Math.Comput.Sci. (2022) 16:20
https://doi.org/10.1007/s11786-022-00540-9

Mathematics in Computer Science

A New Type of Difference Dimension Polynomials

Alexander Levin

Received: 30 September 2021 / Revised: 17 July 2022 / Accepted: 25 July 2022 / Published online: 13 October 2022

Abstract We introduce a new type of characteristic sets of difference polynomials using a generalization of the concept of effective order to the case of partial difference polynomials. Applying properties of these characteristic sets we prove the existence and find invariants of a bivariate dimension polynomial of a finitely generated difference field extension that describes the transcendence degrees of intermediate fields obtained by adjoining transforms of the generators whose orders lie between two given natural numbers. We also consider an application of the properties of introduced characteristic sets to the study of non-reflexive difference polynomial ideals.

Keywords Difference polynomials · Effective order · Autoreduced set · Characteristic set · Dimension polynomial

Mathematics Subject Classification Primary: 12H10; Secondary: 13C15

1 Introduction

This work is dedicated to the memory of Vladimir Gerdt who made numerous contributions to differential and difference algebra, symbolic computation and applications of computational algebraic methods in physics. In recent years Vladimir obtained a number of deep results on difference schemes for systems of algebraic partial differential equations and differential and difference algebraic structures associated with such systems. In particular, he developed new algorithmic methods for differential and difference polynomial ideals and applied them to the consistency analysis of difference schemes for algebraic PDEs, see [1,4–7]. The developed theory allows one to choose optimal difference schemes based on the relationships between radical differential polynomial ideals associated with systems of algebraic PDEs and their counterparts defined by the corresponding systems of difference equations. In this connection, the study of dimensional characteristics of prime and perfect difference polynomial ideals (in particular, dimension polynomials associated with such ideals) is of primary importance for the comparative analysis of systems of algebraic difference equations arisen from the same system of PDEs. Univariate difference dimension polynomials introduced in [12,13] play the same role in the study of difference modules and difference

This work was completed with the support of the NSF grant CCF-1714425.

Alexander Levin (✉)
Department of Mathematics, The Catholic University of America, Washington, DC 20064, USA
e-mail: levin@cua.edu

field extensions as Hilbert polynomials play in the study of the corresponding structures in commutative algebra and algebraic geometry. A similar concept of differential dimension polynomial introduced in [9] plays an important role in the study of finitely generated differential field extensions, differential modules and algebras. The following theorem, whose proof can be found in [11, Theorem 6.4.1], describes a dimension polynomial associated with a finitely generated difference field extension.

Theorem 1.1 *Let K be a difference field of characteristic zero, that is, a field containing $\mathbb{Q}$ considered together with the action of a set $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ of mutually commuting endomorphisms of K. Let T denote the free commutative semigroup of all power products of the form $\tau = \alpha_1^{k_1} \ldots \alpha_m^{k_m}$ $(k_i \geq 0)$, let* ord $\tau = \sum_{i=1}^{m} k_i$, *and for any $r \geq 0$, let $T(r) = \{\tau \in T \mid \text{ord } \tau \leq r\}$. Furthermore, let $L = K\langle \eta_1, \ldots, \eta_n \rangle$ be a difference field extension of K generated by a finite set $\eta = \{\eta_1, \ldots, \eta_n\}$. (As a field, $L = K(\{\tau \eta_j \mid \tau \in T, 1 \leq j \leq n\})$.) Then there exists a polynomial $\phi_{\eta|K}(t) \in \mathbb{Q}[t]$ such that*

(i) $\phi_{\eta|K}(r) = \text{tr. deg}_K\, K(\{\tau\eta_j | \tau \in T(r),\ 1 \leq j \leq n\})$ *for all sufficiently large $r \in \mathbb{Z}$;*

(ii) $\deg \phi_{\eta|K} \leq m$ *and* $\phi_{\eta|K}(t)$ *can be represented as* $\phi_{\eta|K}(t) = \sum_{i=0}^{m} a_i \binom{t+i}{i}$ *where* $a_0, \ldots, a_m \in \mathbb{Z}$;

(iii) $d = \deg \phi_{\eta|K}$, a_m *and* a_d *do not depend on the choice of the system of difference generators η of the extension L/K (clearly, $a_d \neq a_m$ if and only if $d < m$, that is, $a_m = 0$). Moreover, a_m is equal to the difference transcendence degree of L over K (denoted by σ-tr. deg$_K$ L), that is, to the maximal number of elements $\xi_1, \ldots, \xi_k \in L$ such that the set $\{\tau\xi_i \mid \tau \in T, 1 \leq i \leq k\}$ is algebraically independent over K.*

(iv) *If the elements $\eta_1, \ldots, \eta_n$ are difference algebraically independent over K (that is, the set $\{\tau\eta_i \mid \tau \in T, 1 \leq i \leq n\}$ is algebraically independent over K), then $\phi_{\eta|K}(t) = n\binom{t+m}{m}$.*

The polynomial $\phi_{\eta|K}(t)$ is called the *σ-dimension polynomial* of L/K associated with the set of σ-generators $\eta = \{\eta_1, \ldots, \eta_n\}$. Theorem 1.1 allows one to assign dimension polynomials to prime difference ideals of finitely generated difference algebras over difference fields (these are dimensional polynomials of the quotient fields of the corresponding factor rings). Using properties of difference dimension polynomials (in particular, the fact that the set of such polynomials is well ordered with respect to the natural order, $f(t) \leq g(t)$ if $f(r) \leq g(r)$ for all sufficiently large $r \in \mathbb{Z}$), one can efficiently study Krull-type dimension of difference rings, local difference algebras, and extensions of difference fields (see, for example, [11, Chapter 7], [15, Chapter 4], [14,18]). Furthermore, as it is shown in [19] and [15, Chapter 7], the dimension polynomial of a differential or difference polynomial ideal generated by a system of partial differential or, respectively, difference equations expresses Einstein's strength of the system, its important qualitative characteristic introduced in [3]. (See [15, Section 7.7] for the description of the relationship between difference dimension polynomials and Einstein's strength of systems of equations in finite differences.)

