J. Symbolic Computation (2001) **32**, 699–716
doi:10.1006/jsco.2001.0491
Available online at http://www.idealibrary.com on IDEAL®

Towards an Effective Version of a Theorem of Stafford

ANDRE HILLEBRAND AND WILAND SCHMALE

Carl von Ossietzky Universität, FB Mathematik, D-26111 Oldenburg, Germany

A classical theorem of Stafford says: every left ideal of partial differential operators with rational or even polynomial coefficients in n variables can be generated by two elements. The highly involved proof of this theorem is reorganized and completed for rational coefficients in order to yield a procedure which guarantees the computability in finitely many steps. Consequences for an eventual normal form for matrices of such operators are discussed.

1. Introduction

Simplifying a matrix of differential operators by elementary row and column operations is quite a fundamental task. If one considers matrices whose entries are ordinary time-varying differential operators with rational function coefficients (or more generally meromorphic functions) then a classical theorem tells you that by elementary row and column operations an analogue to the Smith form can be achieved (see, for example, Cohn, 1971, Chapter 8.1; Guralnick *et al.*, 1988, the results going back to Jacobson, Nakayama and Teichmüller). In addition, by the simplicity of our ring of entries at most one diagonal entry can be different from 1 or 0. Thus time-varying differential matrices have a "simpler" diagonal form than constant ones.

If one considers matrices whose entries are partial differential operators with rational function coefficients (now in finitely many variables $x_1, \ldots, x_n$) then the ring of entries is still a simple one and one wonders what kind of simple form could be obtained by elementary row and column operations in this case.

This question is obviously related to the following question: how many generators are necessary to generate a left or a right ideal in the ring of the entries? An astonishing theorem of J.T. Stafford from 1978 tells us that always *two* generators will be sufficient and even more: given three operators a, b, c then there must exist operators λ, μ s.t. $a+\lambda c$ and $b+\mu c$ generate the same left ideal as a, b, and c. Thus the column ${}^t[a, b, c]$ can be transformed to the column ${}^t[a+\lambda c, b+\mu c, 0]$ by four elementary row operations provided you are in possession of the according multiplicators.

Stafford's proof (see Stafford, 1978; Björk, 1979) is involved and does not indicate at every stage how one could determine in finitely many steps all the intermediate operators which are necessary to finally obtain two generators for an ideal. In what follows we will give in the main Section 3 a modified proof of this result which is (if at all) only slightly less involved, but which shows that Stafford's approach can be made effective. To prove this we give an algorithmic procedure to find rather simply structured operators λ and μ which will do the job as described above. We will not give complexity bounds but it will

0747–7171/01/120699 + 18 $35.00/0

become obvious that the procedures will break down rapidly when increasing the degrees of the operator polynomials.

While the computation of a minimal set of generators for a left ideal is of interest on its own, simplifying matrices via such a complex procedure seems not advantageous. Therefore, in a short concluding Section 4, matrix simplification under an extended equivalence notion is considered.

In the differential algebra literature it seems that traditionally more often the situation is considered where the coefficients of the operators are polynomials (Weyl algebras) or power series rather than rational functions. But the latter represent an interesting case; see Cohn (1971, Chapter 8). Further motivation for us comes also from control theory, see, for example, Ilchmann *et al.* (1984) and Cotroneo (1999) for a recent source.

We also want to emphasize that the present work proves effectivity in the sense of Cohen *et al.* (1999). To be more precise: we will show how one can compute two generators as stated in Stafford's Theorem in finitely many steps if the differential operators have their coefficients from an effective rational function field (e.g. over $\mathbb{Q}$.) This is of course only the first and theoretical step towards computation in reasonable time and a detailed complexity analysis. Realistic algorithms may well proceed in a very different way. Such a situation seems common in computer algebra, one of various examples being the computation of Galois groups over the rationals, where the general proof of effectiveness (see, for example, van der Waerden, 1964) gives a correct algorithm but of extremely high complexity and has not so much to do with actual procedures for rapid computation up to order 9 say.

We begin with an introductory Section 2 where basic definitions and some fundamental properties are displayed (mostly without proofs).

2. Basic Notions

The following definitions and properties are fundamental. The latter are stated without proofs. We refer to Cohn (1971), Dauns (1982), Adams and Loustaunau (1996) and direct verification. n and r will always be fixed natural numbers. Our main object of investigation is described as follows:

Definition 2.1. Let K be a skew field of characteristic zero.
By $R_r = K(x_1, \ldots, x_n)[D_1, \ldots, D_r]$ we denote a ring with the following properties for $i, j \in \{1, \ldots, r\}$, $l, m \in \{1, \ldots, n\}$ and $k \in K$:

(a) $K(x_1, \ldots, x_n)$ is a quotient skew field of the polynomial ring $K[x_1, \ldots, x_n]$ s.t.: $x_l k = k x_l$ and $x_m x_l = x_l x_m$.
(b) R is generated as an algebra over $K(x_1, \ldots, x_n)$ by $D_1, \ldots, D_r$.
(c) $D_i x_i = 1 + x_i D_i$ and in the case $i \neq m$: $D_i x_m = x_m D_i$.
(d) $D_i D_j = D_j D_i$ and $k D_i = D_i k$.
(e) $\{D^\alpha \in R \mid \alpha \in \mathbb{N}^r\}$ is a commutative monoid (see (c)) and left-linear independent over $K(x_1, \ldots, x_n)$, where as usual $D^\alpha = D_1^{\alpha_1} \cdots D_r^{\alpha_r}$ for $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$ and $x^\beta = x_1^{\beta_1} \cdots x_n^{\beta_n}$ for $\beta \in \mathbb{Z}^n$.

Remark 2.2. Given $K(x_1, \ldots, x_n)$ the rings R_r can be constructed as iterated skew-polynomial rings. (See, for example, Cohn, 1971 or Dauns, 1982.) For $n = 0$ the ring

$R = K\ [D_1, \ldots, D_r]$ is just an ordinary polynomial ring in r commuting variables over a skew field K. The Weyl algebra $A_n = K[x_1, \ldots, x_n\ ;\ D_1, \ldots, D_n]$, K a commutative field, is of course a subring of R_n. Recall also that R_r has no zero-divisors and that its group of units is $K(x_1, \ldots, x_n) \setminus \{0\}$.

COROLLARY 2.3. *For $f \in K[x_1, \ldots, x_n]$ and $k \leq n$ let $\frac{\partial f}{\partial x_k}$ be the formal derivative of f with respect to x_k. Then (in R) one has for $k \leq r$: $D_k f = f D_k + \frac{\partial f}{\partial x_k}$.*

Let $r \leq n$ from now on. By $\leq$ we also denote a monomial order on $\mathbb{N}^r$ or equivalently on $\{D^\alpha \in R \mid \alpha \in \mathbb{N}^r\}$. By $\leq_0$ resp. $<_0$ we denote the weak order on $\mathbb{N}^r \times \mathbb{N}^r$ with the following properties for $\alpha, \beta \in \mathbb{N}^r$: $\alpha \leq_0 \beta$, if for all $i \leq r$ one has $\alpha_i \leq \beta_i$ and $\alpha <_0 \beta$, if $\alpha \leq_0 \beta$ and $\beta \neq \alpha$.

COROLLARY 2.4. *(a)* $R_r = \{\sum_{\alpha \in N} a_\alpha D^\alpha \in R_r \mid a_\alpha \in K(x_1, \ldots, x_n), N \subset \mathbb{N}^r \text{ finite}\}$ $= \{\sum_{\alpha \in N} D^\alpha b_\alpha \in R \mid b_\alpha \in K(x_1, \ldots, x_n), N \subset \mathbb{N}^r \text{ finite}\}$.
(b) According to (a) every $f \in R \setminus \{0\}$ has a (left-)representation as $f = \sum_{\alpha \leq \alpha_0} a_\alpha D^\alpha$, where $a_\alpha \in K(x_1, \ldots, x_n), \alpha_0 \in \mathbb{N}^r$ and $a_{\alpha_0} \neq 0$. From this, one obtains a (right-) representation: $f = \sum_{\alpha \leq \alpha_0} D^\alpha b_\alpha$, where $a_{\alpha_0} = b_{\alpha_0}$ and with some unique b_α. Usually one does not have $a_\alpha = b_\alpha$ for $\alpha < \alpha_0$. Take $D_1 x_1 = 1 + x_1 D_1$ as an example.

