation* on A.

On the free left A-module $\bigoplus_{i=0}^{\infty} Ax^i$, a ring structure is introduced by defining

$$xa = \sigma(a)x + \delta(a) \text{ for all } a \in A.$$

The resulting ring, denoted by $A[x; \sigma, \delta]$, is called a *skew polynomial ring* or an *Ore extension* over A. If $\delta = 0$, then $A[x; \sigma, \delta] = A[x; \sigma]$ is called an Ore extension of automorphism type. If $\sigma = \text{id}$, then $A[x; \sigma, \delta] = A[x; \delta]$ is called an Ore extension of derivation type.

Definition 1.2.1 *(cf., [45]) An algebra A is called* a differential difference algebra *of type (m, n), $m, n \geq 1$, over a subalgebra $R \subseteq A$ if there exist elements $S_1, \ldots, S_m, D_1, \ldots, D_n$ in A such that*

(i) the set $\{S_1^{\alpha_1} \cdots S_m^{\alpha_m} D_1^{\beta_1} \cdots D_n^{\beta_n} : \alpha_i, \beta_j \in \mathbb{N}, 1 \leq i \leq m, 1 \leq j \leq n\}$ forms a basis for A as a free left R-module.

(ii) $D_i r = rD_i + \delta_i(r)$ for any $1 \leq i \leq n$ and $r \in R$, where δ_i is a derivation on R.

(iii) $S_i r = \sigma_i(r) S_i$ for any $1 \leq i \leq m$ and $r \in R$, where σ_i is a k-algebra automorphism on the subalgebra $R[D_1, \ldots, D_n] \subseteq A$ such that $\sigma_i|_R \in \mathrm{Aut}(R)$ and $\sigma_i(D_j) = \sum_{l=1}^{n} a_{ijl} D_l, \quad a_{ijl} \in R$.

(iv) $S_i S_j = S_j S_i$, $1 \leq i, j \leq m$; $D_{i'} D_{j'} = D_{j'} D_{i'}$, $1 \leq i', j' \leq n$.

(v) For any $1 \leq i, j \leq n$ and $1 \leq i', j' \leq m$, the composition $\delta_i \circ \delta_j = \delta_j \circ \delta_i$, $\delta_i \circ \sigma_{i'} = \sigma_{i'} \circ \delta_i$ and $\sigma_{i'} \circ \sigma_{j'} = \sigma_{j'} \circ \sigma_{i'}$.

In the above definition, both subalgebras $R[D_1, \ldots, D_n]$ and $R[S_1, \ldots, S_m]$ of A are iterated Ore extensions over R, where $R[D_1, \ldots, D_n]$ denotes the subalgebra of A generated by $R \cup \{D_1, \ldots, D_n\}$ (and similar for the notation $R[S_1, \ldots, S_m]$). But, in general A is not an iterated Ore extension over R.

The class of differential difference algebras contains several other known classes of algebras. For instance, commutative polynomial algebras are differential difference algebras with identity automorphism and zero derivation; a quantum plane ([39], Chapter IV) is a differential difference algebra of type $(1, 1)$ (see Example 2.2.3). On the other hand, the class of differential difference algebras is different from several known classes of noncommutative algebras. The following example distinguishes differential difference algebras from algebras of solvable type [38], PBW extensions [3], σ-PBW extensions [24], and G-algebras [41].

Example 1.2.2 Let A be the k-algebra generated by $\{D_1, D_2, S\}$ with defining relations $\{D_2D_1 = D_1D_2, D_1S = SD_2, D_2S = SD_1\}$. Then it is easy to see that A is a differential difference algebra of type $(1, 2)$ over k. However, by the defining relations, A is not an algebra of solvable type [38], nor a PBW extension [3] or a σ-PBW extension [24], and also not a G-algebras [41].

Let $\mathcal{D} = \{D_1, \ldots, D_n\}$ and $\mathcal{S} = \{S_1, \ldots, S_m\}$. If A is a differential difference algebra over R defined as Definition 1.2.1, we denote $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$. For $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$ and $r \in R$, we simply write $\sigma^\alpha(r) = \sigma_1^{\alpha_1} \cdots \sigma_m^{\alpha_m}(r)$, $\mathcal{D}^\alpha = D_1^{\alpha_1} \cdots D_m^{\alpha_m}$ and $|\alpha| = \alpha_1 + \cdots + \alpha_m$. In particular, $D_i^0 = 1$, the identity of R. Similarly, we use notation $\delta^\alpha(r)$, S^β ($\beta \in \mathbb{N}^n$), and so on. Then every element in A can be written uniquely in the form: $\sum_{\alpha,\beta} r_{\alpha,\beta}\mathcal{S}^\alpha\mathcal{D}^\beta$, where $r_{\alpha,\beta} \in R$ and only finitely many $r_{\alpha,\beta}$ are nonzero.

The following example, taken from [45] with some modifications, shows where the differential difference algebras come from.

Example 1.2.3 Let $M, n, p \in \mathbb{N}$ and $p \geq 1$. Consider the following system, which arises from the calculation of symmetries of discrete systems (cf., [36]),

$$u_{n+M+1} = \omega(n, u_n, u_{n+1}, \ldots, u_{n+M});$$

$$\mathcal{D}_j F(n, u_n, u_{n+1}, \ldots, u_{n+M}) = 0,\ 1 \leq j \leq p,$$

where F is the unknown function and w is a given function in the field $\mathbb{Q}(n, u_n, \ldots, u_{n+M})$ of rational functions over the rational numbers $\mathbb{Q}$ in indeterminates $n, u_n, u_{n+1}, \ldots, u_{n+M}$, such that $\frac{\partial \omega}{\partial u_n} \neq 0$, and $\mathcal{D}_j : T \to T$ is a linear operator of the form

$$\mathcal{D}_j = \sum_{\alpha=(\alpha_0,\ldots,\alpha_M)\in\mathbb{N}^M,\ \beta\in\mathbb{N}} c_{\alpha,\beta} \circ s^\beta \circ \frac{\partial^{\alpha_0+\cdots+\alpha_M}}{\partial u_n^{\alpha_0} \cdots \partial u_{n+M}^{\alpha_M}},$$

where $T = \mathbb{Q}(n, u_{n+t} : t \in \mathbb{Z})$, $c_{\alpha,\beta} \in \mathbb{Q}(n, u_{n+t} : t \in \mathbb{Z})$ are *multiplication operators* and only finitely many $c_{\alpha,\beta}$ are nonzero, and s is the *shift operator* defined by $s(n) = n + 1$ and $s(u_n) = u_{n+1}$.

A natural approach to deal with this system is to consider the operators $\mathcal{D}_j$ and s as elements of the noncommutative algebra generated by operator variables $\{S, D_n, \ldots, D_{n+M}\}$ over $R = \mathbb{Q}(n, u_{n+t} : t \in \mathbb{Z})$, where S denotes the shift operator s and D_{n+t} denotes the differential operator $\frac{\partial}{\partial u_{n+t}}$ for $0 \leq t \leq M$, subject to the following commutation rules:

$$\begin{aligned}
D_{n+t} \circ S &= S \circ D_{n+t-1} + \frac{\partial \omega}{\partial u_{n+t}} \circ S \circ D_{n+M}, \quad 1 \leq t \leq M; \\
D_n \circ S &= \frac{\partial \omega}{\partial u_n} \circ S \circ D_{n+M}; \\
D_{n+t} \circ D_{n+t'} &= D_{n+t'} \circ D_{n+t}, \qquad 0 \leq t, t' \leq M; \\
S \circ r &= s(r) \circ S, \qquad r \in R; \\
D_{n+t} \circ r &= r \circ D_{n+t} + \frac{\partial r}{\partial u_{n+t}}, \qquad r \in R, 0 \leq t \leq M.
\end{aligned}$$

Then $A = \mathbb{Q}(n, u_{n+t} : t \in \mathbb{Z})[S, \mathcal{D}; \sigma, \delta]$ is a differential difference algebra of type $(1, M+1)$ over R, where $\delta_i = \frac{\partial}{\partial u_i}$ for $n \leq i \leq n+M$ and $\sigma|_R = s, \sigma(D_n) = s^{-1}(\frac{\partial \omega}{\partial u_n})D_{n+M}$, $\sigma(D_{n+t}) = D_{n+t-1} + s^{-1}(\frac{\partial \omega}{\partial u_{n+t}})D_{n+M}$ for

$1 \le t \le M$.

Note that the difference operator Δ, defined by $\Delta(u_i) = u_{i+1} - u_i$ for $i \in \mathbb{Z}$, can be derived from the shift operator: $\Delta = S - \mathrm{id}$. So the differential difference algebra in the above example actually involves both differential and difference operators.

1.2.2 Skew Solvable Polynomial Rings

In order to define skew solvable polynomial rings, let us recall some basic definitions of orderings first. Let $\mathbb{N}$ be the set of nonnegative integers. Suppose $<$ is a *monomial ordering* on $\mathbb{N}^n$, $n \in \mathbb{N}$, i.e., a total ordering on $\mathbb{N}^n$ such that $0 \in \mathbb{N}^n$ is the smallest element in $\mathbb{N}^n$ and $\alpha < \beta$ implies $\alpha + \gamma < \beta + \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{N}^n$. The set of *(standard) monomials* in n indeterminates $\{x_1, \ldots, x_n\}$ is defined as $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha_i \in \mathbb{N}, 1 \le i \le n\}$. We also denote $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ by x^α and call α the *exponent* of x^α (denoted by $\exp(x^\alpha) = \alpha$), where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. We say $x^\alpha < x^\beta$ if $\alpha < \beta$. Thus, a monomial ordering on $\mathbb{N}^n$ is also called a *monomial ordering* on the set of standard monomials.

For any nonzero $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$, where only finitely many constant c_α are nonzero, the *total degree* of f is defined as $\mathrm{tdeg}(f) = \max\{|\alpha| : c_\alpha \neq 0\}$. The monomial $x^\gamma = \max\{x^\alpha : c_\alpha \neq 0\}$ is called the *leading monomial* of f and c_γ is called the *leading coefficient* of f, denoted by $\mathrm{lm}(f)$ and $\mathrm{lc}(f)$, respectively.

Definition 1.2.4 *Fix a monomial ordering $<$ on $\mathbb{N}^n$. Let R and A be two rings with $R \subseteq A$. Then A is called a* skew solvable polynomial ring *over R if the following conditions hold:*

(i) There exist finitely many elements $x_1, \ldots, x_n \in A$ such that A is a free left R-module with basis

$$\mathcal{M} = \{x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}.$$

(ii) *For* $1 \le i \le n$ *and* $r \in R$, $x_i r = \sigma_i(r)x_i + \delta_i(r)$, *where* σ_i *is an injective ring endomorphism of* R, δ_i *is a* σ_i*-derivation of* R, *and, for any* $1 \le i, j \le n$,

$$\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i, \ \delta_i \circ \delta_j = \delta_j \circ \delta_i, \ \sigma_i \circ \delta_j = \delta_j \circ \sigma_i.$$

(iii) *For* $1 \le i < j \le n$, *there exist* $0 \ne c_{ij} \in R$ *and* $p_{ij} \in A$ *with* $\mathrm{lm}(p_{ij}) < x_i x_j$ *such that* $x_j x_i = c_{ij} x_i x_j + p_{ij}$.

Then we write $A = R\langle X; \sigma, \delta, c, p\rangle$. *Clearly every nonzero element in* A *can be uniquely represented as* $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$, *where only finitely many* $c_\alpha \in R$ *are nonzero.*

Skew solvable polynomial rings are generalizations of several well-known skew polynomial rings.

Example 1.2.5 Let $A = R\langle X; \sigma, \delta, c, p\rangle$ be a skew solvable polynomial ring.

(i). If R is a field, $\sigma_i = \mathrm{id}_R$ and $\delta_i = 0$ for all $1 \le i \le n$, then A is a solvable polynomial algebra [38]. Any solvable polynomial algebra can be viewed as a skew solvable polynomial ring in this way.

(ii). If $\mathrm{tdeg}(p_{ij}) = 1$ for all $1 \le i < j \le n$, then A is a skew PBW extension of R [24]. Any skew PBW extension can be viewed as a skew solvable polynomial ring in this way.

Therefore, any ring belonging to the above two classes of rings is a skew solvable polynomial ring, for example, a Weyl algebra, the universal enveloping algebra of a finite dimensional Lie algebra, and an Ore extension of automorphism and/or derivation type. More examples of skew solvable polynomial rings can be found in Chapter 4.

Skew solvable polynomial rings over a field (i.e., R is a field) also admit a Gröbner-Shirshov basis theory and therefore Buchberger algorithm works there. In Chapter 4, we generalize the signature-based algorithm proposed in [52] to skew solvable polynomial ring over a field. The generalized algorithm (Algorithm 4.4.2) can detect redundant reductions in the traditional Buchberger algorithm, and thus it is more efficient.

1.3 Gelfand-Kirillov Dimension

The Gelfand-Kirillov dimension is a very useful and powerful tool for investigating noncommutative algebras and their modules. Algebraists' interest in Gelfand-Kirillov dimension dates mainly from two papers [28, 29] by Gelfand and Kirillov in 1966. These articles contain a conjecture, known as the *Gelfand-Kirillov Conjecture*, about quotient division rings of enveloping algebras. The Gelfand-Kirillov dimension arose from the aim to investigate the conjecture. Another source of Gelfand-Kirillov dimension is a paper published in 1968 by Milnor, [48], where the corresponding notion of the growth of a group was introduced. The Gelfand-Kirillov dimension was then systematically studied by Borho and Kraft [10] in 1976[4]. Since then, the properties of Gelfand-Kirillov dimension have been widely studied and used in many papers and the Gelfand-Kirillov dimension has become one of standard invariants used in the study of noncommutative algebras and modules. Basic properties and applications of Gelfand-Kirillov dimension can be found, for example, in [40], and Chapter 8 of [47].

Now we mainly follow Krause and Lenagan [40] and introduce basic concepts of Gelfand-Kirillov dimension.

Let k be a field and let A be a finitely generated k-algebra. Choose a finite

[4] As mentioned by Krause and Lenagen [40], "the potential user of [10] should beware; the article contains several errors that have come to light in last few years".

dimensional subspace V of A such that $1_A \in V$ and A is generated by V as an algebra (such a V is called a *generating subspace* of A). Let V^n, $n \in \mathbb{N}$, be the subspace of A with the k-basis $\{v_1 v_2 \cdots v_n : v_i \in V, 1 \leq i \leq n\}$. It is obvious that $V^n \subseteq V^{n+1}$, since $1 \in V$. Then we have that

$$k = V^0 \subseteq V \subseteq V^2 \subseteq \cdots \subseteq V^n \subseteq \cdots \subseteq \bigcup_{n=1}^{\infty} V^n = A$$

with $\dim_k(V^n) < \infty$ for all $n \in \mathbb{N}$. The asymptotic behavior of the function $f(n) = \dim_k(V^n)$ provides a useful invariant of the algebra A, known as the *Gelfand-Kirillov dimension* of A, and defined as

$$\operatorname{GKdim}(A) = \overline{\lim_{n \to \infty}} \log_n \dim_k(V^n).$$

It is shown that $\operatorname{GKdim}(A)$ is independent of the choice of the generating subspace V (see, for example, Chapter 2 of[40]).

In general, we have the following

Definition 1.3.1 *Let A be a k-algebra (not necessarily finitely generated). The* Gelfand-Kirillov dimension *of A is given by*

$$\operatorname{GKdim}(A) = \sup_V \overline{\lim_{n \to \infty}} \log_n \dim_k(V^n)$$

where the supremum is taken over all finite dimensional subspaces V of A. Equivalently,

$$\operatorname{GKdim}(A) = \sup\{\operatorname{GKdim}(B) : B \textit{ is a finitely generated subalgebra of } A\}.$$

The Gelfand-Kirillov dimension of (left) modules is defined as follows.

Definition 1.3.2 *Let A be a k-algebra, and let M be a left*[5] *A-module. The* Gelfand-Kirillov dimension *of M is given by*

$$\mathrm{GKdim}(M) = \sup_{V,F} \overline{\lim_{n\to\infty}} \log_n \dim_k(V^n F)$$

where the supremum is taken over all finite dimensional subspace V of A containing 1 and all finite dimensional subspaces F of M. Alternatively,

$$\mathrm{GKdim}(M) = \sup_{B,N} \mathrm{GKdim}({}_B N)$$

where the supremum is taken over all finitely generated subalgebras B of A and all finitely generated left B-submodules N of M. Note that $\mathrm{GKdim}(0) = -\infty$.

From the above definitions, it is clear that $\mathrm{GKdim}(A)$, the Gelfand-Kirillov dimension of A as an algebra, and $\mathrm{GKdim}({}_A A)$, the Gelfand-Kirillov dimension of A as a left A-module, coincide. In general, the Gelfand-Kirillov dimension of a left A-module does not exceed the Gelfand-Kirillov dimension of A, that is, we have the following

Lemma 1.3.3 *([40], Proposition 5.1(d)) Let A be a k-algebra and let M be a left A-module. Then*

$$\mathrm{GKdim}({}_A M) \leq \mathrm{GKdim}(A).$$

We are interested in the Gelfand-Kirillov dimension of modules over differential difference algebras via an algorithmic method. By Lemma 1.3.3, in order to obtain an upper bound of the Gelfand-Kirillov dimension of a module over a differential difference algebra, it is quite natural to investigate the Gelfand-Kirillov dimension of that differential difference algebra first. There have been a number of results concerning Gelfand-Kirillov dimensions of algebras with derivations and/or

[5] The Gelfand-Kirillov dimension of a right A-module is defined similarly.

automorphisms. For example, the Gelfand-Kirillov dimension of Ore extensions of derivation type and automorphism type is studied by Lorenz [43], and Huh and Kim [35], respectively. Matczuk [46] investigates the Gelfand-Kirillov dimension of PBW-extensions. Zhang [53] clarifies the behavior of Gelfand-Kirillov dimension under skew polynomial extensions. Recently, the Gelfand-Kirillov dimension of skew PBW-extensions is studied in [50] by Reyes.

Let us cite an existing result regarding the Gelfand-Kirillov dimension of Ore extensions. Assume that R is a k-algebra. Let σ be an automorphism of R, δ be a σ-derivation of R and $A = R[x; \sigma, \delta]$ be an Ore extension over R. It was shown by Huh and Kim in [35] that

$$\mathrm{GKdim}(A) \geq \mathrm{GKdim}(R) + 1, \tag{1.1}$$

where the inequality becomes an equality provided that the following condition holds:

(∗) each finite dimensional subspace U of R is contained in a finite dimensional subspace V such that $\sigma(V) \subseteq V$ and $\delta(V) \subseteq V^p$ for some $p \geq 1$.

In Chapter 2 we investigate the Gelfand-Kirillov dimension of differential difference algebras. We show that Inequality (1.1) of the Gelfand-Kirillov dimension of Ore extensions can be extended to differential difference algebras, that is, we get a lower bound of the Gelfand-Kirillov dimensions of differential difference algebras. However, owing to the noncommutativity of indeterminates of differential difference algebras, even under conditions similar to (∗), the equality does not hold for differential difference algebras in general. We find an upper bound for the Gelfand-Kirillov dimension of a differential difference algebra satisfying (analogues of) condition (∗), and give a sufficient condition under which the lower bound is reached. We also construct an example to show that the upper bound we obtain cannot be improved.

When looking for an algorithm to compute the Gelfand-Kirillov dimensions of modules over noncommutative algebras, it is natural and reasonable to look at the existing algorithms in commutative algebras. For commutative algebras, the dimension of an algebraic variety is the same as the degree of the related Hilbert polynomial and the latter can be computed by using Gröbner-Shirshov bases (see [2], Section 9.3). The Gelfand-Kirillov dimension of a finitely generated module over a finitely generated algebra is also closely related to the Hilbert function, and thus it is possible to compute it by using Gröbner-Shirshov bases for some specific classes of noncommutative algebras. For example, Bueso et al. [15] computed the Gelfand-Kirillov dimension of a cyclic module over an almost commutative algebra, Torrecillas [33] considered the Gelfand-Kirillov dimension of finitely generated graded modules over multi-graded finitely generated algebras, Li [42] extended this method to cyclic modules over solvable polynomial algebras (also known as PBW algebras), and Bueso et al. [13] extended this method to finitely generated modules over PBW algebras.

In Chapter 3 of the thesis, after we generalize the Gröbner-Shirshov basis theory developed by Mansfield and Szanto [45], we propose an algorithm (Algorithm 3.6.3), based on the construction of Gröbner-Shirshov bases of left ideals of differential difference algebras, to compute the Gelfand-Kirillov dimension of a finitely generated module over a differential difference algebra.

Bibliography

[1] W. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, 1994.

[2] T. Becker and V. Weispfenning, *Gröbner bases: a computational approach to commutative algebra*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, 1993.

[3] A. D. Bell and K. R. Goodearl, *Uniform rank over differential operator rings and Poincaré-Birkhoff-Witt extensions*, Pacific J. Math. **131** (1988), no. 1, 13–37.

[4] L. A. Bokut', *Embeddings into simple associative algebras*, Algebra Logic **15** (1976), no. 2, 73–90.

[5] L. A. Bokut, Yuqun Chen, and Yongshan Chen, *Composition–Diamond lemma for tensor product of free algebras*, J. Algebra **323** (2010), no. 9, 2520–2537.

[6] L. A. Bokut, Yuqun Chen, and Jiapeng Huang, *Gröbner-Shirshov bases for L-algebras*, Internat. J. Algebra Comput. **23** (2013), no. 3, 547–571.

[7] L. A. Bokut, Yuqun Chen, and Cihua Liu, *Gröbner-Shirshov bases for dialgebras*, Internat. J. Algebra Comput. **20** (2010), no. 3, 391–415.

[8] L. A. Bokut, Yuqun Chen, and Qiuhui Mo, *Gröbner-Shirshov bases for semirings*, J. Algebra **385** (2013), 47–63.

[9] L. A. Bokut', Yuqun Chen, and K. P. Shum, *Some new results on Gröbner-Shirshov bases*, Proceedings of International Conference on Algebra 2010–Advances in Algebraic Structures (W. Hemakul, S. Wahyuni, and P. W. Sy, eds.), 2012, pp. 53–102.

[10] W. Borho and H. Kraft, *Über die Gelfand-Kirillov-Dimension*, Math. Ann. **220** (1976), no. 1, 1–24.

[11] B. Buchberger, *Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal*, Ph.D. thesis, University of Innsbruck, 1965.

[12] ______, *A criterion for detecting unnecessary reductions in the construction of Gröbner-bases*, Symbolic and Algebraic Computation, Springer, 1979, pp. 3–21.

[13] J. L. Bueso, J. Gómez-Torrecillas, and F. J. Lobillo, *Computing the Gelfand-Kirillov dimension II*, Lect. Notes Pure Appl. Math. (2001), 33–58.

[14] J. L. Bueso, J. Gómez-Torrecillas, and A. Verschoren, *Algorithmic methods in non-commutative algebra: Applications to quantum groups*, Mathematical Modelling: Theory and Applications, vol. 17, Springer, 2003.

[15] J. L. Bueso, F. J. Jiménez, and P. Jara, *Effective computation of the Gelfand-Kirillov dimension*, Proceedings of the Edinburgh Mathematical Society (Series 2) **40** (1997), no. 1, 111–117.

[16] Yongshan Chen and Yuqun Chen, *Gröbner-Shirshov bases for metabelian Lie algebras*, J. Algebra **358** (2012), 143–161.

[17] F. Chyzak and B. Salvy, *Non-commutative elimination in Ore algebras proves multivariate identities*, J. Symbolic Comput. **26** (1998), no. 2, 187–227.

[18] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, Advances in Cryptology–EUROCRYPT 2000, Springer, 2000, pp. 392–407.

[19] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, vol. 10, Springer, 2007.

[20] J. Ding, J. Buchmann, M. S. E. Mohamed, W. S. A. E. Mohamed, and R.-P. Weinmann, *Mutant XL*, Proceeding of First International Conference on Symbolic Computation and Cryptography, 2008, pp. 16–22.

[21] C. Eder and J. E. Perry, *F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases*, J. Symbolic Comput. **45** (2010), no. 12, 1442–1458.

[22] J. C. Faugère, *A new efficient algorithm for computing Gröbner bases (F4)*, J. Pure Appl. Algebra **139** (1999), no. 1, 61–88.

[23] ______, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ACM, 2002, pp. 75–83.

[24] C. Gallego and O. Lezama, *Gröbner bases for ideals of σ-PBW extensions*, Comm. Algebra **39** (2011), no. 1, 50–75.

[25] A. Galligo, *Some algorithmic questions on ideals of differential operators*, EUROCAL'85, Springer, 1985, pp. 413–421.

[26] S. Gao, Y. Guan, and F. Volny IV, *A new incremental algorithm for computing Gröbner bases*, Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, ACM, 2010, pp. 13–19.

[27] S. Gao, F. Volny IV, and M. Wang, *A new algorithm for computing Gröbner bases*, Cryptology ePrint Archive (2010).

[28] I. M. Gelfand and A. A. Kirillov, *Fields associated with enveloping algebras of Lie algebras*, Dokl. Akad. Nauk SSSR **167** (1966), 407–409.

[29] ______, *Sur les corps liés aux algèbres enveloppantes des algèbres de Lie*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 31, 5–19.

[30] V. P. Gerdt and Y. A. Blinkov, *Involutive bases of polynomial ideals*, Math. Comput. Simulation **45** (1998), no. 5, 519–541.

[31] M. Giesbrecht, G. Reid, and Yang Zhang, *Non-commutative Gröbner bases in Poincaré-Birkhoff-Witt extensions*, Computer Algebra in Scientific Computing (CASC), 2002.

[32] A. Giovini, T. Mora, G. Niesi, L. Robbiano, and C. Traverso, *"one sugar cube, please" or selection strategies in the Buchberger algorithm*, Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, ACM, 1991, pp. 49–54.

[33] J. Gómez-Torrecillas, *Gelfand-Kirillov dimension of multi-filtered algebras*, Proceedings of the Edinburgh Mathematical Society **42** (1999), 155–168.

[34] A. Hashemi and G. Ars, *Extended F5 criteria*, J. Symbolic Comput. **45** (2010), no. 12, 1330–1340.

[35] C. Huh and C. O. Kim, *Gelfand-Kirillov dimension of skew polynomial rings of automorphism type*, Comm. Algebra **24** (1996), no. 7, 2317–2323.

[36] P. E. Hydon, *Symmetries and first integrals of ordinary difference equations*, Proceedings of the Royal Society of London (series A) **456** (2000), 2835–2855.

[37] M. Insa and F. Pauer, *Gröbner bases in rings of differential operators*, London Math. Soc. Lecture Note Ser. (1998), 367–380.

[38] A. Kandri-Rody and V. Weispfenning, *Non-commutative Gröbner bases in algebras of solvable type*, J. Symbolic Comput. **9** (1990), no. 1, 1–26.

[39] C. Kassel, *Quantum groups*, Graduate Texts in Mathematics, vol. 155, Springer-Verlag, 1995.

[40] G. Krause and T. Lenagan, *Growth of algebras and Gelfand-Kirillov dimension*, Graduate Studies in Mathematics, vol. 22, AMS, 2000.

[41] V. Levandovskyy and H. Schönemann, *Plural: a computer algebra system for noncommutative polynomial algebras*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 176–183.