In this paper we introduce a reduction of difference polynomials that takes into account the effective order of such polynomials (we generalize the concept of the effective order of an ordinary difference polynomial defined in [2, Chapter 2, Section 4] to the partial case) and consider a new type of characteristic sets that are associated with this reduction (they are called E-characteristic sets). Then we use properties of E-characteristic sets to prove the existence of a bivariate dimension polynomial of a finitely generated difference field extension that describes the transcendence degrees of intermediate fields obtained by adjoining transforms of the generators whose orders lie between two given natural numbers. We also determine invariants of such polynomials, that is, numerical characteristics of the extension that are carried by any of its bivariate dimension polynomial and that do not depend on the system of difference generators the polynomial is associated with. Furthermore, we use the obtained properties of the E-characteristic sets to prove the existence and describe the dimension polynomial associated with a non-reflexive prime principal difference polynomial ideal. The problem of existence of such a dimension polynomial for an arbitrary non-reflexive prime difference ideal in the ring of partial difference polynomials is still open. In the ordinary case, this problem was solved in [8, Section 4.4], an alternative proof was obtained in [20, Section 5.1]; a constructive proof and an algorithm for computing dimension polynomials of non-reflexive prime difference polynomial ideals in the ordinary case were obtained in [16,17].

2 Preliminaries

Throughout the paper, $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ denote the sets of all non-negative integers, integers, and rational numbers, respectively. If $m \in \mathbb{Z}$, $m \geq 1$, then $\leq_P$ will denote the product order on $\mathbb{N}^m$, that is, a partial order $\leq_P$ such that $(a_1, \ldots, a_m) \leq_P (a'_1, \ldots, a'_m)$ if and only if $a_i \leq a'_i$ for $i = 1, \ldots, m$.

By a ring we always mean an associative ring with unity. Every ring homomorphism is unitary (maps unity to unity), every subring of a ring contains the unity of the ring, and every algebra over a commutative ring is unitary. Every field considered in this paper is supposed to have zero characteristic. $\mathbb{Q}[t_1, \ldots, t_p]$ will denote the ring of polynomials in variables $t_1, \ldots, t_p$ over $\mathbb{Q}$.

By a *difference ring* we mean a commutative ring R considered together with a finite set $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ of injective endomorphisms of R (called *translations*) such that any two mappings α_i and α_j commute. The set σ is called the *basic set* of the difference ring R, which is also called a σ-ring. If R is a field, it is called a *difference field* or a σ-field. (In what follows, we will often use prefix σ- instead of the adjective "difference".)

In what follows T denotes the free commutative semigroup generated by the set σ, that is, the semigroup of all power products $\tau = \alpha_1^{k_1} \ldots \alpha_m^{k_m}$ ($k_i \in \mathbb{N}$). The number $\operatorname{ord} \tau = \sum_{i=1}^{m} k_i$ is called the *order* of τ. Furthermore, for every $r, s \in \mathbb{N}$, $s < r$, we set

$$T(r) = \{\tau \in T \mid \operatorname{ord} \tau \leq r\} \quad \text{and} \quad T(r, s) = \{\tau \in T \mid s \leq \operatorname{ord} \tau \leq r\}.$$

A subring (ideal) R_0 of a σ-ring R is said to be a difference (or σ-) subring of R (respectively, a difference (or σ-) ideal of R) if R_0 is closed with respect to the action of any operator in σ. In this case the restriction of a mapping from σ to R_0 is denoted by the same symbol. If a prime ideal P of R is closed with respect to the action of σ, it is called a *prime difference* (or σ-) *ideal* of R.

If L is a σ-field and K a subfield of L which is also a σ-subring of L, then K is said to be a σ-subfield of L; L, in turn, is called a difference (or σ-) field extension or a σ-overfield of K (we also say that we have a σ-field extension L/K). In this case, if $S \subseteq L$, then the intersection of all σ-subfields of L containing K and S is the unique σ-subfield of L containing K and S and contained in every σ-subfield of L containing K and S. It is denoted by $K\langle S\rangle$. If S is finite, $S = \{\eta_1, \ldots, \eta_n\}$, then L is said to be a finitely generated σ-field extension of K with the set of σ-generators $\{\eta_1, \ldots, \eta_n\}$. In this case we write $L = K\langle \eta_1, \ldots, \eta_n\rangle$. It is easy to see that $K\langle \eta_1, \ldots, \eta_n\rangle$ coincides with the field $K(\{\tau\eta_i \mid \tau \in T, 1 \leq i \leq n\})$. (Here and below we often write $\tau\eta$ for $\tau(\eta)$ where $\tau \in T$, $\eta \in R$.)

If R is a σ-ring and $F \subseteq R$, then the intersection of all σ-ideals of R containing F is, obviously, the smallest σ-ideal of R containing F. This ideal is denoted by $[F]$; as an ideal, it is generated by all elements τf where $\tau \in T$, $f \in F$. If the set F is finite, $F = \{f_1, \ldots, f_k\}$, we say that the σ-ideal $I = [F]$ is finitely generated, write $I = [f_1, \ldots, f_k]$ and call elements of F difference (or σ-) generators of I. A σ-ideal I of R is said to be *reflexive* if for any $\alpha \in \sigma$, the inclusion $\alpha(a) \in I$ implies $a \in I$ (therefore, for any $\tau \in T$, the inclusion $\tau(a) \in I$ implies that $a \in I$).

Let R and S be two difference rings with the same basic set σ, so that elements of σ act on each of the rings as pairwise commuting endomorphisms. (More rigorously, we assume that there exist injective mappings of σ into the sets of endomorphisms of the rings R and S such that the images of any two elements of σ commute. For convenience we will denote these images by the same symbols $\alpha_1, \ldots, \alpha_m$). A ring homomorphism $\phi : R \longrightarrow S$ is called a *difference* (or σ-) *homomorphism* if $\phi(\alpha a) = \alpha\phi(a)$ for any $\alpha \in \sigma$, $a \in R$.

If K is a difference (σ-) field and $Y = \{y_1, \ldots, y_n\}$ is a finite set of symbols, then one can consider a countable set of symbols $TY = \{\tau y_j | \tau \in T, 1 \leq j \leq n\}$ and the polynomial ring $R = K[\{\tau y_j | \tau \in T, 1 \leq j \leq n\}]$ in the set of indeterminates TY over K. This polynomial ring is naturally viewed as a σ-ring where $\tau(\tau' y_j) = (\tau\tau')y_j$ for any $\tau, \tau' \in \sigma$, $1 \leq j \leq n$, and the elements of σ act on the coefficients of the polynomials of R as they act in the field K. The ring R is called the *ring of difference* (or σ-) *polynomials* in the set of difference (σ-) indeterminates $y_1, \ldots, y_n$ over K. This ring is denoted by $K\{y_1, \ldots, y_n\}$ and its elements are called difference (or σ-) polynomials. If $f \in K\{y_1, \ldots, y_n\}$ and $\eta = (\eta_1, \ldots, \eta_n)$ is an n-dimensional vector with coordinates in some σ-overfield of K, then $f(\eta)$ (or $f(\eta_1, \ldots, \eta_n)$) denotes the result of the replacement of every entry τy_i in f with $\tau\eta_i$ ($\tau \in T$, $1 \leq i \leq n$).

