NONSTANDARD METHODS FOR BOUNDS IN DIFFERENTIAL POLYNOMIAL RINGS

MATTHEW HARRISON-TRAINOR, JACK KLYS, AND RAHIM MOOSA

ABSTRACT. Motivated by the problem of the existence of bounds on degrees and orders in checking primality of radical (partial) differential ideals, the nonstandard methods of van den Dries and Schmidt ["Bounds in the theory of polynomial rings over fields. A nonstandard approach.", Inventionnes Mathematicae, 76:77–91, 1984] are here extended to differential polynomial rings over differential fields. Among the standard consequences of this work are: a partial answer to the primality problem, the equivalence of this problem with several others related to the Ritt problem, and the existence of bounds for characteristic sets of minimal prime differential ideals and for the differential Nullstellensatz.

1. INTRODUCTION

This paper is concerned with existence proofs of bounds in the theory of differential polynomial rings over differential fields. We are motivated by the following open question in differential-algebraic geometry: Given a differential-algebraic family of Kolchin-closed sets $\{V_a \subseteq L^n : a \in L^m\}$, where L is a differentially closed field of characteristic zero in several commuting derivations, is the set

$$D := \{a \in L^m : V_a \text{ is irreducible}\}\$$

Kolchin-constructible? Because of quantifier-elimination for differentially closed fields, this is equivalent to asking whether D can be defined by a first-order formula in the language of differential rings. Now if V_a is defined by the vanishing of the finite system S_a of differential polynomials over L, then V_a is irreducible if and only if the radical differential ideal generated by S_a , denoted by $\{S_a\}$, is prime. Membership of f_b in $\{S_a\}$, for a given differential polynomial with coefficients b, is a first-order property of (a, b) because it is equivalent to the vanishing of f_b on V_a . Primality of $\{S_a\}$, on the other hand, is not on the face of it first-order in a because it requires quantification over all (coefficients of) differential polynomials f and g such that $fg \in \{S_a\}$. If, however, we could restrict these quantifications to differential polynomials of bounded degree and order – bounded independently of a – then we would have a first-order definition for D. In fact, one expects to have bounds that are also independent of the base differential field.

Date: May 2nd, 2011.

²⁰⁰⁰ Mathematics Subject Classification. Primary 12H05. Secondary 03H05.

Matthew Harrison-Trainor and Jack Klys were partially supported by an NSERC USRA.. Rahim Moosa was partially supported by an NSERC Discovery Grant.

Conjecture 1.1 (Definability of primality). For every d there exists r = r(d, n, m) such that for every field of characteristic zero equipped with m commuting derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$ and every finite set S of Δ -polynomials in n indeterminates $X = (X_1, \ldots, X_n)$ over k of degree and order $\leq d$, the following are equivalent:

- (i) $\{S\}$, the radical Δ -ideal generated by S, is prime,
- (ii) $\{S\}$ is proper and for all Δ -polynomials f and g in X over k of degree and order $\leq r$, if $fg \in \{S\}$ then $f \in \{S\}$ or $g \in \{S\}$.

The purely algebraic analogue of Conjecture 1.1, which asks for a bound on degrees for checking the primality of radical ideals in polynomial rings over fields, has an affirmative solution, and this is why irreducibility in algebraic families of Zariskiclosed sets is definable (in the language of rings). Constructive proofs go back to the work of Hermann [4] and later Seidenberg [6]. Clearer and more efficient proofs of the *existence* of bounds were given by van den Dries and Schmidt in [7] using a nonstandard approach; that is, by studying ultraproducts of polynomial rings over fields. Our goal here is to extend the methods of van den Dries and Schmidt to the differential setting; to study the ultraproducts of differential polynomial rings over differential fields and to bring that to bear on Conjecture 1.1.

We obtain a partial solution whereby we are able to bound one of the two quantifiers in the definition of primality; see Theorem 5.4 below. We are also able to prove the equivalence of Conjecture 1.1 with four other natural existence-of-bounds conjectures in differential algebra; see Theorem 5.7. Here we are motivated by [2] where a related series of problems around the existence of *algorithms* in computational differential algebra are shown to be equivalent. As a byproduct of our analysis we also obtain quick existence proofs of bounds in two other areas where bounds have been obtained by (or are deducible from) constructive methods; namely for characteristic sets of minimal prime differential ideals (Theorem 6.1) and for the differential Nullstellensatz (Theorem 6.3).

The results described above are proved in the final two sections of the paper, based on the study of *internal* differential polynomials carried out in Section 4. In Sections 2 and 3 below we review the relevant notions from differential algebra and introduce the corresponding nonstandard setting.

We are grateful to Alexey Ovchinnikov for his explanations regarding several points of constructive differential algebra.

2. DIFFERENTIAL-ALGEBRAIC PRELIMINARIES

We begin with a quick review of differential polynomial rings, primarily to set notation. See [5] for details.

Suppose $m, n < \omega$, $(k, \Delta = \{\delta_1, \ldots, \delta_m\})$ is a differential field of characteristic zero in m commuting derivations, and $X = (X_1, \ldots, X_n)$ is an n-tuple of indeterminates. Let $\Theta = \{\delta_1^{e_1} \cdots \delta_m^{e_m} : e_i \geq 0\}$ be the set of Δ -operators and set $\Theta X := \{\theta X_i : \theta \in \Theta, 1 \leq i \leq n\}$. The ring of Δ -polynomials in X over k, denoted by $k\{X\}$, is the ring of (commutative) polynomials in ΘX over k equipped with the natural structure of a Δ -ring. For this reason the X_i are called differential indeterminates while the elements of ΘX are the algebraic indeterminates. For a subset $S \subset k\{X\}$, we use (S), [S], and $\{S\}$ to denote, respectively, the ideal, Δ -ideal, and radical Δ -ideal generated by S. By the degree of a Δ -polynomial $f \in k\{X\}$ we will mean the total degree of f as an element of $k[\Theta X]$, and by its order we mean the maximum order of the Δ -operators that appear in f. (The order of a Δ -operator $\delta_1^{e_1} \cdots \delta_m^{e_m}$ is $e_1 + \cdots + e_m$.)

We rank the algebraic indeterminates by $\delta_1^{e_1} \cdots \delta_m^{e_m} X_i < \delta_1^{f_1} \cdots \delta_m^{f_m} X_j$ if and only if $\left(\sum_{l=1}^m e_l, i, e_1, \dots, e_m\right) < \left(\sum_{l=1}^m f_l, j, f_1, \dots, f_m\right)$ in the lexicographic ordering. According to this ranking we enumerate ΘX as $(Z_h : h < \omega)$, and define the *height* of

an algebraic indeterminate v to be the h such that $v = Z_h$. Given $f \in k\{X\} \setminus k$, the *leader* of f, denoted by v_f , is the highest ranking algebraic indeterminate appearing in f, and the *height* of f is by definition the height of its leader. The leading coefficient when f is written as a polynomial in v_f is called the *initial* of f and is denoted by I_f . Note that the leader of I_f is strictly less than v_f in rank. The derivative of f with respect to v_f is called the *separant* of f and will be denoted by S_f . A consequence of these definitions is that for any $\theta \in \Theta \setminus \{1\}$, the initial of θf is S_f .

The ranking of the algebraic indeterminates extends to Δ -polynomials by the lexicographic ordering on the pair $(v_f, \deg_{v_f}(f))$. So for example both rank $(I_f) < \operatorname{rank}(f)$ and rank $(S_f) < \operatorname{rank}(f)$. This ranking extends also to finite sequences of Δ -polynomials by the following lexicographic-like ranking: rank $(f_1, \ldots, f_r) < \operatorname{rank}(g_1, \ldots, g_s)$ if either there is $k \leq \min(r, s)$ with rank $(f_i) = \operatorname{rank}(g_i)$ for all i < k and rank $(f_k) < \operatorname{rank}(g_k)$, or r > s and rank $(f_i) = \operatorname{rank}(g_i)$ for all $i \leq s$.

Suppose $f, g \in k\{X\}$. Recall that f is reduced with respect to g if θv_g does not appear in f for any $\theta \in \Theta \setminus \{1\}$ and the degree of v_g in f is strictly less than its degree in g. In particular, if $\operatorname{rank}(f) < \operatorname{rank}(g)$ then f is reduced with respect to g, but the converse need not hold; even when f is reduced with respect to g higher ranking algebraic indeterminates than v_g may appear in f, just not any that can be obtained from v_g by applying the derivations. A set of Δ -polynomials is called *autoreduced* if every element is reduced with respect to all the others. Autoreduced sets are always finite, and we canonically view them as finite sequences by ordering the elements of an autoreduced set according to increasing height. This induces a ranking on the autoreduced subsets of $k\{X\}$.

