# Elimination Theory for Differential Difference Polynomials

E.L. Mansfield
Institute of Mathematics and Statistics
University of Kent
Canterbury, United Kingdom
E.L.Mansfield@ukc.ac.uk

A. Szanto*
Department of Mathematics
North Carolina State University
Raleigh, NC, USA
aszanto@ncsu.edu

## ABSTRACT

In this paper we give an elimination algorithm for differential difference polynomial systems. We use the framework of a generalization of Ore algebras, where the independent variables are non-commutative. We prove that for certain term orderings, Buchberger's algorithm applied to differential difference systems terminates and produces a Gröbner basis. Therefore, differential-difference algebras provide a new instance of non-commutative graded rings which are effective Gröbner structures.

## Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms—*algebraic algorithms*

## General Terms

Algorithms

## Keywords

difference equation, differential polynomial, Gröbner basis, Ore algebra

## 1. INTRODUCTION

Let us consider the following problem, which arises in the calculation of symmetries of discrete systems (cf. [11]):
Find a function $F_n = F(n, u_n, u_{n+1}, u_{n+2})$ which for all $n \in \mathbb{N}$ satisfies

$$\begin{aligned} F_{n+3} &= 2F_{n+1} - F_n \\ \tfrac{\partial F_n}{\partial u_{n+2}} &= 0 \\ u_{n+3} &= 2u_{n+1} - u_n. \end{aligned} \tag{1}$$

As we shall see in Example 4.11, by symbolic elimination methods presented in this paper we are able to derive that the solution of (1) must have the form

$$F_n = c_0 u_n + c_1 u_{n+1} + c_2(n) \tag{2}$$

where $c_0$ and $c_1$ are absolute constants and $c_2$ satisfies

$$c_2(n+3) - 2c_2(n+1) + c_2(n) = 0.$$

More generally, let us consider systems of the following type:

$$\begin{aligned} &\mathcal{D}_j\ F(n, u_n, u_{n+1}, \ldots, u_{n+M}) = 0 \quad j = 1, \ldots, p \\ &u_{n+M+1} = \omega(n, u_n, u_{n+1}, \ldots, u_{n+M}). \end{aligned} \tag{3}$$

Here $F$ is the unknown function, $\omega \in \mathbb{Q}(n, u_n, \ldots, u_{n+M})$ is given such that $\frac{\partial \omega}{\partial u_n} \neq 0$, and $\mathcal{D}_j$ are linear operators of the form

$$\mathcal{D}_j = \sum_{\alpha_0, \ldots, \alpha_M, \beta} c_{\vec{\alpha}, \beta} \circ s^\beta \circ \frac{\partial^{\alpha_0 + \cdots + \alpha_n}}{\partial u_n^{\alpha_0} \cdots \partial u_{n+M}^{\alpha_M}} \tag{4}$$

where $c_{\vec{\alpha}, \beta} \in \mathbb{Q}(n, u_{n+t} : t \in \mathbb{Z})$ are *multiplication operators* and $s$ is the *shift operator* defined by

$$s(n) = n + 1, \quad s(u_l) = u_{l+1}. \tag{5}$$

The aim is to find compatibility conditions of (3). These compatibility conditions greatly simplify the computation of the solutions of (3).

A natural approach is to consider operators in (4) as elements of the free non-commutative algebra over the field $\mathbb{Q}(n, u_{n+t} : t \in \mathbb{Z})$ generated by the *operator variables*

$$\{S, D_n, \ldots, D_{n+M}\} \text{ for some } M \in \mathbb{N}$$

where $S$ denotes the shift operator $s$ and $D_{n+t}$ denotes the differential operator $D_{n+t} := \frac{\partial}{\partial u_{n+t}}$ for $0 \leq t \leq M$. Then we have the following commutation relations:

$$\begin{aligned} D_{n+t} \circ S &= S \circ D_{n+t-1} + \tfrac{\partial \omega}{\partial u_{n+t}} \circ S \circ D_{n+M} \quad t \neq 0 \\ D_n \circ S &= \tfrac{\partial \omega}{\partial u_{n+t}} \circ S \circ D_{n+M} \\ D_{n+t} \circ D_{n+t'} &= D_{n+t'} \circ D_{n+t} \\ S \circ p &= s(p) \circ S \\ D_{n+t} \circ p &= p \circ D_{n+t} + \tfrac{\partial p}{\partial u_{n+t}} \end{aligned} \tag{6}$$

for any $p \in \mathbb{Q}(n, u_{n+t} : t \in \mathbb{Z})$ and $0 \leq t, t' \leq M$.

Gröbner bases and elimination algorithms has been studied for a variety of non-commutative structures. For example, structures such as free algebras [18, 19, 20, 3], path algebras [10], solvable polynomial rings [2, 13], skew polynomial rings [23], free group algebras [22], monoid rings and group rings [16] have been proven to have finite constructible

*Research partially supported by EPRSC while a postdoctoral fellow at University of Kent, Canterbury


*ISSAC'03,* August 3–6, 2003, Philadelphia, Pennsylvania, USA.

Gröbner bases. The scenario presented in (6) differ from these structures in that the coefficient ring (elements of $\mathbb{Q}(n, u_{n+t} : t \in \mathbb{Z})$) and the variables ($\{S, D_n, \ldots, D_{n+M}\}$) do not commute with each other.

In [8, 14, 12, 5] Buchberger's Gröbner basis algorithm was extended to multivariate *Ore-algebras* to eliminate variables. Informally, if $\mathbf{R}$ is some coefficient ring and $D_1, \ldots, D_n$ denotes the operator variables, the Ore-algebras in [5] satisfy the following commutation rules:

$$\begin{aligned} D_i \circ D_j &= D_j \circ D_i \\ D_i \circ p &= \sigma_i(p) \circ D_i + \delta_i(p) \quad p \in \mathbf{R} \end{aligned}$$

for some $\sigma_i$ and $\delta_i$ maps on $\mathbf{R}$. In other words, the Ore-algebras in [5] are generalizations of ordinary multivariate polynomial algebras, where the *operator variables* and the *coefficients* do not commute with each other, but the operator variables commute among each other.

The scenario presented in (6) represents a genuine extension of the Ore-algebras in [5] in that here the operator variables do not commute, either. [9] gives a generalization of Gröbner bases in Ore-algebras to Poincaré-Birkhoff-Witt extensions. In Poincaré-Birkhoff-Witt extensions the commutator of a pair of differential variables are smaller (under some term ordering) than the product of the pair, which assumption we do not make in (6). [1] gives sufficient conditions for graded associative rings to be effective left Gröbner structures, i.e. to have algorithmic left Gröbner basis computation (here the different gradings correspond to term orderings). As we shall see in Remark 4.4, the structures considered in this paper do not satisfy the conditions in [1], and as it turns out they give new instances of graded rings with effective Gröbner structure.

In this paper we define *differential-difference algebras* which are extensions of Ore-algebras with two groups of operator variables, the first group corresponding to differential operators, while the second group to shift operators, so that the cross multiplication between the groups is non-commutative. We note here that the difference operator $\Delta$ is given by $S-I$ where $S$ is the shift operator and $I$ is the identity operator. Typically, systems of difference equations are studied by analogy with differential systems. However, the Leibniz rule that $\Delta$ satisfies is not the natural one but the more awkward rule

$$\Delta(FG) = \Delta(F)S(G) - F\Delta(G).$$

On the other hand, the shift operator is an algebra automorphism. Thus we study difference systems in terms of shift operators, and take advantage of their superior properties. We prove that a modified version of Buchberger's algorithm for a left Gröbner basis terminates in differential-difference-algebras with respect to certain admissible term orders. Moreover, we show that the resulting Gröbner bases give a triangular formulation eliminating the shift variables, which facilitates the solution of the system.

## 2. PRELIMINARIES

First we recall the definition of multivariate Ore algebras following the approach in [5]. Ore polynomials are generalizations of commutative polynomials, differential polynomials and difference polynomials. The variables correspond to linear operators and these linear operators are defined by commutation rules.