If $\pi : R = K\{y_1, \dots, y_n\} \to L = K\langle \eta_1, \dots, \eta_n \rangle$ is a natural σ-homomorphism ($\pi(a) = a$ for any $a \in K$ and $y_i \mapsto \eta_i$), then $P = \operatorname{Ker} \pi$ is a prime reflexive σ-ideal of R called the *defining ideal* of the extension L/K. In this case, L is isomorphic to the σ-field $\operatorname{qf}(S/P)$, the quotient field of S/P ($\eta_i \leftrightarrow y_i + P$).

Let K be a σ-field and $\mathcal{U}$ a family of elements of some σ-overfield of K. We say that the family $\mathcal{U}$ is *σ-algebraically dependent* over K, if the family $T\mathcal{U} = \{\tau u \mid \tau \in T,\ u \in \mathcal{U}\}$ is algebraically dependent over K (that is, there exist elements $u_1, \dots, u_k \in T\mathcal{U}$ and a nonzero polynomial f in k variables with coefficients in K such that $f(u_1, \dots, u_k) = 0$). Otherwise, the family $\mathcal{U}$ is said to be *σ-algebraically independent* over K.

If L is a σ-overfield of a σ-field K, then a set $B \subseteq L$ is said to be a *σ-transcendence basis* of L over K if B is σ-algebraically independent over K and every element $a \in L$ is σ-algebraic over $K\langle B \rangle$ (it means that the set $\{\tau a \mid \tau \in T\}$ is algebraically dependent over the field $K\langle B \rangle$). If L is a finitely generated σ-field extension of K, then all σ-transcendence bases of L over K are finite and have the same number of elements (see [15, Proposition 4.1.6]). This number is called the *σ-transcendence degree* of L over K (or the σ-transcendence degree of the extension L/K); it is denoted by $\sigma\text{-tr.deg}_K L$.

DIMENSION POLYNOMIALS OF SUBSETS OF $\mathbb{N}^m$

A polynomial in p variables $f(t_1, \dots, t_p) \in \mathbb{Q}[t_1, \dots, t_p]$ is called *numerical* if $f(r_1, \dots, r_p) \in \mathbb{Z}$ for all sufficiently large $(r_1, \dots, r_p) \in \mathbb{N}^p$. (It means that there exist $s_1, \dots, s_p \in \mathbb{N}$ such that the equality holds for all $(r_1, \dots, r_p) \in \mathbb{N}^p$ with $r_1 \geq s_1, \dots, r_p \geq s_p$.).

Clearly, every polynomial with integer coefficients is numerical. As an example of a numerical polynomial in p variables with noninteger coefficients ($p \geq 1$) one can consider $\prod_{i=1}^{p} \binom{t_i}{m_i}$ where $m_1, \dots, m_p \in \mathbb{N}$. (As usual, $\binom{t}{k}$ denotes the polynomial in t of the form $\dfrac{t(t-1)\dots(t-k+1)}{k!}$ ($k \geq 1$), $\binom{t}{0} = 1$, and $\binom{t}{k} = 0$ if $k < 0$.)

As it is shown in [11, Chapter 2], a numerical polynomial in $f(t_1, \dots, t_p)$ in p variables has a "canonical" representation as

$$f(t_1, \dots, t_p) = \sum_{i_1=0}^{m_1} \dots \sum_{i_p=0}^{m_p} a_{i_1 \dots i_p} \binom{t_1 + i_1}{i_1} \dots \binom{t_p + i_p}{i_p} \tag{2.1}$$

with uniquely defined integer coefficients $a_{i_1 \dots i_p}$ (m_i is the degree of this polynomial with respect to t_i, $1 \leq i \leq p$).

In what follows, if A is a subset of $\mathbb{N}^m$ (m is a positive integer), then V_A will denote the set of all m-tuples $v = (v_1, \dots, v_m) \in \mathbb{N}^m$ such that $a \not\leq_P v$ for every $a \in A$ (i. e., for any $a = (a_1, \dots, a_m) \in A$, there exists i, $1 \leq i \leq m$, such that $a_i > v_i$). Furthermore, for any $r \in \mathbb{N}$, we set $A(r) = \{(a_1, \dots, a_m) \in A \mid \sum_{i=1}^{m} a_i \leq r\}$.

The following theorem about a univariate numerical polynomial associated with a subset of $\mathbb{N}^m$ is due to E. Kolchin, see [10, Chapter 0, Lemma 16].

Theorem 2.1 *Let $A \subseteq \mathbb{N}^m$. Then there exists a numerical polynomial $\omega_A(t)$ such that*

(i) $\omega_A(r) = \text{Card } V_A(r)$ *for all sufficiently large $r \in \mathbb{N}$ (that is, there exists $r_0 \in \mathbb{N}$ such that the equality holds for all $r \in \mathbb{N}$, $r \geq r_0$).*

(ii) $\deg \omega_A \leq m$.

(iii) $\deg \omega_A = m$ *if and only if $A = \emptyset$. In this case* $\omega_A(t) = \binom{t+m}{m}$.

(iv) $\omega_A = 0$ *if and only if* $(0, \dots, 0) \in A$.

The polynomial $\omega_A(t)$ is called the *Kolchin polynomial* of the set $A \subseteq \mathbb{N}^m$.

Note that if $A \subseteq \mathbb{N}^m$ and A' is the set of all minimal elements of A with respect to the product order on $\mathbb{N}^m$, then the set A' is finite (it follows from [10, Ch. 0, Lemma 15] that states that for any infinite set $A \subseteq \mathbb{N}^m$, there exists an infinite sequence of elements of A, strictly increasing relative to the product order). The following theorem proved in [11, Chapter 2] gives an explicit formula for the Kolchin polynomial of a finite subset of $\mathbb{N}^m$.