DEFINITION 2.5. Let f be represented as in Corollary 2.4 (b), then $LM(f) := D^{\alpha_0} \in R$ is the leading monomial and $LK(f) := a_{\alpha_0} = b_{\alpha_0} \in K(x_1, \ldots, x_n)$ the leading coefficient of f with respect to the monomial order $\leq$. This definition is independent of left or right representation of f

One has the familiar rules for LM and LK. Note also that R_1 is a left-(right-) Euclidean ring with respect to $deg : R_1 \setminus \{0\} \to \mathbb{N}$ where $deg(f) = m$, if $LM(f) = D^m$.

We will tacitly use the fact that standard Gröbner basis theory for commutative polynomial rings over a field K (see, for example, Adams and Loustaunau, 1996) extends without difficulty to a (left-/right-) Gröbner basis theory together with a Buchberger algorithm for submodules of R_r^k and syzygy-based computation of intersections of submodules. The effectivity (in the sense of Cohen *et al.*, 1999) of Gröbner bases for left-ideals, modules and intersections (e.g. with rational constants) is assumed to be well known. We will also have to apply a corresponding Hilbert basis theorem. There are various references where "classical" Gröbner basis theory is extended at least partly to more general scenarios. We only mention Chyzak (1998), Pesch (1998), Briançon and Maisonobe (1984) and Castro (1987) as examples. The last two have been pointed out to us by a referee and treat the case of power series and Weyl algebras.

DEFINITION 2.6. Let $f \in R_r$ and $k \leq r$, then we set $f^{(e_k)} := f x_k - x_k f \in R_r$ and iteratively for $m \in \mathbb{N}$ we set $f^{((m+1)e_k)} := (f^{(me_k)})^{(e_k)}$ where $f^{(0,\ldots,0)} := f$. $f^{(me_k)}$ is called the m-th derivative of f with respect to D_k. If $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$, then $f^{(\alpha)} := ((f^{(\alpha_1 e_1)})^{\cdots})^{(\alpha_r e_r)}$ is called the α-th derivative of f.

COROLLARY 2.7. *For $f \in R_r$ and $k \leq r$:*

(a) $f^{(\alpha)}$ is independent from its specific iterative definition.
(b) $f^{(me_k)}$ is the mth formal derivative of f with respect to D_k.

(c) $f^{(\alpha)} \in \sum_{\beta \leq_0 \alpha} R_r f x_1^{\beta_1} \cdots x_r^{\beta_r}$ *for* $\alpha \in \mathbb{N}^r$.

(d) *if* $LM(f) = D^\alpha$, *then* $f^{(\alpha)} \in K(x_1, \ldots, x_n) \setminus \{0\}$.

(e) R_r *is a simple ring, i.e.* R_r *does not possess nontrivial two-sided ideals.*

COROLLARY 2.8. R_r *is a left (and right) Ore-ring, i.e. for all* $a, b \in R_r \setminus \{0\}$ *one has* $R_r a \cap R_r b \neq \{0\}$ ($aR_r \cap bR_r \neq \{0\}$). *In other words, we have non-trivial common left- and right-multiples for non-trivial* a, b.

REMARK 2.9. For $r \geq 2$ the intersection of two left-principal ideals usually is no longer a principal ideal. Therefore one does not always have a least common left-multiple in the usual sense. R_r is not a left-principal ideal ring for $r \geq 2$.

EXAMPLE 2.10. For $g = D_2 \in R_2$ and $f = (D_1 + x_2) \in R_2$ the intersection $R_2 g \cap R_2 f$ is not a principal ideal as is easily verified.

REMARK 2.11. It is worthwhile to recall also, that unless $r = 1$ the ring R_r is atomic but not factorial (see Cohn, 1971 for the corresponding definitions). The latter can be illustrated by the following example:

EXAMPLE 2.12. $a := D_1 D_2^2 + x_2 D_2^2 + 2D_2 \in R_2$ has the following two atomic(!) decompositions: $a = (D_1 D_2 + x_2 D_2 + 2)D_2 = D_2 D_2 (D_1 + x_2)$.

REMARK 2.13. Since R_r is an Ore-ring without zero-divisors, it is possible to form a quotient ring $\mathcal{R}_r = K(x_1, \ldots, x_n)(D_1, \ldots, D_r)$ of the form

$$\mathcal{R}_r = \{f g^{-1} \mid f, g \in R_r, g \neq 0\} = \{g^{-1} f \mid f, g \in R_r, g \neq 0\}.$$

The tedious proof is given in Dauns (1982).

DEFINITION 2.14. We call $c = lclm(a, b) \in R_r$ (resp. $c = lcrm(a, b)$) a least common left- (resp. right-) multiple of $a, b \in R_r \setminus \{0\}$ with respect to $\leq$ if c has the following properties: (a) c is a common left- (right-) multiple of a, b, (b) $LK(c) = 1$ and (c) $LM(c)$ is minimal with respect to $\leq$.

If c is a $lclm(a, b)$, then it is unique, for if $d \in R_r \setminus \{c\}$ satisfies also (a),(b),(c) in 2.14, then set $e = \frac{1}{LK(d-c)}(d - c) \in R_r$. Now e is a normed common left-multiple, but at the same time $LM(e) = LM(d - c) < LM(d) = LM(c)$ contradicting (c).

REMARK 2.15. (a) Note that a $lclm$ in R_r with $r \geq 2$ is in general not a right divisor of all left-multiples. "Least" just means that its leading monomial with respect to the given monomial order is minimal.
(b) Let $a, b \in R_r \setminus \{0\}$ and $G = \{g_1, \ldots, g_m\}$ be the reduced left Gröbner basis of $R_r a \cap R_r b$ with respect to a monomial order $\leq$. Let g_i be the basis element with the least

leading monomial then $g := \frac{1}{LK(g_i)} g_i$ is the unique $lclm(a, b)$. As for the computation of a left Gröbner basis of $R_r a \cap R_r b$ we refer to the syzygy-based approach as outlined in Adams and Loustaunau (1996, Chapter 3.8) and which generalizes straightforwardly.

3. An Effective Version of Stafford's Theorem

Stafford's theorem says that any left ideal from R_r can be generated by two elements. A left ideal generated by $a, b, \ldots$ will be denoted by $\mathcal{I}_l(a, b, \ldots)$.

So for instance the left Gröbner basis $\{D_1, D_2, D_3\} \in R_3$ (with respect to any monomial order) of the ideal $I := \mathcal{I}_l(D_1, D_2, D_3)$ can be shrunk to the generating system $\{D_1, D_2 + x_1 D_3\}$. This follows from the fact that $D_3 = D_1(D_2 + x_1 D_3) - (D_2 + x_1 D_3) D_1 \in \mathcal{I}_l(D_1, D_2 + x_1 D_3)$ and therefore also $D_1, D_2 \in \mathcal{I}_l(D_1, D_2 + x_1 D_3)$.

By Hilbert's Basis Theorem we know already that any left ideal $I \subset R_r$ can be finitely generated. So it suffices to show that from any three generators $a, b, c \in I$ one can construct a new generating set consisting of only two generators. This construction will have various steps which are grouped iteratively according to the number of variables which are involved. The overall method follows as far as possible Stafford's proof as presented in the book of Björk (1979), but various substantial modifications become necessary in order to obtain computability in finitely many steps. Before going into the details we will try to make plausible the main ideas:

(1) For $a, b, c \in R_n$ we will look for generators of the form $a + a_0 c, b + b_0 c \in R_n$ $(a_0, b_0 \in R_n)$ s.t. $\mathcal{I}_l(a + a_0 c, b + b_0 c) = \mathcal{I}_l(a, b, c)$. This will be achieved, if

$$c \in R_n(a + a_0 c) + R_n(b + b_0 c).$$

(2) In order to find such $a_0, b_0 \in R_n$ we will look for $q_r \in R_r \setminus \{0\}$, $a_r, b_r \in R_n$ and successively for decreasing r s.t.

$$q_r c \in R_n(a + a_r c) + R_n(b + b_r c).$$

See below 3.10. For $r = n$ the existence of q_n (with $a_n = b_n = 0$) is guaranteed by the Ore-ring property. Given q_n, in Lemma 3.10 one guarantees the existence of $q_{n-1}, q_{n-2}, \ldots, q_0$. On arriving at $r = 0$ the nonzero element q_0 on the left is a unit and $c \in R_n(a + a_0 c) + R_n(b + b_0 c)$. So what will be done is a kind of elimination of the D_i from q_r. For this the following result is essential and one main ingredient of a finite computational procedure:

(3) For any $v \in R_n \setminus \{0\}$ and $q_{r+1} \in R_{r+1}$ one can find an $f \in \mathbb{Z}[x_1, \ldots, x_n]$ and a $q_r \in R_r \setminus \{0\}$ s.t.

$$q_r \in R_n q_{r+1} + R_n v f,$$

See Lemma 3.9. This means that by the determination of an appropriate and simply structured f one can assure that in the ideal $R_n q_{r+1} + R_n v f$ one finds a nonzero element involving only the first r differential operators despite the fact that q_{r+1} and vf may involve more variables.