Definition 2.1. *Let $R$ be a Noetherian $\mathbb{K}$-algebra for a field $\mathbb{K}$. The skew polynomial ring*

$$R[D_1; \sigma_1, \delta_1] \cdots [D_n; \sigma_n, \delta_n]$$

*is called an Ore algebra if it is the set of polynomials in $D_1, \ldots, D_n$ over $R$ satisfying the following conditions for all $1 \le i, j \le n$, $i \ne j$:*

1. *$\sigma_i$ is a $\mathbb{K}$-algebra automorphism of $R$.*
2. *$\delta_i$ is $\sigma_i$-derivation operator, i.e. a $\mathbb{K}$-linear map of $R$ which satisfies the following Leibniz rule:*
$$\forall a, b \in R \;\; \delta_i(ab) = \sigma_i(a)\delta_i(b) + \delta_i(a)b.$$
3. *The following commutation rules apply:*
$$D_i D_j = D_j D_i \quad 1 \le i, j \le n \;, \tag{7}$$
$$D_i a = \sigma_i(a) D_i + \delta_i(a) \;\; \forall a \in R. \tag{8}$$
4. *$\sigma_i \circ \delta_j = \delta_j \circ \sigma_i$, $\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i$ and $\delta_i \circ \delta_j = \delta_j \circ \delta_i$.*

*We denote the Ore algebra by $R[\mathbf{D}; \boldsymbol{\sigma}, \boldsymbol{\delta}]$. We use the following notation throughout the paper: for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ and $a \in R$*

$$\begin{aligned} \boldsymbol{D}^\alpha &= D_1^{\alpha_1} \cdots D_n^{\alpha_n} \\ \boldsymbol{\sigma}^\alpha(a) &= \sigma_1^{\alpha_1}(\sigma_2^{\alpha_2}(\cdots(\sigma_n^{\alpha_n}(a)\cdots). \end{aligned}$$

**Example** 2.2. *Weyl algebras*

$$\mathbb{K}(x_1, \ldots, x_n)[D_{x_1}; 1, \frac{\partial}{\partial x_1}] \ldots [D_{x_n}; 1, \frac{\partial}{\partial x_n}]$$

*are defined using the commutation rules of partial derivatives.*

In the next proposition we show that if $R$ is a field, then testing divisibility of Ore monomials is as simple as for ordinary monomials. As a consequence, we get a simple expression for the least common multiple of Ore monomials. The proof of the proposition contains a method to compute the quotient of Ore monomials. Divisibility test and quotient computation for Ore monomials are used in Section 4.

Proposition 2.3. *Let $K$ be a field and $K[\mathbf{D}, \boldsymbol{\sigma}, \boldsymbol{\delta}]$ be an Ore-algebra over $K$ as in Definition 2.1. Let $a\boldsymbol{D}^\beta$ and $a'\boldsymbol{D}^{\beta'}$ be Ore-monomials for some $\beta, \beta' \in \mathbb{N}^n$ and $a, a' \in K$. Then $a'\boldsymbol{D}^{\beta'}$ left divides $a\boldsymbol{D}^\beta$ if and only if*

$$\exists \gamma \in \mathbb{N}^n \;\; : \;\; \beta = \beta' + \gamma. \tag{9}$$

*This implies that $a'\boldsymbol{D}^{\beta'}$ left divides $a\boldsymbol{D}^\beta$ if and only if $a'\boldsymbol{D}^{\beta'}$ right divides $a\boldsymbol{D}^\beta$, and*

$$\mathrm{lcm}(a\boldsymbol{D}^\beta, a'\boldsymbol{D}^{\beta'}) = \mathrm{lcm}(\boldsymbol{D}^\beta, \boldsymbol{D}^{\beta'}) = \boldsymbol{D}^\nu$$

*where $\nu$ is the coordinate-wise maximum of $\beta$ and $\beta'$.*

Proof. First we prove the "if" part. Assume that $\beta = \beta' + \gamma$. If we define $p := a\boldsymbol{D}^\gamma \frac{1}{a'} \in K[\mathbf{D}, \boldsymbol{\sigma}, \boldsymbol{\delta}]$ then $D_i D_j = D_j D_i$ implies that

$$a\boldsymbol{D}^\beta = p\boldsymbol{D}^{\beta'}.$$

To prove the "only if" part, assume that $a\boldsymbol{D}^\beta = pa'\boldsymbol{D}^{\beta'}$ for some $p = \sum_{\alpha \in I} c_\alpha \boldsymbol{D}^\alpha \in K[\mathbf{D}, \boldsymbol{\sigma}, \boldsymbol{\delta}]$. Observe that

$$\left(\sum_{\alpha \in I} c_\alpha \boldsymbol{D}^\alpha\right) a' \; \boldsymbol{D}^{\beta'} = \sum_{\alpha \in I} c_\alpha \boldsymbol{\sigma}^\alpha(a') \boldsymbol{D}^{\alpha+\beta'} + P$$

for some $P \in K[\mathbf{D};\boldsymbol{\sigma},\boldsymbol{\delta}]$ such that

$$\max_{\alpha \in I}(\deg_{\text{total}}(\boldsymbol{D}^{\alpha+\beta'})) > \deg_{\text{total}}(P).$$

This implies that the monomials in $\sum_{\alpha\in I} c_\alpha \boldsymbol{\sigma}^\alpha(a')\boldsymbol{D}^{\alpha+\beta'}$ with maximal total degrees cannot be annulled by $P$. Therefore, there is only one monomial in $\sum_{\alpha\in I} c_\alpha \boldsymbol{\sigma}^\alpha(a')\boldsymbol{D}^{\alpha+\beta'}$ with maximal total degree, and it must be equal to $a\boldsymbol{D}^\beta$. Thus $\boldsymbol{D}^\beta$ must be of the form $\boldsymbol{D}^{\alpha+\beta'}$ for some $\alpha$, which proves the claim. □

# 3. DIFFERENTIAL-DIFFERENCE ALGEBRAS

In this section we define and study a more general class of Ore-algebras, where the independent variables are non-commutative. The motivations for the constructions presented here are the differential-difference systems discussed in the introduction.

We assume that the reader is familiar with the notions of $R$-$R$ bi-modules for some ring $R$, tensor products of bi-modules, tensor algebras and general $R$-algebras. For reference see for example [15].

Definition 3.1. *Let $R$ be a Noetherian $\mathbb{K}$-algebra for a field $\mathbb{K}$. Assume that we are given two Ore-algebras*

$$\begin{aligned} R[\mathbf{D},\mathbf{1},\boldsymbol{\delta}] &= R[D_1;\mathrm{id},\delta_1]\cdots[D_n;\mathrm{id},\delta_n] \quad \text{and} \\ R[\boldsymbol{S};\boldsymbol{\xi},\mathbf{0}] &= R[S_1;\xi_1,0]\cdots[S_m;\xi_m,0] \end{aligned}$$

*as in Definition 2.1, where for $1 \le i,j \le m$ and $0 \le k \le n$*

$$\xi_i \circ \delta_k = \delta_k \circ \xi_i; \quad \xi_i \circ \xi_j = \xi_j \circ \xi_i.$$

*Furthermore, for each $1 \le i \le m$ let $\varsigma_i$ be an Ore-algebra automorphism*

$$\varsigma_i : R[\mathbf{D};\mathbf{1},\boldsymbol{\delta}] \to R[\mathbf{D};\mathbf{1},\boldsymbol{\delta}]$$

*such that*

$$\begin{aligned} \varsigma_i|_R &= \xi_i \quad \text{and} \\ \varsigma_i(D_j) &= \textstyle\sum_{i=k}^n a_k D_k \quad \text{for some } a_k \in R. \end{aligned} \tag{10}$$