Theorem 2.2 *Let $A = \{a_1, \ldots, a_n\}$ be a finite subset of $\mathbb{N}^m$ and let $a_k = (a_{k1}, \ldots, a_{km})$ $(1 \leq k \leq n)$. For any $l \in \mathbb{N}$, $0 \leq l \leq n$, let $\Gamma(l, n)$ denote the set of all l-element subsets of the set $\mathbb{N}_n = \{1, \ldots, n\}$. Let $\bar{a}_{\emptyset j} = 0$ and for any $\gamma \in \Gamma(l, n)$, $\gamma \neq \emptyset$, let $\bar{a}_{\gamma j} = \max\{a_{ij} \mid i \in \gamma\}$ $(1 \leq j \leq m)$. Then*

$$\omega_A(t) = \sum_{l=0}^{n} (-1)^l \sum_{\gamma \in \Gamma(l,n)} \binom{t + m - \sum_{j=1}^{m} \bar{a}_{\gamma j}}{m}. \tag{2.2}$$

3 E-Reduction and E-Characteristic Sets of Difference Polynomials

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ and $R = K\{y_1, \ldots, y_n\}$ the algebra of difference polynomials in σ-indeterminates $y_1, \ldots, y_n$ over K. Then R can be viewed as a polynomial ring in the set of indeterminates $TY = \{\tau y_i | \tau \in T, 1 \leq i \leq n\}$ whose elements are called *terms*. The order of a term $u = \tau y_i$ (denoted by $\operatorname{ord} u$) is defined as the order of τ. As usual, if $\tau, \tau' \in T$, we say that τ' divides τ (and write $\tau' | \tau$) if $\tau = \tau' \tau''$ for some $\tau'' \in T$. If $u = \tau y_i$ and $v = \tau' y_j$ are two terms in TY, we say that u divides v (and write $u | v$) if $i = j$ and $\tau | \tau'$. In this case we also say that v is a *transform* of u.

By a *ranking* on R we mean a well-ordering $\leq$ of the set of terms TY that satisfies the following two conditions:

(i) $u \leq \tau u$ for any $u \in TY$, $\tau \in T$. (We denote the order on TY by the usual symbol $\leq$ and write $u < v$ if $u \leq v$ and $u \neq v$.)

(ii) If $u, v \in TY$ and $u \leq v$, then $\tau u \leq \tau v$ for any $\tau \in T$.

A ranking is said to be *orderly* if the inequality $\operatorname{ord} u < \operatorname{ord} v$ $(u, v \in TY)$ implies $u < v$ (as usual, we write $u_1 > u_2$ or $u_2 < u_1$ if $u_2 \leq u_1$ and $u_2 \neq u_1$). In what follows, we assume that the following orderly ranking $\leq$ on R is fixed: if $u_1 = \alpha_1^{k_1} \ldots \alpha_m^{k_m}$, , $u_2 = \alpha_1^{l_1} \ldots \alpha_m^{l_m} \in TY$, then $u_1 \leq u_2$ if and only if

$$(\operatorname{ord} u_1, k_1, \ldots, k_m, i) \leq_{lex} (\operatorname{ord} u_2, l_1, \ldots, l_m, j)$$

($\leq_{lex}$ denotes the lexicographic order on $\mathbb{N}^{m+2}$). In this case we set

$$\mu(u_2, u_1) = (\operatorname{ord} u_2 - \operatorname{ord} u_1, l_1 - k_1, \ldots, l_m - k_m, j - i) \in \mathbb{N} \times \mathbb{Z}^{m+1}.$$

Remark 3.1 Note that for every $r = 1, \ldots, m$, $|l_r - k_r| \leq l_r + k_r \leq \operatorname{ord} u_1 + \operatorname{ord} u_2$. It follows that there is no infinite sequence of terms $u_1, u_2, \cdots \in TY$ such that $u_1 > u_2 > \ldots$.

If $f \in K\{y_1, \ldots, y_n\} \setminus K$, then the greatest (with respect to the ranking $\leq$) term that appears in f is called the *leader* of f; it is denoted by u_f. If $u = u_f$ and $d = \deg_u f$, then the σ-polynomial f can be written as

$$f = I_d u^d + I_{d-1} u^{d-1} + \cdots + I_0$$

where $I_k (0 \leq k \leq d)$ do not contain u. The σ-polynomial I_d is called the *initial* of f; it is denoted by I_f. The lowest term in f is called the *coleader* of f and is denoted by v_f.

Definition 3.2 If $f \in R$, $u_f = \alpha_1^{k_1} \ldots \alpha_m^{k_m} y_i$ and $v_f = \alpha_1^{l_1} \ldots \alpha_m^{l_m} y_j$, then the nonnegative integer $\operatorname{Eord}(f) = \operatorname{ord} u_f - \operatorname{ord} v_f$ is called the **effective order** of f. The $(m+2)$-tuple $\mu(u_f, v_f) \in \mathbb{Z}^{m+2}$ is said to be the **full effective order** of f; it is denoted by $\mathcal{E}ord(f)$.

It follows from the last definition that for any $f \in R$ and for any $\tau \in T$, $\operatorname{Eord}(\tau f) = \operatorname{Eord}(f)$ and $\mathcal{E}ord(\tau f) = \mathcal{E}ord(f)$. Furthermore, if $f, g \in R$ and $\operatorname{Eord}(f) < \operatorname{Eord}(g)$, then $\mu(u_f, v_f) < \mu(u_g, v_g)$ (with respect to the lexicographic order on $\mathbb{Z}^{m+2}$), that is, $\mathcal{E}ord(f) < \mathcal{E}ord(g)$.

Definition 3.3 Let $f, g \in K\{y_1, \ldots, y_n\}$. Then f is said to have **lower rank** than g (we write $\operatorname{rk} f < \operatorname{rk} g$) if either $f \in K$, $g \notin K$, or

$$(\mathcal{E}ord(f), u_f, \deg_{u_f} f) \leq_{lex} (\mathcal{E}ord(g), u_g, \deg_{u_g} g).$$

If the 3-tuples are equal (or $f, g \in K$) we say that f and g are of the same rank and write $\operatorname{rk} f = \operatorname{rk} g$.

Definition 3.4 Let $f, g \in R$. We say that f is **E-reduced** with respect to g if f does not contain any $(\tau u_g)^e$ $(\tau \in T)$ such that $e \geq d = \deg_{u_g} g$ and $\tau v_g \geq v_f$.

Thus, f is not E-reduced with respect to g if f contains some $(\tau u_g)^e$ $(\tau \in T)$ with $e \geq d = \deg_{u_g} g$ and also $\tau v_g \geq v_f$.