[42] H. Li, *Noncommutative Gröbner bases and filtered-graded transfer*, Lecture Notes in Mathematics, vol. 1795, Springer, 2002.

[43] M. Lorenz, *Gelfand-Kirillov dimension of skew polynomial rings*, J. Algebra **77** (1982), no. 1, 186–188.

[44] X. Ma, Y. Sun, and D. Wang, *On computing Gröbner bases in rings of differential operators*, Sci. China Math. **54** (2011), no. 6, 1077–1087.

[45] E. L. Mansfield and A. Szanto, *Elimination theory for differential difference polynomials*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 191–198.

[46] J. Matczuk, *The Gelfand-Kirillov dimension of Poincaré-Birkhoff-Witt extensions*, Perspectives in Ring Theory (F. V. Oystaeyen and L. L. Bruyn, eds.), Kluwer Academic Publishers, 1988, pp. 221–226.

[47] J. C. McConnell, J. C. Robson, and L. W. Small, *Noncommutative Noetherian rings*, Graduate Studies in Mathematics, vol. 30, American Mathematical Society, 2001.

[48] J. Milnor, *A note on curvature and fundamental group*, J. Differential Geom. **2** (1968), 1–7.

[49] F. Mora, *Gröbner bases for non-commutative polynomial rings*, Algebraic algorithms and error-correcting codes (Grenoble, 1985), Lecture Notes in Comput. Sci., vol. 229, Springer, Berlin, 1986, pp. 353–362.

[50] A. Reyes, *Gelfand-Kirillov dimension of skew PBW extensions*, Rev. Colombiana Mat. **47** (2013), no. 1, 95–111.

[51] A. I. Shirshov, *Some algorithmic problems for Lie algebras*, Sibirsk. Mat. Zh. **3** (1962), no. 2, 292–296.

[52] Y. Sun, D. Wang, X. Ma, and Y. Zhang, *A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras*, Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation, ACM, 2012, pp. 351–358.

[53] J. J. Zhang, *A note on GK dimension of skew polynomial extensions*, Proceedings of the American Mathematical Society **125** (1997), no. 2, 363–374.

[54] M. Zhou and F. Winkler, *On computing Gröbner bases in rings of differential operators with coefficients in a ring*, Math. Comput. Sci. **1** (2007), no. 2, 211–223.

Chapter 2

Gelfand-Kirillov Dimension of Differential Difference Algebras

In this chapter, we investigate the Gelfand-Kirillov dimension of differential difference algebras. We give a lower bound of the Gelfand-Kirillov dimension of a differential difference algebra and a sufficient condition under which the lower bound is reached; we also find an upper bound of this Gelfand-Kirillov dimension under some specific conditions and construct an example to show that this upper bound can not be sharpened any further.

The article version [14] of this chapter has been accepted for publication by *LMS Journal of Computation and Mathematics*.

2.1 Introduction

Differential difference algebras (Definition 2.2.1) arose naturally from differential difference equations [2, 10]. The class of differential difference algebras contains several well-known classes of noncommutative algebras, for example, commutative polynomial algebras, quantum planes, and skew polynomial algebras of derivation (or automorphism) type. Rougly speaking, a differential difference algebra is a noncommutative polynomial ring (over an algebra) with two sets D and S of indeterminates, where D originally stands for differential operators and S originally stands for shift operators (the difference operators can be derived from S). Operators in D (S, respectively) commute with each other, but not with those in S (D, respectively). The exact definition is given in Section 2.

Let k be a field and A be a unital associative k-algebra. The Gelfand-Kirillov dimension of A is defined as

$$\mathrm{GKdim}(A) = \sup_V \overline{\lim_{n\to\infty}} \log_n \dim_k(V^n)$$

where the supremum is taken over all finite dimensional subspaces V of A. The Gelfand-Kirillov dimension is a very useful and powerful tool for investigating noncommutative algebras. Basic properties of Gelfand-Kirillov dimension can be found in [7].

There have been a number of results concerning Gelfand-Kirillov dimensions of algebras with derivations and/or automorphisms, for example, the Gelfand-Kirillov dimension of Ore extensions of derivation type [9], of Ore extensions of automorphism type [3], of PBW-extensions [11], and of skew polynomial extensions [13].

Assume that R is a unital associative k-algebra. Let σ be an automorphism of R, δ be a σ-derivation of R and $A = R[x; \sigma, \delta]$ be an Ore extension over R. It was shown in [3] that

$$\mathrm{GKdim}(A) \geq \mathrm{GKdim}(R) + 1; \tag{2.1}$$

the inequality becomes an equality provided that the following condition holds:

(∗) each finite dimensional subspace U of R is contained in a finite dimensional subspace V such that $\sigma(V) \subseteq V$ and $\delta(V) \subseteq V^p$ for some $p \geq 1$.

In this chapter we investigate the Gelfand-Kirillov dimension of differential difference algebras. We show that Inequality (2.1) of the Gelfand-Kirillov dimension of an Ore extension can be extended to differential difference algebras, that is, we get a lower bound of the Gelfand-Kirillov dimensions of differential difference algebras. However, owing to the noncommutativity of indeterminates of differential difference algebras, even under conditions similar to $(*)$, the equality does not hold for differential difference algebras in general. We find an upper bound for the Gelfand-Kirillov dimension of a differential difference algebra satisfying (an analogues of) condition $(*)$, and give a sufficient condition under which the lower bound is reached. We also construct an example to show that the upper bound we obtain cannot be sharpened any more.

This chapter is organized as follows. Definition and examples of differential difference algebras are given in Section 2. The Gelfand-Kirillov dimension of differential difference algebras is investigated in Section 3.

2.2 Preliminaries

Throughout this chapter, we assume that k is a field and all algebras are unital associative k-algebras. Denote the set of k-algebra automorphisms of the algebra A by $\mathrm{Aut}(A)$. If $\sigma \in \mathrm{Aut}(A)$, then a mapping δ on A is called a σ-derivation provided that, for any $a, b \in A$ and $c \in k$, $\delta(ca+b) = c\delta(a)+\delta(b)$ and $\delta(ab) = \sigma(a)\delta(b)+\delta(a)b$. Particularly, if $\sigma = \mathrm{id}$ then δ is called a derivation on A.

First we recall the definition of differential difference algebras, which was introduced by Mansfield and Szanto [10] with some discussions of Gröbner bases.

Definition 2.2.1 *(cf., [10]) An algebra A is called* a differential difference algebra *of type (m,n), $m,n \geq 1$, over a subalgebra $R \subseteq A$ if there exist elements $S_1, \ldots, S_m, D_1, \ldots, D_n$ in A such that* *(i) the set* $\{S_1^{\alpha_1}\cdots S_m^{\alpha_m}D_1^{\beta_1}\cdots D_n^{\beta_n} : \alpha_i,\beta_j\in\mathbb{N}, 1\le i\le m, 1\le j\le n\}$ *forms a basis for* A *as a free left* R*-module.*

(ii) $D_ir = rD_i+\delta_i(r)$ *for any* $1\le i\le n$ *and* $r\in R$*, where* δ_i *is a derivation on* R*.*

(iii) $S_ir = \sigma_i(r)S_i$ *for any* $1\le i\le m$ *and* $r\in R$*, where* σ_i *is a* k*-algebra automorphism on the subalgebra* $R[D_1,\dots,D_n]\subseteq A$ *such that* $\sigma_i|_R\in\mathrm{Aut}(R)$ *and* $\sigma_i(D_j)=\sum_{l=1}^n a_{ijl}D_l, \quad a_{ijl}\in R$*.*

(iv) $S_iS_j=S_jS_i$*,* $1\le i,j\le m$*;* $D_{i'}D_{j'}=D_{j'}D_{i'}$*,* $1\le i',j'\le n$*.*

(v) $D_iS_j=S_j\sigma_j(D_i)$*,* $1\le i\le n, 1\le j\le m$*.*

(vi) For any $1\le i,j\le n$ *and* $1\le i',j'\le m$*, the composition* $\delta_i\circ\delta_j=\delta_j\circ\delta_i$*,* $\delta_i\circ\sigma_{i'}=\sigma_{i'}\circ\delta_i$ *and* $\sigma_{i'}\circ\sigma_{j'}=\sigma_{j'}\circ\sigma_{i'}$*.*

Remark 2.2.2 In the above definition, both subalgebras $R[D_1,\dots,D_n]$ and $R[S_1,\dots,S_m]$ of A are iterated Ore extensions over R. But, in general A is not an iterated Ore extension over R.

The class of differential difference algebras contains several other known classes of algebras, for example, commutative polynomial algebras, quantum planes, and skew polynomial algebras of derivation (or automorphism) type.

Example 2.2.3 *Let* $0\neq q\in k$ *and* I_q *be the two-sided ideal of the free associative algebra* $k\langle x,y\rangle$ *generated by the element* $yx-qxy$*. Then the quotient algebra*

$$k_q[x,y]=k\langle x,y\rangle/I_q$$

is called a quantum plane *([6], Chapter IV). It is easy to see that* $k_q[x,y]$ *is a differential difference algebra of type* $(1,1)$ *over* k*.*

The following example distinguishes differential difference algebras from algebras of solvable type [5], PBW extensions [1], and G-algebras [8].

Example 2.2.4 Let A be the k-algebra generated by $\{D_1, D_2, S\}$ with defining relations $\mathcal{R} = \{D_2D_1 = D_1D_2, D_1S = SD_2, D_2S = SD_1\}$. Then it is easy to see that A is a differential difference algebra of type $(1, 2)$ over k. However, by the defining relations, A is not an algebra of solvable type [5], nor a PBW extension [1] or G-algebras [8].

Let $\mathcal{D} = \{D_1, \ldots, D_n\}$ and $\mathcal{S} = \{S_1, \ldots, S_m\}$. If A is a differential difference algebra over R defined as Definition 2.2.1, we denote $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$. For $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$ and $r \in R$, we simply write $\sigma^\alpha(r) = \sigma_1^{\alpha_1} \cdots \sigma_m^{\alpha_m}(r)$, $\mathcal{D}^\alpha = D_1^{\alpha_1} \cdots D_m^{\alpha_m}$ and $|\alpha| = \alpha_1 + \cdots + \alpha_m$. In particular, $D_i^0 = 1$, the identity of R. Similarly, we use notation $\delta^\alpha(r)$, S^β ($\beta \in \mathbb{N}^n$), and so on. Then every element in A can be written uniquely in the form: $\sum_{\alpha,\beta} r_{\alpha,\beta}\mathcal{S}^\alpha\mathcal{D}^\beta$, where $r_{\alpha,\beta} \in R$ and only finitely many $r_{\alpha,\beta}$ are nonzero.

The following example is taken from [10] with some modifications. This example shows where the differential difference algebras come from.

Example 2.2.5 Let $M, n, p \in \mathbb{N}$ and $p \geq 1$. Consider the following system, which arises from the calculation of symmetries of discrete systems (cf., [4]),

$$u_{n+M+1} = \omega(n, u_n, u_{n+1}, \ldots, u_{n+M});$$

$$\mathcal{D}_j F(n, u_n, u_{n+1}, \ldots, u_{n+M}) = 0,\ 1 \leq j \leq p,$$

where F is the unknown function and w is a given function in the field $\mathbb{Q}(n, u_n, \ldots, u_{n+M})$ of rational functions over the rational numbers $\mathbb{Q}$ in indeterminates $n, u_n, u_{n+1}, \ldots, u_{n+M}$, such that $\frac{\partial\omega}{\partial u_n} \neq 0$, and $\mathcal{D}_j : T \to T$ is a linear operator of the form

$$\mathcal{D}_j = \sum_{\alpha=(\alpha_0,\ldots,\alpha_M)\in\mathbb{N}^M,\ \beta\in\mathbb{N}} c_{\alpha,\beta}\circ s^{\beta}\circ \frac{\partial^{\alpha_0+\cdots+\alpha_M}}{\partial u_n^{\alpha_0}\cdots\partial u_{n+M}^{\alpha_M}},$$

where $T=\mathbb{Q}(n,u_{n+t}:t\in\mathbb{Z})$, $c_{\alpha,\beta}\in\mathbb{Q}(n,u_{n+t}:t\in\mathbb{Z})$ are *multiplication operators* and only finitely many $c_{\alpha,\beta}$ are nonzero, and s is the *shift operator* defined by $s(n)=n+1$ and $s(u_n)=u_{n+1}$.

A natural approach to deal with this system is to consider the operators $\mathcal{D}_j$ and s as elements of the noncommutative algebra A generated by operator variables $\{S,D_n,\ldots,D_{n+M}\}$ over $R=\mathbb{Q}(n,u_{n+t}:t\in\mathbb{Z})$, where S denotes the shift operator s and D_{n+t} denotes the differential operator $\frac{\partial}{\partial u_{n+t}}$ for $0\le t\le M$, subject to the following commutation rules:

$$\begin{aligned}
D_{n+t}\circ S &= S\circ D_{n+t-1}+\frac{\partial\omega}{\partial u_{n+t}}\circ S\circ D_{n+M}, \quad 1\le t\le M;\\
D_n\circ S &= \frac{\partial\omega}{\partial u_n}\circ S\circ D_{n+M};\\
D_{n+t}\circ D_{n+t'} &= D_{n+t'}\circ D_{n+t}, \qquad 0\le t,t'\le M;\\
S\circ r &= s(r)\circ S, \qquad r\in R;\\
D_{n+t}\circ r &= r\circ D_{n+t}+\frac{\partial r}{\partial u_{n+t}}, \qquad r\in R, 0\le t\le M.
\end{aligned}$$

Then $A=\mathbb{Q}(n,u_{n+t}:t\in\mathbb{Z})[S,\mathcal{D};\sigma,\delta]$ is a differential difference algebra of type $(1,M+1)$ over R, where $\delta_i=\frac{\partial}{\partial u_i}$ for $n\le i\le n+M$ and $\sigma|_R=s, \sigma(D_n)=s^{-1}(\frac{\partial\omega}{\partial u_n})D_{n+M}$, $\sigma(D_{n+t})=D_{n+t-1}+s^{-1}(\frac{\partial\omega}{\partial u_{n+t}})D_{n+M}$ for $1\le t\le M$.

Note that the difference operator Δ, defined by $\Delta(u_i)=u_{i+1}-u_i$ for $i\in\mathbb{Z}$, can be derived from the shift operator: $\Delta=S-\mathrm{id}$. So the differential difference algebra in the above example actually involves both differential and difference operators.

2.3 Bounds of the Gelfand-Kirillov Dimension

In this section, we consider the Gelfand-Kirillov dimension of differential difference algebras.

We first fix our notation. Let $\mathrm{GKdim}(A)$ denote the Gelfand-Kirillov dimension of an algebra A, $\dim(V)$ denote the dimension of a k-vector space V, and $\mathrm{card}(T)$ denote the cardinality of a set T. Recall that, for $r, s \in \mathbb{N}$, the binomial coefficient $\binom{r}{s} = \frac{r(r-1)\cdots(r-s+1)}{s(s-1)\cdots 1}$ if $0 \leq s \leq r$; and $\binom{r}{s} = 0$ if $s < 0$ or $s > r$.

The Gelfand-Kirillov dimension of an Ore extension has been discussed in [3].

Proposition 2.3.1 *([3], Corollary 2.4, cf., [7], Proposition 3.5.) Let R be a k-algebra and $A = R[D; \sigma, \delta]$ be an Ore extension. Suppose that, for each finite dimensional subspace U of R, there exists a finite dimensional subspace V of R such that $U \subseteq V$, $\sigma(V) \subseteq V$ and $\delta(V) \subseteq V^p$ for some $p \geq 1$. Then* $\mathrm{GKdim}(A) = \mathrm{GKdim}(R) + 1$.

We want to consider the Gelfand-Kirillov dimension of differential difference algebras satisfying "similar" conditions as in Proposition 2.3.1. Our goal is to find a lower bound and an upper bound of the Gelfand-Kirillov dimension of such a differential difference algebra.

The following proposition gives a general lower bound of the Gelfand-Kirillov dimension of a differential difference algebra.

Proposition 2.3.2 *Let R be a k-algebra and $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra of type (m, n). Then* $\mathrm{GKdim}(A) \geq \mathrm{GKdim}(R) + m + n$.

Proof. Suppose that V is a finite dimensional generating subspace of R and $1 \in V$. Then

$$W = V + \sum_{i=1}^{n} kD_i + \sum_{j=1}^{m} kS_j$$

is a finite dimensional generating subspace of A. For any $r \in \mathbb{N}$,

$$W^{3r} = (V + \sum_{i=1}^{n} kD_i + \sum_{j=1}^{m} kS_j)^{3r} \supseteq \sum_{\substack{\alpha\in\mathbb{N}^m,\beta\in\mathbb{N}^n \\ 0\leq|\alpha|,\ |\beta|\leq r}} V^r\mathcal{S}^\alpha\mathcal{D}^\beta.$$

For any k-basis U of V^r, the set

$$\{u\mathcal{S}^\alpha\mathcal{D}^\beta : u \in U, 0 \leq |\alpha|, |\beta| \leq r, \alpha \in \mathbb{N}^m, \beta \in \mathbb{N}^n\}$$

is a k-basis of $\sum_{0\leq|\alpha|,|\beta|\leq r} V^r\mathcal{S}^\alpha\mathcal{D}^\beta$. Hence, we have that

$$\begin{aligned}
\dim(W^{3r}) &\geq \dim\left(\sum_{0\leq|\alpha|,|\beta|\leq r} V^r\mathcal{S}^\alpha\mathcal{D}^\beta\right) \\
&= \dim(V^r)\cdot \ \mathrm{card}(\{\alpha : 0 \leq \alpha_1 + \ldots + \alpha_m \leq r\}) \\
&\qquad\qquad \cdot\ \mathrm{card}(\{\beta : 0 \leq \beta_1 + \ldots + \beta_n \leq r\}) \\
&= \dim(V^r)\cdot\binom{r+m-1}{m}\cdot\binom{r+n-1}{n},
\end{aligned}$$

where $\binom{r+m-1}{m}$ and $\binom{r+n-1}{n}$ are polynomials in r of degree m and n respectively. Hence,

$$\begin{aligned}
\mathrm{GKdim}(A) &\geq \overline{\lim_{r\to\infty}} \log_r \dim(W^r) = \overline{\lim_{r\to\infty}} \log_r \dim(W^{3r}) \\
&\geq \overline{\lim_{r\to\infty}} \log_r \left(\dim(V^r)\cdot\binom{r+m-1}{m}\cdot\binom{r+n-1}{n}\right) \\
&= \mathrm{GKdim}(R) + m + n
\end{aligned}$$

where the first equality holds since $\dim(W^r)$ and $\dim(W^{3r})$ (as functions of r) have the same growth ([7], Chapter 1 and Lemma 2.1). ■

In the special case $R = k$, the equality in the above proposition holds, i.e., we have the following proposition, which indicates that the lower bound of $\mathrm{GKdim}(A)$

obtained in Proposition 2.3.2 can not be sharpened any more.

Proposition 2.3.3 *Let $A = k[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra of type (m, n) over k. Then* $\operatorname{GKdim}(A) = m + n$.

Proof. Let $V = k + \sum_{i=1}^{n} kD_i + \sum_{j=1}^{m} kS_j$. Then V is a finite dimensional generating subspace of A. For any $r \in \mathbb{N}$,

$$V^r = (k + \sum_{i=1}^{n} kD_i + \sum_{j=1}^{m} kS_j)^r \subseteq \sum_{0 \leq |\alpha|, |\beta| \leq r} k\mathcal{S}^{\alpha}\mathcal{D}^{\beta},$$

where the last inclusion holds since

$$D^{\beta}S^{\alpha} \in \sum_{\beta' \in \mathbb{N}^n, |\beta'| = |\beta|} kS^{\alpha}D^{\beta'}, \quad \alpha \in \mathbb{N}^m, \ \beta \in \mathbb{N}^n.$$

So, $\dim(V^r) \leq \binom{r+m-1}{m} \cdot \binom{r+n-1}{n}$. Hence, $\operatorname{GKdim}(A) \leq m+n$ and thus by Proposition 2.3.2 $\operatorname{GKdim}(A) = m + n$. ■

Now let us turn to upper bounds for $\operatorname{GKdim}(A)$. First we consider the case when R is finitely generated.

Lemma 2.3.4 *Let R be a k-algebra with a finite dimensional generating subspace V, and let $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra of type (m, n). Suppose that $\sigma_i(V) \subseteq V$ for $1 \leq i \leq m$. Then* $\operatorname{GKdim}(A) \leq 2\operatorname{GKdim}(R) + m + n$.

Furthermore, if, for all $1 \leq i \leq m$ and $1 \leq j \leq n$, $\sigma_i(D_j)$ is contained in the vector space over k generated by $\{D_1, \dots, D_n\}$, then $\operatorname{GKdim}(A) = \operatorname{GKdim}(R) + m + n$.

Proof. Since V is a generating subspace, there exists $p \geq 1$ such that

$$a_{ijl} \in V^p, \ \delta_i(V) \subseteq V^p, \ 1 \leq i, l \leq n, \ 1 \leq j \leq m,$$

where the a_{ijl} are the coefficients that appear in Definition 2.2.1. Then

$$\delta_i(V^t) \subseteq V^{p+t},\ \sigma_j(V^t) \subseteq V^t,\ 1 \leq i \leq n,\ 1 \leq j \leq m,\ t \geq 1.$$

So, eventually replacing V by V^p if necessary, we may assume that

$$1 \in V, \delta_i(V) \subseteq V^2, \sigma_j(V) \subseteq V,\ 1 \leq i \leq n,\ 1 \leq j \leq m.$$

Let $X = \sum_{i=1}^{n} kD_i$, $Y = \sum_{j=1}^{m} kS_j$ and $W = V + X + Y$. Then W is a generating subspace of A.

In order to finish the proof of the first statement of the this lemma, we have to prove the following three lemmas first.

Lemma 2.3.5 *For any integer $s \geq 1$,*

(i). $XY \subseteq VYX,\ XV \subseteq VX + V^2,\ YV = VY.$

(ii). $X^sV \subseteq \sum_{i=0}^{s} V^{i+1}X^{s-i}.$

(iii). $X^sY \subseteq \sum_{i=0}^{s-1} V^{s+i}YX^{s-i}.$

(iv). If $\sigma_i(D_j) \in X$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$, then $XY = YX$.

Proof. (i). It follows easily by definition. (ii). (By induction on s.) If $s = 1$, then we have $XV \subseteq VX + V^2$ by the commutation rules of differential difference algebras. Suppose that $X^rV \subseteq \sum_{i=0}^{r} V^{i+1}X^{r-i}$ for $1 \leq r \leq s$. Then

$$\begin{aligned} X^{s+1}V &\subseteq X^s(VX + V^2) \subseteq \sum_{i=0}^{s} V^{i+1}X^{s-i+1} + \sum_{i=0}^{s} V^{i+1}X^{s-i}V \\ &\subseteq \sum_{i=0}^{s} V^{i+1}X^{s-i+1} + \sum_{i=0}^{s} V^{i+1} \sum_{j=0}^{s-i} V^{j+1}X^{s-i-j} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{s} V^{i+1}X^{s-i+1} + \sum_{i=0}^{s}\sum_{j=0}^{s-i} V^{i+j+2}X^{s-i-j} \\
&= \sum_{i=0}^{s} V^{i+1}X^{s-i+1} + \sum_{i=0}^{s}\sum_{l=i+1}^{s+1} V^{l+1}X^{s-l+1} \qquad (l := i+j+1) \\
&= \sum_{i=0}^{s} V^{i+1}X^{s-i+1} + \sum_{l=1}^{s+1} V^{l+1}X^{s-l+1} \\
&= \sum_{i=0}^{s+1} V^{i+1}X^{s-i+1}.
\end{aligned}
$$

Thus (ii) holds for all $s \geq 1$.

(iii). (By induction on s.) If $s = 1$, then we have $V^1YX^1 \supseteq XY$ by (i), and thus (iii) holds. Suppose that $X^rY \subseteq \sum_{i=0}^{r-1} V^{r+i}YX^{r-i}$ for all $1 \leq r \leq s$. Then,

$$
\begin{aligned}
X^{s+1}Y &\subseteq X^s(VYX) \subseteq \sum_{i=0}^{s} V^{i+1}X^{s-i}YX \quad \text{(by (ii))} \\
&= \sum_{i=0}^{s-1} V^{i+1}X^{s-i}YX + V^{s+1}YX \\
&\subseteq \sum_{i=0}^{s-1} V^{i+1} \sum_{j=0}^{s-i-1} V^{s-i+j}YX^{s-i-j+1} + V^{s+1}YX \\
&= \sum_{i=0}^{s-1}\sum_{j=0}^{s-i-1} V^{s+j+1}YX^{s-i-j+1} + V^{s+1}YX \\
&= \sum_{i=0}^{s-1}\sum_{l=i}^{s-1} V^{s+l-i+1}YX^{s-l+1} + V^{s+1}YX \quad (l := i+j) \\
&\subseteq \sum_{i=0}^{s-1}\sum_{l=0}^{s-1} V^{s+l+1}YX^{s-l+1} + V^{s+1}YX \\
&= \sum_{l=0}^{s-1} V^{s+l+1}YX^{s-l+1} + V^{s+1}YX \subseteq \sum_{l=0}^{s} V^{s+l+1}YX^{s-l+1}.
\end{aligned}
$$

Hence (iii) holds.