(4) The task to find such an f will become easier if one works for a while in the ring

$$\mathcal{R} = K(x_1, \ldots, x_n)(D_1, \ldots, D_r)[D_{r+1}, \ldots, D_n]$$

instead of R. The element q_r in (3) will then be a unit. The requirements for $f \in \mathbb{Z}[x_1, \ldots, x_n]$ are then

$$1 \in \mathcal{R} q_{r+1} + \mathcal{R} v f \quad \text{or} \quad \mathcal{R} = \mathcal{R} q_{r+1} + \mathcal{R} v f.$$

See Theorem 3.5.

(5) Since q_{r+1} is already in R_{r+1}, it will be important to separate the variable D_{r+1} in v (see the equation in (4)) from the remaining variables. For this v will be decomposed: $v = \sum_{i=0}^{t} D_{r+1}^i g_i$ where the g_i do not involve D_{r+1}.
Now for any $u \in R_n$ one determines finitely many $h_j \in \mathbb{Z}[x_{r+2}, \ldots, x_n]$ and $f_j \in \mathbb{Z}[x_{r+1}]$ s.t.

$$\mathcal{R}q_{r+1} + \mathcal{R}u + \sum_i \mathcal{R}g_i h_j = \mathcal{R}q_{r+1} + \mathcal{R}\Big(u + \sum_i D_{r+1}^i g_i h_j f_j\Big)$$

and

$$\mathcal{R} = \mathcal{R}q_{r+1} + \sum_j \sum_i \mathcal{R}g_i h_j.$$

Setting $f = \sum_j h_j f_j$ this leads to an equation as in (4).

(6) In order to attack the equations to be solved in (5) they are rewritten with $e_0 := u$, $e_i := g_i h_j, f := f_j, \delta_i := D_{r+1}^{i-1}$. This gives

$$\mathcal{R}q_{r+1} + \sum_{i\geq 0} \mathcal{R}e_i = \mathcal{R}q_{r+1} + \mathcal{R}\Big(e_0 + \sum_{i\geq 1} \delta_i e_i f\Big).$$

Stafford's main trick now is to interpret the e_i $(i = 0, \ldots, m)$ as canonical basis vectors of the left $\mathcal{R}$-module $\mathcal{R}^{m+1}$ and $\mathcal{R}q_{r+1}$ as $\mathcal{R}^{m+1}\rho$ where ρ is from R_{r+1}. Having done this and remembering that in $\mathcal{R}$ nonzero polynomials involving only $D_1, \ldots, D_r$ are units, one realizes that, in our equation to be solved the entries $\rho, e_i, \delta_i e_i f$ have only D_{r+1} as a variable over $= K(x_1, \ldots, x_n)(D_1, \ldots, D_r)$. So one has to look for an $f \in \mathbb{Z}[x_{r+1}]$ which solves the following equation for the ring $S = \overline{K}(x_{r+1})[D_{r+1}]$:

$$S^{m+1} = S^{m+1}\rho + S\Big(e_0 + \sum_{i=1}^{m} D_{r+1}^{i-1} f e_i\Big)$$

where $\overline{K} := K(x_1, \ldots, x_{r-1}, x_{r+1}, \ldots, x_n)(D_1, \ldots, D_r)$. After this an easy linear map gets you back to the situation of (5) together with solutions ready at hand.

In what follows we will go the opposite way since this is mathematically more efficient. So we start with the problem as outlined in (6). All the f and f_j which have to be constructed play a central role for the realization of a constructive approach. It is mainly the wish to find f and f_j which are as simple as possible which makes it necessary to alter and reorganize the proofs for the various steps in Stafford's resp. Björk's approach.

3.1. Some properties of modules in one variable

Let T be a skew field of characteristic zero and $S := T(x)[D]$ with the same properties as R_1. We do not call this ring R_1 for technical reasons.

Lemma 3.1. *Let $\rho, \delta_1, \ldots, \delta_m \in S \setminus \{0\}$ with $deg_D(\delta_i) < deg_D(\delta_{i+1})$ for $i < m$.*

(a) *Let $I := \mathcal{I}_l\left(\left\{\sum_{k=1}^{m} \delta_k x^i e_k \,\middle|\, i \leq deg_D(\delta_m)\right\}\right)$. Then $I = S^m$ where $e_1, \ldots, e_m$ are the canonical basis vectors in S^m.*

(*b*) *Let $M \subset S^m$ be a left S-submodule with $S^m\rho \subset M$ and let $\alpha \in S \setminus \{0\}$. Then one can find a finite subset N of $\mathbb{N}$ such that with $f = \sum_{i\in N} x^i \in \mathbb{Z}[x]$ the following equation is valid:*

$$S^m = M + S\left(\sum_{k=1}^{m} \alpha\delta_k f e_k\right).$$

Proof. (a) For $f \in S$ and $k \in \mathbb{N}$ let $f^{(k)}$ be the kth derivative with respect to to D and for $k \leq deg_D(\delta_m)$ we set $\gamma_k := \sum_{i=1}^{m} \delta_i^{(k)} e_i$ and note that $\gamma_k \in I$ according to Corollary 2.7 (c). Then, by properties of derivative and degree, one obtains for $l = deg_D(\delta_m)$ $\gamma_l = \sum_{i=1}^{m} \delta_i^{(l)} e_i = \delta_m^{(l)} e_m \in T(x)e_m$. Also $e_m \in I$ and for some $s_k \in S$ one has $\gamma_k^* := \sum_{i=1}^{m-1} \delta_i^{(k)} e_i = \gamma_k - s_k e_m \in I$. Considering γ_l^* for $l = deg_D(\delta_{m-1})$ shows that $e_{m-1} \in I$. Iteration proves (a).

(b) The left module S^m/M has finite length since S is left-Euclidean. (b) will be proved now by induction on the length of S^m/M. For $M = S^m$ the statement is trivial. Let the statement be true for all submodules M_1 properly containing M. Thus $length(S^m/M_1) < length(S^m/M)$. According to (a) and with $\alpha\delta_i$ instead of δ_i one can find an $f_0 = \pm x^{k_0}$ s.t. $\alpha\delta_1 f_0 e_1 + \cdots + \alpha\delta_m f_0 e_m \notin M$. Otherwise one would have a contradiction to (a) with $\delta_i := \alpha\delta_i$. Choose now a submodule $M_1 \subset S^m$ properly containing M and of the form

$$M \subset M_1 \subset M + S(\alpha\delta_1 f_0 e_1 + \cdots + \alpha\delta_m f_0 e_m)$$

and M maximal in M_1. Since S is an Ore-domain, one can determine an $s \in S \setminus \{0\}$ which gives $s\alpha\delta_i \in S\rho$ for all $i \leq m$. By the induction hypothesis for $\alpha_1 := s\alpha \in S \setminus \{0\}$ there exists $f_1 = x^{l_1} + \cdots + x^{l_t}$ with

$$S^m = M_1 + S(\alpha_1\delta_1 f_1 e_1 + \cdots + \alpha_1\delta_m f_1 e_m). \qquad (*)$$

Now let $N := M + S\left(\sum_{i=1}^{m} \alpha\delta_i f_1 e_i\right)$. If $N = S^m$, then (b) is proved, otherwise we prove in the sequel that

$$S^m = M + S\left(\sum_{i=1}^{m} \alpha\delta_i (f_0 + f_1) e_i\right) =: N_1,$$

or equivalently that some $f = f_1 + f_0 = f_1 \pm x^{k_0}$ satisfies (b). More precisely: set $f = f_1 + x^{k_0}$ if the k_0th coefficient of f_1 is zero, else set $f = f_1 - x^{k_0}$. Then it is guaranteed that f has only coefficients from $\{0, 1\}$. To prove now that $N_1 = S^m$, let $P := S\left(\sum_{i=1}^{m} \alpha_1\delta_i f_1 e_i\right)$ and $N_0 := M + P$.
Since $S^m = M_1 + P$ (by (*)) we conclude

$$S^m/N_0 = (M_1 + P)/(M + P) \cong M_1/(M + M_1 \cap P).$$

Since furthermore M_1/M by the choice of M_1 and in particular $M_1/M + M_1 \cap P$ are indecomposable, the submodule N_0 of S^m must be maximal. By the equation

$$S^m \neq N = M + S\left(\sum_{i=1}^{m} \alpha\delta_i f_1 e_i\right) \supset M + S\left(\sum_{i=1}^{m} s\alpha\delta_i f_1 e_i\right) = M + P = N_0,$$

we get $N = N_0$. Also $s\alpha\delta_i f_0 \subseteq S\rho$ for all $i \leq m$ and $S^m\rho \subset M$, where from we get

$$P = S\left(\sum_{i=1}^{m} s\alpha\delta_i f_1 e_i\right) \subset S^m\rho \subset M \subset N_1.$$

Therefore $N_1 \supset M + P = N_0 = N$ and by definition of N and N_1 we see $\sum_{i=1}^{m} \alpha\delta_i f_1 e_i \in N_1$ resp. $\sum_{i=1}^{m} \alpha\delta_i f_0 e_i \in N_1$. Since by the choice of M_1 we have $M_1 \subset M + S\left(\sum_{i=1}^{m} \alpha\delta_i f_0 e_i\right) \subset N_1$, we finally obtain the desired result (*).