The last definition and the following definitions of E-autoreduced and E-characteristic sets allow one to develop an analog of the classical method of characteristic sets of difference polynomials (see [11, Section 3.3]) where the reduction does not increase the full effective order of a σ-polynomial. As an application of properties of E-characteristic sets , we obtain a proof of the main theorem (Theorem 4.1) that uses a construction of transcendence bases with terms whose orders are bounded above and below.

Lemma 3.5 *If* $\operatorname{rk} f < \operatorname{rk} g$, *then* f *is* E*-reduced with respect to* g.

Proof Suppose that f contains some $(\tau u_g)^e$ $(\tau \in T)$ such that $e \geq d = \deg_{u_g} g$ and $\tau v_g \geq v_f$. Then $u_f \geq \tau u_g = u_{\tau g}$ and $v_f \leq \tau v_g = v_{\tau g}$, hence $\mathcal{E}ord(f) \geq \mathcal{E}ord(g)$. Also, $u_f \geq \tau u_g \geq u_g$ and if $u_f = u_g = u$, then $e = \deg_u f \geq d = \deg_u g$. Thus, $\operatorname{rk} f \geq \operatorname{rk} g$ contrary to the assumption. □

Definition 3.6 A set $\mathcal{A} \subseteq K\{y_1, \ldots, y_n\}$ is said to be **E-autoreduced** if either it is empty or $\mathcal{A} \bigcap K = \emptyset$ and every element of $\mathcal{A}$ is E-reduced with respect to all other elements of the set $\mathcal{A}$.

Lemma 3.7 *Every* E*-autoreduced set is finite.*

Proof Suppose that there is an infinite E-autoreduced set $\mathcal{A}$. It follows from [10, Chapter 0, Lemma 15] that $\mathcal{A}$ contains a sequence of σ-polynomials $\{f_1, f_2, \ldots\}$ such that $u_{f_i} | u_{f_{i+1}}$ and $\deg_{u_{f_i}} f_i \leq \deg_{u_{f_{i+1}}} f_{i+1}$ for $i = 1, 2, \ldots$.

Let $u_{f_{i+1}} = \tau_i u_{A_i}$ $(i = 1, 2, \ldots)$. Since the set $\mathcal{A}$ is E-autoreduced, it follows that for every $i = 1, 2, \ldots$, the σ-polynomial f_{i+1} is E-reduced with respect to f_i, hence $\tau_i v_{f_i} < v_{f_{i+1}}$ and $\mathcal{E}ord(\tau f_i) = \mathcal{E}ord(f_i) > \mathcal{E}ord(f_{i+1})$. Thus, we obtain a strictly decreasing sequence $\mathcal{E}ord(f_1) > \mathcal{E}ord(f_2) > \ldots$, a contradiction (see Remark 3.1). □

Example Let $\sigma = \{\alpha_1, \alpha_2\}$ and $\mathcal{A} = \{g_1, g_2\} \subseteq K\{y\}$ where

$$g_1 = \alpha_1^2\alpha_2 y + \alpha_2^2 y + 1, \qquad g_2 = \alpha_1^2 y + y.$$

Then $\mathcal{E}ord(g_1) = (1, 2, -1) <_{lex} \mathcal{E}ord(g_2) = (2, 2, 0)$, hence $\operatorname{rk} g_1 < \operatorname{rk} g_2$ and therefore g_1 is E-reduced with respect to g_2. Since g_2 contains no transform of $u_{g_1} = \alpha_1^2\alpha_2 y$, g_2 is reduced with respect to g_1, so the set $\mathcal{A}$ is E-autoreduced. However, since the degree of g_1 with respect to $\alpha_2 u_{g_2}$ is equal to the degree of g_2 with respect to u_{g_2}, the set $\mathcal{A}$ is not autoreduced in the usual sense (where f is said to be reduced with respect to g if f does not contain any $(\tau u_g)^e$ $(\tau \in T)$ such that $e \geq d = \deg_{u_g} g$, see [11, Section 3.3]) or [15, Section 2.4]).

In what follows, while considering E-autoreduced sets we always assume that their elements are arranged in order of increasing rank.

Definition 3.8 Let $\mathcal{A} = \{g_1, \ldots, g_s\}$ and $\mathcal{B} = \{h_1, \ldots, h_t\}$ be two E-autoreduced sets in the ring $K\{y_1, \ldots, y_n\}$. Then $\mathcal{A}$ is said to have **lower rank** than $\mathcal{B}$, written as $\operatorname{rk} \mathcal{A} < \operatorname{rk} \mathcal{B}$, if one of the following two cases holds:

(1) There exists $k \in \mathbb{N}$ such that $k \leq \min\{s, t\}$, $\operatorname{rk} g_i = \operatorname{rk} h_i$ for $i = 1, \ldots, k-1$ and $\operatorname{rk} g_k < \operatorname{rk} h_k$.
(2) $s > t$ and $\operatorname{rk} g_i = \operatorname{rk} h_i$ for $i = 1, \ldots, t$.

If $s = t$ and $\operatorname{rk} g_i = \operatorname{rk} h_i$ for $i = 1, \ldots, s$, then $\mathcal{A}$ is said to have the same rank as $\mathcal{B}$; in this case we write $\operatorname{rk} \mathcal{A} = \operatorname{rk} \mathcal{B}$

Proposition 3.9 *In every nonempty family of* E*-autoreduced sets of difference polynomials there exists an* E*-autoreduced set of lowest rank.*

Proof Let $\mathcal{M}$ be a nonempty family of E-autoreduced sets in the ring $K\{y_1, \ldots, y_n\}$. Let us inductively define an infinite descending chain of subsets of $\mathcal{M}$ as follows: $\mathcal{M}_0 = \mathcal{M}$, $\mathcal{M}_1 = \{\mathcal{A} \in \mathcal{M}_0 \mid \mathcal{A}$ contains at least one element and the first element of $\mathcal{A}$ is of lowest possible rank$\}, \ldots, \mathcal{M}_k = \{\mathcal{A} \in \mathcal{M}_{k-1} \mid \mathcal{A}$ contains at least k elements and the kth element of $\mathcal{A}$ is of lowest possible rank$\}, \ldots$. It is clear that if f and g are any two σ-polynomials in the same set $\mathcal{M}_k$, then $\mathcal{E}ord(f) = \mathcal{E}ord(g)$, $u_f = u_g$ (hence $v_f = v_g$) and $\deg_{u_f} f = \deg_{u_g} g$. Therefore, if all sets $\mathcal{M}_k$ are nonempty, then the set $\{A_k \mid A_k$ is the kth element of some E-autoreduced set in $\mathcal{M}_k\}$ would be an infinite autoreduced set, and this would contradict Lemma 3.7. Thus, there is the smallest positive integer k such that $\mathcal{M}_k = \emptyset$. Clearly, every element of $\mathcal{M}_{k-1}$ is an E-autoreduced set of lowest rank in the family $\mathcal{M}$. □

Let J be any ideal of the ring $K\{y_1, \ldots, y_n\}$. Since the set of all E-autoreduced subsets of J is not empty (if $f \in J \setminus \{0\}$, then $\{f\}$ is an E-autoreduced subset of J), the last statement shows that J contains an E-autoreduced subset of lowest rank. Such an E-autoreduced set is called an *E-characteristic set* of the ideal J.