*Let $F$ be the free $R$-$R$ bi-module with generators*

$$\{S_1,\dots,S_m,D_0,\dots D_n\}$$

*and let $T_R(F)$ be the tensor-algebra on $F$ over $R$. Let $K$ be the two-sided ideal in $T_R(F)$ generated by the infinite set*

$$\begin{aligned} &\{D_i a - aD_i - \delta_i(a) \ : \ 0 \le i \le n, \ \ a \in R\} \\ &\cup\{S_i a - \xi_i(a)\ S_i \ : \ 1 \le i \le m \ \ a \in R\} \\ &\cup\{S_iS_j - S_jS_i \ : \ 1 \le i < j \le m\} \\ &\cup\{D_iD_j - D_jD_i \ : \ 0 \le i < j \le n\} \\ &\cup\{D_iS_j - S_j\,\varsigma_j(D_i) \ : \ 0 \le i \le n, 1 \le j \le m\}. \end{aligned} \tag{11}$$

*The $R$-algebra $T_R(F)/K$ is called a **differential-difference-algebra**. We denote by $R[\mathbf{D};\mathbf{1},\boldsymbol{\delta}][\boldsymbol{S};\boldsymbol{\varsigma},\mathbf{0}]$ the differential-difference-algebra corresponding to $\boldsymbol{\varsigma} = (\varsigma_1,\dots,\varsigma_m)$.*

Remark 3.2.

1. *Fix $1 \le i \le m$. Using (10) and (11), we can write for all $\beta \in \mathbb{N}^n$*

$$\boldsymbol{D}^\beta S_i = \sum_{|\gamma|\le|\beta|} \rho_{i,\beta,\gamma} S_i \boldsymbol{D}^\gamma \tag{12}$$

*for some $\rho_{i,\beta,\gamma} \in R$. Since $\varsigma_i$ is invertible, not all $\rho_{i,\beta,\gamma}$ are zero ($\gamma \in \mathbb{N}^n$, $|\gamma| \le |\beta|$). More generally, we have*

$$\boldsymbol{D}^\beta \boldsymbol{S}^\alpha = \sum_{|\gamma|\le|\beta|} \rho_{\alpha,\beta,\gamma} \boldsymbol{S}^\alpha \boldsymbol{D}^\gamma. \tag{13}$$

*for some $\rho_{\alpha,\beta,\gamma} \in R$.*

2. *Using the fact that $\varsigma_i$ is invertible for $1 \le i \le m$, we can introduce new variables $[\tilde{S}_1;\varsigma_1^{-1},0],\dots,[\tilde{S}_m,\varsigma_m^{-1},0]$ representing the inverse of $S_1,\dots,S_m$, and satisfying the equations*

$$\tilde{S}_iS_i = S_i\tilde{S}_i = 1 \quad\ 1 \le i \le m.$$

3. *We would like to note here that the differential-difference-algebra $R[\mathbf{D};\mathbf{1},\boldsymbol{\delta}][\boldsymbol{S};\boldsymbol{\varsigma},\mathbf{0}]$ is not a Poicaré-Birkhoff-Witt extension of $R$ (see [4, 9]), since the commutators*

$$S_iD_j - D_jS_i \notin R + \sum_{k=1}^n RD_k + \sum_{l=1}^m RS_l.$$

**Example** 3.3. *The example (1) of the introduction corresponds to the differential-difference-algebra over $\mathbb{Q}(n,u_{n+t} : t \in \mathbb{Z})$ with generators*

$$[D_n;\mathrm{id},\frac{\partial}{\partial u_n}],\ [D_{n+1};\mathrm{id},\frac{\partial}{\partial u_{n+1}}],\ [D_{n+2};\mathrm{id},\frac{\partial}{\partial u_{n+2}}]\ [S;\varsigma,0].$$

*The commutation rules given in (6) define the $\mathbb{Q}$-automorphism $\varsigma$ and the following commutation rules:*

$$\begin{aligned} &D_{n+2}S = SD_{n+1} \\ &D_{n+1}S = SD_n + 2SD_{n+2} \\ &D_nS = -SD_{n+2}. \end{aligned}$$

*We can introduce a new shift variable $[\tilde{S};\varsigma^{-1},0]$ corresponding to the dual shift*

$$s^{-1}(n) = n-1, \quad s^{-1}(u_n) = u_{n-1}.$$

*From $u_{n+3} = 2u_{n+1} - u_n$ we get that $u_{n-1} = 2u_n - u_{n+2}$. Then we get the following commutation rules for $\tilde{S}$:*

$$\begin{aligned} &D_n\tilde{S} = \tilde{S}D_{n+1} + 2\tilde{S}D_n \\ &D_{n+1}\tilde{S} = \tilde{S}D_{n+2} \\ &D_{n+2}\tilde{S} = -\tilde{S}D_n. \end{aligned}$$

*One can check that the resulting $\varsigma^{-1}$ is the inverse of $\varsigma$.*

In the next proposition we prove that differential-difference-algebras are isomorphic, as left $R$-modules, to commutative polynomial algebras.

Proposition 3.4. *Let $R$, $[\boldsymbol{S};\boldsymbol{\varsigma},\mathbf{0}]$ and $[\mathbf{D};\mathbf{1},\boldsymbol{\delta}]$ be as in Definition 3.1. Then $R[\mathbf{D};\mathbf{1},\boldsymbol{\delta}][\boldsymbol{S};\boldsymbol{\varsigma},\mathbf{0}]$ is isomorphic, as left $R$-module, to the symmetric algebra $R[\boldsymbol{S},\boldsymbol{D}]$, i.e. each differential-difference polynomial can be uniquely represented in the normal form $\sum_{\alpha,\beta} c_{\alpha,\beta}\boldsymbol{S}^\alpha\boldsymbol{D}^\beta$.*

Proof. Let $F$ be the free $R$-$R$ bi-module with generators $\{D_1,\dots,D_n,S_1,\dots,S_m\}$ and $T_R(F)$ be the tensor-algebra on $F$. Let

$$\mathcal{S} := \{D_jS_i - S_i\varsigma_i(D_j) \ : \ 1 \le i \le m,\ 1 \le j \le n\}$$

and $J$ be the two sided ideal generated by the elements of (11) not in $\mathcal{S}$.
For a term

$$t = \boldsymbol{D}^{\alpha_1}S_{i_1}\boldsymbol{D}^{\alpha_2}S_{i_2}\cdots\boldsymbol{D}^{\alpha_r}S_{i_r} \in T_R(F)/J$$

define the "inversion number" of $t$ to be

$$\mathrm{inv}(t) := \sum_{s=1}^{r} \sum_{q=1}^{s} |\alpha_q|.$$

Choose any admissible term order $\succ$ in $T_R(F)/J$ such that

$$\mathrm{inv}(t) > \mathrm{inv}(t') \;\Rightarrow\; t \succ t' \tag{14}$$

for all terms $t, t' \in T_R(F)/J$. Note that such term orders exist, since the partial order on the terms induced by the inversion number is admissible. Since the Ore-algebras $R[\boldsymbol{S};\boldsymbol{\varsigma},\mathbf{0}]$ and $R[\mathbf{D};\mathbf{1},\boldsymbol{\delta}]$ are isomorphic – as left $R$-modules – to $R[\boldsymbol{S}]$ and $R[\mathbf{D}]$, respectively, it is sufficient to prove that every element of $T_R(F)/J$ reduces to a unique "ordered" element of the form $\sum_{|\alpha|+|\beta|=d} c_{\alpha,\beta}\boldsymbol{S}^\alpha \boldsymbol{D}^\beta$ modulo $S$ w.r.t. $\succ$.
The application of a reduction step w.r.t. $\succ$ by $\mathcal{S}$ to the leading monomial of an element of $T_R(F)/J$ will reduce the inversion number of the leading term, which implies that the reduction algorithm terminates. A reduced element is clearly "ordered", otherwise it has reducible terms. Finally, to prove that the reduced form of elements in $T_R(F)/J$ are unique, we observe that the leading terms of the elements of $\mathcal{S}$ are relatively prime, which implies that $\mathcal{S}$ forms a reduced Gröbner basis (see [21, Lemma 3.3]). $\square$

The following extension of Proposition 2.3 to differential-difference algebras is essential for the proofs of the paper. Since the proof is straightforward, we leave it to the reader.