(iv) is straightforward. ■

Lemma 2.3.6 *For all $r \geq 1$, $W^r \subseteq \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r^2} Y^i X^j$.*

Proof. (By induction on r.) If $r = 1$, then the right hand side of the inclusion is $V^2 + V^2X + V^2Y \supseteq W$. Suppose the statement is true for $r \geq 1$. Then, by induction hypothesis,

$$
\begin{aligned}
& W^{r+1} \subseteq \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r^2} Y^i X^j (V + X + Y) \qquad \text{(induction hypothesis)} \\
= \; & \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r^2} Y^i X^j V + \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r^2} Y^i X^{j+1} + \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r^2} Y^i X^j Y \\
\subseteq \; & \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r^2} Y^i \sum_{l=0}^{j} V^{l+1} X^{j-l} \qquad \text{(by Lemma 2.3.5(ii))} \\
& + \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r^2} Y^i X^{j+1} \\
& + \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r^2} Y^i \sum_{l=0}^{j-1} V^{j+l} Y X^{j-l} \qquad \text{(by Lemma 2.3.5(iii))} \\
= \; & \sum_{i=0}^{r}\sum_{j=0}^{r-i}\sum_{p=0}^{j} V^{2r^2+j-p+1} Y^i X^p \qquad (p := j-l) \\
& + \sum_{i=0}^{r}\sum_{j=1}^{r-i+1} V^{2r^2} Y^i X^j \qquad \text{(shift index } j\text{)} \\
& + \sum_{i=1}^{r+1}\sum_{j=0}^{r-i+1}\sum_{p=1}^{j} V^{2r^2+2j-p} Y^i X^p \qquad \text{(shift } i \text{ and } p := j-l\text{)} \\
\subseteq \; & \sum_{i=0}^{r}\sum_{j=0}^{r-i}\sum_{p=0}^{r-i} V^{2r^2+r-p+1} Y^i X^p + \sum_{i=0}^{r}\sum_{j=1}^{r-i+1} V^{2r^2} Y^i X^j \\
& + \sum_{i=1}^{r+1}\sum_{j=0}^{r-i+1}\sum_{p=1}^{r-i+1} V^{2r^2+2r-p} Y^i X^p \\
\subseteq \; & \sum_{i=0}^{r}\sum_{p=0}^{r-i} V^{2r^2+r-p+1} Y^i X^p + \sum_{i=0}^{r}\sum_{j=1}^{r-i+1} V^{2r^2} Y^i X^j + \sum_{i=1}^{r+1}\sum_{p=1}^{r-i+1} V^{2r^2+2r-p} Y^i X^p \\
\subseteq \; & \sum_{i=0}^{r+1}\sum_{j=0}^{r-i+1} V^{2(r+1)^2} Y^i X^j.
\end{aligned}
$$

Therefore, $W^r \subseteq \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r^2}Y^iX^j$ for any $r \geq 1$. ■

Lemma 2.3.7 *Let $f : \mathbb{N} \to \mathbb{R}$ be an increasing and positive valued function, and $p > 1$. Then*

$$\overline{\lim_{n\to\infty}} \log_n f(pn^2) \leq 2\overline{\lim_{n\to\infty}} \log_n f(n).$$

Proof. Let $d = \overline{\lim_{n\to\infty}} \log_n f(n)$. By Lemma 2.1 of [7],

$$d = \inf\{\rho \in \mathbb{R} : f(n) \leq n^\rho \text{ for almost all } n \in \mathbb{N}\}.$$

Hence, for any $\varepsilon > 0$, $f(n) < n^{d+\varepsilon}$ for almost all n. So

$$f(pn^2) < (pn^2)^{d+\varepsilon} = p^{d+\varepsilon}n^{2d+2\varepsilon} < n^{2d+3\varepsilon} \text{ for almost all } n.$$

Therefore, $\overline{\lim_{n\to\infty}} \log_n f(pn^2) \leq 2d = 2\overline{\lim_{n\to\infty}} \log_n f(n)$. ■

Now let us return to the proof of Lemma 2.3.4. Let $f(r) = \dim(V^r)$ for $r \in \mathbb{N}$. Then

$$\begin{aligned}
\operatorname{GKdim}(A) &= \overline{\lim_{r\to\infty}} \log_r \dim(W^r) \leq \overline{\lim_{r\to\infty}} \log_r \dim\left(\sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r^2}Y^iX^j\right) \\
&= \overline{\lim_{r\to\infty}} \log_r \left(\dim(V^{2r^2})\sum_{i=0}^{r}\sum_{j=0}^{r-i} \dim(Y^i)\dim(X^j)\right) \\
&= \overline{\lim_{r\to\infty}} \log_r \left(f(2r^2)\sum_{i=0}^{r}\sum_{j=0}^{r-i} \binom{i+m-1}{m-1}\binom{j+n-1}{n-1}\right) \\
&\leq \overline{\lim_{r\to\infty}} \log_r f(2r^2) + \overline{\lim_{r\to\infty}} \log_r \sum_{i=0}^{r} \binom{i+m-1}{m-1} \\
&\qquad\qquad + \overline{\lim_{r\to\infty}} \log_r \sum_{j=0}^{r} \binom{j+n-1}{n-1} \\
&\leq 2\operatorname{GKdim}(R) + m + n
\end{aligned}$$

where the last inequality holds because of Lemma 2.3.7 and the fact that if $p(i)$ is a polynomial in i of degree s then $\sum_{i=0}^{r} p(i)$ is a polynomial in r of degree $s+1$.

For the second statement of Lemma 2.3.4, we need the following

Lemma 2.3.8 *Under the assumptions of the second statement of Lemma 2.3.4, we have that* $W^r \subseteq \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r-i-j}Y^iX^j$ *for all* $r \geq 1$.

Proof. Similarly to Lemma 2.3.6, this lemma can be proved by induction on r. It is easy to check that the inclusion is true for $r=1$. Suppose $W^r \subseteq \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r-i-j}Y^iX^j$ for $r \geq 1$. Then, by the induction hypothesis and Lemma 2.3.5(ii) and (iv), we have that

$$\begin{aligned}
W^{r+1} &\subseteq \sum_{i=0}^{r}\sum_{j=0}^{r-i}\left(V^{2r-i-j}Y^iX^jV + V^{2r-i-j}Y^iX^{j+1} + V^{2r-i-j}Y^iX^jY\right) \\
&\subseteq \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r-i-j}Y^i\left(\sum_{l=0}^{j} V^{l+1}X^{j-l}\right) \qquad \text{(by Lemma 2.3.5(ii))} \\
&\qquad + \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r-i-j}Y^iX^{j+1} + \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r-i-j}Y^{i+1}X^j \\
&= \sum_{i=0}^{r}\sum_{j=0}^{r-i}\sum_{t=0}^{j} V^{2r-i-t+1}Y^iX^t \qquad (t := j-l) \\
&\qquad + \sum_{i=0}^{r}\sum_{j=1}^{r+1-i} V^{2r-i-j+1}Y^iX^j \qquad \text{(shift index } j\text{)} \\
&\qquad + \sum_{i=1}^{r+1}\sum_{j=0}^{r-i} V^{2r-i-j+1}Y^iX^j \qquad \text{(shift index } i\text{)} \\
&\subseteq \sum_{i=0}^{r+1}\sum_{j=0}^{r+1-i} V^{2(r+1)-i-j}Y^iX^j
\end{aligned}$$

That proves our lemma. ■

By the above lemma, $W^r \subseteq \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r-i-j}Y^iX^j \subseteq \sum_{i=0}^{r}\sum_{j=0}^{r-i} V^{2r}Y^iX^j$. Hence, by a similar argument as we used in the proof of the first statement of Lemma

2.3.4, we have that $\mathrm{GKdim}(A) \leq \mathrm{GKdim}(R) + m + n$. Thus, by Proposition 2.3.2, $\mathrm{GKdim}(A) = \mathrm{GKdim}(R) + m + n$. ■

Now we are in a position to state our main theorem.

Theorem 2.3.9 *Let R be a k-algebra and $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra of type (m, n). Suppose that for any finite dimensional subspace U of R there exist a finite dimensional subspace V of R and an integer $p \geq 1$ such that*

$$U \subseteq V,\ \sigma_i(V) \subseteq V,\ \delta_j(V) \subseteq V^p,\quad 1 \leq i \leq m, 1 \leq j \leq n.$$

Then

$$\mathrm{GKdim}(R) + m + n \leq \mathrm{GKdim}(A) \leq 2\,\mathrm{GKdim}(R) + m + n.$$

Furthermore, if, for all $1 \leq i \leq m$ and $1 \leq j \leq n$, $\sigma_i(D_j)$ is contained in the vector space over k generated by $\{D_1, \ldots, D_n\}$, then

$$\mathrm{GKdim}(A) = \mathrm{GKdim}(R) + m + n.$$

Proof. Let W be a finite dimensional subspace of A with a k-basis $w_1, \ldots, w_q, q \in \mathbb{N}$. Note that each $w_i, 1 \leq i \leq q$, is a polynomial in $D_1, \ldots, D_n, S_1, \ldots, S_m$ with coefficients in R. Let U be the subspace of R spanned by all the coefficients (in R) of $w_1, \ldots, w_q$ and all a_{ijl} (defined in Definition 2.2.1), $1 \leq i, l \leq n, 1 \leq j \leq m$. Then U is finite dimensional and hence there exist a finite dimensional subspace V of R and an integer $p \geq 1$ such that $U \subseteq V,\ \sigma_i(V) \subseteq V,\ \delta_j(V) \subseteq V^p$ for $1 \leq i \leq m, 1 \leq j \leq n$. Let B be the subalgebra of R generated by V. Then $\sigma_i(B) \subseteq B$, $\sigma_i(D_l) \in B[\mathcal{D}; \delta]$ and $\delta_j(B) \subseteq B$ for $1 \leq i \leq m, 1 \leq j, l \leq n$. That is, $A' = B[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ is a differential difference algebra satisfying the conditions of Lemma 2.3.4. Note that $W \subseteq A'$. So, by Lemma 2.3.4, we have

$$\overline{\lim_{r\to\infty}} \log_r \dim(W^r) \leq \operatorname{GKdim}(A') \leq 2\operatorname{GKdim}(B) + m + n \leq 2\operatorname{GKdim}(R) + m + n.$$

Thus $\operatorname{GKdim}(A) \leq 2\operatorname{GKdim}(R) + m + n$ since W is arbitrary. Therefore, by Lemma 2.3.2, $\operatorname{GKdim}(R) + m + n \leq \operatorname{GKdim}(A) \leq 2\operatorname{GKdim}(R) + m + n$. That completes our proof of the first statement.

The second statement follows similarly by using the second part of Lemma 2.3.4. ■

Immediately from Theorem 2.3.9, we have the following corollaries.

Corollary 2.3.10 *The quantum plane $k_q[x, y]$ has Gelfand-Kirillov dimension* 2.

Recall that an algebra A is called *locally finite dimensional* if every finitely generated subalgebra of A is finite dimensional.

Corollary 2.3.11 *Let R be a k-algebra and $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra of type (m, n) satisfying the conditions of the first statement of Theorem 2.3.9.*

(i). If R is locally finite dimensional, then $\operatorname{GKdim}(A) = m + n$.

(ii). If $\operatorname{GKdim}(R) < \infty$, *then* $\operatorname{GKdim}(A) < \infty$.

Proof. (i). It follows from the fact that $\operatorname{GKdim}(R) = 0$ if and only if R is locally finite dimensional.

(ii). This is clear. ■

Note that if we set $R = k$ in Theorem 2.3.9, then the conditions of the theorem are satisfied. Thus Theorem 2.3.9 implies Proposition 2.3.3.

The following example shows that the upper bound of $\operatorname{GKdim}(A)$ stated in Theorem 2.3.9 is the "best" one under the given conditions.

Example 2.3.12 *Let A be the k-algebra generated by $\{z, z^{-1}, D, S\}$ with defining relations*

$$\mathcal{R} = \{zz^{-1} = 1, \quad z^{-1}z = 1, \qquad Dz = zD, \qquad Sz = zS,$$
$$Dz^{-1} = z^{-1}D, \quad Sz^{-1} = z^{-1}S, \quad DS = zSD\}.$$

Let $R = k[z, z^{-1}]$ be the algebra of Laurent polynomials over k, and let σ be the automorphism of the algebra $R[D] \subseteq A$ defined by

$$\sigma(\sum_{i=0}^{l} c_i D^i) = \sum_{i=0}^{l} c_i (zD)^i, \quad l \geq 0, c_i \in R \text{ for } 0 \leq i \leq l.$$

Then $A = R[S, D; \sigma, 0]$ is a differential difference algebra of type $(1,1)$ and

$$\mathrm{GKdim}(A) = 2\,\mathrm{GKdim}(R) + 1 + 1 = 4.$$

Proof. It is easy to see that A can be thought of as an iterated Ore extension over R: $A = R[S; \mathrm{id}, 0][D; \sigma', 0]$ where σ' is the automorphism over $R[S]$ defined by

$$\sigma'(\sum_{i=0}^{l} c_i S^i) = \sum_{i=0}^{l} c_i (zS)^i, \quad l \geq 0, c_i \in R \text{ for } 0 \leq i \leq l.$$

Hence $\{S^i D^j : i, j \in \mathbb{N}\}$ forms an R-basis of A. Thus A is a differential difference algebra.

Note that the restriction of σ on R is the identity automorphism of R. It is clear that A satisfies all conditions of Theorem 2.3.9. So, by Theorem 2.3.9, $\mathrm{GKdim}(A) \leq 2\,\mathrm{GKdim}(R) + 2$. Since $\mathrm{GKdim}(R) = 1$ (see, for example, Corollary 8.2.15 of [12]), $\mathrm{GKdim}(A) \leq 4$.

Note that $DS = S\sigma(D) = SzD = zSD$. Then one can prove that $D^j S = z^j S D^j$ by induction on j, and then that $D^j S^i = z^{ij} S^i D^j$ by induction on i. Now we claim that

$$B := \{z^l S^i D^j : 0 \leq i+j \leq r, 0 \leq l \leq ij\} \subseteq W^r,\ r \geq 1,$$

where $W = k + kz + kz^{-1} + kD + kS$ is a generating subspace of A. Suppose $r \geq 1, 0 \leq i+j \leq r, 0 \leq l \leq ij$ and write $l = qj + p$ with $0 \leq q \leq i, 0 \leq p < j$. If $q = i$, then $p = 0, l = ij$ and $z^l S^i D^j = z^{ij} S^i D^j = D^j S^i \in W^r$. If $q < i$, then

$$\begin{aligned} &S^{i-q-1} D^p S D^{j-p} S^q = z^p S^{i-q-1} S D^p D^{j-p} S^q \\ &= z^p S^{i-q} D^j S^q = z^{p+qj} S^{i-q} S^q D^j = z^l S^i D^j. \end{aligned}$$

Since $(i-q-1)+p+1+(j-p)+q = i+j \leq r$, $z^l S^i D^j = S^{i-q-1} D^p S D^{j-p} S^q \in W^r$. Thus our claim holds.

It is clear that B is k-linearly independent. Then by our claim,

$$\dim(W^r) \geq \mathrm{card}(B) = \sum_{i=0}^{r} \sum_{j=0}^{r} (ij+1) = \frac{1}{4}r^4 + \frac{1}{2}r^3 + \frac{5}{4}r^2 + 2r + 1.$$

Thus, $\mathrm{GKdim}(A) \geq \overline{\lim_{r\to\infty}} \log_r \dim(W^r) \geq 4$. Therefore, $\mathrm{GKdim}(A) = 4$. ■

Bibliography

[1] A. D. Bell and K. R. Goodearl, *Uniform rank over differential operator rings and Poincaré-Birkhoff-Witt extensions*, Pacific J. Math. **131** (1988), no. 1, 13–37.

[2] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, Advances in Cryptology–EUROCRYPT 2000, Springer, 2000, pp. 392–407.

[3] C. Huh and C. O. Kim, *Gelfand-Kirillov dimension of skew polynomial rings of automorphism type*, Comm. Algebra **24** (1996), no. 7, 2317–2323.

[4] P. E. Hydon, *Symmetries and first integrals of ordinary difference equations*, Proceedings of the Royal Society of London (series A) **456** (2000), 2835–2855.

[5] A. Kandri-Rody and V. Weispfenning, *Non-commutative Gröbner bases in algebras of solvable type*, J. Symbolic Comput. **9** (1990), no. 1, 1–26.

[6] C. Kassel, *Quantum groups*, Graduate Texts in Mathematics, vol. 155, Springer-Verlag, 1995.

[7] G. Krause and T. Lenagan, *Growth of algebras and Gelfand-Kirillov dimension*, Graduate Studies in Mathematics, vol. 22, AMS, 2000.

[8] V. Levandovskyy and H. Schönemann, *Plural: a computer algebra system for noncommutative polynomial algebras*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 176–183.

[9] M. Lorenz, *Gelfand-Kirillov dimension of skew polynomial rings*, J. Algebra **77** (1982), no. 1, 186–188.

[10] E. L. Mansfield and A. Szanto, *Elimination theory for differential difference polynomials*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 191–198.

[11] J. Matczuk, *The Gelfand-Kirillov dimension of Poincaré-Birkhoff-Witt extensions*, Perspectives in Ring Theory (F. V. Oystaeyen and L. L. Bruyn, eds.), Kluwer Academic Publishers, 1988, pp. 221–226.

[12] J. C. McConnell, J. C. Robson, and L. W. Small, *Noncommutative Noetherian rings*, Graduate Studies in Mathematics, vol. 30, American Mathematical Society, 2001.

[13] J. J. Zhang, *A note on GK dimension of skew polynomial extensions*, Proceedings of the American Mathematical Society **125** (1997), no. 2, 363–374.

[14] Yang Zhang and Xiangui Zhao, *Gelfand-Kirillov dimension of differential difference algebras*, LMS J. Comput. Math. **17** (2014), no. 1, 485–495.

Chapter 3

Gelfand-Kirillov Dimension of Modules over Differential Difference Algebras

In this chapter, we investigate the Gelfand-Kirillov dimension of a finitely generated module over a differential difference algebra through a computational method: Gröbner-Shirshov basis method. We develop the Gröbner-Shirshov basis theory of differential difference algebras, and of their finitely generated modules, respectively. Then, via Gröbner-Shirshov bases, we give algorithms for computing the Gelfand-Kirillov dimensions of cyclic modules and finitely generated modules over differential difference algebras.

The article version of this chapter has been accepted for publication by *Algebra Colloquium*.

3.1 Introduction

Let k be a field, A be an associative k-algebra with identity 1, and M be a left A-module. Then the *Gelfand-Kirillov dimension* of M ([15], Chapter 5) is defined by

$$\mathrm{GKdim}(M) = \sup_{V,F} \overline{\lim_{n\to\infty}} \log_n \dim_k(V^n F)$$

where the supremum is taken over all finite dimensional subspaces V of A containing 1 and all finite dimensional subspaces F of M. Gelfand-Kirillov dimension is a very useful tool for investigating modules over noncommutative algebras. Basic properties and applications of Gelfand-Kirillov dimension can be found in [15].

Gröbner-Shirshov basis theory is a powerful computational tool for both commutative and noncommutative algebras (see the survey [7], and more algebraic structures which admit Gröbner-Shirshov basis theory can be found in, for example, dialgebras [5], metabelian Lie algebras [10], L-algebras [4], semirings [6]). For commutative algebras, the dimension of an algebraic variety can be efficiently computed by using Gröbner-Shirshov bases to compute the growth of the Hilbert function (or Hilbert polynomial) (see [2]). The Gelfand-Kirillov dimension of a finitely generated module over a finitely generated algebra is also closely related to the Hilbert function and thus it is possible to compute it for some specific classes of noncommutative algebras by using Gröbner-Shirshov bases. For example, Bueso et al. [9] computed the Gelfand-Kirillov dimension of a cyclic module over an almost commutative algebra, Torrecillas [12] considered the Gelfand-Kirillov dimension of finitely generated graded modules over multi-graded finitely generated algebas, Li [17] extended this method to cyclic modules over solvable polynomial algebras (also known as PBW algebras), and Bueso et al. [8] extended it to finitely generated modules over PBW algebras.

Differential difference algebras were first defined by Mansfield and Szanto in [18], where they arose from the calculation of symmetries of discrete systems. Differential difference algebras are generalizations of several classes of (skew) polynomial rings/algebras, e.g., commutative polynomial algebras, skew polynomials of derivation/automorphism type ([19], Chapter 1) and the quantum plane ([14], Chapter IV). Mansfield and Szanto [18] developed the Gröbner-Shirshov basis theory (where they use the term Gröbner bases instead) of differential difference algebras by using special kinds of left admissible orderings, which they called differential difference orderings. In this chapter, we generalize the Gröbner-Shirshov basis theory of differential difference algebras to any left admissible ordering and develop the Gröbner-Shirshov basis theory of finitely generated free modules over differential difference algebras. By using the theory we develop in this chapter, we compute the Gelfand-Kirillov dimensions of finitely generated modules over differential difference algebras.

This chapter is organized as follows. We give the definition and properties of differential difference algebras in Section 2. In Section 3, we generalize the main results of Mansfield and Szanto [18] on Gröbner-Shirshov bases to differential difference algebras with respect to differential difference monomial orderings (see Definition 3.3.1). Then, in Section 4, we apply the theory we develop to compute the Gelfand-Kirillov dimension of a cyclic module over a differential difference algebra. We develop the Gröbner-Shirshov basis theory of finitely generated modules over differential difference algebras in Section 5. Finally we investigate the Gelfand-Kirillov dimension of finitely generated modules over differential difference algebras in Section 6.

3.2 Preliminaries

Throughout this chapter, we assume that k is a field with characteristic 0 and all algebras are unital associative k-algebras. A mapping δ on a k-algebra A is called a *k-derivation* (or only *derivation* for short) on A provided that, for any $a, b \in A$ and $c \in k$, $\delta(ca+b) = c\delta(a)+\delta(b)$ and $\delta(ab) = a\delta(b)+\delta(a)b$. If $R \subseteq A$ is a subalgebra and $a_1, \ldots, a_p \in A$, where p is a positive integer, then $R\langle a_1, \ldots, a_p\rangle$ denotes the subalgebra of A generated by R and $\{a_1, \ldots, a_p\}$.

First we recall the definition of differential difference algebras.

Definition 3.2.1 *(cf., [18]) An algebra A is called* a differential difference algebra *of type (m, n), $m, n \in \mathbb{N}$, over a subalgebra $R \subseteq A$ if there exist elements $S_1, \ldots, S_m, D_1, \ldots, D_n$ in A such that*

(i) the set $\{S_1^{\alpha_1} \cdots S_m^{\alpha_m} D_1^{\beta_1} \cdots D_n^{\beta_n} : \alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \in \mathbb{N}\}$ forms a basis for A as a free left R-module.

(ii) $D_i r = rD_i + \delta_i(r)$ for any $1 \leq i \leq n$ and $r \in R$, where δ_i is a derivation on R.

(iii) $S_i r = \sigma_i^{-1}(r)S_i$, or equivalently $rS_i = S_i\sigma_i(r)$, for any $1 \leq i \leq m$ and $r \in R$, where σ_i is a k-algebra automorphism on the subalgebra $R\langle D_1, \ldots, D_n\rangle \subseteq A$ such that the restriction $\sigma_i|_R$ is a k-algebra automorphism on R and $\sigma_i(D_j) = \sum_{l=1}^{n} a_{ijl}D_l, \quad a_{ijl} \in R$.

(iv) $D_iS_j = S_j\sigma_j(D_i)$, $1 \leq i \leq n, 1 \leq j \leq m$.

(v) $S_iS_j = S_jS_i$, $1 \leq i, j \leq m$; $D_{i'}D_{j'} = D_{j'}D_{i'}$, $1 \leq i', j' \leq n$.

(vi) For any $1 \leq i, j \leq n$ and $1 \leq i', j' \leq m$, the composition $\delta_i \circ \delta_j = \delta_j \circ \delta_i$, $\delta_i \circ \sigma_{i'} = \sigma_{i'} \circ \delta_i$ and $\sigma_{i'} \circ \sigma_{j'} = \sigma_{j'} \circ \sigma_{i'}$.

Let $\mathcal{D} = \{D_1, \ldots, D_n\}$ and $\mathcal{S} = \{S_1, \ldots, S_m\}$. If A is a differential difference algebra over R as defined above, we denote $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$. Denote $\mathcal{S}^\alpha \mathcal{D}^\beta = S_1^{\alpha_1} \cdots S_m^{\alpha_m} D_1^{\beta_1} \cdots D_n^{\beta_n}$ for $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$.

Remark 3.2.2 Differential difference algebras can be also defined as iterated Ore extensions:

$$R[D_1; \delta_1] \cdots [D_n; \delta_n][S_1; \sigma_1] \cdots [S_m; \sigma_m]$$

with careful choices of σ and δ to get conditions (v) and (vi) in the above definition. In the language of iterated Ore extensions, it is natural to take the set $\{\mathcal{D}^\beta \mathcal{S}^\alpha : \alpha \in \mathbb{N}^m, \beta \in \mathbb{N}^n\}$ as a standard R-basis of A. However, in Definition 3.2.1, we take $\{\mathcal{S}^\alpha \mathcal{D}^\beta : \alpha \in \mathbb{N}^m, \beta \in \mathbb{N}^n\}$ rather than $\{\mathcal{D}^\beta \mathcal{S}^\alpha : \alpha \in \mathbb{N}^m, \beta \in \mathbb{N}^n\}$ as a standard R-basis of A since the former has more advantages related to computational properties of A. For example, the usual degree-lexicographical ordering (Example 3.3.2) works well as a left admissible ordering (which is essential to develop Gröbner-Shirshov basis theory of A) with $\mathcal{S}^\alpha \mathcal{D}^\beta$, but not with $\mathcal{D}^\beta \mathcal{S}^\alpha$.

Several well-known classes of skew polynomial algebras are contained in the class of differential difference algebras. On the other hand, an arbitrary differential difference algebra does not necessarily belong to well-known classes of noncommutative algebras such as algebras of solvable type [13], nor PBW extensions [3] or G-algebras [16], see Example 3.3.4 and Remark 3.3.5.

Example 3.2.3 (i) An Ore extension (also known as a skew polynomial ring, see Section 1.2 of [19]) $R[x; \sigma]$ of automorphism type over an algebra R is a differential difference algebra over R of type $(1, 0)$, while any Ore extension $R[x; \delta]$ of derivation type is a differential difference algebra of type $(0, 1)$.

(ii) Let $0 \neq q \in k$ and I_q be the two-sided ideal of the free associative algebra $k\langle x, y\rangle$ generated by the element $yx - qxy$. Then the quotient algebra $k_q[x, y] =$

$k\langle x,y\rangle/I_q$ is called a *quantum plane* ([14], Chapter IV). It is clear that $k_q[x,y]$ is a differential difference algebra over k of type $(1,1)$.

Next we fix our notation. For $\alpha = (\alpha_1,\ldots,\alpha_m) \in \mathbb{N}^m$, $\beta = (\beta_1,\ldots,\beta_n) \in \mathbb{N}^n$ and $c \in R$, denote $\sigma^\alpha(c) = \sigma_1^{\alpha_1}\cdots\sigma_m^{\alpha_m}(c)$, $|\alpha| = \alpha_1 + \cdots + \alpha_m$. As usual, $D_i^0 = S_j^0 = 1$, the identity of R. An element in $\mathcal{M} = \{\mathcal{S}^\alpha\mathcal{D}^\beta : \alpha \in \mathbb{N}^m, \beta \in \mathbb{N}^n\}$ is called a *standard monomial*. Moreover, set $\mathcal{M}_S = \{\mathcal{S}^\alpha : \alpha \in \mathbb{N}^m\}$ and $\mathcal{M}_{\mathcal{D}} = \{\mathcal{D}^\beta : \beta \in \mathbb{N}^n\}$. Let $u = \mathcal{S}^\alpha\mathcal{D}^\beta \in \mathcal{M}$. Then the *total degree* of u is defined as $\mathrm{tdeg}(u) = |\alpha| + |\beta|$, and the *total degree of u with respect to S_i* (D_j, respectively) is defined as $\mathrm{tdeg}_{S_i}(u) = \alpha_i$ ($\mathrm{tdeg}_{D_j}(u) = \beta_j$, respectively). For $i \in \mathbb{N}$, let $\mathcal{M}_i = \{u \in \mathcal{M} : \mathrm{tdeg}(u) = i\}$ and $\mathcal{M}_{\leq i} = \{u \in \mathcal{M} : \mathrm{tdeg}(u) \leq i\}$.

Define the *support* of $(0 \neq) f \in A$ as $\mathrm{Supp}(f) = \{u_i \in \mathcal{M} : f = \sum c_i u_i, 0 \neq c_i \in R\}$ and define the *(total) degree* of f as $\mathrm{tdeg}(f) = \max\{\mathrm{tdeg}(u) : u \in \mathrm{Supp}(f)\}$. Note that if $0 \neq c \in R$ then $\mathrm{Supp}(c) = \{\mathcal{S}^{\mathbf{0}}\mathcal{D}^{\mathbf{0}}\} = \{1\}$ and $\mathrm{tdeg}(c) = 0$. The degree of 0 is defined as $-\infty$.

With the above notation, we have the following lemmas.