Given a subset $S \subseteq k\{X\}$, a *characteristic set* for S is a lowest ranking autoreduced subset of S. It is a basic fact that every Δ -ideal has a characteristic set. Moreover, prime Δ -ideals are determined by their characteristic sets in the following sense: if P is a prime Δ -ideal and Λ is a characteristic set for P then

$$P = I[\Lambda] := \{g \in k\{X\} : H^t_{\Lambda}g \in [\Lambda], \text{ for some } t \in \mathbb{N}\}$$

where by definition $H_{\Lambda} := \prod_{f \in \Lambda} S_f I_f$. For notational reasons specific to this paper

we are here denoting by $I[\Lambda]$ what is usually denoted in the literature by $[\Lambda] : H_{\Lambda}^{\infty}$. Finally let us recall the characterisation of characteristic sets of prime Δ -ideals. First, given a finite set $\Lambda \subset \{X\}$ and $h < \omega$, $(\Lambda)_h$ denotes the ideal generated by Λ together with all the derivatives of Λ that are of height at most h. An autoreduced set Λ is *coherent* if whenever $f \neq g$ in Λ are such that $\theta_f v_f = \theta_g v_g = Z_h$ for some $\theta_f, \theta_g \in \Theta$, and if θ_f, θ_g are such that the height h is minimal possible, then $S_g \theta_f f - S_f \theta_g g \in (\Lambda)_{h-1}$.

Fact 2.1 (Lemma 2 of §IV.9 of Kolchin [5]). Let Λ be a finite subset of $k \{X\}$. Then Λ is a characteristic set of a prime Δ -ideal if and only if

- (1) Λ is coherent, and
- (2) $I(\Lambda) := \{g \in k \{X\} : H^t_{\Lambda}g \in (\Lambda), \text{ for some } t \in \mathbb{N}\}$ is a prime ideal containing no nonzero elements that are reduced with respect to Λ .

The main usefulness of this criterion rests in the fact that it makes reference only to the ideal (Λ) and not the Δ -ideal [Λ].

3. Internal Δ -polynomials

We will be using nonstandard methods just as they were used in [7], a gentle introduction to which can be found in Section 3 of [8]. Fix once and for all an index set I and a nonprincipal ultrafilter \mathcal{U} on I. We work in the ultrapoduct with respect to \mathcal{U} of whatever universe of algebraic objects we are interested in. For any set A we denote by A^* its nonstandard interpretation, namely $\prod_{\mathcal{U}} A$. Given an

element a of the ultraproduct we will usually fix an \mathbb{I} -indexed sequence representing that element and use a(r) to denote the rth co-ordinate of that representative. We say that a condition P is true of a "co-ordinatewise almost everywhere" if the set of indices $r \in \mathbb{I}$ for which P is true of a(r) is a member of the ultrafilter. This does not depend on the choice of representative for a. Recall that a subset S of an ultraproduct is *internal* if there exists a sequence of subsets $(S_r : r \in \mathbb{I})$, called the *family of components* of S, such that $a \in S$ if and only if $a(r) \in S_r$ almost everywhere. Note that every finite set is internal with components the set of coordinates, that is, $S_r = \{a(r) : a \in S\}$ for all $r \in \mathbb{I}$. We say that a condition P is true of an internal set S "componentwise almost everywhere" if the set of indices $r \in \mathbb{I}$ for which P is true of S_r is a member of the ultrafilter. This too does not depend on the choice of family of components for S.

Suppose $\{K_r : r \in \mathbb{I}\}$ is a sequence of Δ -fields of characteristic zero. Fixing differential indeterminates $X = (X_1, \ldots, X_n)$, we have the Δ -ring of *internal* Δ polynomials over K, namely $\prod_{\mathcal{U}} (K_r\{X\})$, which, following [7] in the algebraic case,

we denote by $K\{X\}_{int}$ where $K := \prod_{\mathcal{U}} K_r$. Almost every differential algebraic no-

tion has an internal analogue in $K\{X\}_{int}$. For example, given $f, g \in K\{X\}_{int}$, we say that f is of lower internal rank than g if it is of lower rank co-ordinatewise almost everywhere, that is, if $\{r \in \mathbb{I} : f(r) \text{ is of lower rank than } g(r)\} \in \mathcal{U}$. Similarly, f is internally reduced with respect to g if it is reduced with respect to gco-ordinatewise almost everywhere. An internal subset $\Lambda \subset K\{X\}_{int}$ is internally autoreduced if it is componentwise autoreduced almost everywhere. Note that unlike for standard autoreduced sets, internally autoreduced subsets of $K\{X\}_{int}$ need not be finite (though they will be componentwise finite almost everywhere). Nevertheless we can rank the internally autoreduced sets by declaring that rank $(\Lambda) <$ rank (Γ) if this is the case componentwise almost everywhere. Similarly, an internally characteristic set for an internal set S, is an internal subset $\Lambda \subset S$ such that Λ_r is characteristic for S_r for almost all r. As an illustration of how these definitions play out, we prove the following straightforward equivalences.

Lemma 3.1. Suppose $S, \Lambda \subset K\{X\}_{int}$ are internal sets.

(i) Λ is internally autoreduced if and only if every element of Λ is internally reduced with respect to every other element of Λ .

4

 (ii) Λ is an internally characteristic set for S if and only if Λ is a minimally ranked internally autoreduced subset of S.

Proof. For the left-to-right direction of (i), suppose $V \in \mathcal{U}$ is such that Λ_r is autoreduced in $K_r \{X\}$ for all $r \in V$. Given $f \neq g$ in Λ , shrinking V if necessary, we have that $f(r) \neq g(r)$ are in Λ_r and hence are reduced with respect to each other. It follows that f and g are internally reduced with respect to each other. For the converse, suppose $W := \{r \in \mathbb{I} : \Lambda_r \text{ is autoreduced}\} \notin \mathcal{U}$. Then $V := \mathbb{I} \setminus W \in \mathcal{U}$. For each $r \in V$, let $f_r \neq g_r$ in Λ_r be such that f_r is not reduced with respect to g_r . Let $f, g \in K\{X\}_{\text{int}}$ be such that $f(r) = f_r$ and $g(r) = g_r$ for almost all r. Then $f \neq g$ are in Λ and f is not internally reduced with respect to g.

Now suppose that Λ is internally characteristic for S, and let $V \in \mathcal{U}$ be coordinates where Λ_r is a characteristic subset of S_r . In particular, Λ is internally autoreduced. Now if $\Sigma \subset S$ is any other internally autoreduced set, after possibly shrinking V, we have that $\Sigma_r \subset S_r$ is autoreduced and hence rank $(\Lambda_r) \leq \operatorname{rank}(\Sigma_r)$, for all $r \in V$. So rank $(\Lambda) \leq \operatorname{rank}(\Sigma)$. This proves that Λ is minimally ranked among the internally autoreduced subset of S. For the converse, suppose that $\Lambda \subset S$ is internally autoreduced but $W := \{r \in \mathbb{I} : \Lambda_r \text{ is characteristic for } S_r\} \notin \mathcal{U}$. Then $V := \mathbb{I} \setminus W \in \mathcal{U}$. Shrinking V we may assume that Λ_r is autoreduced for each $r \in V$. Hence, for each $r \in V$ there must exist an autoreduced subset $\Sigma_r \subset S_r$ with rank $(\Sigma_r) < \operatorname{rank}(\Lambda_r)$. The sequence $(\Sigma_r : r \in V)$ extends to the family of components of an internal set $\Sigma \subset K\{X\}_{\text{int.}}$. It follows that $\Sigma \subset S$ is internally autoreduced subsets of S. This proves (ii). \Box

By an internal Δ -ideal of $K\{X\}_{int}$ we mean an internal subset of $K\{X\}_{int}$ almost all of whose components are Δ -ideals. Note that an internal Δ -ideal is a Δ -ideal of $K\{X\}_{int}$. Given an internal set $S \subset K\{X\}_{int}$, we use $(S)_{int}$, $[S]_{int}$, and $\{S\}_{int}$ to denote the internal ideal whose rth component is, respectively, the ideal, Δ -ideal, and radical Δ -ideal generated by S_r . On the other hand, it is not hard to check that $(S)_{int}$ is contained in every ideal of $K\{X\}_{int}$ containing S, $[S]_{int}$ is contained in every internal Δ -ideal of $K\{X\}_{int}$ containing S, and $\{S\}_{int}$ is contained in every radical internal Δ -ideal of $K\{X\}_{int}$ containing S.

It follows immediately from the definitions that since every Δ -ideal has a characteristic subset, every internal Δ -ideal has an internally characteristic subset. Moreover, a prime internal Δ -ideal is determined by an internally characteristic set in the following sense: if P is a prime internal Δ -ideal and $\Lambda \subset P$ is an internally characteristic set for P then

$$P = I_{\text{int}}[\Lambda] := \{ g \in K\{X\}_{\text{int}} : (H_{\Lambda}^{\text{int}})^N g \in [\Lambda]_{\text{int}}, \text{ for some } N \in \mathbb{N}^* \}$$

where by definition $H_{\Lambda}^{\text{int}} \in K\{X\}_{\text{int}}$ is determined by the sequence $(H_{\Lambda_r} : r \in \mathbb{I})$. Indeed, this is just by transfer from the corresponding fact about standard prime Δ -ideals. Moreover, the characterisation of characteristic sets of prime Δ -ideals (Fact 2.1) transfers easily:

Fact 3.2. An internal set $\Lambda \subset K\{X\}_{int}$ is internally characteristic for a prime internal Δ -ideal if and only if Λ is internally coherent and

$$I_{\rm int}(\Lambda) := \left\{ g \in K\{X\}_{\rm int} : \left(H_{\Lambda}^{\rm int}\right)^N g \in (\Lambda)_{\rm int}, \text{ for some } N \in \mathbb{N}^* \right\}$$

is a prime internal ideal containing no nonzero elements that are internally reduced with respect to Λ .