Proposition 3.5. *Let $K$ be a field and $K[\mathbf{D},\mathbf{1},\boldsymbol{\delta}][\boldsymbol{S};\boldsymbol{\varsigma},\mathbf{0}]$ be a differential-difference algebra over $K$ as in Definition 3.1. Let $a\boldsymbol{S}^\alpha\boldsymbol{D}^\beta$ and $a'\boldsymbol{S}^{\alpha'}\boldsymbol{D}^{\beta'}$ be monomials for some $\alpha,\alpha' \in \mathbb{N}^m$, $\beta,\beta' \in \mathbb{N}^n$ and $a,a' \in K$. Then $a'\boldsymbol{S}^{\alpha'}\boldsymbol{D}^{\beta'}$ left divides $a\boldsymbol{S}^\alpha\boldsymbol{D}^\beta$ if and only if*

$$\exists\delta \in \mathbb{N}^m,\ \gamma \in \mathbb{N}^n \;:\; \alpha = \delta + \alpha' \ \text{ and } \ \beta = \beta' + \gamma. \tag{15}$$

*This implies that $a'\boldsymbol{S}^{\alpha'}\boldsymbol{D}^{\beta'}$ left divides $a\boldsymbol{S}^\alpha\boldsymbol{D}^\beta$ if and only if $a'\boldsymbol{S}^{\alpha'}\boldsymbol{D}^{\beta'}$ right divides $a\boldsymbol{S}^\alpha\boldsymbol{D}^\beta$, and*

$$\mathrm{lcm}(a\boldsymbol{S}^\alpha\boldsymbol{D}^\beta, a'\boldsymbol{S}^{\alpha'}\boldsymbol{D}^{\beta'}) = \mathrm{lcm}(\boldsymbol{S}^\alpha\boldsymbol{D}^\beta, \boldsymbol{S}^{\alpha'}\boldsymbol{D}^{\beta'}) = \boldsymbol{S}^\mu\boldsymbol{D}^\nu$$

*where $\mu$ and $\nu$ are the coordinate-wise maxima $\max(\alpha,\alpha')$ and $\max(\beta,\beta')$, respectively.*

# 4. GRÖBNER BASIS COMPUTATION

In this section we describe an algorithm to compute left Gröbner bases in differential-difference algebras. This algorithm is essentially Buchberger's algorithm in some term order $\succ$ such that $\boldsymbol{S} \succ \boldsymbol{D}$. The condition $\boldsymbol{S} \succ \boldsymbol{D}$ is needed to ensure that the term order is admissible. Using the fact that the shift variables have inverses, we describe a simple way to compute S-polynomials and reduction among differential-difference polynomials. Furthermore, we prove that Buchberger's algorithm on differential-difference polynomials w.r.t $\succ$ terminates. Also, applying Buchberger's algorithm with respect to the lexicographic term order, we prove that the resulting left Gröbner bases eliminate the shift operator variables as much as possible.

In the next proposition we prove that monomial orders which first decide inequality based on the exponents of the shift variables are admissible. Later in this section we use these monomial orders to compute Gröbner bases. We use the notions of monomial order (cf. [7]) and admissible term order (cf. [5]).

Proposition 4.1. *Let $K$ be a field and $K[\mathbf{D};\mathbf{1},\boldsymbol{\delta}][\boldsymbol{S};\boldsymbol{\varsigma},\mathbf{0}]$ be a differential-difference-algebra. Let $\succ$ be the monomial order defined as follows:*

$$\begin{array}{rcll} \boldsymbol{S}^\alpha\boldsymbol{D}^\beta & \succ & \boldsymbol{S}^{\alpha'}\boldsymbol{D}^{\beta'} & \text{iff} \\ \boldsymbol{S}^\alpha & \succ_{\boldsymbol{S}} & \boldsymbol{S}^{\alpha'} & \text{or else} \\ \alpha = \alpha' & \text{and} & \boldsymbol{D}^\beta \succ_{\boldsymbol{D}} \boldsymbol{D}^{\beta'}, & \end{array}$$

*where $\succ_{\boldsymbol{S}}$ is any monomial order on $\{S_1,\dots,S_m\}$ and $\succ_{\boldsymbol{D}}$ is a total degree monomial order on $\{D_1,\dots,D_n\}$, i.e. $\boldsymbol{D}^\beta \succ_{\boldsymbol{D}} \boldsymbol{D}^{\beta'}$ if $\deg_{\text{total}}(\boldsymbol{D}^\beta) > \deg_{\text{total}}(\boldsymbol{D}^{\beta'})$.
Then for all $p \in K[\mathbf{D};\mathbf{1},\boldsymbol{\delta}][\boldsymbol{S};\boldsymbol{\varsigma},\mathbf{0}] - K$ and $c,c' \in K$ the following three conditions hold:*

$$c\boldsymbol{S}^\alpha\boldsymbol{D}^\beta \succ c'\boldsymbol{S}^{\alpha'}\boldsymbol{D}^{\beta'} \Rightarrow \mathrm{lt}(pc\boldsymbol{S}^\alpha\boldsymbol{D}^\beta) \succ \mathrm{lt}(pc'\boldsymbol{S}^{\alpha'}\boldsymbol{D}^{\beta'}), \tag{16}$$

$$\mathrm{lt}(p\,\boldsymbol{S}^\alpha\boldsymbol{D}^\beta) \succ \boldsymbol{S}^\alpha\boldsymbol{D}^\beta, \tag{17}$$

*Every strictly decreasing sequence of terms is finite.* (18)

*Here* lt *denotes the leading term w.r.t. $\succ$ (see Definition 4.2 below).*

Proof. We first prove (16) for

$$p \in K[\mathbf{D};\mathbf{1},\boldsymbol{\delta}],$$

and assume that the total degree of $p$ is $d$. Using the commutation rules in $K[\mathbf{D};\mathbf{1},\boldsymbol{\delta}][\boldsymbol{S};\boldsymbol{\varsigma},\mathbf{0}]$ we have that

$$\begin{aligned} p\,c\,\boldsymbol{S}^\alpha &= (cp+q)\,\boldsymbol{S}^\alpha \\ &= c\boldsymbol{S}^\alpha\boldsymbol{\varsigma}^\alpha(p) + \boldsymbol{S}^\alpha\boldsymbol{\varsigma}^\alpha(q) \end{aligned} \tag{19}$$

for some $q \in K[\mathbf{D};\mathbf{1},\boldsymbol{\delta}]$ of total degree at most $d-1$. Similarly,

$$p\,c'\,\boldsymbol{S}^{\alpha'} = c'\boldsymbol{S}^{\alpha'}\boldsymbol{\varsigma}^{\alpha'}(p) + \boldsymbol{S}^{\alpha'}\boldsymbol{\varsigma}^{\alpha'}(q') \tag{20}$$

for some $q' \in K[\mathbf{D};\mathbf{1},\boldsymbol{\delta}]$ of total degree at most $d-1$. Therefore, the exponents $\alpha$ and $\alpha'$ do not change during the application of the commutation rules. This implies that if $\alpha \neq \alpha'$ then the claim is true. If $\alpha = \alpha'$ then we must have $\boldsymbol{D}^\beta \succ_{\boldsymbol{D}} \boldsymbol{D}^{\beta'}$. Then by the properties of $\succ_{\boldsymbol{D}}$ we have that the leading terms of both (19) and (20) is equal to

$$\boldsymbol{S}^\alpha \mathrm{lt}\,(\boldsymbol{\varsigma}^\alpha(p))\,.$$

(Note that this is where we use that $\boldsymbol{\sigma} = \mathbf{1}$ in $K[\mathbf{D};\mathbf{1},\boldsymbol{\delta}]$.)
Therefore,

$$\mathrm{lt}\,(\boldsymbol{\varsigma}^\alpha(p))\,\boldsymbol{D}^\beta \succ_{\boldsymbol{D}} \mathrm{lt}\,(\boldsymbol{\varsigma}^\alpha(p))\,\boldsymbol{D}^{\beta'},$$

which implies the claim.
The inequality (16) for

$$p \in K[\mathbf{D};\mathbf{1},\boldsymbol{\delta}][\boldsymbol{S};\boldsymbol{\varsigma},\mathbf{0}]$$

simply follows from the fact that left multiplication by $\boldsymbol{S}^\gamma$ acts like commutative multiplication.
To prove (17) it is sufficient to prove that

$$\mathrm{lt}(D_j\boldsymbol{S}^\alpha\boldsymbol{D}^\beta) \succ \boldsymbol{S}^\alpha\boldsymbol{D}^\beta. \tag{21}$$