Lemma 3.2.4 *Suppose $\alpha \in \mathbb{N}^m$, $\beta \in \mathbb{N}^n$, and $f, g \in A$. Then we have*

(i) $\mathrm{tdeg}(\sigma^\beta(\mathcal{D}^\alpha)) = \mathrm{tdeg}(\mathcal{D}^\alpha)$.

(ii) $\mathrm{tdeg}(fg) = \mathrm{tdeg}(f) + \mathrm{tdeg}(g)$.

Proof. One can prove the first statement via the following two steps: $\mathrm{tdeg}(\sigma_i(\mathcal{D}^\alpha)) = \mathrm{tdeg}(\mathcal{D}^\alpha)$ $(1 \leq i \leq m)$ by induction on $|\alpha|$, and $\mathrm{tdeg}(\sigma^\beta(\mathcal{D}^\alpha)) = \mathrm{tdeg}(\mathcal{D}^\alpha)$ by induction on $|\beta|$. The second statement follows from the first one. ■

Lemma 3.2.5 *Suppose $\alpha \in \mathbb{N}^m$ and $\beta = (\beta_1,\ldots,\beta_n) \in \mathbb{N}^n$. Then*

(i) $\mathcal{D}^\beta\mathcal{S}^\alpha = \mathcal{S}^\alpha\sigma^\alpha(\mathcal{D}^\beta) = \mathcal{S}^\alpha[\sigma_1^{\alpha_1}\sigma_2^{\alpha_2}\cdots\sigma_m^{\alpha_m}(\mathcal{D}^\beta)]$. *More generally,* $f\mathcal{S}^\alpha = \mathcal{S}^\alpha\sigma^\alpha(f)$ *for any $f \in R\langle\mathcal{D}\rangle$.*

(ii) $\mathcal{S}^\alpha \mathcal{D}^\beta = \sigma^{-\alpha}(\mathcal{D}^\beta)\mathcal{S}^\alpha = [\sigma_1^{-\alpha_1}\sigma_2^{-\alpha_2}\cdots\sigma_m^{-\alpha_m}(\mathcal{D}^\beta)]\mathcal{S}^\alpha$*, where* $\sigma_i^{-\alpha_i} = (\sigma_i^{-1})^{\alpha_i}$ *for* $1 \le i \le m$*. More generally,* $\mathcal{S}^\alpha f = \sigma^{-\alpha}(f)\mathcal{S}^\alpha$ *for any* $f \in R\langle\mathcal{D}\rangle$*.*

Proof. It follows from the definition of differential difference algebras by induction. ■

For $\alpha, \beta \in \mathbb{N}^n$, we say $\alpha \le \beta$ if $\alpha_i \le \beta_i$ for $1 \le i \le n$. Define $\alpha + \beta = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$ and $\alpha - \beta = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$.

Lemma 3.2.6 *For any* $r \in R$*,* $1 \le i \le n$ *and* $\alpha = (\alpha_1, \ldots, \alpha_i) \in \mathbb{N}^i$*,*

$$\mathcal{D}^\alpha r = \sum_{\beta \le \alpha} \prod_{t=1}^{i} \binom{\alpha_t}{\beta_t} \delta^{\alpha-\beta}(r)\mathcal{D}^\beta$$

where $\beta = (\beta_1, \ldots, \beta_i) \in \mathbb{N}^i$*.*

Proof. It can be proved by induction on $|\alpha|$. ■

The following theorem will be used later.

Theorem 3.2.7 (Hilbert Basis Theorem) *If* R *is Noetherian, then so is the differential difference algebra* $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$*.*

Proof. From the point of view of iterated Ore extensions, this theorem is trivial. One can also give a direct proof by using the following fact (cf., [19], Theorem 1.2.10, and [20], Proposition 3.5.2): Let R be a Noetherian ring, and S be an over-ring generated by R and an element a such that $Ra + R = aR + R$. Then S is Noetherian. ■

Let us conclude this section by recalling a well-known fact from combinatorics. For any $q \in \mathbb{N}$ and $t \in \mathbb{R}$, denote

$$\binom{t}{q} = \frac{t(t-1)\cdots(t-q+1)}{q!}.$$

Then, we have the following well-known fact, which will be used latter.

Lemma 3.2.8 *Let $q \in \mathbb{N}$. Then $h(x) = \binom{x+q}{q}$ is a polynomial in x of degree q, with rational coefficients and positive leading coefficient.*

3.3 Gröbner-Shirshov Bases of Differential Difference Algebras

Throughout this section, let R be a finite field extension of k and $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra of type (m, n), $m, n \in \mathbb{N}$. In this section we develop the Gröbner-Shirshov basis theory of A and we also show that every left ideal of A has a finite left Gröbner-Shirshov basis.

First we introduce some notation. For $f \in A$ and a given well-ordering on $\mathcal{M}$, as in [11], we use $\mathrm{lt}(f), \mathrm{lc}(f)$ and $\mathrm{lm}(f)$ to denote the *leading term*, *leading coefficient* and *leading monomial* of f, respectively. Then we have that $\mathrm{lt}(f) = \mathrm{lc}(f) \cdot \mathrm{lm}(f)$ for any $f \in A$. Denote $\mathrm{lm}(G) = \{\mathrm{lm}(g) : g \in G\}$ for any $G \subseteq A$.

Appropriate orderings on $\mathcal{M}$ are essential to Gröbner-Shirshov basis theory. Mansfield and Szanto [18] developed Gröbner-Shirshov basis theory for A (with $R = k$) by using the so-called differential difference ordering defined as follows: Let $>_{\mathcal{S}}$ be a monomial ordering on $\mathcal{M}_S$ and $>_{\mathcal{D}}$ a total degree monomial ordering on $\mathcal{M}_{\mathcal{D}}$. Then the ordering $>$ on the standard monomials $\mathcal{M}$ defined as follows is called a *differential difference ordering*:

$$\mathcal{S}^{\alpha}\mathcal{D}^{\beta} > \mathcal{S}^{\alpha'}\mathcal{D}^{\beta'} \Leftrightarrow \mathcal{S}^{\alpha} >_{\mathcal{S}} \mathcal{S}^{\alpha'} \text{ or } \alpha = \alpha' \text{ and } \mathcal{D}^{\beta} >_{\mathcal{D}} \mathcal{D}^{\beta'}.$$

A differential difference ordering works well for Gröbner-Shirshov bases since it has the following property: If $>$ is a differential difference ordering, then $u > v$ for any $u \in \mathcal{M}_S$ and $v \in \mathcal{M}_{\mathcal{D}}$. Now we define a more general class of orderings, which does not necessarily have the above property but still works well for Gröbner-Shirshov bases.

Definition 3.3.1 *A differential difference monomial ordering, DD-monomial ordering for short, on $\mathcal{M}$ is a well-ordering $>$ on $\mathcal{M}$ such that*

$$\text{if } \mathcal{S}^\alpha\mathcal{D}^\beta > \mathcal{S}^{\alpha'}\mathcal{D}^{\beta'} \text{ and } 0 \neq f \in A, \text{ then } \mathrm{lm}(f\mathcal{S}^\alpha\mathcal{D}^\beta) > \mathrm{lm}(f\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}).$$

In other words, a DD-monomial ordering is a *left admissible* well-ordering on $\mathcal{M}$. An ordering $>$ on $\mathcal{M}$ (or on $\mathcal{M}_\mathcal{S}$, $\mathcal{M}_\mathcal{D}$) is called a *monomial ordering* (or *admissible ordering*) if it is both left and right admissible; it is called a *total degree ordering* if $u > v$ whenever $\mathrm{tdeg}\, u > \mathrm{tdeg}\, v$, $u, v \in \mathcal{M}$.

Note that, by Proposition 4.1 of [18], any differential difference ordering is a DD-monomial ordering. The following example shows that the class of DD-monomial orderings properly includes the class of differential difference orderings.

Example 3.3.2 *Suppose $\mathcal{M}_S$ and $\mathcal{M}_\mathcal{D}$ are well-ordered by monomial orderings $>_\mathcal{S}$ and $>_\mathcal{D}$ respectively. Define an ordering $>$ on $\mathcal{M}$ as follows:*

$$\begin{aligned}\mathcal{S}^\alpha\mathcal{D}^\beta > \mathcal{S}^{\alpha'}\mathcal{D}^{\beta'} \iff \quad & \mathrm{tdeg}(\mathcal{S}^\alpha\mathcal{D}^\beta) > \mathrm{tdeg}(\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}) \\ \textit{or} \quad & \mathrm{tdeg}(\mathcal{S}^\alpha\mathcal{D}^\beta) = \mathrm{tdeg}(\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}) \textit{ and } \mathcal{S}^\alpha >_\mathcal{S} \mathcal{S}^{\alpha'} \\ \textit{or} \quad & \mathrm{tdeg}(\mathcal{S}^\alpha\mathcal{D}^\beta) = \mathrm{tdeg}(\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}), \alpha = \alpha' \textit{ and } \mathcal{D}^\beta >_\mathcal{D} \mathcal{D}^{\beta'}.\end{aligned}$$

Then $>$ is a total degree DD-monomial ordering.

Proof. It is clear from the definition that $>$ is a total degree ordering. Suppose $\mathcal{S}^\alpha\mathcal{D}^\beta > \mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}$ and $0 \neq f \in A$. We want to prove that $\mathrm{lm}(f\mathcal{S}^\alpha\mathcal{D}^\beta) > \mathrm{lm}(f\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'})$. Since $>$ is a total degree ordering, we may suppose that f is homogeneous, i.e., $\mathrm{tdeg}\, f = \mathrm{tdeg}\, u$ for any $u \in \mathrm{Supp}(f)$. Rewrite f as

$$f = \mathcal{S}^{\gamma_1} f_1 + \cdots + \mathcal{S}^{\gamma_l} f_l, \;\; \gamma_i \in \mathbb{N}^m, \; 0 \neq f_i \in R\langle\mathcal{D}\rangle, 1 \leq i \leq l, \; l \in \mathbb{N}, \mathcal{S}^{\gamma_1} >_\mathcal{S} \cdots >_\mathcal{S} \mathcal{S}^{\gamma_l}.$$

There are three cases.

Case 1: $\mathrm{tdeg}(\mathcal{S}^{\alpha}\mathcal{D}^{\beta}) > \mathrm{tdeg}(\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'})$. Then, by Lemma 3.2.4,

$$\begin{aligned}\mathrm{tdeg}(\mathrm{lm}(f\mathcal{S}^{\alpha}\mathcal{D}^{\beta})) &= \mathrm{tdeg}(f) + \mathrm{tdeg}(\mathcal{S}^{\alpha}\mathcal{D}^{\beta}) \\ &> \mathrm{tdeg}(f) + \mathrm{tdeg}(\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}) \\ &= \mathrm{tdeg}(\mathrm{lm}(f\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}))\end{aligned}$$

and thus $\mathrm{lm}(f\mathcal{S}^{\alpha}\mathcal{D}^{\beta}) > \mathrm{lm}(f\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'})$.

Case 2: $\mathrm{tdeg}(\mathcal{S}^{\alpha}\mathcal{D}^{\beta}) = \mathrm{tdeg}(\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'})$ and $\mathcal{S}^{\alpha} >_{\mathcal{S}} \mathcal{S}^{\alpha'}$. By Lemma 3.2.5,

$$\begin{aligned} f\mathcal{S}^{\alpha}\mathcal{D}^{\beta} &= \mathcal{S}^{\alpha+\gamma_1}\sigma^{\alpha}(f_1)\mathcal{D}^{\beta} + \cdots + \mathcal{S}^{\alpha+\gamma_l}\sigma^{\alpha}(f_l)\mathcal{D}^{\beta}, \qquad (3.1)\\ f\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'} &= \mathcal{S}^{\alpha'+\gamma_1}\sigma^{\alpha'}(f_1)\mathcal{D}^{\beta'} + \cdots + \mathcal{S}^{\alpha'+\gamma_l}\sigma^{\alpha'}(f_l)\mathcal{D}^{\beta'}.\end{aligned}$$

Each $\mathcal{S}^{\alpha+\gamma_i}\sigma^{\alpha}(f_i)\mathcal{D}^{\beta} \neq 0$ and $\mathcal{S}^{\alpha'+\gamma_i}\sigma^{\alpha'}(f_i)\mathcal{D}^{\beta'} \neq 0$ $(1 \leq i \leq l)$, since A has no zerodivisors. Note that f is homogeneous by our assumption, hence, by Lemma 3.2.4, we have that

$$\mathrm{tdeg}(\mathcal{S}^{\alpha+\gamma_1}\sigma^{\alpha}(f_1)\mathcal{D}^{\beta}) = \cdots = \mathrm{tdeg}(\mathcal{S}^{\alpha+\gamma_l}\sigma^{\alpha}(f_l)\mathcal{D}^{\beta}).$$

But $\mathcal{S}^{\gamma_1} >_{\mathcal{S}} \cdots >_{\mathcal{S}} \mathcal{S}^{\gamma_l}$ and $>_{\mathcal{S}}$ is a monomial ordering, which implies that $\mathrm{lm}(f\mathcal{S}^{\alpha}\mathcal{D}^{\beta}) = \mathrm{lm}(\mathcal{S}^{\alpha+\gamma_1}\sigma^{\alpha}(f_1)\mathcal{D}^{\beta})$. Similarly, $\mathrm{lm}(f\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}) = \mathrm{lm}(\mathcal{S}^{\alpha'+\gamma_1}\sigma^{\alpha'}(f_1)\mathcal{D}^{\beta'})$. Since

$$\mathrm{tdeg}(\mathcal{S}^{\alpha+\gamma_1}\sigma^{\alpha}(f_1)\mathcal{D}^{\beta}) = \mathrm{tdeg}(\mathcal{S}^{\alpha'+\gamma_1}\sigma^{\alpha'}(f_1)\mathcal{D}^{\beta'}) \text{ and } \mathcal{S}^{\alpha+\gamma_1} >_{\mathcal{S}} \mathcal{S}^{\alpha'+\gamma_1},$$

we have that

$$\mathrm{lm}(f\mathcal{S}^{\alpha}\mathcal{D}^{\beta}) = \mathrm{lm}(\mathcal{S}^{\alpha+\gamma_1}\sigma^{\alpha}(f_1)\mathcal{D}^{\beta}) > \mathrm{lm}(\mathcal{S}^{\alpha'+\gamma_1}\sigma^{\alpha'}(f_1)\mathcal{D}^{\beta'}) = \mathrm{lm}(f\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}).$$

Case 3: $\mathrm{tdeg}(\mathcal{S}^{\alpha}\mathcal{D}^{\beta}) = \mathrm{tdeg}(\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}), \alpha = \alpha'$ and $\mathcal{D}^{\beta} >_{\mathcal{D}} \mathcal{D}^{\beta'}$. Then, by Lemma 3.2.5,

$$f\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'} = f\mathcal{S}^{\alpha}\mathcal{D}^{\beta'} = \mathcal{S}^{\alpha+\gamma_1}\sigma^{\alpha}(f_1)\mathcal{D}^{\beta'} + \cdots + \mathcal{S}^{\alpha+\gamma_l}\sigma^{\alpha}(f_l)\mathcal{D}^{\beta'}. \quad (3.2)$$

From (3.1) and (3.2),

$$\mathrm{lm}(f\mathcal{S}^{\alpha}\mathcal{D}^{\beta}) = \mathrm{lm}(\mathcal{S}^{\alpha+\gamma_1}\sigma^{\alpha}(f_1)\mathcal{D}^{\beta}), \;\; \mathrm{lm}(f\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}) = \mathrm{lm}(\mathcal{S}^{\alpha+\gamma_1}\sigma^{\alpha}(f_1)\mathcal{D}^{\beta'}).$$

Since $>_{\mathcal{D}}$ is a monomial ordering on $\mathcal{M}_D$, $\mathcal{D}^{\beta} >_{\mathcal{D}} \mathcal{D}^{\beta'}$ and $\sigma^{\alpha}(f_1) \in R\langle\mathcal{D}\rangle$, we have that $\mathrm{lm}(\sigma^{\alpha}(f_1)\mathcal{D}^{\beta}) >_{\mathcal{D}} \mathrm{lm}(\sigma^{\alpha}(f_1)\mathcal{D}^{\beta'})$. Hence

$$\mathrm{lm}(f\mathcal{S}^{\alpha}\mathcal{D}^{\beta}) = \mathrm{lm}(\mathcal{S}^{\alpha+\gamma_1}\sigma^{\alpha}(f_1)\mathcal{D}^{\beta}) > \mathrm{lm}(\mathcal{S}^{\alpha+\gamma_1}\sigma^{\alpha}(f_1)\mathcal{D}^{\beta'}) = \mathrm{lm}(f\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}).$$

Therefore, $>$ is a DD-monomial ordering. ■

Remark 3.3.3 Let $>$ be as in Example 3.3.2.

(i) The ordering $>$ is not necessarily an extension of $>_{\mathcal{S}}$ or $>_{\mathcal{D}}$. For example, let $>_{\mathcal{S}}$ be a lexicographical orderings on $\mathcal{M}_S$ with $S_1 >_{\mathcal{S}} S_2$. Then $S_1 >_{\mathcal{S}} S_2^2$ but $S_1 < S_2^2$.

(ii) The ordering $>$ is not a differential difference ordering, because under $>$ a monomial in $\mathcal{M}_S$ is not necessarily greater than a monomial in $\mathcal{M}_{\mathcal{D}}$, for example, $S_1 < D_1^2$.

(iii) The ordering $>$ is not right admissible in general, see the following example.

Example 3.3.4 Let $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra of type $(1, 2)$ with $\sigma_1(D_1) = D_2$ and $\sigma_1(D_2) = D_1$. Let $>$ be a DD-monomial ordering as in

Example 3.3.2 with $D_2 >_{\mathcal{D}} D_1$. But then

$$\mathrm{lm}(D_2S_1) = \mathrm{lm}(S_1D_1) = S_1D_1 < S_1D_2 = \mathrm{lm}(S_1D_2) = \mathrm{lm}(D_1S_1).$$

Thus $>$ is not right admissible.

Remark 3.3.5 The above example (where $D_2S_1 = S_1D_1$) also shows that a differential difference algebra is not necessarily an algebra of solvable type [13] (or a PBW extension [3], or a G-algebra [16]).

Let $f, g \in A$. If there exists $h \in A$ such that $f = hg$, we say that f is *right divisible* by g, and g (h, respectively) is called a *right factor* or *right quotient* (*left factor* or *left quotient*, respectively) of f. Denote the left quotient $h = \mathrm{LQ}(f, g)$. With the above definitions and notation, we have the following lemma.

Lemma 3.3.6 *Suppose $f, g, h \in A$.*

(i) If g is a right factor of f then $\mathrm{LQ}(f, g) = \mathrm{LQ}(fh, gh)$, but $\mathrm{LQ}(f, g) \neq \mathrm{LQ}(hf, hg)$ in general.

(ii) If hg is a right factor of f then $\mathrm{LQ}(f, hg) \cdot h = \mathrm{LQ}(f, g)$ and $h \cdot \mathrm{LQ}(f, hg) = \mathrm{LQ}(hf, hg)$, but $h \cdot \mathrm{LQ}(f, hg) \neq \mathrm{LQ}(f, g)$ in general.

(iii) If g is a right factor of f and h is a right factor of g, then $\mathrm{LQ}(f, g) \cdot \mathrm{LQ}(g, h) = \mathrm{LQ}(f, h)$.

Proof. It is obvious by definition. ■

Lemma 3.3.7 *$\mathcal{S}^{\alpha}\mathcal{D}^{\beta}$ is right divisible by $\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}$ if and only if*

$$\alpha = \alpha' + \gamma \text{ and } \beta = \beta' + \gamma' \text{ for some } \gamma \in \mathbb{N}^m \text{ and } \gamma' \in \mathbb{N}^n.$$

Proof. The ($\Rightarrow$) part is clear.

($\Leftarrow$). Suppose $\alpha = \alpha' + \gamma$ and $\beta = \beta' + \gamma'$ for some $\gamma \in \mathbb{N}^m$ and $\gamma' \in \mathbb{N}^n$. Then, by Lemma 3.2.5,

$$\mathcal{S}^{\alpha}\mathcal{D}^{\beta} = \mathcal{S}^{\alpha'+\gamma}D^{\beta'+\gamma'} = \mathcal{S}^{\gamma}\sigma^{-\alpha'}(D^{\gamma'}) \cdot \mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}.$$

Hence, $\mathcal{S}^{\alpha}\mathcal{D}^{\beta}$ is right divisible by $\mathcal{S}^{\alpha'}\mathcal{D}^{\beta'}$. ■

However, the "only if" part of the above lemma is not true for the left division. In fact, in Example 3.3.4, $S_1D_2 = D_1S_1$ and thus S_1D_2 is left divisible by D_1, but the exponents of the two monomials do not satisfy the relation stated in Lemma 3.3.7.

From now on to the end of this section, we fix a DD-monomial ordering $>$ on $\mathcal{M}$. Then we have the following lemma, which is similar to Corollary 4.3 of [18].

Lemma 3.3.8 *For any $f, g \in A$, we have*

(i) $\mathrm{lm}(fg) = \mathrm{lm}(f \cdot \mathrm{lm}(g)) = h \cdot \mathrm{lm}(g)$, *for some $h \in A$.*

(ii) $\mathrm{lt}(fg) = \mathrm{lt}(f \cdot \mathrm{lt}(g)) = h' \cdot \mathrm{lt}(g)$, *for some $h' \in A$.*

Furthermore, h and h' in the above are uniquely determined by f and g.

Definition 3.3.9 *Let I be a left ideal of A. A set $G \subseteq I$ is called a* left Gröbner-Shirshov basis *of I with respect to $>$ if, for any $0 \neq f \in I$, there exists $g \in G$ such that* $\mathrm{lm}(f)$ *is right divisible by* $\mathrm{lm}(g)$.

Note that we do not require a Gröbner-Shirshov basis to be finite.

Let $G \subseteq A$. Define the set of words that are irreducible with respect to G as

$$\mathrm{Irr}(G) = \{w \in \mathcal{M} : w \neq f\,\mathrm{lm}(g) \text{ for any } g \in G, f \in A\}.$$

By Lemma 3.3.8, it is easy to see that

$$\begin{aligned}\mathrm{Irr}(G) &= \{w \in \mathcal{M} : w \neq \mathrm{lm}(f\,\mathrm{lm}(g)) \text{ for any } g \in G, f \in A\} \\ &= \{w \in \mathcal{M} : w \neq \mathrm{lm}(u\,\mathrm{lm}(g)) \text{ for any } g \in G, u \in \mathcal{M}\}.\end{aligned}$$

Let $f, h, g \in A$ and $G \subseteq A$. Then f *reduces to* h *modulo* g, denoted by $f \to_g h$, if $h = f - qg$ and $\mathrm{lt}(f) = \mathrm{lt}(qg)$ for some $q \in A$. We say that f *reduces to* h *modulo* G, denoted by $f \to_G h$, if there exists a finite chain of reductions

$$f \to_{g_1} f_1 \to_{g_2} f_2 \to_{g_3} \cdots \to_{g_t} f_t = h,$$

where each $g_i \in G$ and $t \in \mathbb{N}$. Furthermore, if $\mathrm{Supp}(h) \subseteq \mathrm{Irr}(G)$, then h is *irreducible* with respect to G, and we call h a *remainder* of f modulo G.

With these definitions, we have the following lemma.

Lemma 3.3.10 *Let $G \subseteq A$ be a finite set and $f \in A$. Then,*

(i) $f = \sum c_i u_i g_i + r$, where each $c_i \in R, u_i \in \mathcal{M}, g_i \in G$, $\mathrm{lm}(u_i g_i) \leq \mathrm{lm}(f)$ and r is a remainder of f modulo G.

(ii) furthermore, if G is a left Gröbner-Shirshov basis for a left ideal of A, then the remainder of f modulo G is unique (denoted by $\mathrm{Rem}(f, G)$).

Proof. (i) It can be proved by induction on $\mathrm{lm}(f)$.

(ii) Suppose that both r and r' are reminders of f modulo G and that $r \neq r'$. Then $0 \neq r - r' = (f - r') - (f - r) \in I$. Hence $\mathrm{lm}(r - r') \notin \mathrm{Irr}(G)$ by the definition of Gröbner-Shirshov bases. But $\mathrm{lm}(r - r') \in \mathrm{Supp}(r) \cup \mathrm{Supp}(r') \subseteq \mathrm{Irr}(G)$, which is a contradiction. ■

Note that, in general, a remainder of $f \in A$ modulo some subset $G' \subseteq A$ is not unique.

Lemma 3.3.11 Let $f \in A$ and $G \subseteq A$. Then f can be written as

$$f = \sum_{i=1}^{s} a_i u_i + \sum_{j=1}^{t} b_j v_j g_j,$$

where $s, t \in \mathbb{N}$, each $a_i, b_j \in R, u_i \in \mathrm{Irr}(G), v_j \in \mathcal{M}, g_i \in G$ and

$$\mathrm{lm}(f) \geq \mathrm{lm}(u_1) > \cdots > \mathrm{lm}(u_s), \quad \mathrm{lm}(f) \geq \mathrm{lm}(v_1 g_1) > \cdots > \mathrm{lm}(v_t g_t),$$

where exactly one of the monomials $\mathrm{lm}(u_i)$ and $\mathrm{lm}(v_j g_j)$ is equal to $\mathrm{lm}(f)$.

Proof. (By induction on $\mathrm{lm}(f)$.) If $\mathrm{lm}(f) = 1$, then $f \in R$ and the statement holds clearly. Suppose that the statement holds for any polynomial with leading monomial less than $\mathrm{lm}(f)$. We need to show that it also holds for f. Define f_1 as follows. If $\mathrm{lm}(f) \in \mathrm{Irr}(G)$, then set $f_1 = f - \mathrm{lc}(f)\,\mathrm{lm}(f)$. If $\mathrm{lm}(f) \notin \mathrm{Irr}(G)$, i.e., if there exist $g \in G$ and $v \in \mathcal{M}$ such that $\mathrm{lm}(f) = \mathrm{lm}(vg)$, then set $f_1 = f - bvg$ where $b = \mathrm{lc}(f)\,\mathrm{lc}(vg)^{-1} \in R$. Then $\mathrm{lm}(f_1) < \mathrm{lm}(f)$ in either case. Hence, by induction hypothesis, $f_1 = \sum_{1 \leq i \leq s_1} a_i u_i + \sum_{1 \leq j \leq t_1} b_j v_j g_j$ where $s_1, t_1 \in \mathbb{N}$, each $a_i, b_j \in R, g_i \in G, u_i \in \mathrm{Irr}(G), v_j \in \mathcal{M}$, $\mathrm{lm}(f_1) \geq \mathrm{lm}(u_1) > \cdots > \mathrm{lm}(u_{s_1})$ and $\mathrm{lm}(f_1) \geq \mathrm{lm}(v_1 g_1) > \cdots > \mathrm{lm}(v_t g_{t_1})$. Thus $f = f_1 + \mathrm{lc}(f)\,\mathrm{lm}(f)$ (or $f = f_1 + bvg$) has the desired presentation. ■

The following theorem solves the ideal membership problem of A.

Theorem 3.3.12 *Let $G \subseteq A$ be a left Gröbner-Shirshov basis for a left ideal I, and let $f \in A$. Then $f \in I$ if and only if* $\mathrm{Rem}(f, G) = 0$.