In the sequel $\mathcal{R}_r$ denotes the quotient skew field of R_r. □

LEMMA 3.2. *Let $S = \mathcal{R}_r[D_{r+1}]$ and let $\delta_1, \ldots, \delta_m \in S, \rho \in \mathcal{R}_{r+1} \setminus \{0\}$ with $deg_{D_{r+1}}(\delta_i) < deg_{D_{r+1}}(\delta_{i+1})$. Then there exists a finite subset N of $\mathbb{N}$ such that with $f = \sum_{i \in N} x_{r+1}^i \in \mathbb{Z}[x_{r+1}]$ one has*

$$S^{m+1} = S^{m+1}\rho + S\left(e_0 + \delta_1 f e_1 + \cdots + \delta_m f e_m\right).$$

PROOF. For $x = x_{r+1}, D = D_{r+1}$ and $M = S^m\rho$ part (b) Lemma 3.1 gives

$$S^m = S^m\rho + S\left(\sum_{i=1}^{m} \rho\delta_i f e_i\right).$$

Here the trick consists in introducing ρ in the right-hand sum. This implies

$$S^{m+1} = S^{m+1}\rho + S\left(e_0 + \sum_{i=1}^{m} \rho\delta_i f e_i\right) + Se_0.$$

It remains to show that

$$e_0 \in S^{m+1}\rho + S\left((e_0 + \sum_{i=1}^{m} \delta_i f e_i\right),$$

which follows indeed after a short calculation using Lemma 3.1. □

3.2. First step towards a procedure

In this subsection the result from Lemma 3.2 will be translated into a result on left ideals in R_r via a linear transformation (Φ in the proof of Lemma 3.4). Thus Theorem 3.5 tells that the sum of two left principal ideals can give us the whole ring by only modifying one generator by an invertible right factor. In the case of only one variable this is easy to understand: let $q, v \in R_1 \setminus \{0\}$. Since R_1 is a left principal ideal ring, for some $c \in R_1 \setminus \{0\}$ one must have $R_1 q + R_1 v = R_1 c$. If in addition q and v are right coprime, then $c = 1$. Otherwise replace v by vf with $f \in K(x_1, \ldots, x_n)$ in such a way that q and vf become right coprime. When v is no longer from R_1 but rather from R_n then the additional differential operators make impossible a similar approach . This explains the digression on the left S-module S^m. The f occurring in the related results is of central importance. Towards the end of this subsection an explicit procedure will be given for its computation. But before that some more preparation is necessary.

Recall that $\mathcal{R} := \mathcal{R}_r[D_{r+1}, \ldots, D_n]$ where $\mathcal{R}_r$ is the quotient skew field of $R_r = K(x_1, \ldots, x_n)[D_1, \ldots, D_r]$.

LEMMA 3.3. *Asume $a_1, \ldots, a_s \in R_n$ and $q \in R_r \setminus \{0\}$. Then there is a $\rho \in R_r \setminus \{0\}$, s.t. for all $i \leq s$ one has*

$$\rho a_i \in R_n q.$$

PROOF. $a\frac{1}{q} \in \mathcal{R}$ for any $a \in R_n$ and can be written as: $a\frac{1}{q} = \sum_{0\leq_0\gamma\leq_0\beta} b_\gamma D^\gamma$ where $\beta = (0,\ldots,0,\beta_{r+1},\ldots,\beta_n) \in \mathbb{N}^n$ and for some $b_\gamma \in \mathcal{R}_r$, say $b_\gamma = \frac{1}{b_{\gamma 1}} b_{\gamma 2}$ with $b_{\gamma 1}, b_{\gamma 2} \in R_r$. Multiplication by a common left multiple $\in R_r$ of all the $b_{\gamma 1}$ gives $ba\frac{1}{q} = \sum_{0\leq_0\gamma\leq_0\beta} bb_\gamma D^\gamma$ $\in R_n$. Thus $ba \in R_n q$. Applying this we obtain for any $i \leq s$ a certain $b_i \in R_r$, s.t. $b_i a_i \in R_n q$. Therefore, with a nontrivial common left multiple $\rho \in R_r$ of $b_1,\ldots,b_s$ we see that $\rho a_i \in R_n q$ for all $i \leq s$. □

LEMMA 3.4. *Let $q \in R_{r+1} \setminus \{0\}$ and $u \in R_n$. For any $b_0,\ldots,b_t \in R_r[D_{r+2},\ldots,D_n]$ we can find a finite subset set $N \subset \mathbb{N}$ s.t. with $f = \sum_{i\in N} x_{r+1}^i \in \mathbb{Z}[x_{r+1}]$ one has:*

$$\mathcal{R}q + \mathcal{R}u + \sum_{i=0}^{t} \mathcal{R}b_i = \mathcal{R}q + \mathcal{R}\left(u + \sum_{i=0}^{t} D_{r+1}^i f b_i\right).$$

PROOF. By Lemma 3.3 we find $\rho \in R_{r+1} \setminus \{0\}$ s.t.

$$\rho u \in R_n q \qquad \text{and} \qquad \rho b_i \in R_n q$$

for all $0 \leq i \leq t$. For $\delta_i := D_{r+1}^{i-1}$, according to Lemma 3.2 there is an $f = \sum_{j\in N} x_{r+1}^j \in \mathbb{Z}[x_{r+1}]$ satisfying the equation:

$$\mathcal{R}_r^{t+2}[D_{r+1}] = \mathcal{R}_r^{t+2}[D_{r+1}]\rho + \mathcal{R}_r[D_{r+1}](e_0 + D_{r+1}^0 f e_1 + \cdots + D_{r+1}^t f e_{t+1})$$

which leads to

$$\mathcal{R}^{t+2} = \mathcal{R}^{t+2}\rho + \mathcal{R}(e_0 + D_{r+1}^0 f e_1 + \cdots + D_{r+1}^t f e_{t+1}) \qquad (*)$$

since $\mathcal{R}_r[D_{r+1}] \subset \mathcal{R}$. Define the left $\mathcal{R}$-linear map $\Phi : \mathcal{R}^{t+2} \to \mathcal{R}$ by $\Phi(e_0) = u$ and $\Phi(e_i) = b_{i-1}$ for $1 \leq i \leq t+1$. Then

$$\Phi(\mathcal{R}^{t+2}) = \mathcal{R}u + \mathcal{R}b_0 + \cdots + \mathcal{R}b_t$$

which in turn implies

$$\begin{aligned}
\mathcal{R}q + \mathcal{R}u + \sum_{i=0}^{t} \mathcal{R}b_i &= \mathcal{R}q + \Phi(\mathcal{R}^{t+2}) \\
&\overset{(*)}{=} \mathcal{R}q + \Phi\left(\mathcal{R}^{t+2}\rho + \mathcal{R}(e_0 + D_{r+1}^0 f e_1 + \cdots + D_{r+1}^t f e_{t+1})\right) \\
&= \mathcal{R}q + \Phi(\mathcal{R}^{t+2}\rho) + \mathcal{R}\left(u + \sum_{i=0}^{t} D_{r+1}^i f b_i\right). \qquad (**)
\end{aligned}$$

According to our choice of ρ we have $\rho u, \rho b_i \in R_n q \subset \mathcal{R}$ and therefore

$$\Phi(\mathcal{R}^{t+2}\rho) = \mathcal{R}\rho\Phi(e_0) + \cdots + \mathcal{R}\rho\Phi(e_{t+1}) = \mathcal{R}\rho u + \mathcal{R}\rho b_0 + \cdots + \mathcal{R}\rho b_t \subset \mathcal{R}q.$$

The latter has now only to be inserted in $(**)$ in order to prove the Lemma. □

THEOREM 3.5. *For any $v \in R_n \setminus \{0\}$ and any $q \in R_{r+1} \setminus \{0\}$ there is a finite subset N of $\mathbb{N}$ s.t. with $f = \sum_{\alpha\in N} x^\alpha \in \mathbb{Z}[x_1,\ldots,x_n]$ one has $\mathcal{R} = \mathcal{R}q + \mathcal{R}vf$.*

Note that if the characteristic of K is $p \neq 0$, then the theorem does not hold. A simple counterexample is as follows. Let $v = q = D_{r+1}^p$, then $\mathcal{R}D_{r+1}^p$ is a two-sided principal ideal and $\mathcal{R}q + \mathcal{R}vf = \mathcal{R}D_{r+1}^p \neq \mathcal{R}$ for all $f \in \mathcal{R}$.