Using Remark 3.2, we observe that the left hand side of (21) has higher total degree in the variables $\{D_1,\dots,D_n\}$ than the right hand side, which implies (17).
Finally, (18) follows from the fact that $\succ_{\boldsymbol{S}}$ and $\succ_{\boldsymbol{D}}$ are monomial orders. $\square$

DEFINITION 4.2. *A term order $\succ$ satisfying the conditions of Proposition 4.1 is called a* **differential-difference-order**. *We denote by* lm, lt, *and* lc *the leading monomial, leading term and the leading coefficient w.r.t $\succ$.*

The following corollary gives the main property which allows to prove that Buchberger's algorithm terminates in differential-difference algebras.

COROLLARY 4.3. *Let $\succ$ be a differential-difference-order. Then for any $f, g \in K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ we have*

$$\mathrm{lm}(fg) = \mathrm{lm}(f\mathrm{lm}(g)).$$

*This implies that there exists $h \in K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ such that*

$$\mathrm{lm}(fg) = h\mathrm{lm}(g).$$

PROOF. The first claim easily follows from Proposition 4.1 by observing that for each monomial $m$ in $g$ we have

$$\mathrm{lt}(f\mathrm{lm}(g)) \succ \mathrm{lt}(f\,m).$$

To prove the second claim, let $\mathrm{lm}(g) = c\boldsymbol{S}^\alpha \boldsymbol{D}^\beta$. Then it follows from Proposition 3.5 that each term of $f\mathrm{lm}(g)$ is divisible by $\boldsymbol{S}^\alpha \boldsymbol{D}^\beta$ from the right, in particular the leading term, thus we get the second claim from the first one. $\square$

REMARK 4.4. *Note that among differential-difference polynomials the leading term of products is not necessarily the product of leading terms. For example, in Example 3.3, if we take the polynomials*

$$f := D_{n+2} + D_{n+1}, \quad g := S$$

*and any admissible term order such that $S > D_{n+2} > D_{n+1} > D_n$ then $fg = SD_{n+1} + SD_n + 2SD_{n+2}$, thus*

$$\mathrm{lt}(fg) = SD_{n+2} \neq SD_{n+1} = \mathrm{lt}(f)\mathrm{lt}(g).$$

*In [1, Theorem 6] the multiplicativity of the leading terms is assumed in order to prove that certain associative rings are effective Gröbner structures. In this paper we show that differential-difference-algebras provide a new instance of effective Gröbner structures.*

Now we are ready to state the definition of left Gröbner bases for differential-difference algebras.

DEFINITION 4.5. *Let $K$ be a field and $K[\mathbf{D}, \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ be a differential-difference algebra. Let $\succ$ be a differential-difference order. Then $G = \{g_1, \ldots, g_s\} \subset K[\mathbf{D}, \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ is a left Gröbner basis w.r.t. $\succ$ for a left-ideal $\mathcal{I}$ if and only if $g_1, \ldots, g_s$ generates $\mathcal{I}$ as a left ideal and for any $h \in \mathcal{I}$ we have that $\mathrm{lt}(h)$ is in the left ideal generated by $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s)$.*

Next we describe the algorithm to compute left Gröbner bases in differential-difference-algebras. Throughout the algorithms we assume that we present each differential difference polynomial in $K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ as the sum of monomials in the normal form

$$\boldsymbol{S}^\alpha c_{\alpha,\beta} \boldsymbol{D}^\beta$$

where $\alpha \in \mathbb{N}^m$, $\beta \in \mathbb{N}^n$ and $c_{\alpha,\beta} \in K$. In other words, the shift variables precede the coefficients in this normal form. This assumption is not necessary but it makes the presentation of the algorithms simpler. Note that

$$\boldsymbol{S}^\alpha c_{\alpha,\beta} \boldsymbol{D}^\beta = c'_{\alpha,\beta} \boldsymbol{S}^\alpha \boldsymbol{D}^\beta$$

where $c'_{\alpha,\beta} = \boldsymbol{\xi}^\alpha(c_{\alpha,\beta})$.

We introduce the new variables $[\tilde{S}_1, \varsigma_1^{-1}, 0], \ldots, [\tilde{S}_m, \varsigma_m^{-1}, 0]$ for the inverses of the shift variables. We use these variables to divide out shift variables. As we point out in the description of the algorithms, the use of the inverse shift variables can be avoided since if $\alpha \geq \alpha'$ coordinate-wise then

$$\boldsymbol{S}^\alpha\; p\; \tilde{\mathbf{S}}^{\alpha'} = \boldsymbol{S}^{\alpha-\alpha'} \boldsymbol{\varsigma}^{-\alpha'}(p),$$

and we always maintain that $\alpha \geq \alpha'$.

Note that we use the left-division and the least common multiple algorithms among monomials in $K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}]$ described in the proof of Proposition 2.3. The first subroutine of the left-Gröbner basis algorithm is the reduction algorithm, which is the analogue of the Division Algorithm in [6].

**Reduction algorithm**

**Input** $h$ and $F = \{f_1, \ldots, f_t\}$ elements of $K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$.
A differential-difference-order $\succ$.
Assume that $\mathrm{lm}(f_t) \succeq \cdots \succeq \mathrm{lm}(f_1)$.

**Output** $r$ and $q_1, \ldots, q_t$ in $K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ such that $r = h - \sum_{i=1}^t q_i f_i$ and for all non-zero monomials $m$ in $r$ and all $1 \leq i \leq t$

$$\nexists p_i : \quad m = p_i \mathrm{lm}(f_i).$$

**Algorithm**

```
r := 0, g := h, and q_i := 0 for 1 ≤ i ≤ t
WHILE g ≠ 0 DO
  s := 1
  divisionoccurred := false
  WHILE s ≤ t AND divisionoccurred = false DO
    S^α c D^β := lm(g) and S^α' c' D^β' := lm(f_s)
    IF α ≥ α'   AND   β ≥ β'   THEN
      compute  p  such that  c D^β = p c' D^β'
      g := g − S^α p S̃^α' f_s,  q_s := q_s + S^(α−α') ς^(−α')(p)
      divisionoccurred := true
    ELSE
      s := s + 1
    FI
  OD
  IF divisionoccurred = false THEN
    r := r + lm(g), g := g − lm(g)
  FI
OD
```

LEMMA 4.6. *Let $\succ$ be a differential-difference-order. Then for all $h$ and $F = \{f_1, \ldots, f_t\}$ in $K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ the reduction algorithm terminates and returns $r$ which satisfies the output specifications. Furthermore, for all $1 \leq s \leq t$ we have*

$$\mathrm{lm}(h) \succeq \mathrm{lm}(q_s f_s).$$

PROOF. First we prove that the inner while loop is finite. Suppose on the contrary that this loop produces an infinite sequence $\{g_j\}$. Each time we enter the inner loop of the reduction algorithm we either increase the looping variable $s$

or we eliminate the leading term of $g$. This would imply that we have infinite number of elimination step. At each elimination step we replace $\mathrm{lt}(g)$ by $\boldsymbol{S}^{\alpha-\alpha'}\boldsymbol{\varsigma}^{-\alpha'}(p)(f_s - \mathrm{lm}(f_s))$ for some $1 \le s \le t$, $p \in K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}]$ and $\alpha, \alpha' \in \mathbb{N}^m$. By (16), at every elimination step the leading term of $g$ is replaced by a set of terms strictly smaller than it. Therefore, our assumptions would result in an infinite sequence of strictly decreasing monomials, which contradicts (18). To prove that the outer loop is finite, we can again argue that the sequence of the leading terms $\{\mathrm{lm}(g_j)\}$ is strictly decreasing.