Proof. If $f \in I$ then, by Lemma 3.3.10, $\mathrm{Rem}(f, G) = 0$. On the other hand, if $\mathrm{Rem}(f, G) = 0$, then $f = f - \mathrm{Rem}(f, G) \in I$. ■

The following proposition indicates that the definition of Gröbner-Shirshov bases in this chapter is equivalent to Definition 4.5 of [18] if the ordering under consideration is a differential difference ordering.

Proposition 3.3.13 *Let I be a left ideal of A and $G \subseteq I$. Then*

(i) G is a Gröbner-Shirshov basis for I if and only if $\mathrm{lm}(G)$ and $\mathrm{lm}(I)$ generate the same left ideal of A.

(ii) If G is a left Gröbner-Shirshov basis for I, then G generates I as a left ideal of A.

Proof. (i) ($\Rightarrow$) It follows from the definition of Gröbner-Shirshov bases.

($\Leftarrow$) Let $0 \neq f \in I$. Since $\mathrm{lm}(G)$ and $\mathrm{lm}(I)$ generate the same left ideal of A, $\mathrm{lm}(f) = \sum a_i \,\mathrm{lm}(g_i)$ where $a_i \in A, g_i \in G$. Then $\mathrm{lm}(f) \in \mathrm{Supp}(a_i \,\mathrm{lm}(g_i))$ for some i. Hence $\mathrm{lm}(f)$ is right divisible by $\mathrm{lm}(g_i)$.

(ii) Suppose $f \in I$. By Lemma 3.3.10, we can write $f = \sum b_i g_i + r$ where $b_i \in A$, $g_i \in G$ and r is irreducible with respect to G. Thus $r = f - \sum b_i g_i \in I$. Suppose $r \neq 0$. Since G is a Gröbner-Shirshov basis for I, $\mathrm{lm}(r)$ is right divisible by $\mathrm{lm}(g_i)$ for some $g_i \in G$, contradicting our assumption that r is irreducible with respect to G. Hence $r = 0$ and thus $f = \sum b_i g_i$ is in the left ideal of A generated by G. Therefore, I is generated by G as a left ideal of A. ■

Let $\mathcal{S}^\alpha \mathcal{D}^\beta, \mathcal{S}^{\alpha'} \mathcal{D}^{\beta'} \in \mathcal{M}$. Then the *least common left multiple* of $\mathcal{S}^\alpha \mathcal{D}^\beta$ and $\mathcal{S}^{\alpha'} \mathcal{D}^{\beta'}$ is defined as

$$\mathrm{lclm}(\mathcal{S}^\alpha \mathcal{D}^\beta, \mathcal{S}^{\alpha'} \mathcal{D}^{\beta'}) = \mathcal{S}^\mu \mathcal{D}^\nu,$$

where $\mu = (\mu_1, \ldots, \mu_m) \in \mathbb{N}^m$, $\nu = (\nu_1, \ldots, \nu_n) \in \mathbb{N}^n$, each $\mu_i = \max\{\alpha_i, \alpha'_i\}$, $\nu_j = \max\{\beta_j, \beta'_j\}$. For the sake of convenience, for any $f, g \in A$, $\mathrm{lclm}(\mathrm{lm}(f), \mathrm{lm}(g))$ is sometimes denoted by $\mathrm{lclm}(f, g)$. Let $f, g \in A$. Then there exists a unique pair of polynomials $f', g' \in A$ such that

$$f' \,\mathrm{lt}(f) = \mathrm{lclm}(f, g) = g' \,\mathrm{lt}(g).$$

Then, the polynomial $f'f - g'g \in A$ is called the *S-polynomial* of f and g, denoted by $\mathrm{SPoly}(f,g)$, that is,

$$\begin{aligned} \mathrm{SPoly}(f,g) &= f'f - g'g \\ &= \mathrm{LQ}(\mathrm{lclm}(f,g), \mathrm{lt}(f))f - \mathrm{LQ}(\mathrm{lclm}(f,g), \mathrm{lt}(g))g. \end{aligned} \tag{3.3}$$

Note that $\mathrm{lc}(f' \, \mathrm{lt}(f)) = 1$.

Lemma 3.3.14 *Let $f, g \in A$. Then* $\mathrm{lm}(\mathrm{SPoly}(f,g)) < \mathrm{lclm}(f,g)$.

Proof. By Lemma 3.3.8, $\mathrm{lt}(f'f) = \mathrm{lt}(f' \, \mathrm{lt}(f)) = \mathrm{lt}(g' \, \mathrm{lt}(g)) = \mathrm{lt}(g'g)$. Hence $\mathrm{lm}(\mathrm{SPoly}(f,g)) = \mathrm{lm}(f'f - g'g) < \mathrm{lm}(f'f) = \mathrm{lclm}(f,g)$. ■

The following lemma can be proved by using a telescoping argument as in Lemma 5 of Chapter 2.6 in [11].

Lemma 3.3.15 *(cf. [18], Lemma 4.8, and [11], Lemma 5 of Chapter 2.6) Let $f = c_1 f_1 + \cdots + c_s f_s$ for $f_1, \ldots, f_s \in A$, $c_1, \ldots, c_s \in R$ and $s \in \mathbb{N}$. Suppose that for all $1 \le i \le s$, $\mathrm{lm}(f_i) = u$ for some $u \in \mathcal{M}$. If $\mathrm{lm}(f) < u$, then there exist $d_{ij} \in R$ $(1 \le i, j \le s)$ such that*

$$f = \sum_{i,j=1}^{s} d_{ij} \, \mathrm{SPoly}(f_i, f_j).$$

Theorem 3.3.16 *Let $G \subseteq A$ and I be the left ideal of A generated by G. Then G is a left Gröbner-Shirshov basis for I if and only if $\mathrm{SPoly}(g_1, g_2) \to_G 0$ for any $g_1, g_2 \in G$.*

Proof. ($\Rightarrow$) Suppose G is a Gröbner-Shirshov basis for I. Since $\mathrm{SPoly}(g_1, g_2) \in I$ for any $g_1, g_2 \in G$, by Theorem 3.3.12, $\mathrm{Rem}(\mathrm{SPoly}(g_1, g_2), G) = 0$, i.e., $\mathrm{SPoly}(g_1, g_2) \to_G 0$ as desired.

($\Leftarrow$) Suppose that $\mathrm{SPoly}(g_1, g_2) \to_G 0$ for any $g_1, g_2 \in G$. We want to prove that for any $0 \ne f \in I$, $\mathrm{lm}(f)$ is right divisible by $\mathrm{lm}(g)$ for some $g \in G$. Since $f \in I$, f

can be written as

$$f = \sum_{i=1}^{t} h_i g_i, \quad t \in \mathbb{N},\ h_i \in A,\ g_i \in G,\ \operatorname{lm}(h_1 g_1) \geq \operatorname{lm}(h_2 g_2) \geq \cdots \geq \operatorname{lm}(h_t g_t). \tag{3.4}$$

Let $u = \operatorname{lm}(h_1 g_1)$. Assume that among all possible expressions of f of the form (3.4) we chose one with minimal u. Suppose

$$\operatorname{lm}(h_1 g_1) = \operatorname{lm}(h_2 g_2) = \cdots = \operatorname{lm}(h_s g_s) > \operatorname{lm}(h_{s+1} g_{s+1}) \geq \cdots \geq \operatorname{lm}(h_t g_t), \quad s \in \mathbb{N}.$$

Note that $\operatorname{lm}(f) \leq u$. Now we prove that $\operatorname{lm}(f) = u$. By way of contradiction, we suppose that $\operatorname{lm}(f) < u$. By Lemma 3.3.8, $\operatorname{lt}(h_i g_i) = h'_i \operatorname{lt}(g_i)$ for some $h'_i \in A$, $1 \leq i \leq t$. Then $\operatorname{lt}(h_i g_i) = \operatorname{lt}(h'_i \operatorname{lt}(g_i)) = \operatorname{lt}(h'_i g_i)$ and thus $\operatorname{lm}((h_i - h'_i) g_i) < \operatorname{lm}(h_i g_i)$. Rewrite

$$f = \sum_{\operatorname{lm}(h_i g_i) = u} h'_i g_i + \sum_{\operatorname{lm}(h_i g_i) = u} (h_i - h'_i) g_i + \sum_{\operatorname{lm}(h_l g_l) < u} h_l g_l. \tag{3.5}$$

Then

$$\operatorname{lm}\left(\sum_{\operatorname{lm}(h_i g_i) = u} (h_i - h'_i) g_i + \sum_{\operatorname{lm}(h_l g_l) < u} h_l g_l \right) < u.$$

Hence $\operatorname{lm}\left(\sum_{\operatorname{lm}(h_i g_i) = u} h'_i g_i \right) < u$ since $\operatorname{lm}(f) < u$. By Lemma 3.3.15, there exist $d_{ij} \in k$ for $1 \leq i, j \leq s$ such that

$$\sum_{\operatorname{lm}(h_i g_i) = u} h'_i g_i = \sum_{i,j=1}^{s} d_{ij} \operatorname{SPoly}(h'_i g_i, h'_j g_j).$$

Since $\operatorname{lclm}(\operatorname{lm}(h'_i g_i), \operatorname{lm}(h'_j g_j)) = \operatorname{lclm}(u, u) = u$ for all $1 \leq i, j \leq s$, it follows from Equation (3.3) and Lemma 3.3.6 that

$$\operatorname{SPoly}(h'_i g_i, h'_j g_j) \quad = \quad \operatorname{LQ}(u, \operatorname{lt}(h'_i g_i)) h'_i g_i - \operatorname{LQ}(u, \operatorname{lt}(h'_j g_j)) h'_j g_j$$

$$
\begin{aligned}
&= \mathrm{LQ}(u, h_i' \operatorname{lt}(g_i))h_i' g_i - \mathrm{LQ}(u, h_j' \operatorname{lt}(g_j))h_j' g_j \\
&= \mathrm{LQ}(u, \operatorname{lt}(g_i))g_i - \mathrm{LQ}(u, \operatorname{lt}(g_j))g_j \\
&= \mathrm{LQ}(u, \operatorname{lclm}(g_i, g_j))\,\mathrm{LQ}(\operatorname{lclm}(g_i, g_j), \operatorname{lt}(g_i))g_i \\
&\quad - \mathrm{LQ}(u, \operatorname{lclm}(g_i, g_j))\,\mathrm{LQ}(\operatorname{lclm}(g_i, g_j), \operatorname{lt}(g_j))g_j \\
&= \mathrm{LQ}(u, \operatorname{lclm}(g_i, g_j))\,\mathrm{SPoly}(g_i, g_j).
\end{aligned}
$$

Hence

$$
\sum_{\operatorname{lm}(h_i g_i)=u} h_i' g_i = \sum_{i,j=1}^{s} d_{ij}\,\mathrm{LQ}(u, \operatorname{lclm}(g_i, g_j))\,\mathrm{SPoly}(g_i, g_j) \longrightarrow_G 0.
$$

Thus by Lemma 3.3.10 (i),

$$
\sum_{\operatorname{lm}(h_i g_i)=u} h_i' g_i = \sum_{j \in J} c_j u_j g_j, \quad \operatorname{lm}(u_j g_j) \le \operatorname{lm}\left(\sum_{\operatorname{lm}(h_i g_i)=u} h_i' g_i \right) < u,
$$

where $c_j \in k, u_j \in \mathcal{M}, g_j \in G$ and J is a finite index set. Now we can rewrite (3.5) as

$$
f = \sum_{j \in J} c_j u_j g_j + \sum_{\operatorname{lm}(h_i g_i)=u} (h_i - h_i')g_i + \sum_{\operatorname{lm}(h_l g_l)<u} h_l g_l, \tag{3.6}
$$

where $\operatorname{lm}(u_j g_j) < u$, $\operatorname{lm}((h_i - h_i')g_i) < u$ and $\operatorname{lm}(u_l g_l) < u$. That is, (3.6) is an expression of f of form (3.4) with all leading monomials of summands less than u, which contradicts the minimality of u. Therefore, we proved that $\operatorname{lm}(f) = u$.

Now, by Lemma 3.3.8, $\operatorname{lm}(f) = u = \operatorname{lm}(h_1 g_1) = h' \operatorname{lm}(g_1)$ for some $h' \in A$. That is, $\operatorname{lm}(f)$ is right divisible by $\operatorname{lm}(g_1)$. ■

Now we have the following algorithm.

Algorithm 3.3.17 (Left Gröbner-Shirshov Basis Algorithm)

Input: $F = \{f_1, \ldots, f_s\} \subset A$, $s \in \mathbb{N}$, each $f_i \neq 0$.

Output: a Gröbner-Shirshov basis $G = \{g_1, \ldots, g_t\}$ for I, $t \in \mathbb{N}$, with $F \subseteq G$.

Initialization: $G := F$, $P := \{\{p, q\} : p \neq q, p, q \in F\}$.

While $P \neq \emptyset$ **Do**

Choose any pair $\{p, q\} \in P$, $P := P \setminus \{\{p, q\}\}$

$r :=$ a remainder of $\mathrm{SPoly}(p, q)$ modulo G

If $r \neq 0$ **Then**

$G := G \cup \{r\}$, $P := P \cup \{\{g, r\} : g \in G\}$

End do

Theorem 3.3.18 *Let I be a left ideal of A generated by nonzero elements $f_1, \ldots, f_l \in A$. Then Algorithm 3.3.17 returns a finite Gröbner-Shirshov basis for I.*

Proof. We first prove that the algorithm terminates after finitely many steps. After each pass through the main loop (i.e., the while loop), if there is a nonzero remainder r, then G consists of the old G (denoted by G') together with the nonzero remainder r, i.e., $G = G' \cup \{r\}$. Since $r \in \mathrm{Irr}(G')$, it is easy to show that $\mathrm{lt}(G')A$, the left ideal of A generated by $\mathrm{lt}(G')$, is properly contained in $\mathrm{lt}(G)A$. By the Hilbert Basis Theorem 3.2.7, any ascending chain of left ideals of A will stabilize. Hence, after finitely many iterations of the main loop, there is no nonzero remainder any more. Hence P will be exhausted (i.e., $P = \emptyset$) after finitely many iterations of the main loop, and then the algorithm terminates and return G.

By Theorem 3.3.16, the return G is a Gröbner-Shirshov basis for I. ■

Theorem 3.3.19 *Let $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra, where R is a field extension of k. Then every left ideal of A has a finite left Gröbner-Shirshov basis.*

Proof. It follows by Theorem 3.3.18 and the Hilbert Basis Theorem 3.2.7. ■

The following theorem plays a key role in the Gelfand-Kirillov dimension computation in the next section.

Theorem 3.3.20 *Let $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra, where R is a field extension of k. Let $G \subseteq A$, and I be the left ideal of A generated by G. For $f \in A$, let $\overline{f} = f + I$, which belongs to the left A-modulo A/I. Then G is a left Gröbner-Shirshov basis for I if and only if the set $B = \{\overline{u} | u \in \mathrm{Irr}(G)\}$ is an R-basis of the left A-module A/I.*

Proof. ($\Rightarrow$) Suppose that G is a left Gröbner-Shirshov basis for I. For any $\overline{f} = f + I \in A/I$, by Lemma 3.3.11,

$$\overline{f} = \sum_{i=1}^{s} a_i u_i + \sum_{j=1}^{t} b_j v_j g_j + I = \sum_{i=1}^{s} a_i u_i + I = \sum_{i=1}^{s} a_i (u_i + I) = \sum_{i=1}^{s} a_i \overline{u_i},$$

where $s, t \in \mathbb{N}$, each $a_i, b_j \in R, u_i \in \mathrm{Irr}(G), v_j \in \mathcal{M}, g_i \in G$. Thus, B spans A/I as an R-space.

In order to prove that B is R-linearly independent, suppose that

$$a_1 \overline{u_1} + a_2 \overline{u_2} + \cdots + a_t \overline{u_t} = \overline{0},\ a_i \in R,\ u_i \in \mathrm{Irr}(G),\ i = 1, \ldots, t,\ \ t \in \mathbb{N},$$

and that $u_1 > u_2 > \cdots > u_t$. Let $f = a_1 u_1 + a_2 u_2 + \cdots + a_t u_t$. Then $\overline{f} = \overline{0}$ and thus $f \in I$. If $a_1 \neq 0$ then $\mathrm{lm}(f) = u_1 \in \mathrm{Irr}(G)$; but $\mathrm{lm}(f) \notin \mathrm{Irr}(G)$ since G is a left Gröbner-Shirshov basis for I. Hence $a_1 = 0$ and similarly $a_2 = a_3 = \cdots = a_t = 0$. Therefore B is R-linearly independent.

($\Leftarrow$) Suppose B is an R-basis of A/I and $0 \neq f \in I$. It suffices to prove that $\mathrm{lm}(f)$ is right divisible by $\mathrm{lm}(g)$ for some $g \in G$. By Lemma 3.3.11, we can write $f = \sum\limits_{i=1}^{s} a_i u_i + \sum\limits_{j=1}^{t} b_j v_j g_j$, where $s, t \in \mathbb{N}$, each $a_i, b_j \in R, u_i \in \mathrm{Irr}(G), v_j \in \mathcal{M}, g_i \in G$ and

$$\mathrm{lm}(f) \geq \mathrm{lm}(u_1) > \cdots > \mathrm{lm}(u_s),\ \ \mathrm{lm}(f) \geq \mathrm{lm}(v_1 g_1) > \cdots > \mathrm{lm}(v_t g_t).$$

Then $\overline{0} = \overline{f} = a_1 \overline{u_1} + \cdots + a_s \overline{u_s}$. Since B is an R-basis of A/I, $a_1 = \cdots = a_s = 0$. Hence $\mathrm{lm}(f) = \mathrm{lm}(v_1 g_1)$ and thus, by Lemma 3.3.8, $\mathrm{lm}(f)$ is right divisible by $\mathrm{lm}(g_1)$.

■

3.4 Gelfand-Kirillov Dimension of Cyclic A-modules

In this section, we compute the Gelfand-Kirillov dimension of cyclic modules over a differential difference algebra. We assume that the reader is familiar with the notions of gradings and filtrations of algebras and modules. We refer the reader to Chapter 6 of [15] for more details.

Let A be a graded k-algebra and let $M = \bigoplus_{i \in \mathbb{N}} M_i$ be a graded left A-module. Then the *Hilbert function* of M is defined as the mapping:

$$\mathrm{HF}_M : \mathbb{N} \to \mathbb{N},\ \mathrm{HF}_M(i) = \dim_k(M_0 \oplus \cdots \oplus M_i),\ i \in \mathbb{N}.$$

The following lemma relates the Gelfand-Kirillov dimension and the Hilbert function of a finitely generated module over a finitely generated algebra.

Lemma 3.4.1 *([15], Lemma 6.1) If A is a finitely generated k-algebra and M is a finitely generated left A-module, then* $\mathrm{GKdim}(M) = \overline{\lim_{i \to \infty}} \log_i \mathrm{HF}_M(i)$.

From now on to the end of this section, we fix the following notation. Let $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra of type (m, n), $m, n \in \mathbb{N}$, where R is a finite field extension of k (it is easy to see that if $\dim_k R = \infty$ then $\mathrm{GKdim}(M) = \infty$). Let $V = \{v_1, \ldots, v_d\}$ ($d \in \mathbb{N}$) be a k-basis of R and I be a proper left ideal of A.

Denote the left A-module A/I by M. Let A_i, $i \in \mathbb{N}$, be the R-subspace of A spanned by $\mathcal{M}_i = \{\mathcal{S}^\alpha \mathcal{D}^\beta : |\alpha| + |\beta| = i\}$. Then each A_i is spanned as a k-space by

$\{vu : v \in V, u \in \mathcal{M}_i\}$ and $\{A_i\}_{i\in\mathbb{N}}$ is a grading of A, i.e.,

$$A = \bigoplus_{i\in\mathbb{N}} A_i, \quad \text{and } A_i \cdot A_j \subseteq A_{i+j} \quad \text{for all } i, j \in \mathbb{N}.$$

It induces a grading of the left A-module $M = A/I = \bigoplus_{i\in\mathbb{N}} M_i$, where $M_i = (A_i+I)/I$ is a k-subspace of M. Recall that if $f \in A$ we denote the element $f + I$ of M by $\overline{f}$.

Proposition 3.4.2 *Let $G \subseteq A$ be a left Gröbner-Shirshov basis for I with respect to a total degree DD-monomial ordering. Then the following hold:*

(i) The set $B_i = \{\overline{vu} : v \in V,\ u \in \operatorname{Irr}(G) \cap \mathcal{M}_{\leq i}\}$ is a k-basis of $M_{\leq i} = M_0 \oplus \cdots \oplus M_i$, $i \in \mathbb{N}$.

(ii) The Hilbert function of M is given by

$$\mathrm{HF}_M(i) = d \cdot |\operatorname{Irr}(G) \cap \mathcal{M}_{\leq i}|, \ i \in \mathbb{N},$$

where $|\operatorname{Irr}(G) \cap \mathcal{M}_{\leq i}|$ denotes the cardinality of the set $\operatorname{Irr}(G) \cap \mathcal{M}_{\leq i}$.

Proof. (i) First we prove that $B'_i = \{\overline{u} : u \in \operatorname{Irr}(G) \cap \mathcal{M}_{\leq i}\}$ is an R-base of $M_{\leq i}$ as a left R-module. By Theorem 3.3.20, B'_i is linearly independent over R for any $i \in \mathbb{N}$. Thus it suffices to prove that B'_i spans $M_{\leq i}$ as a left R-module. Note that $M_{\leq i} = \{\overline{f} \in M : f \in A, \operatorname{tdeg} f \leq i\}$. For $f \in A$ with $\operatorname{tdeg} f \leq i$, by Lemma 3.3.11, $\overline{f} = \sum_{j=1}^{s} a_j \overline{u_j}$, where $s \in \mathbb{N}$, each $a_j \in R, u_j \in \operatorname{Irr}(G)$ and $\operatorname{lm}(f) \geq \operatorname{lm}(u_1) > \cdots > \operatorname{lm}(u_s)$. Since $>$ is a total degree DD-monomial ordering, for $1 \leq j \leq s$, $\operatorname{tdeg} u_j \leq \operatorname{tdeg} f \leq i$ and thus $\overline{u_j} \in B'_i$. Hence B'_i spans M_i.

Since V is a k-basis of R, we have that $B_i = \{\overline{vu} : v \in V,\ u \in \operatorname{Irr}(G) \cap \mathcal{M}_{\leq i}\}$ is a k-basis of $M_{\leq i}$.

(ii) By (i), it is sufficient to show that $|B'_i| = |\operatorname{Irr}(G) \cap \mathcal{M}_{\leq i}|$. It is clear that $|B'_i| \leq |\operatorname{Irr}(G) \cap \mathcal{M}_{\leq i}|$. For the other direction, for $u, v \in \operatorname{Irr}(G) \cap \mathcal{M}_{\leq i}$ with $\overline{u} = \overline{v}$, we want to prove that $u = v$. If $u \neq v$, without loss of generality, we suppose $u > v$.

Then $0 \neq f = u - v \in I$ and thus $u = \operatorname{lm} f \notin \operatorname{Irr}(G)$ since G is a Gröbner-Shirshov basis for I, a contradiction. Hence $u = v$. Thus $|B_i'| = |\operatorname{Irr}(G) \cap \mathcal{M}_{\leq i}|$. ■

For convenience, denote $x_i = S_i, x_{m+j} = D_j$ for $1 \leq i \leq m, 1 \leq j \leq n$ and let $l = m + n$. Denote $X^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_l^{\alpha_l}$ for $\alpha = (\alpha_1, \ldots, \alpha_l) \in \mathbb{N}^l$. Then $\mathcal{M} = \{X^\alpha : \alpha \in \mathbb{N}^l\}$. For $u = X^\alpha \in \mathcal{M}$ and $p \in \mathbb{N}$, we define that (cf., Section 9.3 of [2])

$$\operatorname{top}_p(u) = \{i \in \mathbb{N} : 1 \leq i \leq l, \alpha_i \geq p\}$$

and

$$\operatorname{sh}_p(u) = X^\beta, \text{ where } \beta = (\beta_1, \ldots, \beta_l) \in \mathbb{N}^l, \beta_i = \min\{p, \alpha_i\}, 1 \leq i \leq l,$$

i.e., $\operatorname{top}_p(u)$ is the set of indices where "u tops p" and $\operatorname{sh}_p(u)$ is "t shaved at p". For $W \subseteq \mathcal{M}$, we define a relation $\sim_p$ on W as follows: for any $u, v \in W$,

$$u \sim_p v \text{ if } \operatorname{sh}_p(u) = \operatorname{sh}_p(v).$$

Then we have the following lemma, whose proof is straightforward.

Lemma 3.4.3 *Let $W \subseteq \mathcal{M}$ and $p \in \mathbb{N}$. Then*

(i) $\sim_p$ is an equivalence relation on W.

(ii) Let $[u]_p = \{v \in W : u \sim_p v\}$ and $W/_{\sim_p} = \{[u]_p : u \in W\}$. If $\operatorname{sh}_p(u) \in W$ for all $u \in W$, then the set

$$W_p = \{u \in W : \operatorname{sh}_p(u) = u\}$$

is a set of normal forms for $W/_{\sim_p}$ (i.e., a system of unique representatives for $W/_{\sim_p}$). The set W_p can also be described as

$$W_p = \{X^\alpha \in W : \alpha_i \leq p, \ 1 \leq i \leq l\}.$$

(iii) For any $u = X^\alpha \in W_p$,

$$[u]_p = \{X^\beta \in W : \alpha \leq \beta,\ \alpha_i = \beta_i \text{ for } i \notin \mathrm{top}_p(u)\}.$$

Now we are in a position to prove our main result in this section.

Theorem 3.4.4 *Let R be a finite field extension of k. Let $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra, I be a left ideal of A and G be a finite Gröbner-Shirshov basis for I with respect to a total degree DD-monomial ordering. Set $p = \max\{\mathrm{tdeg}_{x_i}(\mathrm{lm}(g)) : g \in G, 1 \leq i \leq l\}$. Then*

(i) There exists a unique polynomial $h \in \mathbb{Q}[x]$ such that the Hilbert function HF_M of the left A-module $M = A/I$ satisfies $\mathrm{HF}_M(t) = h(t)$ for all $t \geq lp$.