Of course, here *internally coherent* means coherent in almost all components.

4. Comparing $K\{X\}_{int}$ and $K\{X\}$

Since $K = \prod_{\mathcal{U}} K_r$ is equipped with the natural (co-ordinatewise) Δ -field structure we also have the Δ -polynomial ring $K\{X\}$. There is a natural embedding of $K\{X\}$ into $K\{X\}_{int}$ over K which essentially "unpacks" the coefficients of the polynomial. More precisely, if we list all of the monomials in ΘX as M_1, M_2, \ldots , then we can write an element of $K\{X\}$ as $\sum_{i=1}^{\infty} a_i M_i$ with the $a_i \in K$, all but finitely many of which are zero. Then we can define $\phi : K\{X\} \to K\{X\}_{int}$ by

$$\left[\phi\left(\sum_{i=1}^{\infty}a_{i}M_{i}\right)\right](r) = \sum_{i=1}^{\infty}a_{i}(r)M_{i}$$

It is easy to check that ϕ is an embedding of Δ -rings that is the identity on K. This allows us to view $K\{X\}_{int}$ as a Δ -ring extension of $K\{X\}$. Following the approach of [7], we study the extent to which the properties of $K\{X\}$ are reflected in this extension.

We have the following intrinsic characterisation of $K\{X\}$: it is the subring of elements $f \in K\{X\}_{int}$ for which for some $V \in \mathcal{U}$ there is a bound on the degree and order of f(r) independently of $r \in V$. Indeed, if f has this property then there are finitely many monomials M_1, \ldots, M_N such that for all $r \in V$ there are $a_{i,r} \in K_r$ such that $f(r) = \sum_{i=1}^N a_{i,r} M_i$, and so f is $\phi\left(\sum_{i=1}^N a_i M_i\right)$ where $a_i \in K$ is such that $a_i(r) = a_{i,r}$ for all $r \in V$. Conversely, from the definition of ϕ it follows that if $f \in K\{X\}$ then there is a set $V \in \mathcal{U}$ such that for all $r \in V$, $\phi(f)(r)$ has the same "shape" as f, i.e. a monomial M appears with a nonzero coefficient in f if and only if it does in $\phi(f)(r)$ as well.

Let us first consider $K\{X\}_{int}$ purely as a ring extension of $K\{X\}$. Recall that $Z = (Z_i : i < \omega)$ is an enumeration of the algebraic indeterminates according to height. The underlying ring structure of $K\{X\}$ is simply the pure polynomial ring K[Z], while that of $K\{X\}_{int}$ is the ring of internal polynomials $K[Z]_{int} := \prod_{\mathcal{U}} K_r[Z]$. In the following proposition we extend some of the results of van den Dries and Schmidt – which were proved in [7] for finitely generated polynomial rings – to this infinitary setting.

Proposition 4.1. The ring $K\{X\}_{int}$ is a faithfully flat $K\{X\}$ -module. Moreover, for any ideal I of $K\{X\}$,

- (a) I is prime in $K{X}$ if and only if $IK{X}_{int}$ is prime in $K{X}_{int}$, and
- (b) $\{g \in K\{X\} : g^N \in IK\{X\}_{int} \text{ for some } N \in \mathbb{N}^*\} = \sqrt{I}$

Proof. As above, $K\{X\} = K[Z]$ and $K\{X\}_{int} = K[Z]_{int}$, where $Z = (Z_i : i < \omega)$ is an enumeration of the algebraic indeterminates according to height.

For flatness consider a homogeneous linear equation

$$f_1Y_1 + \cdots + f_\ell Y_\ell = 0$$

where $f_1, \ldots, f_\ell \in K[Z]$. We denote this equation by FY = 0. Suppose $g \in K[Z]_{\text{int}}^{\ell}$ is a solution. We need to show that g is a $K[Z]_{\text{int}}$ -linear combination of

solutions in $K[Z]^{\ell}$. We do this by passing first to $K[Z_i: i < h]_{int}$, where h is such that $f_1, \ldots, f_{\ell} \in K[Z_i: i < h]$, and then to $K[Z_i: i < h]_{int}$ by the finite variable case. For each $r \in \mathbb{I}$, let $h_r \ge h$ be such that $g(r) \in K_r[Z_i: i < h_r]^{\ell}$. Since, for almost all r, g(r) is a solution to F(r)Y = 0, and since $K_r[Z_i: i < h_r]$ is flat over $K_r[Z_i: i < h]$, we have that g(r) is a $K_r[Z_i: i < h_r]$ -linear combination of solutions to F(r)Y = 0 in $K_r[Z_i: i < h]^{\ell}$. Now, as the coefficients of the equation are of bounded degree independently of r, Theorem 1.4 of [7] gives us a bound α , independent of r, such that all solutions in $K_r[Z_i: i < h]^{\ell}$ are $K_r[Z_i: i < h]$ -linear combinations of solutions with degree bounded by α . Let N be the K_r -dimension of the subspace of $K_r[Z_i: i < h]^{\ell}$ made up of tuples of polynomials with degree bounded by α . Then N depends only on α and h, and hence not on r. Moreover, for each r, there exist solutions $e_{1,r}, \ldots, e_{N,r} \in K_r[Z_i: i < h]^{\ell}$ such that g(r) is a $K_r[Z_i: i < h]$, and so each e_j is a $K[Z_i: i < h]^{\ell}$ such that $e_j(r) = e_{j,r}$ almost everywhere, we have that g is a $K[Z_i: i < h]_{int}$ -linear combination of $\{e_1, \ldots, e_N\}$. Theorem 1.1 of [7] tells us that $K[Z_i: i < h]_{int}$ is a flat extension of $K[Z_i: i < h]^{\ell}$. Hence g is a $K[Z]_{int}$ -linear combination of solutions in $K[Z_i: i < h]_{int}$ is a flat extension of $K[Z_i: i < h]^{\ell}$. Hence g is a $K[Z]_{int}$ -linear combination of solutions in $K[Z_i: i < h]^{\ell}$.

For faithful flatness, suppose AY = B is a system of k linear equations in ℓ unknowns over K[Z] with a solution in $K[Z]_{int}^{\ell}$. Let h be a bound on the heights of the entries of A and B. Then working co-ordinatewise, and using the fact that $K_r[Z]$ is faithfully flat over $K_r[Z_i : i < h]$, we have that AY = B has a solution in $K[Z_i : i < h]_{int}$. But the latter is faithfully flat over $K[Z_i : i < h]$ by Theorem 1.8 of [7]. Hence we get a solution in $K[Z]^{\ell}$, as desired.

The right-to-left direction of part (a) of the "moreover" clause is an immediate consequences of the fact that by faithfull flatness $IK\{X\}_{int} \cap K\{X\} = I$. For the converse, note first of all that since checking any instance of primeness of $IK{X}_{int}$ involves only finitely many elements from I, it would suffice to prove the result with $I \cap K[Z_i : i < h]$, which is still prime, in place of I, for each $h < \omega$. But $I \cap K[Z_i : i < h]$ is finitely generated, and hence it will suffice to prove the result for finitely generated I. That is, we assume $(\Lambda)K\{X\}$ is prime for some finite subset $\Lambda \subset K\{X\}$, and prove that $(\Lambda)K\{X\}_{int}$ is prime. Let h be such that $\Lambda \subset K[Z_i : i < h]$. Since K[Z] is faithfully flat over $K[Z_i : i < h]$, $(\Lambda)K[Z] \cap$ $K[Z_i: i < h] = (\Lambda)K[Z_i: i < h]$ and hence the latter is prime. By Theorem 2.5 of [7], $(\Lambda)K[Z_i: i < h]_{int}$ is prime. Note that $(\Lambda)K[Z_i: i < h]_{int}$, being finitely generated, is an internal ideal with family of components $((\Lambda_r)K_r [Z_i : i < h] : r \in$ I) where $\Lambda_r := \{f(r) : f \in \Lambda\}$. Hence, for almost all $r, (\Lambda_r)K_r [Z_i : i < h]$ is prime. But then, passing to a polynomial ring extension over the same field, we have that $(\Lambda_r)K_r[Z]$ is prime for almost all r. It follows that the corresponding internal ideal $(\Lambda)K[Z]_{\text{int}}$ is prime, as desired.