To prove the second claim, first note that at each step in the algorithm the following equality holds:

$$h = g + \sum_{i=1}^{t} q_i f_i + r$$

Since $g = 0$ at termination, we have $r = h - \sum_{i=1}^{r} q_i f_i$.

To prove that all monomials of $r$ are reduced, note that all monomials of $r$ equal to some $\mathrm{lm}(g)$ such that $\mathrm{lm}(g)$ is reduced, since no reduction occurred by the polynomials $f_1, \ldots, f_s$.

The last claim follows from the fact that $q_s$ is the sum of the polynomials of the form $\boldsymbol{S}^{\alpha-\alpha'}\boldsymbol{\varsigma}^{-\alpha'}(p)$ where

$$\mathrm{lm}(g) = \boldsymbol{S}^{\alpha-\alpha'}\boldsymbol{\varsigma}^{-\alpha'}(p)\mathrm{lm}(f_s)$$

for some intermediate result $g$ in the algorithm. Therefore, all monomials of $q_s\mathrm{lm}(f_s)$ are equal to some $\mathrm{lm}(g)$, in particular,

$$\mathrm{lm}(q_s f_s) = \mathrm{lm}(q_s \mathrm{lm}(f_s)) = \mathrm{lm}(g)$$

for some intermediate polynomial $g$ in the algorithm. Since the leading monomials of the intermediate results form a decreasing sequence, thus $\mathrm{lm}(h) \succ \mathrm{lm}(g)$, which implies the claim. □

The second subroutine is the S-polynomial computation process:

**S-polynomial algorithm**

**Input** $f$ and $g$ elements of $K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$. A differential-difference-order $\succ$.

**Output** $h$ and $p, q$ in $K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ such that $h = p\,f - q\,g$ and h satisfies the following property:

$$\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) \succ \mathrm{lm}(h), \tag{22}$$

where the lcm is computed as in Proposition 3.5.

**Initialization** Let $\mathrm{lm}(f) = \boldsymbol{S}^{\alpha} c \boldsymbol{D}^{\beta}$ and $\mathrm{lm}(g) = \boldsymbol{S}^{\alpha'} c' \boldsymbol{D}^{\beta'}$.

**Lcm** Compute $\overline{p}$, $\overline{q} \in K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}]$ such that

$$\boldsymbol{D}^{\nu} = \mathrm{lcm}(c\boldsymbol{D}^{\beta}, c'\boldsymbol{D}^{\beta'}) = \overline{p} c \boldsymbol{D}^{\beta} = \overline{q} c' \boldsymbol{D}^{\beta'}$$

where $\nu$ is the coordinate-wise maximum of $\beta$ and $\beta'$. (For the computation of $\overline{p}$ and $\overline{q}$ see the proof of Proposition 2.3.)

**Return** $p := \boldsymbol{S}^{\mu-\alpha}\boldsymbol{\varsigma}^{-\alpha}(\overline{p})$, $q := \boldsymbol{S}^{\mu-\alpha'}\boldsymbol{\varsigma}^{-\alpha'}(\overline{q})$ and

$$h := \left(\boldsymbol{S}^{\mu}\overline{p}\,\tilde{\mathbf{S}}^{\alpha}\right) f - \left(\boldsymbol{S}^{\mu}\overline{q}\,\tilde{\mathbf{S}}^{\alpha'}\right) g \tag{23}$$

where $\mu$ is the coordinate-wise maximum of $\alpha$ and $\alpha'$.

Lemma 4.7. *For each $f, g \in K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ the output of the S-polynomial algorithm satisfies the output specification.*

Proof. To prove that $h = p\,f - q\,g$ we simply observe that $p = \boldsymbol{S}^{\mu-\alpha}\boldsymbol{\varsigma}^{-\alpha}(\overline{p}) = \boldsymbol{S}^{\mu}\overline{p}\,\tilde{\mathbf{S}}^{\alpha}$ and similarly for $q$, so the claim follows from the definition of $h$.

To prove that $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) \succ \mathrm{lm}(h)$, let $\mathrm{lm}(f) = \boldsymbol{S}^{\alpha} c \boldsymbol{D}^{\beta}$ and $\mathrm{lm}(g) = \boldsymbol{S}^{\alpha'} c' \boldsymbol{D}^{\beta'}$. Then by Proposition 3.5 we have

$$\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) = \boldsymbol{S}^{\mu}\boldsymbol{D}^{\nu}$$

where $\mu$ is the coordinate-wise maximum of $\alpha$ and $\alpha'$ and $\nu$ is the coordinate-wise maximum of $\beta$ and $\beta'$. Since $p\,\mathrm{lm}(f)$ and $q\,\mathrm{lm}(g)$ are monomials, thus $\mathrm{lm}(pf) = \mathrm{lm}(p\mathrm{lm}(f)) = p\mathrm{lm}(f) = \boldsymbol{S}^{\mu}\boldsymbol{D}^{\nu}$ and $\mathrm{lm}(qg) = \mathrm{lm}(q\mathrm{lm}(g)) = q\mathrm{lm}(g) = \boldsymbol{S}^{\mu}\boldsymbol{D}^{\nu}$, therefore the leading monomials of $pf$ and $qg$ annulate each other, thus $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) = \boldsymbol{S}^{\mu}\boldsymbol{D}^{\nu} \succ \mathrm{lm}(pf - qg)$, which proves the claim. □

The following lemma is the analogue of [6, Chapter 2.6 Lemma 5], and needed in the main theorem of the paper.

Lemma 4.8. *Let $f_1 \ldots f_s \in K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ and suppose that for all $1 \le i \le s$ $\mathrm{lt}(f_i) = t$ for some term $t$. If $t \succ \mathrm{lt}(\sum_{i=1}^{s} c_i f_i)$ ($c_i \in K$), then there exists $d_{i,j} \in K$ such that*

$$\sum_{i=1}^{s} c_i f_i = \sum_{i,j=1}^{s} d_{i,j}\mathrm{Spoly}(f_i, f_j).$$

Proof. For the proof we refer to the proof of [6, Chapter 2.6 Lemma 5]. This proof uses a telescoping argument to generalize the fact that the S-polynomial of a pair with equal leading terms is a linear combination of the two polynomials. The same argument works also for differential-difference polynomials. □

Finally, we describe the left-Gröbner basis algorithm for differential difference systems.

**Left-Gröbner basis algorithm**

**Input** $F \subset K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ a finite, non-empty set and a differential-difference order $\succ$.