Proposition 3.10 *Let $\mathcal{A} = \{f_1, \ldots, f_d\}$ be an E-characteristic set of a σ-ideal J of the ring $R = K\{y_1, \ldots, y_n\}$. Then an element $g \in J$ is E-reduced with respect to the set $\mathcal{A}$ if and only if $g = 0$.*

Proof First of all, note that if $g \neq 0$ and rk $g <$ rk f_1, then rk $\{g\} <$ rk $\mathcal{A}$ that contradicts the fact that $\mathcal{A}$ is an E-characteristic set of the ideal J. Let rk $g >$ rk f_1 and let $f_1, \ldots, f_j$ $(1 \leq j \leq d)$ be all elements of $\mathcal{A}$ whose rank is lower than the rank of g. Then the set $\mathcal{A}' = \{f_1, \ldots, f_j, g\}$ is E-autoreduced. Indeed, by the conditions of the theorem, σ-polynomials $f_1, \ldots, f_j$ are reduced with respect to each other and g is reduced with respect to the set $\{f_1, \ldots, f_j\}$. Furthermore, each f_i $(1 \leq i \leq j)$ is reduced with respect to g because rk $f_i <$ rk g. Since rk $\mathcal{A}' <$ rk $\mathcal{A}$, $\mathcal{A}$ is not an E-characteristic set of J that contradicts the conditions of the proposition. Thus, $g = 0$. □

The following proposition shows that if f is an irreducible σ-polynomial in the ring of difference polynomials $R = K\{y_1, \ldots, y_n\}$ (K is a difference field with a basic set σ), then an arbitrary nonzero element of the σ-ideal $[f]$ of R is not E-reduced with respect to f.

Proposition 3.11 *Let f be an irreducible σ-polynomial in $R = K\{y_1, \ldots, y_n\}$. Let M be a nonzero σ-polynomial in the ideal $[f]$ of R written in the form*

$$M = \sum_{i=1}^{s} C_i f_i \tag{3.1}$$

$(s \geq 1)$ where $C_i \in R$ $(1 \leq i \leq s)$ and $f_i = \tau_i f$ for some distinct elements $\tau_1, \ldots, \tau_s \in T$. Furthermore, let u_i and v_i denote the leader and coleader of the σ-polynomial f_i, respectively $(i = 1, \ldots, l)$. Then there exists $j \in \mathbb{N}$, $1 \leq j \leq s$, such that $\deg_{u_j} M \geq \deg_{u_j} f_j$ and $v_M \leq v_j$.

Proof By [15, Theorem 2.4.15], there exists $j \in \{1, \ldots, s\}$ such that $\deg_{u_j} M \geq \deg_{u_j} f_j$. In order to show that $v_M \leq v_j$ it is sufficient to show that $v_M \leq v$ where v is the lowest coleader among $v_1, \ldots, v_s$. Without loss of generality we can assume that $v = v_1$. Let $d = \deg_v f_1$, so f_1 can be written as

$$f_1 = J_d v^d + \cdots + J_1 v + J_0$$

where all terms in J_i $(0 \leq i \leq d)$ are greater than v. Since $\tau_i \neq \tau_j$, $v < v_j$ for any $j > 1$. We can also assume that $s > 1$, since for $s = 1$ the statement is obvious. Considering each C_i as a polynomial of v, we can use reduction with respect to f_1 to eliminate in C_i all powers v^k with $k \geq d$: there exists $e_i \in \mathbb{N}$ such that $J_d^{e_i} C_i \equiv C_i' \,(mod\,(f_1))$ and $\deg_v C_i' < d$. Setting $e = e_1 + \cdots + e_s$ and multiplying both sides of (3.1) by J_d^e, we obtain that

$$J^e M \equiv \sum_{i=2}^{s} C_i'' f_i \,(mod\,(f_1))$$

where $\deg_v C_i'' < d$ for $i = 1, \ldots, s$, so the degree of the polynomial in the right-hand side with respect to v is less that d. Since $\deg_v f_1 = d$, we obtain that $\deg_v M \geq d$, hence $v_M \leq v$. □

Corollary 3.12 *Let f be an irreducible σ-polynomial in the ring $R = K\{y_1, \dots, y_n\}$. Then $\{f\}$ is an E-characteristic set of the σ-ideal $[f]$.*

Proof By Proposition 3.11, the σ-ideal $[f]$ does not contain σ-polynomials reduced with respect to f, and if $M \in [f]$, then $\operatorname{rk} M \geq \operatorname{rk} f$. Therefore, if $\mathcal{A} = \{g_1, \dots, g_t\}$ is an E-characteristic set of $[f]$ (recall that we assume $\operatorname{rk} g_1 < \cdots < \operatorname{rk} g_t$), then either $\operatorname{rk} f < \operatorname{rk} g_1$, contrary to the assumption that $\mathcal{A}$ is an E-characteristic set, or $rkf = \operatorname{rk} g_1$. In the last case, $t = 1$ (since no g_i, $i > 1$, is reduced with respect to f and therefore with respect to g_1) and $\operatorname{rk} \mathcal{A} = \operatorname{rk}\{f\}$, so $\{f\}$ is also an E-characteristic set of $[f]$. □

We conclude this section with an application of the results on E-characteristic sets to the problem of existence of a dimension polynomial associated with a non-reflexive prime difference polynomial ideal.