Finally, for (b), suppose $g \in K\{X\}$ and $N \in \mathbb{N}^*$ are such that $g^N \in IK\{X\}_{int}$. Let Λ be a finite subset of I such that $g^N \in (\Lambda)K\{X\}_{int}$. We show that $g \in \sqrt{(\Lambda)}$. Let h be such that $\Lambda \subset K[Z_i:i < h]$ and $g \in K[Z_i:i < h]$. Then, for almost all $r, g(r)^{N(r)} \in (\Lambda_r)K_r[Z] \cap K_r[Z_i:i < h] = (\Lambda_r)K_r[Z_i:i < h]$. That is, $g \in \sqrt[int]{(\Lambda)K[Z_i:i < h]_{int}}$. Corollary 2.7 of [7] says that $\sqrt[int]{(\Lambda)K[Z_i:i < h]_{int}} = \sqrt{(\Lambda) \cdot K[Z_i:i < h]_{int}}$. By the faithful flatness of $K[Z_i:i < h]_{int}$ over $K[Z_i:i < h]$, we get $g \in \sqrt{(\Lambda)}$, as desired. The reverse containment of part (b) is clear.

Now let us consider $K\{X\}_{int}$ as a Δ -ring extension of $K\{X\}$. Note that many of the internal notions discussed in the last section restrict to the usual ones on $K\{X\}$. For example, suppose $f, g \in K\{X\}$. Then f is internally of lower rank than g in $K{X}_{int}$ (respectively internally reduced with respect to g) if and only if it is of lower rank than q in $K\{X\}$ (respectively reduced with respect to q). This is because rank and reducedness depend only on the shape of Δ -polynomials, and elements of $K\{X\}$ have the same shape as their co-ordinates almost everywhere. Similarly, a finite subset of $K\{X\}$ is autoreduced in $K\{X\}$ if and only if, as an internal subset of $K\{X\}_{int}$, it is internally autoreduced. Also, the ranking of internally autoreduced subsets of $K{X}_{int}$ restricts to the usual ranking of autoreduced (finite) subsets of $K\{X\}$. In particular, if $\Lambda \subset K\{X\}$ is an internally characteristic set of a prime internal Δ -ideal of $K\{X\}_{int}$, then Λ is a characteristic set of a prime Δ *ideal of* $K\{X\}$. Indeed, if $P \subset K\{X\}_{int}$ is a prime internal Δ -ideal witnessing the truth of the antecedent of the above statement, then $P \cap K\{X\}$ witnesses the consequent. The converse, however, is not so straightforward, and constitutes the main goal of this section (cf. Theorem 4.3 below). We will use the characterisation of characteristic subsets of prime Δ -ideals given by Fact 2.1 (and its nonstandard analogue Fact 3.2). The following lemma is the main technical result that will allow us to do so.

Lemma 4.2. Let $\Lambda \subset K\{X\}$ be a finite set. Then

- (a) Λ is coherent in $K\{X\}$ if and only if Λ is internally coherent in $K\{X\}_{int}$.
- (b) If $I(\Lambda)$ is prime in $K\{X\}$ then $I_{int}(\Lambda) = I(\Lambda)K\{X\}_{int}$, and hence $I_{int}(\Lambda)$ is prime in $K\{X\}_{int}$.
- (c) Suppose Λ is autoreduced and $I(\Lambda)$ is prime in $K\{X\}$. Then $I(\Lambda)$ contains a nonzero element that is reduced with respect to Λ if and only if $I_{int}(\Lambda)$ contains a nonzero element that is internally reduced with respect to Λ .

Proof. Toward a proof of part (a), let F be the set of pairs (f, g) of distinct elements from Λ such that there exists $\theta_1, \theta_2 \in \Theta$ with $\theta_1 v_f = \theta_2 v_g$. If $(f, g) \in F$, let θ_f and θ_g be such that $\theta_f v_f = \theta_g v_g$ is of minimal height, say h(f, g). Note that despite the notation both operators θ_f and θ_g depend on the pairt (f, g).

Suppose that Λ is coherent. By the coherence of Λ , if $(f,g) \in F$ then $S_g(\theta_f f) - S_f(\theta_g g) \in (\Lambda)_{h(f,g)-1}$. It follows that for some $V_{f,g} \in \mathcal{U}$ and all $r \in V_{f,g}$, $S_{g(r)}(\theta_f f(r)) - S_{f(r)}(\theta_g g(r)) \in (\Lambda_r)_{h(f,g)-1}$ in $K_r\{X\}$. We are using here also the fact that the separant of a Δ -polynomial can be computed co-ordinatewise almost everwhere.

Let $V = \bigcap_{(f,g)\in F} V_{f,g}$. We have already pointed out that internal autoreducedness

extends autoreducedness, so, shrinking V if necessary, we may assume that Λ_r is autoreduced for all $r \in V$. Shrinking V further, we may also assume that f and f(r) have the same shape for all $f \in \Lambda$, and that if $f \neq g$ in Λ then $f(r) \neq g(r)$ in Λ_r . We now show that for each $r \in V$, Λ_r is coherent in $K_r \{X\}$. Suppose $f(r), g(r) \in \Lambda_r$ are distinct and there are $\theta_1, \theta_2 \in \Theta$ such that $\theta_1 v_{f(r)} = \theta_2 v_{g(r)}$ is of height h, and that h is minimal such. Since this is a fact just about the shape of f(r) and g(r), it follows that $(f, g) \in F$, $\theta_1 = \theta_f$, $\theta_2 = \theta_g$, and h = h(f, g). Hence, as $r \in V_{f,g}$ we have that $S_{g(r)}(\theta_1 f(r)) - S_{f(r)}(\theta_2 g(r)) \in (\Lambda_r)_{h-1}$. This proves that Λ_r is coherent. Hence Λ is internally coherent.

8

For the converse, suppose that Λ is internally coherent. Then Λ is internally autoreduced and hence autoreduced. Suppose $(f,g) \in F$ and set $P := S_g(\theta_f f) - S_f(\theta_g g)$. Let $\{Q_1, \ldots, Q_\ell\}$ be Λ together with its derivatives up to height h(f,g)-1. We need to show that $P \in (Q_1, \ldots, Q_\ell)K\{X\}$. Let $V \in U$ be such that for all $r \in V$, Λ_r is coherent, $\theta_f v_{f(r)} = \theta_g v_{g(r)}$ with height h(f,g), and this height is minimal such. Shrinking V further we may also assume that $\{Q_1(r), \ldots, Q_\ell(r)\}$ is Λ_r together with all its derivatives up to height h(f,g) - 1. By coherence,

$$P(r) \in (\Lambda_r)_{h(f,q)-1} = (Q_1(r), \dots, Q_\ell(r)) K_r \{X\}$$

Hence $P \in (Q_1, \ldots, Q_\ell) K\{X\}_{int}$. But P and the Q_j 's are in $K\{X\}$, and, by Proposition 4.1, $K\{X\}_{int}$ is faithfully flat over $K\{X\}$. Hence $P \in (Q_1, \ldots, Q_\ell) K\{X\}$, as desired.

For part (b), recall first of all that by definition

$$I(\Lambda) = \left\{ g \in K \left\{ X \right\} : H_{\Lambda}^{t} g \in (\Lambda) K \left\{ X \right\}, \text{ for some } t \in \mathbb{N} \right\}$$

and

$$H_{\rm int}(\Lambda) = \left\{ g \in K\{X\}_{\rm int} : \left(H_{\Lambda}^{\rm int}\right)^N g \in (\Lambda)_{\rm int}, \text{ for some } N \in \mathbb{N}^* \right\}$$

But $H_{\Lambda}^{\text{int}} = H_{\Lambda}$ since separants and initials of elements in $K\{X\}$ can be computed co-ordinatewise almost everywhere. Similarly, $(\Lambda)_{\text{int}} = (\Lambda) K\{X\}_{\text{int}}$ because Λ is finite and hence $(\Lambda) K\{X\}_{\text{int}}$ is internal with components $(\Lambda_r)K_r\{X\}$ where $\Lambda_r := \{f(r) : f \in \Lambda\}$. So in fact,

$$I_{\rm int}(\Lambda) = \left\{ g \in K\{X\}_{\rm int} : H^N_\Lambda g \in (\Lambda) K\{X\}_{\rm int}, \text{ for some } N \in \mathbb{N}^* \right\}$$

It follows that $I(\Lambda) \subset I_{int}(\Lambda)$, and so $I(\Lambda)K\{X\}_{int} \subseteq I_{int}(\Lambda)$

For the reverse containment, suppose toward a contradiction that $g \in I_{\text{int}}(\Lambda)$ and $g \notin I(\Lambda)K\{X\}_{\text{int}}$. Then $H^N_{\Lambda}g \in (\Lambda)K\{X\}_{\text{int}} \subset I(\Lambda)K\{X\}_{\text{int}}$ for some $N \in \mathbb{N}^*$. Since $I(\Lambda)$ is prime by assumption, Proposition 4.1(a) tells us that $I(\Lambda)K\{X\}_{\text{int}}$ is also prime. Hence $H^N_{\Lambda} \in I(\Lambda)K\{X\}_{\text{int}}$. By Proposition 4.1(b), $H^t_{\Lambda} \in I(\Lambda)$ for some $t \in \mathbb{N}$. Increasing t if necessary, $H^t_{\Lambda} \in (\Lambda)$. But this means that $1 \in I(\Lambda)$, contradicting the primality of that ideal. We have shown that $I_{\text{int}}(\Lambda) = I(\Lambda)K\{X\}_{\text{int}}$. In particular, by Proposition 4.1(a), $I_{\text{int}}(\Lambda)$ is prime.