**Output** $G \subset K[\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}][\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}]$ finite set such that

$$\mathrm{reduction}_{\succ}(\mathrm{Spoly}_{\succ}(g, g'),\ G) = 0 \quad \forall g, g' \in G.$$

**Initialization** $G := F$, $P := \{\{f, g\} \ :\ f \neq g;\ f, g, \in F\}$.

**Loop** While $P \neq \emptyset$ do
$P := P - \{f, g\}$
$h := \mathrm{reduction}_{\succ}(\mathrm{Spoly}_{\succ}(f, g),\ G)$
If $h \neq 0$ then
$P := P \cup \{\{f, h\} \ :\ f \in G\}$; $\quad G := G \cup \{h\}$
fi
od

**Return** $G$.

**Theorem** 4.9. *Let $\succ$ be a differential-difference order and $F = \{f_1, \ldots, f_r\} \subset K[\boldsymbol{S}; \boldsymbol{\varsigma}, \mathbf{0}][\mathbf{D}; \mathbf{1}, \boldsymbol{\delta}]$. Then the left-Gröbner basis algorithm terminates and the output $G = \{g_1, \ldots, g_s\}$ is a left-Gröbner basis w.r.t. $\succ$ for the ideal generated by $F$.*

PROOF. Assume that the algorithm does not terminate but computes an infinite sequence $\{g_j\}$. Since each $g_j$ is reduced by the set $\{g_1, \ldots, g_{j-1}\}$, the leading monomial of $g_j$ is not left divisible by any of the leading monomials $\{\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_{j-1})\}$. Using Proposition 3.5, we have that $\boldsymbol{S}^{\alpha'} a' \boldsymbol{D}^{\beta'}$ left divides $\boldsymbol{S}^{\alpha} a \boldsymbol{D}^{\beta}$ if and only if

$$\exists \tilde{\alpha} \in \mathbb{N}^m, \tilde{\beta} \in \mathbb{N}^{n+1} \ : \ \alpha = \alpha' + \tilde{\alpha}, \ \beta = \beta' + \tilde{\beta}.$$

Therefore, similarly as in [17], we can apply Dickson's lemma and conclude that the sequence $\{\mathrm{lt}(g_j)\}$ is finite.

We prove that the output $G$ is a left-Gröbner basis w.r.t. $\succ$ following a proof similar to the one in [6, Chapter 2.6, Theorem 6]. First note that $F$ and $G$ generate the same left-ideal, since $F \subseteq G$ and for all $g \in G$, $g$ is in the left-ideal generated by $F$ by construction. Then, by Definition 4.5, we need to prove that for any $h$ in the left ideal generated by $G$ we have that $\mathrm{lt}(h)$ is in the left ideal generated by $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s)$. By our assumption on $h$ we have that

$$h = \sum_{i=1}^{r} p_i g_i \tag{24}$$

for some $p_i \in K[\boldsymbol{S}; \boldsymbol{\varsigma}, \boldsymbol{0}][\mathbf{D}; \boldsymbol{1}, \boldsymbol{\delta}]$. Assume that

$$\max_i(\mathrm{lt}(p_i g_i)) = t$$

where the maximum is taken with respect to $\succ$, and that among all possible expressions of the form (24) we chose one with minimal $t$.

First assume that $\mathrm{lt}(h) = t$. Since we have (by Corollary 4.3)

$$\mathrm{lt}(p_i g_i) = \mathrm{lt}(p_i \mathrm{lm}(g_i)) = q_i \mathrm{lm}(g_i) = \tilde{q}_i \mathrm{lt}(g_i)$$

for some $q_i, \tilde{q}_i \in K[\boldsymbol{S}; \boldsymbol{\varsigma}, \boldsymbol{0}][\mathbf{D}; \boldsymbol{1}, \boldsymbol{\delta}]$, therefore there exists $1 \le i \le s$ such that

$$\mathrm{lt}(h) = t = \mathrm{lt}(p_i g_i) = \tilde{q}_i \mathrm{lt}(g_i),$$

thus $\mathrm{lt}(h)$ is in the left-ideal generated by $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s)$.

Secondly, assume that $t \succ \mathrm{lt}(h)$. In this case we will produce an expression $h = \sum_{i=1}^{r} \overline{p}_i g_i$ where $t \succ \max_i(\mathrm{lt}(\overline{p}_i g_i))$, contradicting the minimality of $t$.

For $1 \le i \le s$ let $q_i$ such that

$$\mathrm{lm}(p_i g_i) = q_i \mathrm{lm}(g_i).$$

Rewrite

$$h = \sum_{\mathrm{lt}(p_i g_i) = t} q_i\, g_i \ + \sum_{\mathrm{lt}(p_i g_i) = t} (p_i - q_i)\, g_i \ + \sum_{t \succ \mathrm{lt}(p_i g_i)} p_i\, g_i.$$

Then the second and third term on the right hand side involve only monomials which are smaller than $t$. Thus $\sum_{\mathrm{lt}(p_i g_i) = t} q_i\, g_i$ satisfies the conditions of Lemma 4.8 with $f_i = q_i\, g_i$. Therefore, there exist $d_{i,j} \in K$ such that

$$\sum_{\mathrm{lt}(p_i g_i) = t} q_i\, g_i = \sum_{i,j=1}^{s} d_{i,j} \mathrm{Spoly}(q_i g_i, q_j g_j).$$

However,

$$\begin{aligned} \mathrm{Spoly}(q_i g_i, q_j g_j) &= \frac{t}{q_i \mathrm{lm}(g_i)} q_i g_i - \frac{t}{q_j \mathrm{lm}(g_j)} q_j g_j \\ &= \frac{t}{\mathrm{lcm}(\mathrm{lt}(g_i), \mathrm{lt}(g_j))} \mathrm{Spoly}(g_i, g_j) \end{aligned}$$

where $q_i \mathrm{lm}(g_i)$ and $q_j \mathrm{lm}(g_j)$ are monomials, and the ratio of monomials are taken using Proposition 3.5. Thus

$$\sum_{\mathrm{lt}(p_i g_i) = t} q_i\, g_i = \sum_{i,j=1}^{s} d_{i,j} \frac{t}{\mathrm{lcm}(\mathrm{lt}(g_i), \mathrm{lt}(g_j))} \mathrm{Spoly}(g_i, g_j).$$

By the properties of the left-Gröbner basis algorithm we have that $\mathrm{Spoly}(g_i, g_j)$ reduces to 0 modulo $G$ for all $1 \le i, j \le s$. Therefore, by Lemma 4.6 there exist $a_{i,j,k} \in K[\boldsymbol{S}; \boldsymbol{\varsigma}, \boldsymbol{0}][\mathbf{D}; \boldsymbol{1}, \boldsymbol{\delta}]$ such that

$$\mathrm{Spoly}(g_i, g_j) = \sum_{k=1}^{s} a_{i,j,k} g_k$$

and

$$\mathrm{lt}(\mathrm{Spoly}(g_i, g_j)) \succeq \mathrm{lt}(a_{i,j,k} g_k).$$

By (22) and (16) we have that

$$t \succ \mathrm{lt}\left(\frac{t}{\mathrm{lcm}(\mathrm{lt}(g_i), \mathrm{lt}(g_j))} \mathrm{Spoly}(g_i, g_j)\right) \succeq \mathrm{lt}(b_{i,j,k} g_k)$$

where

$$b_{i,j,k} := \frac{t}{\mathrm{lcm}(\mathrm{lt}(g_i), \mathrm{lt}(g_j))} a_{i,j,k}.$$

Therefore,

$$\sum_{\mathrm{lt}(p_i g_i) = t} q_i\, g_i = \sum_{i,j=1}^{s} d_{i,j} \left( \sum_{k=1}^{s} b_{i,j,k} g_k \right) = \sum_{k=1}^{s} \overline{q}_k\, g_k$$

with all term on the right hand side smaller than $t$. Thus replacing $h = \sum_{i=1}^{s} p_i g_i$ by

$$\sum_{i=1}^{s} p_i g_i - \sum_{\mathrm{lt}(p_i g_i) = t} q_i\, g_i + \sum_{k=1}^{s} \overline{q}_k\, g_k$$

gives the desired contradiction. $\square$

REMARK 4.10. *We can define "minimal" and "reduced" left-Gröbner bases in differential-difference algebras similarly as in [6, Chapter 2.7 Definition 5]. Then one can design a self-reduction algorithm which turns a left-Gröbner basis into a minimal or reduced left-Gröbner basis analogously as in the polynomial algebra case.*
*We also note here that if the differential-difference-order is an elimination order (e.g. the lexicographic order), then the reduced left-Gröbner basis contains, as a subset, a left-Gröbner basis for the elimination left ideals eliminating the* $\boldsymbol{S}$ *variables first.*

In the next example we demonstrate how the left-Gröbner basis algorithm give a solution for the system in (1).