Proof. We decompose v as follows:

$$v = \sum_{i=0}^{t} D_{r+1}^i g_i \qquad \text{with} \quad g_0, \ldots, g_t \in \mathcal{R}_{\setminus\{r+1\}} := \mathcal{R}_r[D_{r+2}, \ldots, D_n], \qquad t \in \mathbb{N}. \tag{1}$$

For a nonzero coefficient g_k we determine its leading monomial in $\mathcal{R}_{\setminus\{r+1\}}$: $D^\alpha := D^{(\alpha_{r+2},\ldots,\alpha_n)} := LM(g_k)$. Note that

$$\mathcal{R}_{\setminus\{r+1\}} = (K(x_{r+1}))\,(x_1, \ldots, x_r, x_{r+2}, \ldots, x_n)(D_1, \ldots, D_r)[D_{r+2}, \ldots, D_n].$$

Thus $\mathcal{R}_{\setminus\{r+1\}}$, up to renumbering, is one of the rings we have been investigating until now. Thus we know that $g_k^{(\alpha)} \in K(x_1, \ldots, x_n)(D_1, \ldots, D_r) \setminus \{0\}$ by 2.7 (c) and (d) and that $g_k^{(\alpha)} \in \sum_{\beta \leq_0 \alpha} \mathcal{R}_{\setminus\{r+1\}} g_k x_{r+2}^{\beta_{r+2}} \cdots x_n^{\beta_n}$. Defining

$$\{h_0, \ldots, h_m\} := \left\{ x_{r+2}^{\beta_{r+2}} \cdots x_n^{\beta_n} \;\middle|\; \beta \leq_0 \alpha \right\} \tag{2}$$

we arrive at the equality $\mathcal{R} = \mathcal{R}g_k^{(\alpha)} = \sum_{j=0}^{m} \mathcal{R}g_k h_j$, and then, of course, also

$$\mathcal{R} = \sum_{j=0}^{m} \sum_{i=0}^{t} \mathcal{R}g_i h_j + \mathcal{R}q. \tag{3}$$

Now apply Lemma 3.4 with $b_i := g_i h_0$ and $u := 0$ to obtain $f_0 = \sum_{i \in N} x_{r+1}^i$ with some finite subset $N \subset \mathbb{N}$ and which satisfies

$$\mathcal{R}q + \sum_{i=0}^{t} \mathcal{R}g_i h_0 = \mathcal{R}q + \mathcal{R}\left(\sum_{i=0}^{t} D_{r+1}^i f_0 g_i h_0 \right).$$

Since $g_i \in \mathcal{R}_{\setminus\{r+1\}}$, f_0 commutes with g_i for $0 \leq i \leq t$ and remembering that $v = \sum_{i=0}^{t} D_{r+1}^i g_i$ we get

$$\mathcal{R}q + \sum_{i=0}^{t} \mathcal{R}g_i h_0 \subseteq \mathcal{R}q + \mathcal{R}(v f_0 h_0). \tag{4}$$

Note that for later use in an algorithm here and later on in the proof we do not apply the complete information of Lemma 3.4 which would give us equality. Define now $f := f_0 h_0$, $b_i := g_i h_1$ and $u := vf$. Then again by Lemma 3.4 we find $f_1 \in \mathbb{Z}[x_{r+1}]$ with $\mathcal{R}q + \mathcal{R}vf + \sum_{i=0}^{t} \mathcal{R}g_i h_1 \subseteq \mathcal{R}q + \mathcal{R}\big(vf + \sum_{i=0}^{t} D_{r+1}^i f_1 g_i h_1\big)$ and since also f_1 commutes with the g_i, this time we arrive at the inclusion $\mathcal{R}q + \mathcal{R}vf + \sum_{i=0}^{t} \mathcal{R}g_i h_1 \subseteq \mathcal{R}q + \mathcal{R}(vf + v f_1 h_1)$. Applying (4) we obtain:

$$\mathcal{R}q + \sum_{i=0}^{t} \mathcal{R}g_i h_0 + \sum_{i=0}^{t} \mathcal{R}g_i h_1 \subseteq \mathcal{R}q + \mathcal{R}(vf + v f_1 h_1). \tag{5}$$

After updating f as $f := f + f_1 h_1$ this appears as follows:

$$\mathcal{R}q + \sum_{i=0}^{t} \mathcal{R}g_i h_0 + \sum_{i=0}^{t} \mathcal{R}g_i h_1 \subseteq \mathcal{R}q + \mathcal{R}vf. \tag{6}$$

We now proceed in the same way. This time we apply Lemma 3.4 with $b_i := g_i h_2$ and $u := vf$ to obtain $f_2 \in \mathbb{Z}[x_{r+1}]$, s.t.

$$\mathcal{R}q + \mathcal{R}vf + \sum_{i=0}^{t} \mathcal{R}g_i h_2 \subseteq \mathcal{R}q + \mathcal{R}(vf + vf_2h_2). \tag{7}$$

Applying (6), now we obtain

$$\mathcal{R}q + \sum_{i=0}^{t} \mathcal{R}g_i h_0 + \sum_{i=0}^{t} \mathcal{R}g_i h_1 + \sum_{i=0}^{t} \mathcal{R}g_i h_2 \subseteq \mathcal{R}q + \mathcal{R}(vf + vf_2h_2).$$

Then we update f again, $f := f + f_2h_2$, and obtain $\mathcal{R}q + \sum_{j=0}^{2}\sum_{i=0}^{t} \mathcal{R}g_i h_j \subseteq \mathcal{R}q + \mathcal{R}vf$. After m steps (or eventually already earlier) we must arrive at the inclusion $\mathcal{R}q + \sum_{j=0}^{m}\sum_{i=0}^{t} \mathcal{R}g_i h_j \subseteq \mathcal{R}q + \mathcal{R}vf$ with some $f = f_0h_0 + \cdots + f_mh_m$. The equation (3) then shows us that finally $\mathcal{R} = \mathcal{R}q + \mathcal{R}vf$. □

Algorithm 3.6. The following algorithm proceeds as indicated by the foregoing proof and explicitly determines an f.

Let $\leq$ be a monomial order on $\{D_{r+1}^{\alpha_{r+1}} \cdots D_n^{\alpha_n} \in \mathcal{R} \mid \alpha_{r+1}, \ldots, \alpha_n \in \mathbb{N}\}$
Input: $v \in R_n \setminus \{0\}, q \in R_{r+1} \setminus \{0\}$
Output: $f \in \mathbb{Z}[x_1, \ldots, x_n]$ satisfying the equality $\mathcal{R} = \mathcal{R}q + \mathcal{R}vf$

Start: decompose v as $v = \sum_{i=0}^{t} D_{r+1}^i g_i, g_t \neq 0$ with $g_i \in \mathcal{R}_{\setminus\{r+1\}}$
$D^\alpha := D^{(\alpha_{r+2},\ldots,\alpha_n)} := LM(g_t)$
For $i = 0$ to $t-1$ repeat:
$D_{r+2}^{\beta_{r+2}} \cdots D_n^{\beta_n} := LM(g_i)$
If $g_i \neq 0$ and $\prod_{i=r+2}^{n}(\beta_i + 1) < \prod_{i=r+2}^{n}(\alpha_i + 1)$ then set $\alpha := \beta$
End For
Set $J := \{x_{r+2}^{\gamma_{r+2}} \cdots x_n^{\gamma_n} \mid \gamma \leq_0 \alpha\}$
Reduce J to $\{h_1, \ldots, h_m\} \subset J$, s.t. still $\sum_{j=1}^{m}\sum_{i=0}^{t} \mathcal{R}g_i h_j + \mathcal{R}q = \mathcal{R}$
$k := 1,\ f := 0$
Repeat:
Compute a left Gröbner basis G_k of $\mathcal{R}q + \sum_{j=1}^{k}\sum_{i=0}^{t} \mathcal{R}g_i h_j$
Repeat:
Choose in a systematic way a finite set $N \in \mathbb{N}$
and f_k of the form $f_k := \sum_{i \in N} x_{r+1}^i$
Compute a left Gröbner basis F_k of $\mathcal{R}q + \mathcal{R}v(f + f_kh_k)$
Until $\sum_{g \in G_k} \mathcal{R}g \subset \sum_{h \in F_k} \mathcal{R}h$
$f := f + f_kh_k$
$k := k + 1$
Until $\mathcal{R}$ is generated by F_k
Display f
End.