We now turn to part (c); Λ is autoreduced and $I(\Lambda)$ is prime. One direction is straightforward: a nonzero element of $I(\Lambda)$ reduced with respect to Λ is itself a nonzero element of $I_{int}(\Lambda)$ internally reduced with respect to Λ . For the converse, let $Z = (Z_i : i < \omega)$ again enumerate the algebraic indeterminates according to height. Consider the leaders $T := \{v_f : f \in \Lambda\}$ and let $Y := \{Z_i : Z_i \text{ is not a derivative of any } v_f \in T\}$. Since Λ is autoreduced, all the algebraic indeterminates appearing in Λ come from $Y \cup T$. It follows, as is remarked after Lemma 2 of Chapter 4 of [5], that $I(\Lambda)$ is generated by $I := I(\Lambda) \cap K[Y,T]$. Hence, $I_{int}(\Lambda)$, which by part (b) is equal to $I(\Lambda)K[Z]_{int}$, is in fact equal to $IK[Z]_{int}$.

Now suppose $g \in I_{\text{int}}(\Lambda) = IK[Z]_{\text{int}}$ is nonzero and internally reduced with respect to Λ . Let $V \in \mathcal{U}$ be such that g(r) is reduced with respect to $\Lambda_r := \{f(r) : f \in \Lambda\}$ for all $r \in V$. In particular, $g(r) \in K_r[Y, T]$, and so $g \in K[Y, T]_{\text{int}} \cap IK[Z]_{\text{int}}$. But $K[Z]_{\text{int}}$ is faithfully flat over $K[Y, T]_{\text{int}}$ since, for all $r, K_r[Z]$ is faithfully flat over $K_r[Y, T]$. So $g \in IK[Y, T]_{\text{int}}$.

For each $r \in \mathbb{I}$, set L_r to be the field $K_r(Y)$ and let L be the corresponding internal field. Note that L is the fraction field of $R := K[Y]_{\text{int}}$ The ultraproduct of the polynomial rings $L_r[T]$ gives rise to the ring of internal polynomials $L[T]_{\text{int}}$, which extends L[T] via the usual embedding. Since $\deg_{v_f}(g(r)) < \deg_{v_f}(f)$, for all $r \in V$ and $f \in \Lambda$, we have that $g \in L[T]$. But we saw above that $g \in IK[Y,T]_{int} \subset IL[T]_{int}$. By the faithful flatness of $L[T]_{int}$ over L[T], $IL[T]_{int} \cap L[T] = IL[T]$. So $g \in IL[T]$. Now we can clear denominators: there is $h \in R = K[Y]_{int}$ such that $f := hg \in IR[T]$. Note that f is still internally reduced with respect to Λ as we have only multiplied by an internal polynomial in which no derivatives of T appear, co-ordinatewise almost everywhere.

Write $f = h_1 g_1 + \cdots + h_\ell g_\ell$ where $g_1, \ldots, g_\ell \in I \subset K[Y, T]$ and $h_1, \ldots, h_\ell \in R[T]$. Letting $(M_j : j \in J)$ be the monomials in T that appear in f, the h_i 's, g_i 's, and $h_i g_i$'s, we can write

$$f = \sum_{j \in J} f_j M_j$$
$$h_i = \sum_{j \in J} h_{i,j} M_j$$
$$g_i = \sum_{j \in J} g_{i,j} M_j$$

where $f_j, h_{i,j} \in K[Y]_{\text{int}}$ and $g_{i,j} \in K[Y]$. Let $J' \subset J$ be those indices j such that $f_j \neq 0$. Then for each $j \in J'$,

$$f_j = \sum_{i=1}^{\ell} \sum_{M_{j_1} M_{j_2} = M_j} h_{i,j_1} g_{i,j_2}$$

and for each $j \in J \setminus J'$,

$$0 = \sum_{i=1}^{\ell} \sum_{M_{j_1}M_{j_2}=M_j} h_{i,j_1} g_{i,j_2}$$

That is, the f_j 's and $h_{i,j}$'s are a solution in $K[Y]_{int}$ to the system of linear equations over K[Y] given by

$$0 = -S_j + \sum_{i=1}^{\ell} \sum_{M_{j_1}M_{j_2}=M_j} g_{i,j_2} S_{i,j_1}$$

for $j \in J'$, and

$$0 = \sum_{i=1}^{\ell} \sum_{M_{j_1}M_{j_2}=M_j} g_{i,j_2} S_{i,j_1}$$

for $j \in J \setminus J'$. Note that $J' \neq \emptyset$ as $f \neq 0$. By the flatness of $K[Y]_{\text{int}}$ over K[Y], our solution is a $K[Y]_{\text{int}}$ -linear combination of solutions in K[Y]. In particular, there must exist a solution $(f'_j, h'_{i,j})$ in K[Y]. In fact, we can find such a solution such that for some $j \in J'$, $f'_j \neq 0$. Hence $f' := \sum_{j \in J'} f'_j M_j \neq 0$. Moreover, setting $h'_i := \sum_{j \in J} h'_{i,j} M_j \in K[Y,T]$, we get that $f' = h'_1 g_1 + \cdots + h'_\ell g_\ell \in I \subset I(\Lambda)$. Note that as $f' \in K[Y,T]$ and in each T-variable the degree of f' is no greater than it was in f, f' is reduced with respect to Λ . We have found a nonzero element of $I(\Lambda)$ that is reduced with respect to Λ , as desired.

We can now apply Facts 2.1 and 3.2 to see that characteristic sets for prime Δ -ideals in $K\{X\}$ can be recognised in $K\{X\}_{int}$.

Theorem 4.3. Suppose $\Lambda \subset K\{X\}$ is finite. Then Λ is a characteristic set for a prime Δ -ideal of $K\{X\}$ if and only if it is an internally characteristic set for a prime internal Δ -ideal of $K\{X\}$ _{int}.

Proof. The right-to-left direction we have already mentioned: If Λ is internally characteristic for $P \subset K\{X\}_{int}$ then it is characteristic for $P \cap K\{X\}$. This is because internal autoreducedness and rank in $K\{X\}_{int}$ restrict to autoreducedness and rank in $K\{X\}$. (See the discussion on page 8.)

For the converse, suppose Λ is characteristic for a prime Δ -ideal $P \subset K\{X\}$. By Fact 2.1, Λ is coherent and $I(\Lambda)$ is a prime ideal of $K\{X\}$ containing no nonzero elements reduced with respect to Λ . By Lemma 4.2, Λ is internally coherent in $K\{X\}_{int}$, $I_{int}(\Lambda)$ is prime, and $I_{int}(\Lambda)$ contains no nonzero element internally reduced with respect to Λ . Hence, by Fact 3.2, Λ is an internally charcateristic set for a prime internal Δ -ideal.

Recall that for $\Lambda \subset K\{X\}$, $I[\Lambda] = \{g \in K\{X\} : H_{\Lambda}^{n}g \in [\Lambda]\}$, for some $n \in \mathbb{N}\}$ and $I_{\text{int}}[\Lambda] = \{g \in K\{X\}_{\text{int}} : H_{\Lambda}^{N}g \in [\Lambda]_{\text{int}}$, for some $N \in \mathbb{N}^{*}\}$. (We are using here again the fact that, since $\Lambda \subset K\{X\}$, $H_{\Lambda} = H_{\Lambda}^{\text{int}}$.) One would like to prove, analogously to Lemma 4.2(b), that if $I[\Lambda]$ is prime and Λ is its characteristic set, then $I_{\text{int}}[\Lambda] = \{I[\Lambda]\}_{\text{int}}$. But we are not able to do so. In fact, as we will see in the next section (see statement (B) of Proposition 5.5), this would imply the definability of primality conjecture discussed in the introduction. Nevertheless, we can use Theorem 4.3 to show that $I_{\text{int}}[\Lambda]$ is least among the prime internal Δ -ideals that lie above $I[\Lambda]$.

Corollary 4.4. Suppose $\Lambda \subset K\{X\}$ is a characteristic set for a prime Δ -ideal. Then $I_{int}[\Lambda]$ is a prime internal Δ -ideal, $I_{int}[\Lambda] \cap K\{X\} = I[\Lambda]$, and if P is any prime internal Δ -ideal of $K\{X\}_{int}$ with $P \cap K\{X\} = I[\Lambda]$ then $I_{int}[\Lambda] \subset P$.

Proof. By Theorem 4.3, Λ is internally characteristic for a prime internal Δ -ideal of $K\{X\}_{int}$, which must therefore be $I_{int}[\Lambda]$. It follows that $I_{int}[\Lambda] \cap K\{X\}$ is prime and that Λ , being minimally ranked among the autoreduced subsets of this ideal, is characteristic for $I_{int}[\Lambda] \cap K\{X\}$. But then $I_{int}[\Lambda] \cap K\{X\} = I[\Lambda]$.