(ii) The Gelfand-Kirillov dimension of M is equal to the degree of h, which is given as,

$$\mathrm{GKdim}(M) = \deg h = \max\{|\,\mathrm{top}_p(u)| : u \in \mathrm{Irr}(G) \cap \mathcal{M}_{\leq t}, \mathrm{sh}_p(u) = u\} \text{ for any } t \geq lp.$$

Proof. (i) (Existence) Let $t \in \mathbb{N}$ and $t \geq lp$. We will construct the desired polynomial h by counting the elements of the set $W = \mathrm{Irr}(G) \cap \mathcal{M}_{\leq t}$. By Proposition 3.4.2, $\mathrm{HF}_{A/I}(t) = d \cdot |W|$. Note that if $u \in W$ then $\mathrm{sh}_p(u) \in W$. By Lemma 3.4.3 (ii), $W_p = \{u \in W : \mathrm{sh}_p(u) = u\}$ is a set of normal forms of $W/_{\sim_p}$ and thus

$$|W| = \sum_{u \in W_p} |[u]_p|, \tag{3.7}$$

where $[u]_p$ is the equivalence class of u with respect to $\sim_p$. By Lemma 3.4.3 (iii), supposing $u = X^\alpha \in W_p$,

$$[u]_p = \{X^\beta \in W : \alpha \leq \beta,\ \alpha_i = \beta_i \text{ for } i \notin \mathrm{top}_p(u)\}.$$

Hence,

$$|[u]_p| = \binom{t - \operatorname{tdeg}(u) + |\operatorname{top}_p(u)|}{|\operatorname{top}_p(u)|}, \tag{3.8}$$

which is a polynomial in t of degree $|\operatorname{top}_p(u)|$. Now, by (3.7) and (3.8),

$$|W| = \sum_{u \in W_p} \binom{t - \operatorname{tdeg}(u) + |\operatorname{top}_p(u)|}{|\operatorname{top}_p(u)|}.$$

Let

$$h(x) = d \cdot \sum_{u \in W_p} \binom{x - \operatorname{tdeg}(u) + |\operatorname{top}_p(u)|}{|\operatorname{top}_p(u)|}.$$

Then h is a rational polynomial of degree $\max\{|\operatorname{top}_p(u)| : u \in W_p\}$ such that $\operatorname{HF}_M(t) = h(t)$ for all $t \geq lp$.

(Uniqueness) Suppose $h' \in \mathbb{Q}[x]$ and $\operatorname{HF}_M(t) = h'(t)$ for all $t \geq lp$. Then $h - h' \in \mathbb{Q}[x]$ and $h(t) - h'(t) = 0$ for infinitely many t. Hence $h - h' = 0$, or, $h = h'$.

(ii) It follows from part (i) and Lemma 3.4.1. ■

Theorem 3.4.4 together with Algorithm 3.3.17 gives an algorithm to compute the Gelfand-Kirillov dimension of a cyclic module over a differential difference algebra over R.

3.5 Gröbner-Shirshov Bases for A-modules

In this section, we develop the Gröbner-Shirshov basis theory of finitely generated modules over a differential difference algebra, which will be used to compute the Gelfand-Kirillov dimension of a finitely generated module over a differential difference algebra in the next section.

Let R be a finite field extension of k, $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra of type (m, n), and let $l = m + n$. Let A^p ($p \geq 1$) be the free left A-module of rank p with the standard A-basis

$$\boldsymbol{e}_1 = (1, 0, 0, \ldots, 0), \boldsymbol{e}_2 = (0, 1, 0, \ldots, 0), \ldots, \boldsymbol{e}_p = (0, \ldots, 0, 1).$$

A *monomial* in A^p is an element of the form $\boldsymbol{m} = X^\alpha \boldsymbol{e}_i = x_1^{\alpha_1} \cdots x_l^{\alpha_l} \boldsymbol{e}_i$, where $\alpha = (\alpha_1, \ldots, \alpha_l) \in \mathbb{N}^l$ and $1 \leq i \leq p$. The *total degree* of $\boldsymbol{m}$ is defined as $\operatorname{tdeg}(\boldsymbol{m}) = \operatorname{tdeg}(X^\alpha) = |\alpha|$. Then the set $\mathcal{N} = \{X^\alpha \boldsymbol{e}_i : \alpha \in \mathbb{N}^l, 1 \leq i \leq p\}$ of monomials in A^p is an R-basis of A^p. Thus every element $f \in A^p$ can be written in a unique way as an R-linear combination of monomials

$$f = \sum_{i=1}^{q} c_i \boldsymbol{m}_i, \quad 0 \neq c_i \in R, q \in \mathbb{N}, \boldsymbol{m}_i \in \mathcal{N}.$$

The *total degree* of f is defined as $\operatorname{tdeg}(f) = \max\{\operatorname{tdeg}(\boldsymbol{m}_i) : 1 \leq i \leq q\}$.

We say $\boldsymbol{m} = X^\alpha \boldsymbol{e}_i$ is right (left, respectively) divisible by $\boldsymbol{n} = X^\beta \boldsymbol{e}_j$, $1 \leq i, j \leq p$, if and only if $i = j$ and X^α is right (left, respectively) divisible by X^β, equivalently, if and only if $i = j$ and $\alpha_s \geq \beta_s$ for all $1 \leq s \leq l$. Suppose $f = \sum_{i=1}^q c_i \boldsymbol{m}_i \in A^p$ and $\boldsymbol{n}, \boldsymbol{n}_1, \ldots, \boldsymbol{n}_t \in \mathcal{N}$ for some $t \geq 1$. If each $\boldsymbol{m}_i$ is not right divisible by $\boldsymbol{n}$, then we say that f is irreducible with respect to $\boldsymbol{n}$. If f is irreducible with respect to every $\boldsymbol{n}_j$ $(1 \leq j \leq t)$ then we say that f is irreducible with respect to $\{\boldsymbol{n}_1, \ldots, \boldsymbol{n}_t\}$.

Proposition 3.5.1 *Every submodule of A^p is finitely generated.*

Proof. By Hilbert Basis Theorem 3.2.7, A is noetherian and thus so is A^p. Hence every submodule of A^p is finitely generated. ■

As for monomials in A, we can similarly define *leading monomial* $\operatorname{lm}(f)$, *leading coefficient* $\operatorname{lc}(f)$, *leading term* $\operatorname{lt}(f)$, *left quotient* $\operatorname{LQ}(f, g)$ and *irreducible monomials* $\operatorname{Irr}(G)$ with respect to G, for $f \in A^p$, $g \in A$ and $G \subseteq A^p$.

Definition 3.5.2 *A differential difference monomial ordering, DD-monomial ordering for short, on $\mathcal{N}$ is a well-ordering $>$ on $\mathcal{N}$ such that*

$$\textit{if } \boldsymbol{m} > \boldsymbol{n} \textit{ then } \operatorname{lm}(f\boldsymbol{m}) > \operatorname{lm}(f\boldsymbol{n}) \textit{ for all } \boldsymbol{m}, \boldsymbol{n} \in \mathcal{N} \textit{ and } 0 \neq f \in A.$$

Example 3.5.3 Let $>$ be a DD-monomial ordering on $\mathcal{M}$ (recall that $\mathcal{M}$ is the set of monomials of A). Then $>$ can be extended to a DD-monomial ordering on $\mathcal{N}$ as follows.

(1) We say $X^\alpha \boldsymbol{e}_i >_1 X^\beta \boldsymbol{e}_j$ if and only if $X^\alpha > X^\beta$, or $X^\alpha = X^\beta$ and $i < j$. It is easy to see that $>_1$ is a DD-monomial ordering on $\mathcal{N}$. We call $>_1$ the TOP extension of $>$, where TOP stands for "term over position", following terminology in [1].

(2) Similarly, we can introduce the POT ("position over term") extension $>_2$ of $>$. Define $X^\alpha \boldsymbol{e}_i >_1 X^\beta \boldsymbol{e}_j$ if and only if $i < j$ or $i = j$ and $X^\alpha > X^\beta$. It is easy to see that $>_2$ is also a DD-monomial ordering on $\mathcal{N}$.

Note that if the ordering $>$ in the above example is a total degree DD-monomial ordering then so is the TOP extension $>_1$.

The following lemma is similar to Lemma 3.3.10 (i) and it can be proved by induction on $\operatorname{lm}(f)$.

Lemma 3.5.4 *Let $>$ be a DD-monomial ordering on $\mathcal{N}$ and let $f_1, \dots, f_q \in A^p$, $q \in \mathbb{N}$. Then every element $f \in A^p$ can be written as*

$$f = a_1 f_1 + \cdots + a_q f_q + r,$$

where each $a_i \in A$, each $\operatorname{lm}(a_i f_i) \leq \operatorname{lm}(f)$, $r \in A^p$ and either $r = 0$ or r is irreducible with respect to $\{\operatorname{lm}(f_j) : 1 \leq j \leq q\}$.

In the above lemma, r is called a *remainder* of f on division by $\{f_1, \dots, f_q\}$. We say that f is reduced to r by $\{f_1, \dots, f_q\}$.

Definition 3.5.5 *Let $>$ be a DD-monomial ordering on $\mathcal{N}$ and M be a submodule of A^p. A subset $G \subseteq M$ is called a left Gröbner-Shirshov basis for M with respect to $>$ if, for any $0 \neq f \in M$, there exists $g \in G$ such that $\mathrm{lm}(f)$ is right divisible by $\mathrm{lm}(g)$.*

Let $\boldsymbol{m} = X^\alpha \boldsymbol{e}_i$ and $\boldsymbol{n} = X^\beta \boldsymbol{e}_j$ be two monomials. Define the *least common left multiple* of $\boldsymbol{m}$ and $\boldsymbol{n}$ as

$$\mathrm{lclm}(\boldsymbol{m}, \boldsymbol{n}) = \begin{cases} 0 & \text{if } i \neq j \\ \mathrm{lclm}(X^\alpha, X^\beta)\ \boldsymbol{e}_i & \text{if } i = j \end{cases}.$$

Fix a monomial ordering on A^p. Suppose $f, g \in A^p$ and $\boldsymbol{m} = \mathrm{lclm}(\mathrm{lm}(f), \mathrm{lm}(g))$. Then the *S-vector* of f and g is defined as

$$\mathrm{Svect}(f, g) = \mathrm{LQ}(\boldsymbol{m}, \mathrm{lt}(f))f - \mathrm{LQ}(\boldsymbol{m}, \mathrm{lt}(g))g.$$

Then we have the following criterion for left Gröbner-Shirshov bases.

Theorem 3.5.6 *Let G be a subset of A^p and let M be the submodule of A^p generated by G. Then G is a left Gröbner-Shirshov basis for M if and only if $\mathrm{Svect}(g_i, g_j)$ can be reduced to 0 by G for all $g_i, g_j \in G$.*

The proof of the following theorem is similar to that of Theorem 3.3.20.

Theorem 3.5.7 *Let G be a Gröbner-Shirshov basis for a submodule M for A^p. Then $\mathrm{Irr}(G)$ is an R-basis for the left A-module A^p/M.*

3.6 Gelfand-Kirillov Dimension of Finitely Generated Modules

As in the previous section, let $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra of type (m, n), where R is a finite field extension (of k) of degree d (suppose $V =$

$\{v_1, \ldots, v_d\}$ is a k-basis of R). Let $l = m + n$. In this section, we use the Gröbner-Shirshov basis theory of A^p ($p \geq 1$) developed in the previous section to compute the Gelfand-Kirillov dimension of a finitely generated left A-module.

Let M be a finitely generated left A-module. Since every finitely generated left A-module is isomorphic to a quotient module of a finitely generated free left A-module, we may suppose that, throughout this section, $M = A^p/N$ for some $p \geq 1$ and some submodule N of A^p. As in the previous section, denote the standard basis of A^p by $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_p\}$. Let E be the k-subspace of M generated by $\{\boldsymbol{e}_1 + N, \ldots, \boldsymbol{e}_p + N\}$. Then $M = AE$. Recall that A has a natural grading: $A = \oplus_{i\in\mathbb{N}} A_i$, where A_i is the k-subspace of A spanned by $\mathcal{M}_i = \{X^\alpha : \alpha \in \mathbb{N}^l, |\alpha| = i\}$, which induces a grading of $M = A^p/N$, i.e., $M = \oplus_{i\in\mathbb{N}} M_i$, where $M_i = A_i E$ for $i \in \mathbb{N}$. Let $\mathcal{N}_i = \{u\boldsymbol{e}_j : u \in \mathcal{M}_i, 1 \leq j \leq p\}$ and $\mathcal{N}_{\leq i} = \mathcal{N}_0 \cup \cdots \cup \mathcal{N}_i$, $i \in \mathbb{N}$. Then, similar to Proposition 3.4.2, we have the following

Proposition 3.6.1 *Let N be a submodule of A^p and let G be a left Gröbner-Shirshov basis for N with respect to a total degree DD-monomial ordering. Then the following hold:*

(i) The set $B_i = \{\overline{vu} : v \in V, u \in \mathrm{Irr}(G) \cap \mathcal{N}_{\leq i}\}$ is a k-basis of $M_{\leq i} = M_0 \oplus \cdots \oplus M_i$, $i \in \mathbb{N}$.

(ii) The Hilbert function of M is given by

$$\mathrm{HF}_M(i) = d \cdot |\,\mathrm{Irr}(G) \cap \mathcal{N}_{\leq i}|, i \in \mathbb{N}.$$

For a monomial $X^\alpha \boldsymbol{e}_i$ and $q \in \mathbb{N}$, define $\mathrm{top}_q(X^\alpha \boldsymbol{e}_i) = \mathrm{top}_q(X^\alpha)$ and $\mathrm{sh}_q(X^\alpha \boldsymbol{e}_i) = \mathrm{sh}_q(u)\boldsymbol{e}_i$.

The following theorem gives a relation between the Gelfand-Kirillov dimension and a finite Gröbner-Shirshov basis for a finitely generated module over a differential difference algebra.

Theorem 3.6.2 *Let R be a finite field extension of k and $A = R[\mathcal{S}, \mathcal{D}; \sigma, \delta]$ be a differential difference algebra. Let N be a submodule of the free A-module A^p ($p \geq 1$), and G be a left Gröbner-Shirshov basis for N with respect to a total degree DD-monomial ordering. Denote the left A-module A^p/N by M. Set*

$$q = \max\{\mathrm{tdeg}_{x_i}(\mathrm{lm}(g)) : g \in G, 1 \leq i \leq l\}.$$

Then the following hold:

(i) There exists a unique polynomial $h \in \mathbb{Q}[x]$ such that the Hilbert function HF_M of M satisfies $\mathrm{HF}_M(t) = h(t)$ for all $t \geq lq$.

(ii) The Gelfand-Kirillov dimension of M is equal to the degree of h, which is given by

$$\mathrm{GKdim}(M) = \deg h = \max\{|\,\mathrm{top}_q(u)| : u \in \mathrm{Irr}(G) \cap \mathcal{N}_{\leq t}, \mathrm{sh}_q(u) = u\}, \;\; t \geq lq.$$

Proof. (i) Let $t \in \mathbb{N}$ and $W_p = \{u \in \mathrm{Irr}(G) : \mathrm{tdeg}(u) \leq t, \mathrm{sh}_q(u) = u\}$. Similar to Theorem 3.4.4, one can show that

$$\mathrm{HF}_M(t) = h(t) = pd \cdot \sum_{u \in W_p} \binom{t - \mathrm{tdeg}(u) + |\,\mathrm{top}_q(u)|}{|\,\mathrm{top}_q(u)|},$$

which is a rational polynomial of degree $\max\{|\,\mathrm{top}_q(u)| : u \in W_p\}$.

(ii) It follows from (i). ■

Now we can easily write an algorithm from Theorem 3.5.6 and Theorem 3.6.2.

Algorithm 3.6.3 (GK-dimension of f.g. A-Modules)

Input: $F = \{f_1, \ldots, f_s\} \subset A^p$, $s \in \mathbb{N}$, each $f_i \neq 0$.

Output: $\mathrm{GKdim}(A^p/N)$, where N is the left submodule of A^p generated by F.

Initialization: $G := F$, $P := \{\{p, q\} : p \neq q, p, q \in F\}$.

WHILE $P \neq \emptyset$ DO

Choose any pair $\{p, q\} \in P$, $P := P \setminus \{\{p, q\}\}$

$r :=$ a remainder of $\mathrm{Svect}(p, q)$ modulo G

IF $r \neq 0$ THEN

$G := G \cup \{r\}$, $P := P \cup \{\{g, r\} : g \in G\}$

END DO

$q := \max\{\mathrm{tdeg}_{x_i}(\mathrm{lm}(g)) : g \in G, 1 \leq i \leq l\}$

Return $\max\{|\operatorname{top}_q(u)| : u \in \mathrm{Irr}(G) \cap \mathcal{N}_{\leq t}, \mathrm{sh}_q(u) = u\}$

Bibliography

[1] W. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, 1994.

[2] T. Becker and V. Weispfenning, *Gröbner bases: a computational approach to commutative algebra*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, 1993.

[3] A. D. Bell and K. R. Goodearl, *Uniform rank over differential operator rings and Poincaré-Birkhoff-Witt extensions*, Pacific J. Math. **131** (1988), no. 1, 13–37.

[4] L. A. Bokut, Yuqun Chen, and Jiapeng Huang, *Gröbner-Shirshov bases for L-algebras*, Internat. J. Algebra Comput. **23** (2013), no. 3, 547–571.

[5] L. A. Bokut, Yuqun Chen, and Cihua Liu, *Gröbner-Shirshov bases for dialgebras*, Internat. J. Algebra Comput. **20** (2010), no. 3, 391–415.

[6] L. A. Bokut, Yuqun Chen, and Qiuhui Mo, *Gröbner-Shirshov bases for semirings*, J. Algebra **385** (2013), 47–63.

[7] L. A. Bokut', Yuqun Chen, and K. P. Shum, *Some new results on Gröbner-Shirshov bases*, Proceedings of International Conference on Algebra 2010–Advances in Algebraic Structures (W. Hemakul, S. Wahyuni, and P. W. Sy, eds.), 2012, pp. 53–102.

[8] J. L. Bueso, J. Gómez-Torrecillas, and F. J. Lobillo, *Computing the Gelfand-Kirillov dimension II*, Lect. Notes Pure Appl. Math. (2001), 33–58.

[9] J. L. Bueso, F. J. Jiménez, and P. Jara, *Effective computation of the Gelfand-Kirillov dimension*, Proceedings of the Edinburgh Mathematical Society (Series 2) **40** (1997), no. 1, 111–117.

[10] Yongshan Chen and Yuqun Chen, *Gröbner-Shirshov bases for metabelian Lie algebras*, J. Algebra **358** (2012), 143–161.

[11] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, vol. 10, Springer, 2007.

[12] J. Gómez-Torrecillas, *Gelfand-Kirillov dimension of multi-filtered algebras*, Proceedings of the Edinburgh Mathematical Society **42** (1999), 155–168.

[13] A. Kandri-Rody and V. Weispfenning, *Non-commutative Gröbner bases in algebras of solvable type*, J. Symbolic Comput. **9** (1990), no. 1, 1–26.

[14] C. Kassel, *Quantum groups*, Graduate Texts in Mathematics, vol. 155, Springer-Verlag, 1995.

[15] G. Krause and T. Lenagan, *Growth of algebras and Gelfand-Kirillov dimension*, Graduate Studies in Mathematics, vol. 22, AMS, 2000.

[16] V. Levandovskyy and H. Schönemann, *Plural: a computer algebra system for noncommutative polynomial algebras*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 176–183.

[17] H. Li, *Noncommutative Gröbner bases and filtered-graded transfer*, Lecture Notes in Mathematics, vol. 1795, Springer, 2002.

[18] E. L. Mansfield and A. Szanto, *Elimination theory for differential difference polynomials*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 191–198.

[19] J. C. McConnell, J. C. Robson, and L. W. Small, *Noncommutative Noetherian rings*, Graduate Studies in Mathematics, vol. 30, American Mathematical Society, 2001.

[20] L. H. Rowen, *Ring theory*, Pure and applied mathematics, vol. 127, Academic Press, Inc., 1988.

Chapter 4

A Signature-Based Algorithm for Computing Gröbner-Shirshov Bases in Skew Solvable Polynomial Rings

Signature-based algorithms are efficient algorithms for computing Gröbner-Shirshov bases in commutative polynomial rings, and some noncommutative rings. In this chapter, we first define skew solvable polynomial rings, which are generalizations of solvable polynomial algebras and (skew) PBW extensions. Then we present a signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings over fields.

4.1 Introduction

Gröbner-Shirshov basis is a powerful tool in mathematics, science, engineering, and computer science. The theory of Gröbner-Shirshov bases was introduced independently by A.I. Shirshov [19] for Lie algebras in 1962, and by B. Buchberger ([3]) for commutative algebras in 1965. Buchberger([3]) gave the first algorithm to compute Gröbner-Shirshov bases in commutative polynomial rings. However, Buchberger's algorithm is not efficient since it has to reduce the S-polynomial for every pair of elements from the input set. There have been extensive efforts to improve the efficiency of Buchberger's algorithm in commutative polynomial rings, and several more efficient signature-based algorithms have been proposed, such as F5 by Faugère ([6, 7]), G2V and GVW by Gao et al.([10, 11]). The essential idea in these algorithms is to detect "useless" S-polynomials, i.e., S-polynomials which can be reduced to zero (and thus the computations of these S-polynomials are redundant), in Buchberger's algorithm.

Noncommutative Gröbner-Shirshov bases and their computations have also been widely investigated (see the survey [2]), especially for various skew polynomial rings, for example, Gröbner-Shirshov basis theory for Weyl algebras [9], solvable polynomial algebras [14], rings of differential operators [13, 22, 16], G-algebras [15], skew polynomial rings [5], differential difference algebras [17, 21], PBW algebras [4, 12] and skew PBW extensions [8]. Owing to the noncommutativity, it is difficult to detect and reject redundant computations effectively. In ISSAC 2012, a signature-based algorithm was presented by Sun et al. [20] to compute Gröbner-Shirshov bases in solvable polynomial algebras.

In this chapter, we define skew solvable polynomial rings, which are generalizations of several well-known classes of rings such as solvable polynomial algebras and (skew) Poincaré-Birkhoff-Witt extensions (see Definition 4.2.1 and Examples 4.2.2 and 4.2.3). We extend the signature-based algorithm proposed in [20] to skew solvable polynomial rings over fields. The signature-based algorithms for more general skew solvable polynomial rings will be investigated in the near future.

This chapter is organized as follows. In Section 2, we introduce basic definitions of skew solvable polynomial rings and Gröbner-Shirshov bases. Then we define and investigate strong Gröbner-Shirshov bases of skew solvable polynomial rings in Section 3. Finally a signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings is given in Section 4.

4.2 Preliminaries

4.2.1 Skew solvable polynomial rings

In order to define skew solvable polynomial rings, let us recall some basic definitions of orderings first. Let $\mathbb{N}$ be the set of nonnegative integers. Suppose $<$ is a *monomial ordering* on $\mathbb{N}^n$, $n \in \mathbb{N}$, i.e., a total ordering on $\mathbb{N}^n$ such that $0 \in \mathbb{N}^n$ is the smallest element in $\mathbb{N}^n$ and $\alpha < \beta$ implies $\alpha + \gamma < \beta + \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{N}^n$. The set of *(standard) monomials* in n indeterminates $\{x_1, \ldots, x_n\}$ is defined as $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha_i \in \mathbb{N}, 1 \leq i \leq n\}$. We also denote $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ by x^α and call α the *exponent* of x^α (denoted by $\exp(x^\alpha) = \alpha$), where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. We say $x^\alpha < x^\beta$ if $\alpha < \beta$. Thus, a monomial ordering on $\mathbb{N}^n$ is also called a monomial ordering on the set of standard monomials.

The *multiple degree* and the *total degree* of a monomial x^α are defined as $\mathrm{mdeg}(x^\alpha) = \alpha$ and $\mathrm{tdeg}(x^\alpha) = |\alpha| = \alpha_1 + \cdots + \alpha_n$, respectively. For any nonzero $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$, where only finitely many constants c_α are nonzero, the *multiple degree* and the *total degree* of f are defined as $\mathrm{mdeg}(f) = \max\{\alpha : c_\alpha \neq 0\}$ and $\mathrm{tdeg}(f) = \max\{|\alpha| : c_\alpha \neq 0\}$, respectively. The monomial $x^\gamma = \max\{x^\alpha : c_\alpha \neq 0\}$ is called the *leading monomial* of f and c_γ is called the *leading coefficient* of f, denoted by $\mathrm{lm}(f)$ and $\mathrm{lc}(f)$, respectively.

From now on, we fix a monomial ordering $<$ on $\mathbb{N}^n$.

Throughout this chapter, we suppose all rings considered are unitary and associative. If R is a ring and σ is a ring endomorphism of R, then a mapping

$\delta : R \to R$ is called a *σ-derivation* of R if for any $a, b \in R$, $\delta(a+b) = \delta(a) + \delta(b)$ and $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$.

Definition 4.2.1 *Let R and A be two rings with $R \subseteq A$. Then A is called a* skew solvable polynomial ring *over R if the following conditions hold:*

(i) There exist finitely many elements $x_1, \dots, x_n \in A$ such that A is a free left R-module with basis

$$\mathcal{M} = \{x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \ \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n\}.$$

(ii) For $1 \leq i \leq n$, there are an injective ring endomorphism σ_i of R and a σ_i-derivation δ_i of R such that $x_i r = \sigma_i(r)x_i + \delta_i(r)$ for any $r \in R$. Furthermore, for any $1 \leq i, j \leq n$,

$$\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i, \ \ \delta_i \circ \delta_j = \delta_j \circ \delta_i, \ \ \sigma_i \circ \delta_j = \delta_j \circ \sigma_i.$$

(iii) For $1 \leq i < j \leq n$, there exist $0 \neq c_{ij} \in R$ and $p_{ij} \in A$ with $\mathrm{lm}(p_{ij}) < x_i x_j$ such that $x_j x_i = c_{ij} x_i x_j + p_{ij}$.

Then we write $A = R\langle X; \sigma, \delta, c, p\rangle$. Clearly every nonzero element in A can be uniquely represented as $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$, where only finitely many $c_\alpha \in R$ are nonzero.

Skew solvable polynomial rings are generalizations of several well-known kinds of skew polynomial rings.

Example 4.2.2 *Let $A = R\langle X; \sigma, \delta, c, p\rangle$ be a skew solvable polynomial ring.*

(i). If R is a field, $\sigma_i = \mathrm{id}_R$ and $\delta_i = 0$ for all $1 \leq i \leq n$, then A is a solvable polynomial algebra [14]. Any solvable polynomial algebra can be viewed as a skew solvable polynomial ring in this way.

(ii). If $\mathrm{tdeg}(p_{ij}) = 1$ for all $1 \leq i < j \leq n$, then A is a skew PBW extension of R [8]. Any skew PBW extension can be viewed as a skew solvable polynomial ring in this way.

Therefore, any ring belonging to the above two classes of rings is a skew solvable polynomial ring, for example, a Weyl algebra, the universal enveloping algebra of a finite dimensional Lie algebra, and an Ore extension of automorphism and/or derivation type.