Proof. This algorithm follows the proof of Theorem 3.5. At first v is decomposed as in (1). Then in the For-loop a good coefficient g_i and its leading monomial $LM(g_i) =$

D^α are determined in such a way that the set J becomes as small as possible ($|J| = \prod_{i=r+2}^{n}(\alpha_i + 1)$, see (2)). Thereafter (not necessary for the algorithm to work) one can apply some strategy in order to minimize the set J without violating (3).

Now the proper algorithm starts: in the repeat loop a left Gröbner basis G_k of $\mathcal{R}q + \sum_{i=0}^{t}\sum_{j=1}^{k}\mathcal{R}g_ih_j$ is computed. This is done to eventually "simplify" the generating system of the ideal. After this one tries various $f_k = \sum_{i\in N} x_{r+1}^i$ and computes in each case a left Gröbner basis F_k of $\mathcal{R}q + \mathcal{R}(f + f_kh_k)$. This must be done until the left $\mathcal{R}$-ideal generated by F_k contains the left $\mathcal{R}$-ideal generated by G_k in which case $\mathcal{R}q + \sum_{j=1}^{k}\sum_{i=0}^{t}\mathcal{R}g_ih_j \subseteq \mathcal{R}q + \mathcal{R}(f + f_kh_k)$ (see (4), (5), (7) in the proof of Theorem 3.5).

At this point the following questions arise:

(a) How can one check the inclusion $\sum_{g\in G_k}\mathcal{R}g \subseteq \sum_{h\in F_k}\mathcal{R}h$?
(b) How can one find the f_k in such a way that the algorithm stops after finitely many steps?

(a): Since F_k is a left Gröbner basis of $\sum_{h\in F_k}\mathcal{R}h$, a polynomial g is from $\sum_{h\in F_k}\mathcal{R}h$ if and only if the reduction remainder $\overline{g}^{F_k,l}$ is zero.
Therefore $\sum_{g\in G_k}\mathcal{R}g \subseteq \sum_{h\in F_k}\mathcal{R}h$ only if $\overline{g}^{F_k,l} = 0$ for all $g \in G_k$.
(b): We know that an $f_k = \sum_{i\in N} x_{r+1}^i$, which makes the algorithm stop, must exist, see (4), (5), (7). Therefore, taking successively $f = 1,\ x_{r+1},\ x_{r+1}+1,\ x_{r+1}^2,\ x_{r+1}^2 + 1,\ x_{r+1}^2 + x_{r+1},\ x_{r+1}^2 + x_{r+1} + 1,\ x_{r+1}^3, \ldots$ after finitely many steps one must meet a good choice. Apparently any section-finite linear order for the admitted monomial sums can be used.
The algorithm as a whole stops at the latest when $k = m + 1$ because of (3). □

The foregoing Theorem and the algorithm prove the effectiveness of the determination of a very simple "trivializing" polynomial f. Note that there is no need to determin lengths of quotient modules or other objects which have been of importance in the preparation of the mathematical background via the Lemma 3.1 to 3.4.

Example 3.7. Let $v = D_3^2 + x_3$, $q = D_1 + x_2$ and $\mathcal{R} = K(x_1, x_2, x_3)[D_1, D_2, D_3]$, so in this case $r = 0$. q is an element of R_1. As a monomial order let us take the lexicographic order with $D_1 < D_2 < D_3$.
The decomposition of v in this example is trivial. One has $v = g_0 = D_3^2 + x_3$. Since the leading monomial of g_0 is D_3^2, we get $J = \{1, x_3, x_3^2\}$. J can be reduced to $J = \{h_1, h_2\} = \{x_3, 1\}$, since $\{1\}$ is a left Gröbner basis of $\mathcal{I}_l(q, g_0h_1, g_0h_2)$. Now we enter the repeat loop. One computes $G_1 = \{D_1 + x_2, x_3D_3^2 + x_3^2 + 2D_3\}$ as a Gröbner basis of $\mathcal{I}_l(q, g_0h_1)$. Since $g_0 = v$, already $f_1 = 1$ is a good choice. The algorithm then updates $f := 0 + f_1h_1 = x_3$. For the second way through the main repeat loop the algorithm determines $G_2 = \{1\}$ as a left Gröbner basis for $\mathcal{I}_l(q, g_0h_1, g_0h_2)$. The choice $f_2 = 1$ is not a good one in this case, but the choice $f_2 = x_1$ is good, since the set $\{q, v(f + f_2h_2)\}$ left-generates the whole ring.
Thus the output of the algorithm in this simple example is $f := x_3 + x_1$.

Remark 3.8. Computation in the foregoing simple example and in Example 3.13 below can still be done by hand. More complex examples have been computed with the help of

MapleV5-versions of the algorithms in this article and applying the Gröbner basis and multiplication facility of Chyzak's nice Ore-algebra package (to be used carefully).

3.3. An effective version of Stafford's theorem

In this subsection the proof of Stafford's theorem will be completed and an algorithm will be presented to compute generators as stated in the theorem. To achieve this, and as a first step, we will have to interpret for the ring R_r our results for $\mathcal{R}$:

Lemma 3.9. *Let $v \in R_n \setminus \{0\}, q_{r+1} \in R_{r+1} \setminus \{0\}$ and $f \in \mathbb{Z}[x_1, \ldots, x_n]$ s.t. $\mathcal{R} = \mathcal{R}q_{r+1} + \mathcal{R}vf$ (see Theorem 3.5). Then the following statements hold and are equivalent:*

(*a*) *There is a $q_r \in R_r \setminus \{0\}$ s.t. $q_r \in R_n q_{r+1} + R_n vf$.*
(*b*) *If $\leq$ is a monomial order on R_n with $D_i < D_j$ for all $i \in \{1, \ldots, r\}$ and $j \in \{r+1, \ldots, n\}$, and if $\{h_1, \ldots, h_k\} \subset R_n \setminus \{0\}$ is a left Gröbner basis of $R_n q_{r+1} + R_n vf$, then at least one of the h_i is from R_r and the Gröbner basis element with least leading monomial is one such h_i.*

Proof. At first the correctness of (a) will be proved.
For $\mathcal{R} = \mathcal{R}_r[D_{r+1}, \ldots, D_n]$ Theorem 3.5 some $r_1, r_2 \in \mathcal{R}, f \in \mathbb{Z}[x_1, \ldots, x_n]$ must exist satisfying

$$1 = r_1 q_{r+1} + r_2 vf \qquad (*)$$

r_1 and r_2 cannot both be zero. If $r_1 \neq 0$, then we can write

$$r_1 = \sum_{\substack{\alpha \in \mathbb{N}^n \\ \alpha_1 = \cdots = \alpha_r = 0}} \frac{1}{a_\alpha} b_\alpha D^\alpha$$

with some nonzero $a_\alpha \in R_r$ and some $b_\alpha \in R_r$. Let $a \in R_r \setminus \{0\}$ be a common left multiple of all the a_α and suppose $a = a^*_\alpha a_\alpha$, then

$$r_1 = \frac{1}{a} \sum_{\substack{\alpha \in \mathbb{N}^n \\ \alpha_1 = \cdots = \alpha_r = 0}} a^*_\alpha b_\alpha D^\alpha =: \frac{1}{a} \underbrace{b}_{\in R_n}.$$

If $r_2 \neq 0$, then we can represent r_2 in a similar way as $r_2 = \frac{1}{c} d$ with $c \in R_r, d \in R_n$. Let $a := 1$ resp. $c := 1$ in the case $r_1 = 0$ resp. $r_2 = 0$. Now, with a common left multiple $q_r \in R_r$ of a and c the equation $(*)$ translates to

$$q_r = q_r r_1 q_{r+1} + q_r r_2 vf = \underbrace{q_r \frac{1}{a} b}_{\in R_n} q_{r+1} + \underbrace{q_r \frac{1}{c} d}_{\in R_n} vf.$$

This proves (a). Clearly (b) implies (a) but it remains to show the converse:
Since there is a $q_r \in R_r \setminus \{0\}$ s.t. $q_r \in R_n q_{r+1} + R_n vf$, one of the leading monomials $LM(h_i)$ $(i \leq k)$ must divide $LM(q_r) \in R_r$, which implies $LM(h_i) \in R_r$ and because of the particular monomial order also $h_i \in R_r$. The rest of the statement is now immediate.