Suppose P is a prime internal Δ -ideal of $K\{X\}_{int}$ with $P \cap K\{X\} = I[\Lambda]$. Note that $H_{\Lambda} \notin P$ else it would be in $P \cap K\{X\} = I[\Lambda]$ forcing the latter to be all of $K\{X\}$. Suppose $g \in I_{int}[\Lambda]$ so that $H_{\Lambda}^N g \in [\Lambda]_{int} \subset P$, for some $N \in \mathbb{N}^*$. Since $H_{\Lambda} \notin P$, $H_{\Lambda}(r) \notin P_r$ for almost all r, and so by primality $g(r) \in P_r$ for almost all r. Hence $g \in P$. So $I_{int}[\Lambda] \subset P$, as desired.

Corollary 4.5. Suppose $S \subset K\{X\}$. Then $\{S\}_{int} \cap K\{X\} = \{S\}$.

Proof. If $\{S\} = K\{X\}$ then $\{S\}_{int} = K\{X\}_{int}$ and we are done. Otherwise $\{S\}$ is a proper radical Δ -ideal and by the differential prime decomposition theorem there must exist finitely many prime Δ -ideals, $P_1, \ldots, P_\ell \subset K\{X\}$, such that $\{S\} =$ $P_1 \cap \cdots \cap P_\ell$. For each $i = 1, \ldots, \ell$, let $P_i = I[\Lambda_i]$ where Λ_i is characteristic for P_i . By Corollary 4.4, each $I_{int}[\Lambda_i]$ is a prime internal Δ -ideal and $I_{int}[\Lambda_i] \cap K\{X\} = P_i$. In particular, $I_{int}[\Lambda_1] \cap \cdots \cap I_{int}[\Lambda_\ell]$ is a radical internal Δ -ideal of $K\{X\}_{int}$ that contains S. It follows that $\{S\}_{int} \subset I_{int}[\Lambda_1] \cap \cdots \cap I_{int}[\Lambda_\ell]$. So, working in $K\{X\}$,

$$\{S\} \subset \{S\}_{int} \cap K\{X\} \subset (I_{int}[\Lambda_1] \cap \dots \cap I_{int}[\Lambda_\ell]) \cap K\{X\} = (I_{int}[\Lambda_1] \cap K\{X\}) \cap \dots \cap (I_{int}[\Lambda_\ell] \cap K\{X\}) = P_1 \cap \dots \cap P_\ell = \{S\}$$

which proves that $\{S\}_{int} \cap K\{X\} = \{S\}.$

Remark 4.6. We do not know if $[S]_{int} \cap K\{X\} = [S]$ for all finite sets $S \subset K\{X\}$. Since our proof of Corollary 4.5 goes via prime Δ -ideals it does not help. One might hope to imitate what happens in the algebraic setting, where $(S)_{int} \cap K\{X\} = (S)$ follows by faithful flatness from the fact that $(S)_{int} = (S)K\{X\}_{int}$. The latter holds because if $g \in (S)_{int}$ then for almost all r we have $g(r) = \sum_{f \in S} g_{f,r}f(r)$ where the $g_{f,r}$ are in $K_r\{X\}$, and hence $g = \sum_{f \in S} g_f f$ where g_f is chosen so that $g_f(r) = g_{f,r}$ almost everywhere. But this argument cannot be extended to Δ -ideals; it is not necessarily the case that $[S]_{int}$ is the Δ -ideal of $K\{X\}_{int}$ generated by S. For a counterexample consider the case when Δ is a single derivation δ , X is a single variable, and $\mathbb{I} = \omega$. The internal δ -ideal generated by the variable X in $K\{X\}_{int}$ clearly contains the internal δ -polynomial $\delta^{\omega}X$ whose rth co-ordinate is $\delta^r X$. But $\delta^{\omega}X$ is not in the δ -ideal generated by X in $K\{X\}_{int}$ since the latter is the ideal generated by the set $\{\delta^m X : m < \omega\}$. Note that this counterexample is radical (indeed prime), so that even passing to radicals does not avoid the problem.

5. Definability of primality and related problems

Throughout this section all nonstandard notions are with respect to a fixed nonprincipal ultrafilter \mathcal{U} on ω . Also, we continue to work with m commuting derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$ in n differential indeterminates $X = (X_1, \ldots, X_n)$.

The original motivation for this work was to apply nonstandard methods to the problem of the existence of uniform bounds in checking if the radical Δ -ideal generated by a given finite set of Δ -polynomials is prime. This is the definability of primality problem discussed in the introduction (Conjecture 1.1). The algebraic analogue of Conjecture 1.1 was proved using nonstandard methods by van den Dries and Schmidt [7], and we have tried here to extend their approach to the differential setting. The following translates definability of primality into a statement about rings of internal Δ -polynomials.

Proposition 5.1 (Nonstandard formulation of definability of primality). Conjecture 1.1 of the introduction is equivalent to the following statement:

(A) For any internal Δ -field K and internal $S \subset K\{X\}$, if $\{S\}_{int} \cap K\{X\}$ is prime in $K\{X\}$ then $\{S\}_{int}$ is prime in $K\{X\}_{int}$.

Proof. If the conjecture fails then there exists a $d < \omega$, and for every $r < \omega$ a Δ -field K_r with a finite set $S_r \subset K_r\{X\}$ of order and degree $\leq d$ such that $\{S_r\}$ is not prime, but it is proper and for all $f, g \in K_r\{X\}$ of degree and order $\leq r$, if $fg \in \{S_r\}$ then either f or g is in $\{S\}$. Passing to the ultraproduct we obtain an internal Δ -field K whose components are K_r and an internal set $S \subset K\{X\}$ int whose components are S_r . Since the degrees and orders of the elements of S_r were

bounded independently of r, S is in fact a subset of $K\{X\}$. Since the $\{S_r\}$ were not prime, $\{S\}_{int}$ is not prime. On the other hand, $\{S\}_{int} \cap K\{X\}$ is prime. Indeed, it is proper since each $\{S_r\}$ was proper and hence $\{S\}_{int}$ omits $1 \in K\{X\}$. Moreover, if $f, g \in K\{X\}$ with $fg \in \{S\}_{int}$, then for almost all r, $f(r), g(r) \in K_r\{X\}$ are of degree and order $\leq r$ (as they are almost everywhere equal to that of f and g), and $f(r)g(r) \in \{S_r\}$, and hence one of f(r) and g(r) is in $\{S_r\}$. Depending on which of these is favoured by the ultrafilter, we get that either f or g is in $\{S\}_{int}$. We have shown that $\{S\}_{int} \cap K\{X\}$ is prime but $\{S\}_{int}$ is not. That is, statement (A) is false.

Conversely, suppose Conjecture 1.1 holds, K is an internal Δ -field, and $S \subset K\{X\}$ is an internal set. Let $(S_r : r < \omega)$ be a family of components for S. The fact that $S \subset K\{X\}$ means that for some $V \in \mathcal{U}$ there is a bound on the orders and degrees of the elements of S_r for all $r \in V$, that is independent of r. Let d be this bound and let N = r(d, n, m) be given by Conjecture 1.1. Now suppose that $\{S\}_{int}$ is not prime. We show that $\{S\}_{int} \cap K\{X\}$ cannot be prime, thereby verifying the contrapositive of (A). Shrinking V if necessary, $\{S_r\}$ is not prime for all $r \in V$. Hence there is $f_r, g_r \in K_r\{X\}$ of degree and order $\leq N$ witnessing the nonprimality of $\{S_r\}$. (Note that while S_r need not be finite, there exists finite $T_r \subset S_r$ with $\{S_r\} = \{T_r\}$ by the Ritt-Raudenbush basis theorem, and hence Conjecture 1.1 applies.) Let $f, g \in K\{X\}_{int}$ be such that $f(r) = f_r$ and $g(r) = g_r$ almost everywhere. Then, as the degrees and orders are bounded, we have that $f, g \in K\{X\}$. Moreover, f, g witness the nonprimality of $\{S\}_{int}$. That is, $\{S\}_{int} \cap K\{X\}$ is not prime.

Remark 5.2. The above proposition remains true even if we change statement (A) to consider only *finite* subsets $S \subset K\{X\}$. Indeed, when we were proving above that a counterexample to Conjecture 1.1 leads to a counterexample to (A), we could have taken the S_r to be of bounded size independently of r without changing $\{S_r\}$. This is because the Δ -polynomials in $K_r\{X\}$ of order and degree bounded by d form a K_r -vector space whose (finite) dimension depends only on d (not on r). Choosing the S_r to be of uniformly bounded size would then have lead to a finite counterexample S.

Unfortunately, the results we obtained in the last section only go part way toward proving statement (A). The proof of the following weak form of (A) illustrates what goes wrong.

Proposition 5.3. Suppose K is an internal Δ -field and $S \subset K\{X\}$ is such that $\{S\}_{int} \subseteq K\{X\}_{int}$ satisfies: for all $f \in K\{X\}$ and $g \in K\{X\}_{int}$, if $fg \in \{S\}_{int}$ then $f \in \{S\}_{int}$ or $g \in \{S\}_{int}$. Then $\{S\}_{int}$ is prime.