Let P be a non-reflexive prime σ-ideal of the ring of σ-polynomials $R = K\{y_1, \dots, y_n\}$ over a σ-field K ($\operatorname{Card} \sigma = m$). Then the induced translations of the factor ring R/P are not injective, so they cannot be extended to translations of the quotient field of R/P. However, one still can consider a dimension function of $\operatorname{qf}(R/P)$ defined as follows. For any $r \in \mathbb{N}$, let $R_r = K[\{\tau y_i \mid \tau \in T(r), 1 \leq i \leq n\}]$. In other words, R_r is a polynomial ring over K in indeterminates τy_i such that $\operatorname{ord} \tau \leq r$. Let $P_r = P \bigcap R_r$, and let L and L_r denote the quotient fields of the integral domains R/P and R_r/P_r respectively. If η_i denotes the canonical image of y_i in R/P, then $L = K\langle \eta_1, \dots, \eta_n \rangle$ and L_r can be identified with the subfield $K(\{\tau \eta_i \mid \tau \in T(r),\ 1 \leq i \leq n\})$ of L, so we obtain an ascending chain (L_r) of intermediate fields of the σ-field extension L/K.

Proposition 3.13 *With the above notation, suppose that a prime σ-ideal P of the ring $R = K\{y_1, \dots, y_n\}$ is generated by one irreducible σ-polynomial f, $P = [f]$. Then the numerical polynomial*

$$\phi_P(t) = n\binom{t+m}{m} - \binom{t+m-\operatorname{ord} u_f}{m} \tag{3.2}$$

has the property that $\phi_P(r) = \operatorname{tr.deg}_K L_r$ for all $r \in \mathbb{N}$.

Proof Let V denote the set of all elements $\tau \eta_i \in L$ such that $u_f \nmid \tau y_i$ ($\tau \in T$, $1 \leq i \leq n$) and for any $r \in \mathbb{N}$, let $V_r = \{\tau \eta_i \in V \mid \operatorname{ord} \tau \leq r\}$. By Corollary 3.12, $\{f\}$ is an E-characteristic set of $P = [f]$. If g is a polynomial in k variables over K and $g(v_1, \dots, v_k) = 0$ for some $v_1 = \tau_1 \eta_{i_1}, \dots, v_k = \tau_k \eta_{i_k} \in V$, then $g(\tau_1 y_{i_1}, \dots, \tau_k y_{i_k}) \in P$ and this σ-polynomial is E-reduced with respect to f. By Proposition 3.10, $g = 0$, so the set V (and therefore every set V_r, $r \in \mathbb{N}$) is algebraically independent over K. It remains to show that L_r is an algebraic extension of the field $K(V(r))$. Let us write f as a polynomial of u_f:

$$f = I_d u_f^d + \cdots + I_1 u_f + I_0$$

where $I_d \neq 0$ and every term in I_d is smaller than u_f with respect to our ordering of the set of terms TY. Furthermore, for any $\tau \in T$, $\mathcal{E}ord(\tau(I_d)) = \mathcal{E}ord(I_d) < \mathcal{E}ord(f)$ hence $\operatorname{rk} I_d < \operatorname{rk} f$. By Lemma 3.5, I_d is reduced with respect to f, and it follows from Proposition 3.10 that $\tau(I_d) \notin P$.

Since $f \in P$,

$$f(\eta) = I_d(\eta) u_f(\eta)^d + \cdots + I_1(\eta) u_f(\eta) + I_0(\eta) = 0.$$

Let $w = \tau u_f$ and $\operatorname{ord} w \leq r$ for some $r \in \mathbb{N}$. Applying τ to both sides of the last equality and taking into account that $\tau(I_d) \notin P$ (and therefore $\tau(I_d(\eta)) \neq 0$), we obtain an equality that shows that $w(\eta)$ is algebraic over the field $K(\{u(\eta) \mid u = \tau' y_i$ for some $\tau' \in T(r)$, $1 \leq i \leq n$ and $u < u_f\})$. Now the induction on the set TY with the introduced well-ordering completes the proof of the fact that L_r is an algebraic extension of $K(V(r))$.

If $u_f = \alpha_1^{k_1} \dots \alpha_m^{k_m} y_i$ ($1 \leq i \leq n$), then for any $r \in \mathbb{N}$, we have $\operatorname{Card} V(r) = \operatorname{Card} V'(r) + \operatorname{Card} V''(r)$ where

$$V'(r) = \{\alpha_1^{k_1} \dots \alpha_m^{k_m} y_j \mid k_1 + \cdots + k_m \leq r,\ j \neq i\} \text{ and } V''(r) = \{w = \tau y_i \mid \tau \in T(r), u_f \nmid w\}.$$

Applying part (iii) of Theorem 2.1 and a trivial case of Theorem 2.2 with $A = \{(k_1, \dots, k_m)\}$, we obtain

$$\operatorname{Card} V(r) = (n-1)\binom{r+m}{m} + \left[\binom{r+m}{m} - \binom{r+m-\sum_{i=1}^m k_i}{m}\right]$$

and therefore equality (3.2). □

Remark 3.14 It is easy to see that the arguments of the proof of the last proposition can be applied to any non-reflexive prime difference polynomial ideal P such that the initials of the elements of an E-characteristic set of P do not lie in the reflexive closure of P, that is, in the prime reflexive difference ideal defined as $\{h \in K\{y_1, \dots, y_n\} \mid \tau(h) \in P$ for some $\tau \in T\}$. If $\mathcal{U}$ is a class of all such prime difference ideals (in particular, it contains all linear prime difference ideals, since their initials lie in the field K), then each ideal $P \in \mathcal{U}$ has an associated dimension polynomial similar to one associated with a prime reflexive difference ideal (defined by Theorem 1.1 where the σ-field L is the difference quotient field of $K\{y_1, \dots, y_n\}/P$). It allows one to use the technique of dimension polynomials to obtain analogs of the results of [14,18] on Krull-type dimension with respect to the class $\mathcal{U}$.

Note also that the proof of Proposition 3.13 heavily uses the fact that for any $\tau \in T$, one has $\mathcal{E}ord(\tau(I_d)) = \mathcal{E}ord(I_d) < \mathcal{E}ord(f)$ and therefore $\tau(I_d) \notin P$ (we use the notation of the proof). This argument cannot be applied if one tries to use the classical notion of reduction and the corresponding notions of autoreduced and characteristic sets defined in [11, Section 3.3].

4 The Main Theorem

The following theorem is the main result of the paper.