Example 4.2.3 *([18]) Let $0 \neq q \in k$. The coordinate ring of quantum Euclidean space, denoted by $\mathcal{O}_q(\mathfrak{o}k^{2n+1})$, is the k-algebra generated by $2n+1$ variables w, $x_1, \ldots,$ x_n, $y_1, \ldots, y_n$ with the following relations:*

$$\begin{aligned}
wy_j &= qy_jw, && 1 \leq j \leq n,\\
wx_j &= q^{-1}x_jw, && 1 \leq j \leq n,\\
y_jy_i &= q^{-1}y_iy_j, && i < j,\\
y_jx_i &= q^{-1}x_iy_j, && i \neq j,\\
x_jx_i &= qx_ix_j, && i < j,\\
y_jx_j &= x_jy_j + f_{jj}, && 1 \leq j \leq n,
\end{aligned}$$

where

$$f_{jj} = q^{1-j}(q^{1/2} - q^{-1/2})w^2 + (q^2 - 1)\sum_{1 \leq l < j} q^{l-j}y_lx_l.$$

Let $R = k[w]$. For $1 \leq i \leq n$, let $x_{n+i} = y_i$, σ_i be the k-algebra isomorphism over R determined by $\sigma_i(w) = qw$, σ_{n+i} be the k-algebra isomorphism over R determined by $\sigma_{n+i}(w) = q^{-1}w$, and $\delta_j = 0$ be the zero mapping for any $1 \leq j \leq 2n$. Let

$$c_{ij} = \begin{cases} q, & i < j \leq n,\\ q^{-1}, & n < i < j, \text{ or } i < n < j \text{ and } i \neq j - n,\\ 1, & i = j - n, \end{cases}$$

and

$$p_{ij} = \begin{cases} 0, & i \neq j, \\ f_{ij}, & i = j. \end{cases}$$

It is easy to prove by induction that, for any $1 \leq j \leq n$, f_{jj} (and thus p_{jj}) can be written as

$$f_{jj} = \sum_{1 \leq l < j} c_l x_l y_l + c w^2, \ c_l, c \in k.$$

Let $>$ be a monomial ordering on $\{x^\alpha : \alpha \in \mathbb{N}^{2n}\}$ such that $x_{2n} > x_{2n-1} > \cdots > x_1$. With the above notation, it is easy to check that $\mathcal{O}_q(\mathfrak{o}k^{2n+1}) = R\langle X; \sigma, \delta, c, p\rangle$ is a skew solvable polynomial ring.

In this chapter, we consider Gröbner-Shirshov bases in a skew solvable polynomial ring over a field (i.e., R is a field) and the general case will be studied in the near future.

From now on, let $R = k$ be a field and $A = R\langle X; \sigma, \delta, c, p\rangle$ be a skew solvable polynomial ring.

Let us fix more notation. Denote $\sigma_1^{\alpha_1} \cdots \sigma_n^{\alpha_n}(c) = \sigma^\alpha(c)$ and $\delta_1^{\alpha_1} \cdots \delta_n^{\alpha_n}(c) = \delta^\alpha(c)$ for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ and $c \in k$. Suppose $x^\alpha, x^\beta \in \mathcal{M}$. Then the *least common multiple* of x^α and x^β is defined as $\mathrm{lcm}(x^\alpha, x^\beta) = x^\gamma$ where $\gamma = (\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_n, \beta_n\}) \in \mathbb{N}^n$. We say that x^α is *divisible* by x^β, or x^β *divides* x^α, if $x^\alpha = \mathrm{lm}(t x^\beta)$ for some $t \in \mathcal{M}$. For convenience, denote $\frac{x^\alpha}{x^\beta} = x^{\alpha - \beta}$ (but keep in mind that $x^{\alpha-\beta} x^\beta \neq x^\alpha$ in general in a skew solvable polynomial ring). We make the convention that $\mathrm{lm}(0) = 0 < t$ for any $0 \neq t \in \mathcal{M}$.

With the above notation, the proof of the following lemma is straightforward.

Lemma 4.2.4 *Suppose $x^\alpha, x^\beta, x^\gamma \in \mathcal{M}$. We have:*

(i) $\mathrm{lm}(x^\alpha x^\beta) = x^{\alpha+\beta} = \mathrm{lm}(x^\beta x^\alpha)$.

(ii) x^β divides x^α if and only if $\alpha - \beta \in \mathbb{N}^n$.

(iii) If $x^\alpha < x^\beta$ *then* $\mathrm{lm}(x^\gamma x^\alpha) < \mathrm{lm}(x^\gamma x^\beta)$.

4.2.2 Gröbner-Shirshov Bases of Skew Solvable Polynomial Rings

In this subsection, we briefly introduce concepts related to Gröbner-Shirshov bases and Buchberger's algorithm for skew solvable polynomial rings.

Definition 4.2.5 *Let I be a left ideal of A. A* (left) Gröbner-Shirshov basis *(with respect to $<$) is a finite subset $G \subset I$ with the property that for every nonzero $f \in I$,* $\mathrm{lm}(f)$ *is divisible by* $\mathrm{lm}(g)$ *for some $g \in G$.*

Let $f, g \in A$ be nonzero. Suppose that

$$t_f = \frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}(f)} \text{ and } t_g = \frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}(g)}.$$

The *S-polynomial* of f and g, denoted by $\mathrm{SPoly}(f, g)$, is defined as

$$\mathrm{SPoly}(f, g) = t_f f - c t_g g \in I, \quad \text{where } c = \frac{\mathrm{lc}(t_f f)}{\mathrm{lc}(t_g g)} = \frac{\sigma^{\exp(t_f)}(\mathrm{lc}(f))}{\sigma^{\exp(t_g)}(\mathrm{lc}(g))}.$$

Suppose $f, g \in I$. We say f is *reducible* by g if there exists a $t \in \mathcal{M}$ such that $\mathrm{lm}(tg) = \mathrm{lm}(f)$. Moreover, if $G \subseteq A$ and $g \in G$, then $f \to_G f - ctg$ is called *one-step-reduction* by G. If an element $r \in A$ is obtained from f by finitely many one-step-reductions by G and r is not reducible by G, then we say that r is a *remainder* of f modulo G.

The following algorithm is an analogue of the Buchberger's Algorithm for (commutative) polynomial algebras.

Algorithm 4.2.6 (Algorithm for (left) Gröbner-Shirshov bases)

Input: $F = \{f_1, \ldots, f_m\} \subseteq A$

Output: A Gröbner-Shirshov basis G of the left ideal I of A generated by F.

$G := F$

Pairs:= $\{(f, g) : f, g \in G\}$

While Pairs$\neq \emptyset$ **Do**

Choose $(f, g) \in$ Pairs

Pairs:=Pairs $\setminus\{(f, g)\}$

$h :=$ a remainder of SPoly(f, g) modulo G

If $h \neq 0$ **Then**

Pairs:=Pairs $\cup\{(h, h') : h' \in G\} \cup \{(h', h) : h' \in G\}$

$G := G \cup \{h\}$

End If

End Do

Return G

The correctness and termination of the above algorithm can be proved in a way similar to the case of commutative polynomial algebras ([3]).

4.3 Strong Gröbner-Shirshov Bases

In this section, we introduce the definition of strong Gröbner-Shirshov bases and investigate their properties which will be used in the next section.

Recall that A is a skew solvable polynomial ring over a field k. Let

$$\boldsymbol{f} = (f_1, \dots, f_m) \in A^m,\ m \in \mathbb{N}.$$

We denote by I the left ideal of A generated by $f_1, \dots, f_m$. Then an element $f \in I$ can be written as

$$f = u_1 f_1 + \cdots + u_m f_m = \boldsymbol{u} \cdot \boldsymbol{f}, \quad \text{where } \boldsymbol{u} = (u_1, \dots, u_m) \in A^m.$$

Note that this expression for f is not unique, i.e., there may exist $\boldsymbol{u}' \in A^m$ such that $\boldsymbol{u}' \neq \boldsymbol{u}$ and $f = \boldsymbol{u}' \cdot \boldsymbol{f}$. We write $f^{[\boldsymbol{u}]} \in I \times A^m$ to indicate $f \in I$, $\boldsymbol{u} \in A^m$ and $f = \boldsymbol{u} \cdot \boldsymbol{f}$. That is, $f^{[\boldsymbol{u}]}$ is actually a pair $(f, \boldsymbol{u}) \in I \times A^m$ such that $f = \boldsymbol{u} \cdot \boldsymbol{f}$. With this convention, for $a \in A$, $f^{[\boldsymbol{u}]}, g^{[\boldsymbol{v}]}, h^{[\boldsymbol{w}]} \in I \times A^m$, by the equation $h^{[\boldsymbol{w}]} = f^{[\boldsymbol{u}]} + ag^{[\boldsymbol{v}]}$ it means $h = f + ag$ and $\boldsymbol{w} = \boldsymbol{u} + a\boldsymbol{v}$, particularly, $h^{[\boldsymbol{w}]} = f^{[\boldsymbol{u}]}$ if and only if $h = f$ and $\boldsymbol{w} = \boldsymbol{u}$.

Note that A^m is a left A-module with the standard basis $\{\boldsymbol{e}_i : 1 \leq i \leq m\}$, where $\boldsymbol{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with the i-component 1 and the other components 0. The set of *(standard) monomials* in A^m is

$$\mathcal{N} = \{x^\alpha \boldsymbol{e}_i : \alpha \in \mathbb{N}^n, 1 \leq i \leq m\}.$$

A *(left) monomial ordering* on $\mathcal{N}$ is a well-ordering on $\mathcal{N}$ such that

$$\text{if } \boldsymbol{m} > \boldsymbol{n} \text{ then } \mathrm{lm}(\boldsymbol{t}\boldsymbol{m}) > \mathrm{lm}(\boldsymbol{t}\boldsymbol{n}) \text{ for all } \boldsymbol{m}, \boldsymbol{n} \in \mathcal{N} \text{ and } \boldsymbol{t} \in \mathcal{M}.$$

A monomial ordering on $\mathcal{M}$ can be extended to a monomial ordering on $\mathcal{N}$.

Example 4.3.1 Let $<_0$ be a monomial ordering on $\mathcal{M}$. Then $<_0$ can be extended to monomial orderings on $\mathcal{N}$ as follows.

(i) We say $x^\alpha \boldsymbol{e}_i <_1 x^\beta \boldsymbol{e}_j$ if and only if $x^\alpha <_0 x^\beta$, or $x^\alpha = x^\beta$ and $i < j$. It is easy to see that $<_1$ is a monomial ordering on $\mathcal{N}$. We call $<_1$ the TOP extension of $<_0$, where TOP stands for "term over position", following terminology in [1].

(ii) Similarly, we can introduce the POT ("position over term") extension [1]: Define $x^\alpha \boldsymbol{e}_i <_2 x^\beta \boldsymbol{e}_j$ if and only if $i < j$ or $i = j$ and $x^\alpha <_0 x^\beta$. It is easy to see that $<_2$ is also a monomial ordering on $\mathcal{N}$.

From now on, we fix a monomial ordering, also denoted by $<$, on $\mathcal{N}$ such that it is *compatible* with the monomial ordering on $\mathcal{M}$, i.e., for any $x^\alpha, x^\beta \in \mathcal{M}$ and $1 \leq i \leq m$, if $x^\alpha < x^\beta$ in $\mathcal{M}$ then $x^\alpha \boldsymbol{e}_i < x^\beta \boldsymbol{e}_i$ in $\mathcal{N}$.

Every element $\boldsymbol{u} \in A^m$ can be written uniquely as a k-linear combination of monomials: $\boldsymbol{u} = \sum_{1\leq i\leq q} c_i \boldsymbol{m}_i$ where $q \in \mathbb{N}, 0 \neq c_i \in k, \boldsymbol{m}_i \in \mathcal{N}$. Then, as what we did for elements in A, we can define the *leading monomial* $\mathrm{lm}(\boldsymbol{u})$ and *leading coefficient* $\mathrm{lc}(\boldsymbol{u})$ of $\boldsymbol{u}$.

Definition 4.3.2 *Given $f^{[\boldsymbol{u}]} \in I \times A^m$, the leading monomial $\mathrm{lm}(\boldsymbol{u})$ is called the* signature *of $f^{[\boldsymbol{u}]}$.*

Definition 4.3.3 *A finite set $G = \{g_1^{[\boldsymbol{v}_1]}, \ldots, g_s^{[\boldsymbol{v}_s]}\} \subseteq I \times A^m$ is called a* strong Gröbner-Shirshov basis *(cf., [11, 20]) of I if, for any $f^{[\boldsymbol{u}]} \in I \times A^m$, there exist $g_i^{[\boldsymbol{v}_i]} \in G$ and $t \in \mathcal{M}$ such that $\mathrm{lm}(t\boldsymbol{v}_i) = \mathrm{lm}(\boldsymbol{u})$ and $\mathrm{lm}(tg_i) \leq \mathrm{lm}(f)$.*

We call G a $\boldsymbol{t}$-strong Gröbner-Shirshov basis *for a monomial $\boldsymbol{t}$ in A^m if for any $f^{[\boldsymbol{u}]} \in I \times A^m$ with $\mathrm{lm}(\boldsymbol{u}) < \boldsymbol{t}$, there exist $g_i^{[\boldsymbol{v}_i]} \in G$ and $t \in \mathcal{M}$ such that $\mathrm{lm}(t\boldsymbol{v}_i) = \mathrm{lm}(\boldsymbol{u})$ and $\mathrm{lm}(tg_i) \leq \mathrm{lm}(f)$.*

Lemma 4.3.4 *Suppose that $G = \{g_1^{[\boldsymbol{v}_1]}, \ldots, g_s^{[\boldsymbol{v}_s]}\}$ is a strong Gröbner-Shirshov basis of I. Then $G' = \{g_1, \ldots, g_s\}$ is a Gröbner-Shirshov basis of I.*

Proof. By way of contradiction, we suppose that G' is not a Gröbner-Shirshov basis, i.e., the following set E is not empty:

$$E = \{f^{[\boldsymbol{u}]} \in I \times A^m : f \neq 0, \mathrm{lm}(f) \text{ is not divisible by } \mathrm{lm}(g) \text{ for any } g \in G'\}.$$

We choose $f^{[\boldsymbol{u}]} \in E$ such that $f^{[\boldsymbol{u}]}$ has minimal signature among E. By the definition of a strong Gröbner-Shirshov basis, there exist $g^{[\boldsymbol{v}]} \in G$ and $t \in \mathcal{M}$ such that $\mathrm{lm}(t\boldsymbol{v}) = \mathrm{lm}(\boldsymbol{u})$ and $\mathrm{lm}(tg) \leq \mathrm{lm}(f)$. If $\mathrm{lm}(tg) = \mathrm{lm}(f)$, then $\mathrm{lm}(f)$ is divisible by $\mathrm{lm}(g)$, contradicting our assumption that $f \in E$. Hence $\mathrm{lm}(tg) < \mathrm{lm}(f)$. Let $h^{[\boldsymbol{w}]} = f^{[\boldsymbol{u}]} - ctg^{[\boldsymbol{v}]}$ where $c = \frac{\mathrm{lc}(\boldsymbol{u})}{\sigma^{\exp(t)}(\mathrm{lc}(\boldsymbol{v}))}$. Then $\mathrm{lm}(h) = \mathrm{lm}(f)$ and thus $\mathrm{lm}(h)$ is not divisible by $\mathrm{lm}(g')$ for any $g' \in G'$. Hence $h^{[\boldsymbol{w}]} \in E$. By the choice of c, we have that

$\mathrm{lm}(\boldsymbol{u}) = \mathrm{lm}(ct\boldsymbol{v})$ and thus $\mathrm{lm}(\boldsymbol{w}) < \mathrm{lm}(\boldsymbol{u})$, which contradicts the minimality of $f^{[\boldsymbol{u}]}$ in E. ■

In a similar way, we can prove the following

Lemma 4.3.5 *Suppose that G is a $\boldsymbol{t}$-strong Gröbner-Shirshov basis of I. Then, for any $f^{[\boldsymbol{u}]} \in I \times A^m$ with $\mathrm{lm}(\boldsymbol{u}) < \boldsymbol{t}$, there exist $g^{[\boldsymbol{v}]} \in G$ and $t \in \mathcal{M}$ such that $\mathrm{lm}(tg) = \mathrm{lm}(f)$ and $\mathrm{lm}(t\boldsymbol{v}) \leq \mathrm{lm}(\boldsymbol{u})$.*

Suppose that $f^{[\boldsymbol{u}]}, g^{[\boldsymbol{v}]} \in I \times A^m$ are nonzero and $\mathrm{lm}(t_f\boldsymbol{u}) \geq \mathrm{lm}(t_g\boldsymbol{v})$ where

$$t_f = \frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}(f)},\ t_g = \frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}(g)}.$$

Then the ordered 4-tuple $(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]})$ is called the *critical pair* of $f^{[\boldsymbol{u}]}$ and $g^{[\boldsymbol{v}]}$. Furthermore, the critical pair $(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]})$ is said to be *regular* if $\mathrm{lm}(t_f\boldsymbol{u}) > \mathrm{lm}(t_g\boldsymbol{v})$. With the above notation, we have the following

Lemma 4.3.6 *Suppose that $(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]})$ is the critical pair of $f^{[\boldsymbol{u}]}$ and $g^{[\boldsymbol{v}]}$. Then $\mathrm{lm}(\mathrm{SPoly}(f, g)) < \mathrm{lm}(t_f f) = \mathrm{lm}(t_g g)$.*

Recall that a *non-strict partial order* on a set P is a binary relation $\leq_P$ over P which is reflexive, antisymmetric, and transitive. We call $<_P$ a *(strict) partial order* over P.

Now we are in a position to introduce the rewriting criterion.

Definition 4.3.7 (Rewriting Criterion) *Let $S = \{f_j^{[\boldsymbol{u}_j]} : j \in J\} \subseteq I \times A^m$ where $J \subseteq \mathbb{N}$ is a nonempty index set, and $<_S$ be a partial order on S. Suppose that $f^{[\boldsymbol{u}]} \in S$ and $t \in \mathcal{M}$. Then $t(f^{[\boldsymbol{u}]})$ is called* rewritable *by S (with respect to $<_S$) if there exist $g^{[\boldsymbol{v}]} \in S$ and $t' \in \mathcal{M}$ such that $\mathrm{lm}(t'\boldsymbol{v}) = \mathrm{lm}(t\boldsymbol{u})$ and $g^{[\boldsymbol{v}]} <_S f^{[\boldsymbol{u}]}$. In particular, a critical pair $(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]})$ of S is called* rewritable *by S if either $t_f(f^{[\boldsymbol{u}]})$ or $t_g(g^{[\boldsymbol{v}]})$ is rewritable by S.*

Lemma 4.3.8 *Suppose that $t(f^{[\boldsymbol{u}]})$ is rewritable by a finite subset $S \subseteq I \times A^m$ with respect to a partial order $<_S$ on S. Then there exist $g^{[\boldsymbol{v}]} \in S$ and $t' \in \mathcal{M}$ such that $\operatorname{lm}(t'\boldsymbol{v}) = \operatorname{lm}(t\boldsymbol{u})$, $g^{[\boldsymbol{v}]} <_S f^{[\boldsymbol{u}]}$ and $t'(g^{[\boldsymbol{v}]})$ is not rewritable by S.*

Proof. Since $t(f^{[\boldsymbol{u}]})$ is rewritable by S, by definition, there exist $g_0^{[\boldsymbol{v}_0]} \in S$ and $t_0 \in \mathcal{M}$ such that $\operatorname{lm}(t_0\boldsymbol{v}) = \operatorname{lm}(t\boldsymbol{u})$ and $g_0^{[\boldsymbol{v}_0]} <_S f^{[\boldsymbol{u}]}$. If $t_0(g_0^{[\boldsymbol{v}_0]})$ is not rewritable by S, then $g^{[\boldsymbol{v}]} := g_0^{[\boldsymbol{v}_0]}$ is as required. We assume that $t_0(g_0^{[\boldsymbol{v}_0]})$ is rewritable by S. Then there exist $g_1^{[\boldsymbol{v}_1]} \in S$ and $t_1 \in \mathcal{M}$ such that $\operatorname{lm}(t_1\boldsymbol{v}_0) = \operatorname{lm}(t_0\boldsymbol{u}_0)$ and $g_1^{[\boldsymbol{v}_1]} <_S g_0^{[\boldsymbol{v}_0]}$. If $t_1(g_1^{[\boldsymbol{v}_1]})$ is not rewritable by S, then $g^{[\boldsymbol{v}]} := g_1^{[\boldsymbol{v}_1]}$ is as required. Otherwise, if $t_1(g_1^{[\boldsymbol{v}_1]})$ is rewritable by S then we repeat the above process and obtain a chain

$$f^{[\boldsymbol{u}]} >_S g_0^{[\boldsymbol{v}_0]} >_S g_1^{[\boldsymbol{v}_1]} >_S g_2^{[\boldsymbol{v}_2]} >_S \cdots$$

where each g_i is rewritable by $g_{i+1}^{[\boldsymbol{v}_{i+1}]} \in S$. Since S is finite, the above chain contains only finitely many g_i, say it ends with $g_n^{[\boldsymbol{v}_n]}$ for some $n \in \mathbb{N}$. Then $g^{[\boldsymbol{v}]} := g_n^{[\boldsymbol{v}_n]}$ is as required. ■

The following is a key lemma for deriving the criterion for strong Gröbner-Shirshov bases (Theorem 4.3.10). Roughly speaking, this lemma tells us that, among elements with the same signature, a nonrewritable one has a minimal leading monomial.

Lemma 4.3.9 *Let $\boldsymbol{t}$ be a monomial in A^m and let G be a $\boldsymbol{t}$-strong Gröbner-Shirshov basis of I with a partial order $<_G$. Suppose that every regular critical pair of G is rewritable by G. For any $t_0 \in \mathcal{M}$ and $f_0^{[\boldsymbol{u}_0]} \in G$ with $\operatorname{lm}(t_0\boldsymbol{u}_0) \leq \boldsymbol{t}$, if $t_0(f_0^{[\boldsymbol{u}_0]}])$ is not rewritable by G, then $\operatorname{lm}(t_0 f_0) \leq \operatorname{lm}(f)$ for any $f^{[\boldsymbol{u}]} \in I \times A^m$ with $\operatorname{lm}(\boldsymbol{u}) = \operatorname{lm}(t_0\boldsymbol{u_0})$.*

Proof. By way of contradiction, we assume that $N \neq \emptyset$, where

$$\begin{aligned} N = \{(t_0, f_0^{[\boldsymbol{u}_0]}) \in \mathcal{M} \times G : \operatorname{lm}(t_0\boldsymbol{u}_0) \leq \boldsymbol{t},\ t_0(f_0^{[\boldsymbol{u}_0]}]) \text{ not rewritable by } G, \\ \operatorname{lm}(t_0 f_0) > \operatorname{lm}(f) \text{ for some } f^{[\boldsymbol{u}]} \in I \times A^m \text{ with } \operatorname{lm}(\boldsymbol{u}) = \operatorname{lm}(t_0\boldsymbol{u_0})\}. \end{aligned}$$

Suppose $(t_0, f_0^{[\boldsymbol{u}_0]}) \in N$ with minimal $\mathrm{lm}(t_0\boldsymbol{u}_0)$ among N and suppose $t_0 = x^\alpha$. Then there exists an $f^{[\boldsymbol{u}]} \in I \times A^m$ such that $\mathrm{lm}(\boldsymbol{u}) = \mathrm{lm}(t_0\boldsymbol{u_0})$ and $\mathrm{lm}(t_0 f_0) > \mathrm{lm}(f)$. Let $\overline{f}^{[\overline{\boldsymbol{u}}]} = t_0(f_0^{[\boldsymbol{u}_0]}) - cf^{[\boldsymbol{u}]} \in I \times A^m$ where $c = \frac{\sigma^\alpha(\mathrm{lc}(\boldsymbol{u}_0))}{\mathrm{lc}(\boldsymbol{u})}$. Then

$$\mathrm{lm}(\overline{f}) = \mathrm{lm}(t_0 f_0) \text{ and } \mathrm{lm}(\overline{\boldsymbol{u}}) < \mathrm{lm}(t_0\boldsymbol{u}_0) \leq \boldsymbol{t}.$$

Since G is a $\boldsymbol{t}$-strong Gröbner-Shirshov basis, by Lemma 4.3.5, there exist $g^{[\boldsymbol{v}]} \in G$ and $t_g \in \mathcal{M}$ such that $\mathrm{lm}(t_g g) = \mathrm{lm}(\overline{f})$ and $\mathrm{lm}(t_g\boldsymbol{v}) \leq \mathrm{lm}(\overline{\boldsymbol{u}})$. Let

$$D = \{(t_g, g^{[\boldsymbol{v}]}) \in \mathcal{M} \times G : \mathrm{lm}(t_g g) = \mathrm{lm}(\overline{f}),\ \mathrm{lm}(t_g\boldsymbol{v}) \leq \mathrm{lm}(\overline{\boldsymbol{u}})\}.$$

Suppose $(t_g, g^{[\boldsymbol{v}]})$ is a minimal pair in D, i.e., there is no pair $(t_{g'}, g'^{[\boldsymbol{v}']}) \in D$ such that either $\mathrm{lm}(t_{g'}\boldsymbol{v}') < \mathrm{lm}(t_g\boldsymbol{v})$, or $\mathrm{lm}(t_{g'}\boldsymbol{v}') = \mathrm{lm}(t_g\boldsymbol{v})$ and $g'^{[\boldsymbol{v}']} <_G g^{[\boldsymbol{v}]}$.

We claim that $(\overline{t_0}, f_0^{[\boldsymbol{u}_0]}, \overline{t_g}, g^{[\boldsymbol{v}]})$ is a regular critical pair of $f_0^{[\boldsymbol{u}_0]}$ and $g^{[\boldsymbol{v}]}$, where

$$\overline{t_0} = \frac{\mathrm{lcm}(\mathrm{lm}(f_0), \mathrm{lm}(g))}{\mathrm{lm}(f_0)} \text{ and } \overline{t_g} = \frac{\mathrm{lcm}(\mathrm{lm}(f_0), \mathrm{lm}(g))}{\mathrm{lm}(g)}.$$

To obtain a contradiction, we assume that $\mathrm{lm}(\overline{t_0}\boldsymbol{u}_0) \leq \mathrm{lm}(\overline{t_g}\boldsymbol{v})$. Note that $\mathrm{lm}(t_0 f_0) = \mathrm{lm}(t_g g)$ is a multiple of $\mathrm{lcm}(\mathrm{lm}(f_0), \mathrm{lm}(g)) = \mathrm{lm}(\overline{t_0} f_0) = \mathrm{lm}(\overline{t_g} g)$. Thus $\overline{t_0}$ divides t_0, $\overline{t_g}$ divides t_g, and $t_0/\overline{t_0} = t_g/\overline{t_g}$. Hence

$$\mathrm{lm}((t_0/\overline{t_0})\,\mathrm{lm}(\overline{t_0}\boldsymbol{u}_0)) = \mathrm{lm}((t_g/\overline{t_g})\,\mathrm{lm}(\overline{t_0}\boldsymbol{u}_0)) \leq \mathrm{lm}((t_g/\overline{t_g})\,\mathrm{lm}(\overline{t_g}\boldsymbol{v})),$$

i.e., $\mathrm{lm}(t_0\boldsymbol{u}_0)) \leq \mathrm{lm}(t_g\boldsymbol{v})$, contradicting the fact $\mathrm{lm}(t_g\boldsymbol{v}) \leq \mathrm{lm}(\overline{\boldsymbol{u}}) < \mathrm{lm}(t_0\overline{\boldsymbol{u}_0})$. Hence our claim is true.