**Example** 4.11. *Using the notation in Example 3.3, the equations in (1) correspond to the following polynomials in the differential algebra* $\mathbb{Q}(n, u_{n+s} : s \in \mathbb{Z})[D_{n+i}, 1, \frac{\partial}{\partial u_{n+i}}]_{i=0}^{2}[S, \varsigma, 0]$*:*

$$f_1 := S^3 - 2S + 1 \quad f_2 := D_{n+2}.$$

*We use the lexicographic ordering with* $S \succ D_{n+2} \succ D_{n+1} \succ D_n$*. The S-polynomial of* $f_1$ *and* $f_2$ *is*

$$\varsigma^{-3}(D_{n+2}) f_1 - S^3 f_2 = (-D_{n+2} + 2D_{n+1} + 4D_n) f_1 - S^3 f_2$$

*which reduces to*

$$f_3 := S D_{n+1} - D_{n+1} + 2S D_n - 2D_n.$$

*Then the S-polynomial of* $f_1$ *and* $f_3$ *is*

$$\varsigma^{-3}(D_{n+1}) f_1 - S^2 f_3 = (-D_{n+1} - 2D_n) f_1 - S^2 f_3$$

*which reduces to*

$$f_4 := SD_n - D_n.$$

*Similarly*

$$\begin{aligned}\text{Spoly}(f_2, f_3) &\to f_5 := D_n D_{n+1} + 2D_n^2 \\ \text{Spoly}(f_1, f_5) &\to f_6 := D_n^2 \\ \text{Spoly}(f_3, f_5) &\to f_7 := D_{n+1}^2.\end{aligned}$$

*One can check that the set $G := \{f_1, \ldots, f_7\}$ forms a left-Gröbner basis for the left-ideal generated by $f_1, f_2$.*
*Using $G$ we can infer that the solution $F_n = F(n, u_n, u_{n+1}, u_{n+2})$ of (1) has the form (2) as follows: From $f_2, f_5, f_6$ and $f_7$ we deduce that*

$$F_n = c_0(n)u_n + c_1(n)u_{n+1} + c_2(n)$$

*and then from $f_3$ and $f_4$ we obtain*

$$c_0(n) \equiv c_0, \qquad c_1(n) \equiv c_1$$

*and then from $f_1$ we obtain*

$$c_2(n+3) - 2c_2(n+1) + c_2(n) = 0.$$

The last example has non-constant coefficients:

**Example** 4.12. *Consider the following polynomials in the differential algebra $\mathbb{Q}(n, u_{n+s} : s \in \mathbb{Z})[D_{n+i}, 1, \frac{\partial}{\partial u_{n+i}}]_{i=0}^{1}[S, \varsigma, 0]$:*

$$\begin{aligned}\omega :&\quad u_{n+2} - 2\frac{u_{n+1}^2}{u_n} \\ f_1 :&\quad u_n^2 S^2 - 4u_n u_{n+1} S + 2u_{n+1}^2 I \\ f_2 :&\quad D_{n+1}\end{aligned}$$

*The commutation rules are:*

$$\begin{aligned}D_n S &= -2\frac{u_{n+1}^2}{u_n^2} SD_{n+1} \\ D_{n+1} S &= SD_n + 4\frac{u_{n+1}}{u_n} SD_{n+1}.\end{aligned}$$

*Then we have*

$$Spoly(f_1, f_2) \to 2u_n^2 SD_n - (u_{n-1} - 2u_n)S - 2u_n^2 D_0 n$$

*Note that the variable $u_{n-1}$ in $Spoly(f_1, f_2)$ is a function of $u_n$ and $u_{n+1}$. In this example the constraint $s^{-1}(\omega)$ is "reversible", i.e. we can express $u_{n-1} = 2u_n^2/u_{n+1}$. Thus here we can simply use a substitution. In general, if the constraint $s^{-1}(\omega)$ is not reversible, we can keep $u_{n-1}$ in the coefficients and use implicit differentiation on $s^{-1}(\omega)$ to compute the differentials of $u_{n-1}$ by $D_n$ and $D_{n+1}$.*


## 5. ACKNOWLEDGEMENTS

We would like to thank Peter Hydon for providing us the problem. We would also like to thank the anonymous reviewers for pointing out related bibliographical references and for simplifying some of the proofs of the paper.


## 6. REFERENCES


[1] J. Apel. Computational ideal theory in finitely generated extension rings. *Theoretical Computer Science*, 244(1–2):1–33, 2000.

[2] J. Apel and W. Lassner. An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras. *Journal of Symbolic Computation*, (6):361–370, 1988.

[3] F. Baader. Unification in commutative theories, Hilbert's basis theorem and Gröbner bases. In *Proc. 3rd UNIF'89*, 1989.

[4] A. D. Bell and K. D. Goodearl. Uniform rank over differential operator rings and Poincaré-Birkhoff-Witt extensions. *Pacific Journal of Mathematics*, 131(1):13–37, 1988.

[5] F. Chyzak and B. Salvy. Non-commutative elimination in Ore algebras proves multivariate identities. *Journal of Symbolic Computation*, 26(2):187–227, 1998.

[6] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Springer, 1997.

[7] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Springer, 1999.

[8] A. Galligo. Some algorithmic questions on ideals of differential operators. In *Proc. EUROCAL'85*, lncs 204, pages 413–421. Springer, 1985.

[9] M. Giesbrecht, G. Reid, and Y. Zhang. Non-commutative Gröbner bases in Poincaré-Birkhoff-Witt extensions. In *Conference on Computer Algebra and Scientific Computation (CASC'2002)*, pages 97–106, 2002.

[10] E. Green. An introduction to non-commutative Gröbner bases. In K. D. Fisher, editor, *Computational Algebras*, Lecture Notes in Pure and Applied Mathematics 151, pages 167–190. Dekker, New York.

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

[12] M. Insa and F. Pauer. Gröbner bases in rings of differential operators. In B. Buchberger and F. Winkler, editors, *Gröbner bases and applications*, LMS Lecture Notes series 251, pages 367–381. Cambridge University Press, 1998.

[13] A. Kandri-Rody and V. Weispfenning. Non-commutative Gröbner bases in algebras of solvable type. *Journal of Symbolic Computation*, (9):1–26, 1990.

[14] H. Kredel. *Solvable Polynomial Rings*. Verlag Shaker, Aachen., 1993.

[15] S. Mac Lane. *Homology*. Springer-Verlag, 1963.

[16] K. Madlener and B. Reinert. Computing Gröbner bases in monoid and group rings. In *Proc. ISSAC'93*, pages 254–263. ACM, 1993.

[17] E. L. Mansfield and P. A. Clarkson. Applicatioms of the differential algebra package `diffgob2` to classical symmetries of differential equations. *Journal of Symbolic Computation*, 23:517–533, 1997.

[18] T. Mora. Gröbner bases for non-commutative polynomial rings. In *Proc. AAECC-3*, volume 229 of *Lecture Notes in Computer Science*, pages 353–362. Springer, 1985.

[19] T. Mora. Standard bases and non-Noetherianity: non-commutative polynomial rings. In *Proc. AAECC-4*, volume 307 of *Lecture Notes in Computer Science*, pages 98–109. Springer, 1987.

[20] T. Mora. Gröbner bases in non-commutative algebras. In *ISSAC'88*, volume 359 of *Lecture Notes in Computer Science*, pages 150–161. Springer, 1988.

[21] T. Mora. An introduction to commutative and non-commutative Gröbner bases. *Theor. Comp. Sci.*, (134):131–173, 1994.

[22] A. Rosenmann. An algorithm for constructing Gröbner and free Schreier bases in free group algebras. *Journal of Symbolic Computation*, (16):523–549, 1993.

[23] V. Weispfenning. Finite Gröbner bases in non-Noetherian skew polynomial rings. In *Proc. ISSAC'92*, pages 329–334. ACM, 1992.