Proof. Note that our assumption on $\{S\}_{int}$ implies that $\{S\}_{int} \cap K\{X\}$ is prime.¹ Theorem 4.3 tells us that if Λ is a characteristic for $\{S\}_{int} \cap K\{X\}$ then $I_{int}[\Lambda]$ is prime. We will show that $\{S\}_{int} = I_{int}[\Lambda]$. Since $I_{int}[\Lambda]$ contains $I[\Lambda] = \{S\}_{int} \cap K\{X\} \supset S$, we have $\{S\}_{int} \subset I_{int}[\Lambda]$. For the reverse containment, suppose $g \in I_{int}[\Lambda]$. Then $H_{\Lambda}^N g \in [\Lambda]_{int} \subset \{S\}_{int}$ for some $N \in \mathbb{N}^*$. It follows that $(H_{\Lambda}g)^N \in \{S\}_{int}$. Since $\{S\}_{int}$ is componentwise radical almost everywhere, $H_{\Lambda}g \in \{S\}_{int}$. Now $H_{\Lambda} \notin \{S\}_{int}$, else it would be in $I[\Lambda]$ and the latter would then not be proper.

¹We know by Corollary 4.5 that $\{S\}_{int} \cap K\{X\} = \{S\}$, but we don't use this fact here.

Since $H_{\Lambda} \in K\{X\}$, our assumption on $\{S\}_{int}$ implies that $g \in \{S\}_{int}$, as desired.

We leave it to the reader to deduce from the above proposition the following standard consequence which bounds one of the two universal quantifiers in the definition of primality.

Theorem 5.4. For every d there exists r = r(d, n, m) such that for every Δ -field k and and every finite set of Δ -polynomials $S \subset k\{X\}$ of degree and order $\leq d$, the following are equivalent:

(i) $\{S\}$ is prime

14

(ii) $\{S\}$ is proper and for all $f, g \in k\{X\}$ with f of degree and order $\leq r$, if $fg \in \{S\}$ then either f or g is in $\{S\}$.

Now we turn our attention away from trying to prove definability of primality, and instead toward proving that it is equivalent to other existence-of-bounds problems in differential algebra. In this we are informed by [2] where Golubitsky, Kondratieva, and Ovchinnikov show, under some natural computability-theoretic assumptions on the base Δ -field², the equivalence of several computational problems in differential algebra. We are interested in the existence-of-bounds analogues of some of their existence-of-algorithm problems.

Proposition 5.5. Statement (A) of Proposition 5.1 is equivalent to each of the following statements: For any internal Δ -field K,

- (B) If $P \subset K\{X\}_{int}$ is a prime internal Δ -ideal with an internally characteristic set from $K\{X\}$ then $P = \{S\}_{int}$ for some internal $S \subset K\{X\}$.
- (C) Suppose $P, Q \subset K\{X\}_{int}$ are prime internal Δ -ideals with internally characteristic sets from $K\{X\}$. If $P \cap K\{X\} \subset Q$ then $P \subset Q$.
- (D) Suppose $S \subset K\{X\}$ is internal and $P, Q \subset K\{X\}_{int}$ are minimal prime internal Δ -ideals containing S. If $P \cap K\{X\} \subset Q$ then P = Q.
- (E) If $S \subset K\{X\}$ is internal and $f \in K\{X\}$ is not a zero divisor in $K\{X\}/\{S\}$ then f is not a zero divisor in $K\{X\}_{int}/\{S\}_{int}$.

Proof. Suppose (A) holds and let $\Lambda \subset K\{X\}$ be internally characteristic for a prime internal Δ -ideal P. Then $P = I_{int}[\Lambda]$, and by Theorem 4.3, Λ is characteristic for the prime Δ -ideal $I[\Lambda]$ of $K\{X\}$. Let $S \subset K\{X\}$ be finite so that $I[\Lambda] = \{S\}$. By Corollary 4.4, P is least among the prime internal Δ -ideals that lie above $\{S\}$. By Corollary 4.5, $\{S\}_{int} \cap K\{X\} = \{S\}$, and by (A), $\{S\}_{int}$ is prime. Hence $P \subset \{S\}_{int}$. The reverse containment is clear. This proves (B).

That (B) implies (C) is immediate.

Note that (D) does not follow tautologically from (C), because the prime internal Δ -ideals P and Q appearing in (D) are not assumed to have internally characteristic sets from $K\{X\}$. However, by the following lemma, P and Q do in fact have internally characteristic sets from $K\{X\}$, and so (C) does imply (D).

Lemma 5.6. If $S \subset K\{X\}$ and $P \subset K\{X\}$ int is a minimal prime internal Δ -ideal containing S, then P has an internally characteristic set from $K\{X\}$.

²Namely that k is a computable Δ -field and that there is an algorithm for determining if a univariate polynomial over k is irreducible.

Proof of Lemma 5.6. Consider the prime Δ -ideal $Q := P \cap K\{X\}$, and let $\Lambda \subset K\{X\}$ be a characteristic set for Q. By Theorem 4.3, Λ is internally characteristic for the prime internal Δ -ideal $I_{int}[\Lambda]$. We show that $P = I_{int}[\Lambda]$. By Corollary 4.4, $I_{int}[\Lambda]$ is least among the prime internal Δ -ideals of $K\{X\}_{int}$ whose intersection with $K\{X\}$ is Q. Hence $I_{int}[\Lambda] \subset P$. On the other hand, $S \subset P \cap K\{X\} = Q \subset I_{int}[\Lambda]$. So by the minimality of $P, P = I_{int}[\Lambda]$, as desired.

In order to prove that (D) implies (E), we first show, unconditionally, that if $S \subset K\{X\}$ is internal and $\Lambda \subset K\{X\}$ is characteristic for a minimal prime Δ -ideal containing S, then $I_{\text{int}}[\Lambda]$ is a minimal prime internal Δ -ideal of $K\{X\}_{\text{int}}$ containing S. Indeed, by Theorem 4.3, $I_{\text{int}}[\Lambda]$ is a prime internal Δ -ideal containing S, and hence by transfer from the standard setting, there exists $P \subset I_{\text{int}}[\Lambda]$ minimal such. But then, by Lemma 5.6, $P = I_{\text{int}}[\Sigma]$ where $\Sigma \subset K\{X\}$ is internally characteristic for P. Intersecting with $K\{X\}$, we get $S \subset I[\Sigma] \subset I[\Lambda]$, and hence $I[\Sigma] = I[\Lambda]$ by minimality. Therefore $P = I_{\text{int}}[\Sigma] = I_{\text{int}}[\Lambda]$, as desired.

Now we show that (D) implies:

(D') If $Q \subset K\{X\}_{int}$ is a minimal prime internal Δ -ideal containing S, then $Q \cap K\{X\}$ is a minimal prime Δ -ideal of $K\{X\}$ containing S.

Indeed, let $Q' \subset Q \cap K\{X\}$ be a minimal prime Δ -ideal containing S. Let $\Lambda \subset K\{X\}$ be characteristic for Q', so that $Q' = I[\Lambda]$. Then, by the previous paragraph, $P := I_{\text{int}}[\Lambda]$ is another minimal prime internal Δ -ideal of $K\{X\}_{\text{int}}$ containing S. As $P \cap K\{X\} = I[\Lambda] \subset Q$, (D) implies that P = Q. So, $Q \cap K\{X\} = I[\Lambda] = Q'$

We are ready to prove that (D) implies (E). We use the following characterisation of zero divisors that comes from the prime decomposition theorem (see, for example, Lemma 1 of [2]): $f \in K\{X\}$ is a zero divisor modulo $\{S\}$ if an only if f belongs to one of, but not all of, the minimal prime Δ -ideals of $K\{X\}$ that contain S. Working componentwise almost everywhere we also have: $f \in K\{X\}_{int}$ is a zero divisor in $K\{X\}_{int}/\{S\}_{int}$ if an only if f belongs to one of, but not all of, the minimal prime internal Δ -ideals of $K\{X\}_{int}$ that contain S. Now, toward a proof of the contrapositive of (E), suppose that $f \in K\{X\}$ is a zero divisor in $K\{X\}_{int}/\{S\}_{int}$, and let P and Q be minimal prime internal Δ -ideals containing S such that $f \in$ $P \setminus Q$. But then $f \in (P \cap K\{X\}) \setminus (Q \cap K\{X\})$. As $P \cap K\{X\}$ and $Q \cap K\{X\}$ are minimal prime internal Δ -ideals containing S by (D'), it follows that f is a zero divisor of $K\{X\}/\{S\}$.

Finally, we show that (E) implies (A). Assuming (E), suppose that $S \subset K\{X\}$ is an internal set such that $\{S\}_{int}$ is not prime in $K\{X\}_{int}$. We need to prove that $\{S\}_{int} \cap K\{X\}$ is not prime in $K\{X\}$. By Corollary 4.5, $\{S\}_{int} \cap K\{X\} = \{S\}$. Now by Proposition 5.3, the fact that $\{S\}_{int}$ is not prime is witnessed by some $f \in K\{X\}$ and $g \in K\{X\}_{int}$ neither of which are in $\{S\}_{int}$ but such that $fg \in \{S\}_{int}$. That is, f is a zero divisor in $K\{X\}_{int}/\{S\}_{int}$. As $f \in K\{X\}$, (E) implies that f is a zero divisor in $K\{X\}/\{S\}$. Hence $\{S\}$ is not prime in $K\{X\}$, as desired. \Box

Theorem 5.7. The following statements in differential algebra are equivalent:

- (1) Definability of primality. Conjecture 1.1.
- (2) Bounds for generators of a prime Δ-ideal given a characteristic set.
 For every d there exists r = r(d, n, m) such that for every Δ-field k, if P is a prime Δ-ideal of k{X} with a characteristic set whose elements

are of degree and order $\leq d$, then P is radically differentially generated by Δ -polynomials of order and degree $\leq r$.