By the hypothesis of the lemma, the regular critical pair $(\overline{t_0}, f_0^{[\boldsymbol{u}_0]}, \overline{t_g}, g^{[\boldsymbol{v}]})$ is rewritable by G, i.e., either $\overline{t_0}(f_0^{[\boldsymbol{u}_0]})$ or $\overline{t_g}(g^{[\boldsymbol{v}]})$ is rewritable by G. Since $\overline{t_0}$ divides t_0, if $\overline{t_0}(f_0^{[\boldsymbol{u}_0]})$ is rewritable by G then so is $t_0(f_0^{[\boldsymbol{u}_0]})$, which is a contradiction. Thus

$\overline{t_g}(g^{[\boldsymbol{v}]})$ is rewritable by G and hence so is $t_g(g^{[\boldsymbol{v}]})$. By Lemma 4.3.8, there exist $g_0^{[\boldsymbol{v}_0]} \in G$ and $t_0' \in \mathcal{M}$ such that $\mathrm{lm}(t_0'\boldsymbol{v}_0) = \mathrm{lm}(t_g\boldsymbol{v})$, $g_0^{[\boldsymbol{v}_0]} <_G g^{[\boldsymbol{v}]}$, and $t_0'(g_0^{[\boldsymbol{v}_0]})$ is not rewritable by G. Now we claim that $\mathrm{lm}(t_0'g_0) \leq \mathrm{lm}(t_g g)$. Otherwise, if $\mathrm{lm}(t_0'g_0) > \mathrm{lm}(t_g g)$, then it is easy to see that $(t_0', g_0^{[\boldsymbol{v}_0]}) \in N$ (note that $t_g(g^{[\boldsymbol{v}]}) \in I$ and $\mathrm{lm}(t_0'\boldsymbol{v}_0) = \mathrm{lm}(t_g\boldsymbol{v}) \leq \mathrm{lm}(\overline{\boldsymbol{u}}) < \boldsymbol{t}$). But, $\mathrm{lm}(t_0'\boldsymbol{v}_0) = \mathrm{lm}(t_g\boldsymbol{v}) < \mathrm{lm}(t_0\boldsymbol{u}_0)$, contradicting the fact that $(t_0, f_0^{[\boldsymbol{u}_0]})$ has minimal $\mathrm{lm}(t_0\boldsymbol{u}_0)$ among N. Thus our claim holds true.

Now we have two cases to consider: $\mathrm{lm}(t_0'g_0) = \mathrm{lm}(t_g g)$ and $\mathrm{lm}(t_0'g_0) < \mathrm{lm}(t_g g)$. Our goal is to deduce a contradiction for each case and thus end the proof of the lemma. If $\mathrm{lm}(t_0'g_0) = \mathrm{lm}(t_g g) = \mathrm{lm}(\overline{f})$, since $\mathrm{lm}(t_0'\boldsymbol{v}_0) = \mathrm{lm}(t_g\boldsymbol{v}) \leq \mathrm{lm}(\overline{\boldsymbol{u}})$, we have $(t_0', g_0^{[\boldsymbol{v}_0]}) \in D$. By the minimality of $(t_g, g^{[\boldsymbol{v}]})$ among D, we have $g^{[\boldsymbol{v}]} \leq_G g_0^{[\boldsymbol{v}_0]}$, which contradicts the fact that $g_0^{[\boldsymbol{v}_0]} <_G g^{[\boldsymbol{v}]}$. Now consider the second case: $\mathrm{lm}(t_0'g_0) < \mathrm{lm}(t_g g)$. Let

$$\overline{g}^{[\overline{\boldsymbol{v}}]} = t_g(g^{[\boldsymbol{v}]}) - ct_0'(g_0^{[\boldsymbol{v}_0]}) \in G, \quad c = \frac{\sigma^{\exp(t_g)}\,\mathrm{lc}(\boldsymbol{v})}{\sigma^{\exp(t_0')}\,\mathrm{lc}(\boldsymbol{v}_0)}.$$

Then $\mathrm{lm}(\overline{g}) = \mathrm{lm}(t_g g)$ and $\mathrm{lm}(\overline{\boldsymbol{v}}) < \mathrm{lm}(t_g\boldsymbol{v}) < \mathrm{lm}(t_0\boldsymbol{u}_0) \leq \boldsymbol{t}$. Since G is a $\boldsymbol{t}$-strong Gröbner-Shirshov basis, by Lemma 4.3.5, there exist $h^{[\boldsymbol{w}]} \in G$ and $t_h \in \mathcal{M}$ such that $\mathrm{lm}(t_h h) = \mathrm{lm}(\overline{g}) = \mathrm{lm}(t_g g) = \mathrm{lm}(t_0 f_0)$ and $\mathrm{lm}(t_h\boldsymbol{w}) \leq \mathrm{lm}(\overline{\boldsymbol{v}}) < \mathrm{lm}(t_g\boldsymbol{v}) \leq \mathrm{lm}(\overline{\boldsymbol{u}})$. Thus, $h^{[\boldsymbol{w}]} \in D$. But then the inequality $\mathrm{lm}(t_h\boldsymbol{w}) < \mathrm{lm}(t_g\boldsymbol{v})$ implies that $(t_g, g^{[\boldsymbol{v}]})$ is not minimal in D, which is a contradiction. ■

The following theorem gives a criterion for strong Gröbner-Shirshov bases.

Theorem 4.3.10 *Let A be a skew solvable polynomial ring and let I be a left ideal of A generated by $m \in \mathbb{N}$ elements. Suppose that $G = \{g_i^{[\boldsymbol{u}_i]} : 1 \leq i \leq s\} \subseteq I \times A^m$ with a partial order $<_G$, where $s \in \mathbb{N}$. Then G is a strong Gröbner-Shirshov basis of I if the following conditions hold:*

(i) For any $1 \leq i \leq m$, there exists a $g^{[\boldsymbol{u}]} \in G$ such that $\mathrm{lm}(\boldsymbol{u}) = \boldsymbol{e}_i$.

(ii) Every regular critical pair of elements from G is rewritable by G with respect to

$<_G$.

Proof. (By contradiction.) Suppose G is not a strong Gröbner-Shirshov basis, i.e., $N \neq \emptyset$ where

$$N = \{f^{[\boldsymbol{u}]} \in I \times A^m : \text{ there exist no } (t, g^{[\boldsymbol{v}]}) \in \mathcal{M} \times G \text{ such that}$$
$$\operatorname{lm}(t\boldsymbol{v}) = \operatorname{lm}(\boldsymbol{u}), \operatorname{lm}(tg) \leq \operatorname{lm}(f)\}.$$

Let $f^{[\boldsymbol{u}]} \in N$ with the minimal signature $\operatorname{lm}(\boldsymbol{u})$ among N. Suppose $\operatorname{lm}(\boldsymbol{u}) = t\boldsymbol{e}_j$ for some $t \in \mathcal{M}$ and $1 \leq j \leq m$. Then G is a $t\boldsymbol{e}_j$-strong Gröbner-Shirshov basis. By condition (i) of the theorem, there exists a $g^{[\boldsymbol{v}]} \in G$ such that $\operatorname{lm}(\boldsymbol{v}) = \boldsymbol{e}_j$. Then $\operatorname{lm}(t\boldsymbol{v}) = \operatorname{lm}(\boldsymbol{u})$. If $t(g^{[\boldsymbol{v}]})$ is rewritable by G, then there exist $f_1^{[\boldsymbol{v}_1]} \in G$ and $t_1 \in \mathcal{M}$ such that $\operatorname{lm}(t_1\boldsymbol{v}_1) = \operatorname{lm}(t\boldsymbol{v}) = \operatorname{lm}(\boldsymbol{u})$ and $f_1^{[\boldsymbol{v}_1]} <_G g^{[\boldsymbol{v}]}$. Repeating this process and by a similar argument as in the proof of Lemma 4.3.8, we can prove that there exist $h^{[\boldsymbol{w}]} \in G$ and $s \in \mathcal{M}$ such that $\operatorname{lm}(s\boldsymbol{w}) = \operatorname{lm}(\boldsymbol{u})$ and $s(h^{[\boldsymbol{w}]})$ is not rewritable by G. Applying Lemma 4.3.9 gives that $\operatorname{lm}(sh) \leq \operatorname{lm}(f)$. But the facts $\operatorname{lm}(s\boldsymbol{w}) = \operatorname{lm}(\boldsymbol{u})$ and $f^{\boldsymbol{u}} \in N$ imply that $\operatorname{lm}(sh) > \operatorname{lm}(f)$, which is a contradiction. ■

4.4 A Signature-based Algorithm

In this section, we present a signature-based algorithm for computing a strong Gröbner-Shirshov basis in skew solvable polynomial rings.

As before, let $A = k\langle x; \sigma, \delta, c, p\rangle$ be a skew solvable polynomial ring over k, $f_1, \ldots, f_m \in A$, $m \in \mathbb{N}$, and let I be the left ideal of A generated by $f_1, \ldots, f_m$.

Suppose $f^{[\boldsymbol{u}]}, g^{[\boldsymbol{v}]} \in I \times A^m$. We say $f^{[\boldsymbol{u}]}$ is *reducible* by $g^{[\boldsymbol{v}]}$ if there exists a $t \in \mathcal{M}$ such that $\operatorname{lm}(tg) = \operatorname{lm}(f)$ and $\operatorname{lm}(t\boldsymbol{v}) < \operatorname{lm}(\boldsymbol{u})$. Moreover, if $G \subseteq A \times A^m$ and $g^{[\boldsymbol{v}]} \in G$, then $f^{[\boldsymbol{u}]} \to_G f^{[\boldsymbol{u}]} - ct(g^{[\boldsymbol{v}]})$ is said to be a *one-step-reduction* by G where $c = \operatorname{lc}(f)/\operatorname{lc}(tg)$. If $f'^{[\boldsymbol{u}']}$ is obtained from $f^{[\boldsymbol{u}]}$ by finitely many one-step-reductions by G and $f'^{[\boldsymbol{u}']}$ is not reducible by G, then we say that $f'^{[\boldsymbol{u}']}$ is a *remainder* of $f^{[\boldsymbol{u}]}$ modulo G.

The following lemma follows directly from the above definitions.

Lemma 4.4.1 *Suppose that* $f'^{[\boldsymbol{u}']}$ *is a remainder of* $f^{[\boldsymbol{u}]}$ *modulo* G*. Then* $\mathrm{lm}(f') < \mathrm{lm}(f)$ *and* $\mathrm{lm}(\boldsymbol{u}') = \mathrm{lm}(\boldsymbol{u})$*.*

Now we are in a position to state our main algorithm.

Algorithm 4.4.2 (Algorithm for strong Gröbner bases)

Input: $F = \{f_1^{[\boldsymbol{e}_1]}, \ldots, f_m^{[\boldsymbol{e}_m]}\} \subseteq A \times A^m$

Output: A strong Gröbner-Shirshov basis G of the left ideal I of A generated by F.

1. $G := F$
2. CPairs:= $\{$regular critical pair $(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]}) : f^{[\boldsymbol{u}]}, g^{[\boldsymbol{v}]} \in G\}$
3. **While** CPairs$\neq \emptyset$ **Do**
4. Choose $(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]}) \in$ CPairs
5. CPairs:=CPairs $\setminus\{(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]})\}$
6. **If** $(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]})$ is not rewritable by G **then**
7. $\quad h^{[\boldsymbol{w}]} :=$ a remainder of SPoly$(f^{[\boldsymbol{u}]}, g^{[\boldsymbol{v}]})$ modulo G
8. $\quad$ CPairs := CPairs $\cup\{$regular critical pair $(t_h, h^{[\boldsymbol{w}]}, t_{h'}, h'^{[\boldsymbol{w}']}) : h'^{[\boldsymbol{w}']} \in G\}$
   $\cup\,\{$regular critical pair $(t_{h'}, h'^{[\boldsymbol{w}']}, t_h, h^{[\boldsymbol{w}]}) : h'^{[\boldsymbol{w}']} \in G\}$
9. $\quad G := G \cup \{h^{[\boldsymbol{w}]}\}$
10. **End If**
11. **End Do**
12. **Return** G

Note that in Line 6 of the above algorithm, a partial order on G is needed. The GVW-orders implied by the criterion in [11] will be used in our algorithm, which can be updated automatically when a new element is added to G, i.e., when $G := G \cup \{h^{[\boldsymbol{w}]}\}$ in the algorithm.

Definition 4.4.3 *A partial order $<_G$ on $G \subseteq I \times A^m$ is called a* GVW-order *if, for any $f^{[\boldsymbol{u}]}, g^{[\boldsymbol{v}]} \in G$, we have $f^{[\boldsymbol{u}]} <_G g^{[\boldsymbol{v}]}$ whenever one of the following conditions hold:*

(a) $\mathrm{lm}(t'g) < \mathrm{lm}(tf)$ *where* $t' = \frac{\mathrm{lcm}(\mathrm{lm}(\boldsymbol{u}),\mathrm{lm}(\boldsymbol{v}))}{\mathrm{lm}(\boldsymbol{v})}$ *and* $t = \frac{\mathrm{lcm}(\mathrm{lm}(\boldsymbol{u}),\mathrm{lm}(\boldsymbol{v}))}{\mathrm{lm}(\boldsymbol{u})}$.

(b) $\mathrm{lm}(t'g) = \mathrm{lm}(tf)$ *and $g^{[\boldsymbol{v}]}$ is added to G later than $f^{[\boldsymbol{u}]}$.*

Theorem 4.4.4 *If a GVW-order is used in the Rewriting Criterion of Algorithm 4.4.2, then the algorithm terminates after finitely many steps and returns a strong Gröbner-Shirshov basis of I.*

Proof. (Correctness.) If the algorithm terminates after finitely many steps, then its correctness follows clearly from Theorem 4.3.10.

(Termination.) Similarly to [20], we introduce a map $\varphi : A \times A^m \to k[Y, Z, W]$ to investigate the termination of the algorithm, where $Y = \{y_1, \ldots, y_n\}$, $Z = \{z_1, \ldots, z_m\}$, $W = \{w_0, \ldots, w_n\}$, and $k[Y, Z, W]$ denotes the polynomial algebra over k with indeterminates $Y \cup Z \cup W$. Define $\varphi : A \times A^m \to k[Y, W, Z]$ as follows: for $(f, \boldsymbol{u}) \in A \times A^m$ with $\mathrm{lm}(\boldsymbol{u}) = x^\alpha \boldsymbol{e}_i$ and $\mathrm{lm}(f) = x^\beta$, where $\alpha, \beta \in \mathbb{N}^n$ and $1 \le i \le m$, let

$$\varphi(f, \boldsymbol{u}) = \begin{cases} y^\alpha z_i = y_1^{\alpha_1} \cdots y_n^{\alpha_n} z_i, & \text{if } f = 0, \\ y^\alpha z_i w_0 w^\beta = y_1^{\alpha_1} \cdots y_n^{\alpha_n} z_i w_0 w_1^{\beta_1} \cdots w_n^{\beta_n}, & \text{if } f \neq 0. \end{cases}$$

Suppose that $(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]})$ is a regular critical pair and not rewritable by G with respect to a GVW-order $<_G$, and that $h^{[\boldsymbol{w}]}$ is a remainder of $h'^{[\boldsymbol{w}']}$ modulo G where $h'^{[\boldsymbol{w}']} = \mathrm{SPoly}(f^{[\boldsymbol{u}]}, g^{[\boldsymbol{v}]})$ (and thus $\boldsymbol{w}' = t_f \boldsymbol{u} - t_g \boldsymbol{v}$). We claim that $\varphi(h^{[\boldsymbol{w}]})$ is not divisible by $\varphi(h_0^{[\boldsymbol{w}_0]})$ for any $h_0^{[\boldsymbol{w}_0]} \in G$. Otherwise, we assume that $\varphi(h^{[\boldsymbol{w}]})$ is divisible by $\varphi(h_0^{[\boldsymbol{w}_0]})$ for some $h_0^{[\boldsymbol{w}_0]} \in G$. Now we have the following three cases and we deduce a contradiction for each case, which ends the proof of the claim.

Case (1): $h_0 = 0$. In this case, it is easy to see from the definition of φ that $\operatorname{lm}(\boldsymbol{w}_0)$ divides $\operatorname{lm}(\boldsymbol{w})$. Then $\operatorname{lm}(s\boldsymbol{w}_0) = \operatorname{lm}(\boldsymbol{w})$ for some monomial $s \in \mathcal{M}$. Note that $\operatorname{lm}(\boldsymbol{w}') = \operatorname{lm}(t_f\boldsymbol{u})$ since $(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]})$ is regular. Thus, from Lemma 4.4.1, $\operatorname{lm}(s\boldsymbol{w}_0) = \operatorname{lm}(\boldsymbol{w}) = \operatorname{lm}(\boldsymbol{w}') = \operatorname{lm}(t_f\boldsymbol{u})$. Recall that the GVW-order $<_G$ is used in the algorithm and $\operatorname{lm}(sh_0) = 0 < \operatorname{lm}(t_f f)$. Thus, $t_f(f^{[\boldsymbol{u}]})$ is rewritable by $h_0^{[\boldsymbol{w}_0]}$, which is a contradiction.

Case (2): $h_0 \neq 0$ and $h = 0$. From the definition of φ, it is impossible that $\varphi(h_0^{[\boldsymbol{w}_0]})$ divides $\varphi(h^{[\boldsymbol{w}]})$.

Case (3): $h_0 \neq 0$ and $h \neq 0$. Let $s = \operatorname{lm}(\boldsymbol{w})/\operatorname{lm}(\boldsymbol{w}_0)$ and $t = \operatorname{lm}(h)/\operatorname{lm}(h_0)$. If $s \leq t$, then, by Lemmas 4.3.6 and 4.4.1, we have that $\operatorname{lm}(sh_0) \leq \operatorname{lm}(th_0) = \operatorname{lm}(h) < \operatorname{lm}(t_f f)$ and $\operatorname{lm}(s\boldsymbol{w}_0) = \operatorname{lm}(\boldsymbol{w}) = \operatorname{lm}(\boldsymbol{w}') = \operatorname{lm}(t_f\boldsymbol{u})$. Suppose that

$$s' = \frac{\operatorname{lcm}(\operatorname{lm}(\boldsymbol{w}_0), \operatorname{lm}(\boldsymbol{u}))}{\operatorname{lm}(\boldsymbol{w}_0)} \quad \text{and } t'_f = \frac{\operatorname{lcm}(\operatorname{lm}(\boldsymbol{w}_0), \operatorname{lm}(\boldsymbol{u}))}{\operatorname{lm}(\boldsymbol{u})}.$$

Then s' divides s, t'_f divides t_f, and $s/s' = t_f/t'_f$. Hence $\operatorname{lm}(s'h_0) < \operatorname{lm}(t'_f f)$ (otherwise, $\operatorname{lm}(s'h_0) < \operatorname{lm}(t'_f f)$ implies $\operatorname{lm}((s/s')s'h_0) < \operatorname{lm}((t_f/t'_f)t'_f f)$, i.e., $\operatorname{lm}(sh_0) < \operatorname{lm}(t_f f)$, a contradiction). Since $<_G$ is a GVW-order, it follows from Definition 4.4.3 that $h_0^{[\boldsymbol{w}_0]} <_G f^{[\boldsymbol{u}]}$. Thus $t_f(f^{[\boldsymbol{u}]})$ is rewritable by $h_0^{[\boldsymbol{w}_0]}$, which is a contradiction. Now suppose $s > t$. Then $\operatorname{lm}(th_0) = \operatorname{lm}(h)$ and $\operatorname{lm}(t\boldsymbol{w}_0) < \operatorname{lm}(s\boldsymbol{w}_0) = \operatorname{lm}(\boldsymbol{w})$. Hence, $h^{[\boldsymbol{w}]}$ is reducible by the set $\{h_0^{[\boldsymbol{w}_0]}\} \subset G$ and thus by G, which contradicts the assumption that $h^{[\boldsymbol{w}]}$ is a remainder modulo G.

Now return to the proof of the termination of the algorithm. In the "While Loop" of the algorithm (Lines 3–11), if $(t_f, f^{[\boldsymbol{u}]}, t_g, g^{[\boldsymbol{v}]})$ is regular and not rewritable by G with respect to $<_G$, then $h^{[\boldsymbol{w}]}$ is added to G, and the new G is denoted as

$G' = G \cup \{h^{[\boldsymbol{w}]}\}$. From the above claim, the ideal (of $k[Y, Z, W]$) generated by $\varphi(G)$ is strictly contained in the ideal generated by $\varphi(G')$. By the Hilbert basis theorem of polynomial algebras, after finitely many repeats of the while loop, every critical pair in CPairs is regular and thus the algorithm terminates. ∎

In summary, a signature-based algorithm for computing Gröbner-Shirshov bases in skew solvable polynomial rings over a field has been presented in this chapter. This algorithm can detect redundant S-polynomials (i.e., the S-polynomials corresponding to nonregular critical pairs) and therefore it is more efficient than Buchberger's algorithm. The implementation of the proposed algorithms in a computer algebra system (e.g., Maple, and Singular) and computing examples will be discussed in the near future.

Bibliography

[1] W. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, 1994.

[2] L. A. Bokut', Yuqun Chen, and K. P. Shum, *Some new results on Gröbner-Shirshov bases*, Proceedings of International Conference on Algebra 2010–Advances in Algebraic Structures (W. Hemakul, S. Wahyuni, and P. W. Sy, eds.), 2012, pp. 53–102.

[3] B. Buchberger, *Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal*, Ph.D. thesis, University of Innsbruck, 1965.

[4] J. L. Bueso, J. Gómez-Torrecillas, and A. Verschoren, *Algorithmic methods in non-commutative algebra: Applications to quantum groups*, Mathematical Modelling: Theory and Applications, vol. 17, Springer, 2003.

[5] F. Chyzak and B. Salvy, *Non-commutative elimination in Ore algebras proves multivariate identities*, J. Symbolic Comput. **26** (1998), no. 2, 187–227.

[6] J. C. Faugère, *A new efficient algorithm for computing Gröbner bases (F4)*, J. Pure Appl. Algebra **139** (1999), no. 1, 61–88.

[7] ______, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ACM, 2002, pp. 75–83.

[8] C. Gallego and O. Lezama, *Gröbner bases for ideals of σ-PBW extensions*, Comm. Algebra **39** (2011), no. 1, 50–75.

[9] A. Galligo, *Some algorithmic questions on ideals of differential operators*, EUROCAL'85, Springer, 1985, pp. 413–421.

[10] S. Gao, Y. Guan, and F. Volny IV, *A new incremental algorithm for computing Gröbner bases*, Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, ACM, 2010, pp. 13–19.

[11] S. Gao, F. Volny IV, and M. Wang, *A new algorithm for computing Gröbner bases*, Cryptology ePrint Archive (2010).

[12] M. Giesbrecht, G. Reid, and Yang Zhang, *Non-commutative Gröbner bases in Poincaré-Birkhoff-Witt extensions*, Computer Algebra in Scientific Computing (CASC), 2002.

[13] M. Insa and F. Pauer, *Gröbner bases in rings of differential operators*, London Math. Soc. Lecture Note Ser. (1998), 367–380.

[14] A. Kandri-Rody and V. Weispfenning, *Non-commutative Gröbner bases in algebras of solvable type*, J. Symbolic Comput. **9** (1990), no. 1, 1–26.

[15] V. Levandovskyy and H. Schönemann, *Plural: a computer algebra system for noncommutative polynomial algebras*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 176–183.

[16] X. Ma, Y. Sun, and D. Wang, *On computing Gröbner bases in rings of differential operators*, Sci. China Math. **54** (2011), no. 6, 1077–1087.

[17] E. L. Mansfield and A. Szanto, *Elimination theory for differential difference polynomials*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 191–198.

[18] S.-Q. Oh, *Catenarity in a class of iterated skew polynomial rings*, Comm. Algebra **25** (1997), no. 1, 37–49.

[19] A. I. Shirshov, *Some algorithmic problems for Lie algebras*, Sibirsk. Mat. Zh. **3** (1962), no. 2, 292–296.

[20] Y. Sun, D. Wang, X. Ma, and Y. Zhang, *A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras*, Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation, ACM, 2012, pp. 351–358.

[21] Yang Zhang and Xiangui Zhao, *Gelfand-Kirillov dimension of differential difference algebras*, LMS J. Comput. Math. **17** (2014), no. 1, 485–495.

[22] M. Zhou and F. Winkler, *On computing Gröbner bases in rings of differential operators with coefficients in a ring*, Math. Comput. Sci. **1** (2007), no. 2, 211–223.

Chapter 5

Conclusion and Future Work

In this thesis, we investigate the theories, algorithms, and applications of Gröbner-Shirshov bases of differential difference algebras and skew solvable polynomial rings.

Chapter 2 gives both upper and lower bounds of the Gelfand-Kirillov dimension of a differential difference algebra (Theorem 2.3.9). Particularly, the Gelfand-Kirillov dimension of a differential difference algebra A of type (m, n) over a finite field extension of the base field k is $m + n$. This particular result implies that the Gelfand-Kirillov dimension of a finitely generated A-module M is at most $m + n$ and gives an insight into the computation of $\mathrm{GKdim}(M)$, which is studied in Chapter 3 by using the Gröbner-Shirshov basis method.

In Chapter 3, we generalize the Gröbner-Shirshov basis theory of differential difference algebras to any left admissible ordering and develop the Gröbner-Shirshov basis theory for finitely generated free modules over differential difference algebras. As an application, we use the generalized theory to compute the Gelfand-Kirillov dimensions of cyclic modules (Theorem 3.4.4) and (more generally) finitely generated modules (Algorithm 3.6.3) over differential difference algebras.

In Chapter 4, we study algorithms of Gröbner-Shirshov bases in skew solvable polynomial rings. We propose a signature-based algorithm (Algorithm 4.4.2) for the computation of Gröbner-Shirshov bases. Our algorithm can detect redundant reductions and thus it is more efficient than the traditional Buchberger algorithm.

With the above findings, this thesis provides theoretical and algorithmic contributions to knowledge in its research area.

Based on the results we obtained, we propose the following possible future work.

(i). Implement Algorithms 3.6.3 and 4.4.2 in computer algebra systems, for example, Maple and Singular. Analyse the efficiency of Algorithm 4.4.2 by experimental data.

One of the challenges here is how to present the noncommutative structure of differential difference algebras and skew solvable polynomial rings in a computer algebra system.

(ii). Apply the Gröbner-Shirshov basis theory of differential difference algebras developed in Chapter 3 to simplify/solve differential difference equations.

It is well-known that Gröbner-Shirshov basis theory of differential algebras can be applied to solve differential equations (see, for example, [4]). Similarly, computational properties of differential difference algebras can be applied to differential difference equations. Using algorithms obtained in Chapter 3, we can compute Gröbner-Shirshov bases and simplify given differential difference systems. Then it will be easier to find solutions or investigate properties of solutions for the given systems.

(iii). Apply Gröbner-Shirshov basis theory of differential difference algebras to homological computations.

Gröbner-Shirshov basis theory has some applications in homological computations, for example, computing free resolutions [3] and Ext modules [2]. It is also possible to study free resolutions and Ext modules of differential difference algebras.

(iv). Develop theories and applications of Gröbner-Shirshov bases for differential difference algebras over rings.

Many of the basic techniques we used in Chapter 3 will become more complicated for a differential difference algebra over a ring, because we now have to deal with ideas of coefficients in a ring where we cannot do division and deduction as in Section 3.3. Then we need other technique (e.g., the method of syzygy as used in Chapter 4 of [1]) to construct a reduction algorithm.

Bibliography

[1] W. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, 1994.

[2] J. L. Bueso, J. Gómez-Torrecillas, and F. J. Lobillo, *Homological computations in PBW modules*, Algebr. Represent. Theory **4** (2001), no. 3, 201–218.

[3] V. Dotsenko and A. Khoroshkin, *Free resolutions via Gröbner bases*, arXiv preprint: 0912.4895 (2009).

[4] M. Saito, B. Sturmfels, and N. Takayama, *Gröbner deformations of hypergeometric differential equations*, Springer, 1999.