The following Lemma and the subsequent Theorem 3.11 will imply directly the Theorem of Stafford. The proof of the Lemma will then lead to the second part of the procedure for the computation of a two-element basis for a given left ideal of R. □

LEMMA 3.10. *Let $a, b, c \in R_n \setminus \{0\}$. For all $0 \leq r \leq n$ there exist $a_r, b_r \in R_n$ and $q_r \in R_r \setminus \{0\}$ s.t.*

$$q_r c \in R_n(a + a_r c) + R_n(b + b_r c).$$

PROOF. With $a_n = 0$ and $b_n = 0$ and a common left multiple $q_n c$ of a, c we see that the statement is true for $r = n$. We proceed by induction from $r + 1$ to r, where $n - 1 \geq r \geq 0$. Assume that we have found some $a_{r+1}, b_{r+1} \in R_n$ and $q_{r+1} \in R_{r+1} \setminus \{0\}$, s.t. $q_{r+1}c \in R_n(a + a_{r+1}c) + R_n(b + b_{r+1}c)$. Suppose

$$q_{r+1}c = h_1(a + a_{r+1}c) + h_2(b + b_{r+1}c) \tag{1}$$

with $h_1, h_2 \in R_n$. We can assume that $h_1 \neq 0$, otherwise one only has to interchange a, a_{r+1} and b, b_{r+1}. One has to perform now a series of tricky substitutions (going back to Stafford). Since R_n is also right Ore, there are some $g_1, g_2 \in R_n, g_2 \neq 0$ satisfying

$$h_1 g_1 + h_2 g_2 = 0 \tag{2}$$

and also some $s, t \in R_n \setminus \{0\}$ satisfying

$$s q_{r+1} c = t(b + b_{r+1}c). \tag{3}$$

For $v = tg_2 \neq 0$ Lemma 3.9 gives us $f \in \mathbb{Z}[x_1, \ldots, x_n]$ and $q_r \in R_r$ s.t. with some $p_1, p_2 \in R_n$ one has $q_r = p_1 q_{r+1} + p_2 t g_2 f$. The latter, right-multiplied by c, gives

$$q_r c = p_1 q_{r+1} c + p_2 t g_2 f c. \tag{4}$$

Now one can construct the new parameters. With the help of $a_r := a_{r+1} + g_1 f,\ b_r := b_{r+1} + g_2 f,\ d = (p_1 - p_2 s),\ h_1^* = dh_1,\ h_2^* = dh_2 + p_2 t$ it will be shown that

$$q_r c = h_1^*(a + a_r c) + h_2^*(b + b_r c) \tag{5}$$

which completes induction. In order to prove (5) we now compute as follows:

$$\begin{aligned}
&h_1^*(a + a_r c) + h_2^*(b + b_r c) \\
&= dh_1(a + a_{r+1}c + g_1 f c) + dh_2(b + b_{r+1}c + g_2 f c) + p_2 t(b + b_{r+1}c + g_2 f c) \\
&= d(\underbrace{h_1(a + a_{r+1}c) + h_2(b + b_{r+1}c)}_{= q_{r+1}c \text{ by induction hypothesis}} + \underbrace{(h_1 g_1 + h_2 g_2)}_{= 0 \text{ by (2)}} f c) + p_2 t(b + b_{r+1}c + g_2 f c) \\
&= d q_{r+1} c + p_2 \underbrace{t(b + b_{r+1}c)}_{= s q_{r+1} c \text{ by (3)}} + p_2 t g_2 f c \\
&= (p_1 - p_2 s) q_{r+1} c + p_2 s q_{r+1} c + p_2 t g_2 f c \\
&= p_1 q_{r+1} c + p_2 t g_2 f c = (p_1 q_{r+1} + p_2 t g_2 f) c \\
&= q_r c \quad \text{by (4).} \square
\end{aligned}$$

An easy application of the foregoing Lemma leads to:

THEOREM 3.11. *For any $a, b, c \in R_n \setminus \{0\}$ there exist $\widetilde{a}, \widetilde{b} \in R_n$ s.t.*

$$\mathcal{I}_l(a + \widetilde{a}c, b + \widetilde{b}c) = \mathcal{I}_l(a, b, c).$$

PROOF. Lemma 3.10 for $r = 0$ guarantees the existence of a nonzero $q_0 \in R_0 = K(x_1, \ldots, x_n)$ and $a_0, b_0 \in R_n$ s.t.: $q_0 c \in R_n(a + a_0 c) + R_n(b + b_0 c)$. But then c and also a and b must be from $R_n(a + a_0 c) + R_n(b + b_0 c)$. Set $\widetilde{a} := a_0$ and $\widetilde{b} := b_0$.

For examples see Example 3.13.

With the help of Lemma 3.10, Theorem 3.11 and Algorithm 3.6 we now can give an algorithm which computes a two-element basis for a left ideal which is generated by three elements.□

ALGORITHM 3.12. Let $\leq$ be the lexicographic monomial order on $\{D^\alpha | \ \alpha \in \mathbb{N}^n\}$ s.t. $D_1 < \cdots < D_n$.
Input: $a, b, c \in R_n \setminus \{0\}$.
Output: $a^*, b^* \in R_n$ s.t. $\mathcal{I}_l(a^*, b^*) = \mathcal{I}_l(a, b, c)$.

Start: $a^* := a,\ b^* := b$.
compute $lclm(a, c)$.
$h_1 := lclm(a, c)\frac{1}{a},\ h_2 := 0 \in R_n$.
$q := lclm(a, c)\frac{1}{c}$
Choose minimal r s.t. $q \in R_{r+1}, r \geq -1$.
While $q \notin K(x_1, \ldots, x_n)$ repeat:
If $h_1 = 0$, interchange a^* with b^* and h_1 with h_2.
If $h_2 = 0$, set $g_1 := 0,\ g_2 := 1$,
else set $g_1 := \frac{1}{h_1} lcrm(h_1, h_2),\ g_2 := -\frac{1}{h_2} lcrm(h_1, h_2)$.
Compute $lclm(qc, b^*)$.
$s := lclm(qc, b^*)\frac{1}{qc},\ t := lclm(qc, b^*)\frac{1}{b^*}$.
$v := tg_2$.
Compute an $f \in \mathbb{Z}[x_1, \ldots, x_n]$ s.t. $\mathcal{R} = \mathcal{R}q + \mathcal{R}vf$.
Compute a left Gröbner basis G for $\mathcal{I}_l(q, vf)$.
$q^* :=$ element out of G with minimal $LM(q^*)$
Compute p_1 and p_2 s.t. $q^* =: p_1 q + p_2 vf$.
$q := q^*$ Choose minimal r s.t. $q \in R_{r+1}, r \geq -1$.
$a^* := a^* + g_1 fc,\ b^* := b^* + g_2 fc$.
$h_1 := (p_1 - p_2 s)h_1,\ h_2 := (p_1 - p_2 s)h_2 + p_2 t$.
End While.
Display a^* and b^*.
End.

PROOF. The algorithm follows the proof of Lemma 3.10:
At first an $lclm(a, c)$ is computed. This can be done by means of a Gröbner basis computation. Next q is determined as the unique result of a polynomial division. The minimal r can then be extracted from q. h_1 and h_2 now satisfy equation (11) in the proof of 3.10. If q is already in $K(x_1, \ldots, x_n)$, we are done, if not, then the following is repeated until q is finally in $K(x_1, \ldots, x_n)$:
To assure that v stays nonzero one has to interchange eventually the polynomials h_1, h_2, a^*, b^*. During the next step the algorithm determines $g_1,\ g_2$ in such a way that (2) in the proof of 3.10 will be satisfied. Thereafter s, t are determined s.t. (3) in the proof of 3.10 is valid. After this f is computed by Algorithm 3.6. In order to obtain a new q for

the next passage through the main loop the algorithm now computes a left Gröbner basis for $\mathcal{I}_l(q, vf)$. From this basis q^* (which will become the new q) is extracted according to Lemma 3.9. Now p_1, p_2 can be determined by tracing back the foregoing Gröbner basis computation. From Lemma 3.9 we know that at this stage the new r must be definitively smaller than the one before. So after at most n iterations the most recent q will be an element of $R_0 = K(x_1, \ldots, x_n)$. A final update gives the desired generators a^* and b^*. □

Example 3.13. We give two examples to illustrate Algorithm 3.12 and Theorem 3.11. The first one can still be verified by hand in short time.