- (3) Bounds for checking ⊂ among prime Δ-ideals given characteristic sets. For every d there exists r = r(d, n, m) such that for every Δ-field k and all prime Δ-ideals P, Q ⊂ k{X} with characteristic sets whose elements are of degree and order ≤ d, if every Δ-polynomial in P of degree and order ≤ r is in Q then P ⊂ Q.
- (4) Bounds for distinguishing minimal prime Δ-ideals.
 For every d there exists r = r(d, n, m) such that for every Δ-field k, every set S ⊂ k{X} of Δ-polynomials of degree and order ≤ d, and every pair P and Q of minimal prime Δ-ideals containing S, if every Δ-polynomial in P of degree and order ≤ r is in Q then P = Q.
- (5) Definability of zero-divisibility.
 - For every d there exists r = r(d, n, m) such that for every Δ -field k, every set $S \subset k\{X\}$ of Δ -polynomials of degree and order $\leq d$, and every $g \in$ $k\{X\}$ of degree and order $\leq d$, if $gf \notin \{S\}$ for all $f \notin \{S\}$ of degree and order $\leq r$, then g is not a zero divisor modulo $\{S\}$.

Proof. These statements are just standard formulations of the corresponding statements (A) through (E) of Proposition 5.5. The equivalence of (A) and (1) is Proposition 5.1, and very similar arguments yield the equivalence of (B) to (2), (C) to (3), (D) to (4), and (E) to (5). The theorem then follows immediately from Proposition 5.5.

Remark 5.8. The existence-of-algorithms analogue of (3) would say that there is an algorithm for deciding whether one prime Δ -ideal is contained in another given their characteristic sets. This is Kolchin's Problem 3 of §IV.9 of [5], a solution to which would solve the Ritt problem of computing the prime components of the radical Δ -ideal generated by a given finite set of Δ -polynomials.

6. Two standard consequences

We conclude by extracting the existence of some bounds in the theory of Δ -polynomial rings from our understanding of the ring of internal Δ -polynomials.

Throughout $\Delta = \{\delta_1, \dots, \delta_m\}$ and $X = (X_1, \dots, X_n)$.

6.1. Characteristic sets for minimal prime Δ -ideals. Given a finite set of Δ -polynomials S, consider the problem of finding the minimal prime Δ -ideals that contain S. In constructive differential algebra there has been significant work on bounds in differential elimination algorithms from which it seems that explicit bounds on characteristic sets for the minimal prime Δ -ideals containing S should be deducible. We have in mind [1] and [3]. Here we show the *existence* of such bounds as an immediate consequence of our study of $K\{X\}_{int}$.

Theorem 6.1. Suppose $d \in \mathbb{N}$. There is $r = r(d, n, m) \in \mathbb{N}$ such that for every Δ -field k and every finite set of Δ -polynomials $S \subset k\{X\}$ of degree and order $\leq d$, each minimal prime Δ -ideal containing S has a characteristic set of Δ -polynomials of degree and order $\leq r$.

Proof. Suppose not. Then for each $r \in \mathbb{N}$ there is a Δ -field K_r , a finite set $S_r \subset K_r\{X\}$ of Δ -polynomials of degree and order bounded by d, and a minimal prime Δ -ideal $P_r \subset K_r\{X\}$ containing S_r all of whose characteristic sets contain at least one element of either degree or order strictly bigger than r.

Fix a non-principal ultrafilter \mathcal{U} on ω , and work in the ultraproduct $K\{X\}_{\text{int}}$. Let $S \subset K\{X\}_{\text{int}}$ be the internal set with components S_r , and let $P \subset K\{X\}_{\text{int}}$ be the prime internal Δ -ideal with components P_r . Then P is a minimal prime internal Δ -ideal containing S. As the degrees and orders of the elements of S_r were bounded independently of r, we actually have that $S \subset K\{X\}$. By Lemma 5.6, P has an internally characteristic set from $K\{X\}$, say $\Lambda \subset K\{X\}$. It follows that for almost all r, $\Lambda_r := \{f(r) : f \in \Lambda\}$ is characteristic for P_r . Since for $f \in K\{X\}$, f and f(r) have the same shape, if t is the maximum of the degrees and orders of the elements of Λ_r . Letting $r \geq t$, this contradicts the fact that P_r has no characteristic set bounded by r in this way.

When $\{S\}$ itself is prime we get from the above theorem the existence of a bound for a characteristic set of $\{S\}$. In this case an explicit bound (at least for orders) is given by Lemma 14 of [3].

Corollary 6.2. There is $r = r(d, n, m) \in \mathbb{N}$ such that for every Δ -field k and every prime Δ -ideal $P = \{S\}$, where S is a finite set of Δ -polynomials of degree and order $\leq d$, P has a characteristic set of Δ -polynomials of degree and order $\leq r$.

6.2. Differential Nullstellensatz. Consider finally the problem of determining if a Δ -polynomial g is in the radical Δ -ideal generated by a finite set of Δ polynomials S. An explicit bound on how many derivatives one has to apply to S to witness this membership, depending only on the orders and degrees of the elements of $S \cup \{g\}$, was found in [3]. Again, the mere *existence* of such a bound can be seen as an immediate corollary of our study of $K\{X\}_{int}$, as we now point out. Another proof of the existence of a bound, also using ultraproducts (though of differentially closed fields), was given by Singer (cf. §6 of [3]). However Singer's bound depends also on the size of S.

Theorem 6.3. Suppose $d \in \mathbb{N}$. There is $r = r(d, n, m) \in \mathbb{N}$ such that for every Δ -field k and every finite set of Δ -polynomials $S \subset k\{X\}$ of degree and order $\leq d$, the following holds:

if $g \in \{S\}$ is of order and degree $\leq d$ then $g^r \in (\theta f \mid f \in S, \theta \in \Theta, \operatorname{ord} \theta \leq r)$.

Proof. Suppose not. Then for each $r \in \mathbb{N}$ there is a Δ-field K_r , a finite set $S_r \subset K_r\{X\}$, and $g_r \in \{S_r\}$, such that every element of $S_r \cup \{g_r\}$ is of degree and order bounded by d, and $g_r^r \notin (\theta f \mid f \in S_r, \theta \in \Theta, \operatorname{ord} \theta \leq r)$. Let $S \subset K\{X\}_{int}$ be the internal set with components S_r , and $g \in K\{X\}_{int}$ the internal Δ-polynomial with co-ordinates g_r . Then $g \in \{S\}_{int}$. Since the order and degrees of the components were bounded, we have $S \subset K\{X\}$ and $g \in K\{X\}$. Hence $g \in \{S\}_{int} \cap K\{X\} = \{S\}$ by Corollary 4.5. It follows that for some $f_1, \ldots, f_\ell \in S$ and some $t \in \mathbb{N}$, $g^t \in (\theta f_i \mid 1 \leq i \leq \ell, \theta \in \Theta, \operatorname{ord}(\theta) \leq t)K\{X\}$. So for almost all $r \in \mathbb{N}, g_r^t \in (\theta f_i(r) \mid 1 \leq i \leq \ell, \theta \in \Theta, \operatorname{ord}(\theta) \leq t)K_r\{X\}$. Since $f_i(r) \in S_r$, we have $g_r^t \in (\theta f \mid f \in S_r, \theta \in \Theta, \operatorname{ord}(\theta \leq r)K_r\{X\}$.

References

- O. Golubitsky, M. Kondratieva, M. Moreno Maza, and A. Ovchinnikov. A bound for Rosenfeld-Groebner algorithm. *Journal of Symbolic Computation*, 43(8):582–610, 2008.
- [2] O. Golubitsky, M. Kondratieva, and A. Ovchinnikov. On the generalized Ritt problem as a computational problem. *Fundamental' naya i Prikladnaya Matematika*, 14(4):109–120, 2008.
- [3] O. Golubitsky, M. Kondratieva, A. Ovchinnikov, and A. Szanto. A bound for orders in differential Nullstellensatz. *Journal of Algebra*, 322(11):3852–3877, 2009.
- [4] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Mathematische Annalen, 95(1):736–788, 1926.
- [5] E. R. Kolchin. Differential algebra and algebraic groups. Academic Press, New York, 1973. Pure and Applied Mathematics, Vol. 54.
- [6] A. Seidenberg. Constructions in algebra. Transactions of the American Mathematical Society, 197:273–313, 1974.
- [7] L. van den Dries and K. Schmidt. Bounds in the theory of polynomial rings over fields. A nonstandard approach. *Inventiones Mathematicae*, 76:77–91, 1984.
- [8] L. van den Dries and A. J. Wilkie. Gromov's theorem on groups of polynomial growth and elementary logic. *Journal of Algebra*, 89(2):349–374, 1984.

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L $3\mathrm{G1}$

18