(a) Let $a := D_1 + x_2,\ b := D_3^2 + x_3$ and $c := D_2 + x_1$. These generators commute in R_3, but in contrast to commutative polynomial rings, here we can produce the same ideal by two generators only. Note that $\{a, b, c\}$ is the reduced Gröbner basis with respect to lexicographic order. Algorithm 3.12 starts by computing $lclm(a, c) = 1 + x_1D_1 + x_1x_2 + D_2D_1 + x_2D_2$ and then sets: $h_1 := D_2 + x_1,\ h_2 := 0,\ q := D_1 + x_2$. The latter gives $r := 0$. This means that there will be only one iteration. Since $h_2 = 0$, the polynomials g_1, g_2 are specified as follows: $g_1 := 0,\ g_2 := 1$. Next one computes $lclm(qc, b^*) = x_1D_3^2D_1 + x_2D_3^2D_2 + x_3D_2D_1 + x_3x_1x_2 + x_3 + x_2x_3D_2 + x_1x_3D_1 + D_3^2 + x_1x_2D_3^2 + D_3^2D_2D_1$ and right division by b^* gives $t = D_3^2 + x_3$ and $v = tg_2 = D_3^2 + x_3$. Now Algorithm 3.6 is applied to compute $f = x_1 + x_3$ (compare Example 3.7). This f is in fact a good choice since $\{1\}$ is a left Gröbner basis for $\mathcal{I}_l(q, vf)$. Thus we can choose $q^* = 1$ at this stage, which leads to $q := 1$, which makes the algorithm stop. The output will be now

$$a^* = D_1 + x_2, \qquad b^* = D_3^2 + x_3 + x_1x_3 + x_1^2 + (x_3 + x_1)D_2.$$

This result can easily be checked by computing a Gröbner basis for $\mathcal{I}_l(a^*, b^*)$, which gives $[D_2 + x_1, D_1 + x_2, D_3^2 + x_3] = [c, a, b]$. The operation which leads from (a, b, c) to (a^*, b^*) is

$$(a, b, c) \longmapsto (a, b + fc, c) \longmapsto (a^*, b^*, 0).$$

Of course there are other polynomials f which lead to a generating pair. By Algorithm 3.6 the variables are considered in the order x_3, x_2, x_1. Therefore x_3 happens to appear in f. As a referee noted, also $f = x_1$ would do the job.

(b) The following generators do not commute. Let $a := x_2D_3D_1 + D_1^2, b := D_2D_1 + x_3D_1^2, c := x_2D_3D_1^2 + (-x_2 + x_2^2)D_3D_1 - x_2^2D_3 - D_2^2D_1 + D_2^2 - x_3D_2D_1^2 + x_3D_2D_1 + D_1^3 + (x_2 - 1)D_1^2 - x_2D_1$. They generate an ideal whose reduced left Gröbner bases for total-degree and different lexicographical orderings consist of three elements. Here with $f := D_2$ and $g := D_1 + x_2$ one has $\mathcal{I}_l(a + fc, b + gc) = \mathcal{I}_l(a, b, c)$. While the determination of an appropriate f and g is cumbersome the verification of the latter equation is relatively easy.

The main results behind us it, is merely a formality to arrive at the following

Theorem 3.14. *Theorem of Stafford*
Any left ideal in R_n can be generated by two elements. An analogous statement can be proved for right ideals.

Proof. By Hilbert's Basis Theorem any left ideal $I \subset R_n$ can be generated finitely and it remains to apply Theorem 3.11 finitely often. □

REMARK 3.15. The original Theorem of Stafford as presented in Björk (1979) or Stafford (1978) says more than Theorem 3.14. Even for left ideals in the Weyl algebra $K[x_1, \ldots, x_n][D_1, \ldots, D_n]$ the Theorem holds. To arrive at this result additional elimination of the variables $x_n, \ldots, x_1$ from $q_0 \in K[x_1, \ldots, x_n]$ as given in Lemma 3.10 must be done effectively. Due to the symmetry of Weyl algebras this should be possible in a way similar to the elimination of $D_n, \ldots, D_1$. Since our interest is in matrices over R_r we will not continue here in this direction.

4. Remarks on Matrices of Differential Operators

It was the problem of simplifying matrices over R_r which led us to this specific Theorem of Stafford's. The Jacobson-Teichmüller normal form over R_1 with its deep uniqueness Theorem by Nakayama (see Cohn, 1971) and results from control theory indicate that the study of matrices over R_r merits interest on its own. Applying Stafford's Theorem it is in principal possible to reduce such matrices applying Theorem 3.11 as indicated in the introduction. But the computation of new generators by Algorithm 3.12 is apparently a rather great effort. Relaxing the notion of equivalence in order to admit enlargements of matrices by zero rows and zero columns the following approach usually will give considerable simplification much more rapidly in many cases.
Assume that the matrix has two columns and at least two non-zero rows and a right column module which cannot be generated by just one column. Proceed as follows:

(1) Add a random right multiple of the second column to the first column.
(2) enlarge the matrix by zero rows in order to admit the computation of a left Gröbner basis of the entries of the first column by elementary row operations.

Now the *conjecture* is that generically you will get $\{1\}$ as a Gröbner basis. Thus the Jacobson–Teichmüller–Nakayama normal form (see introduction) seems to appear in a weakened form also in more than one variable. We illustrate this by the following example:

EXAMPLE 4.1. Consider the matrix $M := \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \\ 0 & 0 \end{bmatrix}$, which has already been enlarged by a zero row. Add the λ-right-multiple of the second column to the first column. Choose e.g. $\lambda = (x_1 + x_2)$. This choice of λ was proposed by a referee and makes calculations a bit easier. Now the new first column has $\{1\}$ as left Gröbner basis. Therefore M can be transformed by a total of two right column and several left row operations to

$$N := \begin{bmatrix} 1 & 0 \\ 0 & (x_1 + x_2)D_1\, {D_2}^2 + 2\, D_1\, D_2 - {D_2}^2 \\ 0 & {D_1}^2\, D_2 \end{bmatrix}.$$

The matrices M and N are equivalent. In a similar fashion $diag(D_1, D_2, D_3)$ enlarged by a zero row is equivalent to a matrix whose first two columns are the first two canonical vectors. Random examples apart from eventual complexity problems yield the same behavior. Together with Stafford's Theorem this would mean that any full right column rank matrix over R_r with at least two non-zero rows is (after an appropriate zero

extension) equivalent to a matrix of the form

$$\begin{bmatrix} 1 & 0 & \cdots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & & 1 & 0 \\ 0 & & \cdots & & p \\ 0 & & \cdots & & q \\ 0 & & & & 0 \\ \vdots & & & & \vdots \\ 0 & & & & 0 \end{bmatrix}.$$

The only difference from the one-variable case is that there are two eventually nonzero entries in the last column.

References

Adams, W. W., Loustaunau, P. (1996). *An Introduction to Gröbner Bases*. Providence RI, USA, American Mathematical Society.

Björk, J. E. (1979). *Rings of Differential Operators*. North-Holland.

Briancon, J., Maisonobe, P. (1984). Idéaux de germes d'opérateurs différentiels à une variable. *L'Enseignement de Mathématique*, **30**, 7–30.

Castro, F. J. (1987). Calculs effectives pour les idéaux d'opérateurs différentiels, *Géometrie et Applications, III: Géometrie Reelle: Systèmes Différentiels et Théorie de Hodge*, Paris.

Chyzak, F. (1998). Fonctions holonomes en calcul formel, Thèse de doctorat, École polytechnique.

Cohn, P. M. (1971). *Free Rings and their Relations*, 2nd edn. London Mathematical Society.

Cotroneo, T. (1999). Observability of linear differential behaviors. In Polderman, J. W., Trentelman, H. eds, *The Mathematics of Systems and Control: from Intelligent Control to Behavioral Systems*. Groningen University.

Cohen, A. *et al.* (1999). *Some Tapas of Computer Algebra*. Springer.

Dauns, J. (1982). *A Concrete Approach to Division Rings*. Berlin, Helderman.

Ilchmann, A., Nürnberger, I., Schmale, W. (1984). Time-varying polynomial matrix systems. *Int. J. Control*, **40**, 329–362.

Guralnick, R. M., Levy, L. S., Odenthal, C. (1988). Elementary divisor theorem for noncommutative PID-s. *Proc. AMS*, **103**, 1003–1011.

Pesch, M. (1998). Two-sided Groebner bases in iterated Ore extensions. In Manuel, B. *et al.* eds., *Symbolic Rewriting Techniques. Papers from the Workshop held in Ascona, Switzerland, April 30–May 4, 1995*, pp. 225–243. Basel, Birkhaeuser.

Stafford, J. T. (1978). Module Structure of Weyl algebras. *J. London Math. Soc., Ser. II*, **18**, 429–442.

van der Waerden, B. L. (1964). *Algebra*. Springer.

Received 31 August 2000
Accepted 15 March 2001