Theorem 4.1 *Let $L = K\langle \eta_1, \dots, \eta_n \rangle$ be a σ-field extension generated by a set $\eta = \{\eta_1, \dots, \eta_n\}$. Then there exists a polynomial $\psi_{\eta|K}(t_1, t_2) \in \mathbb{Q}[t_1, t_2]$ and $r_0, s_0, s_1 \in \mathbb{N}$ with $s_1 < r_0 - s_0$ such that*

(i) $\psi_{\eta|K}(r, s) = \text{tr.deg}_K\, K(\{\tau\eta_j \mid \tau \in T(r, s), 1 \le j \le n\})$ *for all* $(r, s) \in \mathbb{N}^2$ *with* $r \ge r_0$, $s_1 \le s \le r - s_0$.

(ii) $\psi_{\eta|K}(t_1, t_2) = \psi^{(1)}_{\eta|K}(t_1) - \psi^{(2)}_{\eta|K}(t_2)$ *where* $\deg \psi^{(i)}_{\eta|K}(t) \le m$ $(i = 1, 2)$, *so* $\psi_{\eta|K}(t_1, t_2)$ *can be written as*

$$\psi_{\eta|K}(t_1, t_2) = \sum_{i=0}^{m} a_i \binom{t_1 + i}{i} - \sum_{j=0}^{m} b_j \binom{t_2 + j}{j} \tag{4.1}$$

where $a_i, b_j \in \mathbb{Z}$.

(iii) $\psi^{(1)}_{\eta|K}(r) = \phi_{\eta|K}(r)$ *for all sufficiently large* $r \in \mathbb{N}$ *and* $a_m = b_m = \sigma\text{-tr.deg}_K L$. *Furthermore,* $d = \deg_{t_1} \psi_{\eta|K}$, *and a_d are also invariants of the extension L/K, that is, they do not depend on the system of σ-generators of L/K. Finally,* $\deg \psi^{(1)}_{\eta|K} \ge \psi^{(2)}_{\eta|K}$ *and if* $\deg \psi^{(1)}_{\eta|K} = \psi^{(2)}_{\eta|K} = e < m$, *then b_e is also an invariant of the extension.*

Proof Let $P \subseteq R = K\{y_1, \dots, y_n\}$ be the defining σ-ideal of the extension L/K and let $\mathcal{A} = \{f_1, \dots, f_p\}$ be an E-characteristic set of P. Let u_i and v_i denote the leader and coleader of f_i, respectively $(1 \le i \le p)$. For any $r, s \in \mathbb{N}$ such that $s \le r$, let

$$W(r, s) = \{w \in TY \mid s \le \text{ord}\, w \le r\}, \quad W_\eta(r, s) = \{w(\eta) \mid w \in W(r, s)\},$$
$$U'(r, s) = \{u \in TY \mid s \le \text{ord}\, u \le r \quad \text{and} \quad u_i \nmid u\ (i = 1, \dots, p)\}, \quad U'_\eta(r, s) = \{u(\eta) \mid u \in U'(r, s)\},$$
$$U''(r, s) = \{u \in TY \mid s \le \text{ord}\, u \le r, \quad u \text{ is divisible by the leader of some } f_i \text{ and whenever } \quad u = \tau u_i$$
$$\text{for some } \quad \tau \in T, 1 \le i \le p, \quad \text{one has} \quad \text{ord}(\tau v_i) < s\}, \quad \text{and}$$
$$U''_\eta(r, s) = \{u(\eta) \mid u \in U''(r, s)\}.$$

Furthermore, let

$$U(r, s) = U'(r, s) \cup U''(r, s) \quad \text{and} \quad U_\eta(r, s) = U'_\eta(r, s) \cup U''_\eta(r, s).$$

We are going to show that for every $(r, s) \in \mathbb{N}^2$, $s < r$, the set $U_\eta(r, s)$ is a transcendence basis of the field $K(W_\eta(r, s))$ over K. First, notice that this set is algebraically independent over K. Indeed, if $f(w_1(\eta), \dots, w_k(\eta)) = 0$ for some elements $w_1, \dots, w_k \in U(r, s)$, then the σ-polynomial $f(w_1, \dots, w_k)$ lies in P and it is E-reduced with respect to $\mathcal{A}$. (If f contains a term $w = \tau u_i$, $1 \le i \le p$, $\tau \in T$, such that $\deg_w f \ge \deg_{u_i} f_i$, then $w \in U''(r, s)$,

so $\operatorname{ord}(\tau v_i) < s \leq \operatorname{ord} v_f$ hence $\tau v_i < v_f$. It follows that f is E-reduced with respect to $\mathcal{A}$.) By Proposition 3.10, $f = 0$, so the set $U_\eta(r, s)$ is algebraically independent over K.

Now let us prove that if $0 \leq s \leq r - s_0$, where $s_0 = \max\{\operatorname{Eord} f_i \mid 1 \leq i \leq p\}$, then every element $\tau\eta_k \in W_\eta(r, s) \setminus U_\eta(r, s)$ $(\tau \in T, 1 \leq k \leq n)$ is algebraic over the field $K(U_\eta(r, s))$. In this case $\tau y_k \notin U(r, s)$, hence τy_k is equal to some term of the form $\tau' u_i$ where $\tau' \in T$ and $\operatorname{ord}(\tau' v_i) \geq s$. Let us represent f_i as a polynomial in u_i:

$$f_i = I_{d_i}^{(i)} u_i^{d_i} + \cdots + I_1^{(i)} u_i + I_0^{(i)}$$

where $I_0^{(i)}, I_1^{(i)}, \ldots I_{d_i}^{(i)}$ do not contain u_i (therefore, all terms in these σ-polynomials are lower than u_i). Since $f_i \in P$, $f_i(\eta) = 0$, that is,

$$I_{d_i}^{(i)}(\eta)(u_i(\eta))^{d_i} + \cdots + I_1^{(i)}(\eta) u_i(\eta) + I_0^{(i)}(\eta) = 0. \tag{4.2}$$

There exists q, $0 \leq q \leq d_i$, such that $I_q^{(i)}$ contains v_i and therefore $I_q^{(i)}$ is E-reduced with respect to $\mathcal{A}$. ($I_q^{(i)}$ is obviously E-reduced with respect to f_i; if $I_q^{(i)}$ is not E-reduced with respect to some f_j with $j \neq i$, then f_i would not be E-reduced with respect to f_j, contrary to the assumption that $\mathcal{A}$ is an E-autoreduced set.) Since $I_q^{(i)} \neq 0$, Proposition 3.10 shows that $I_q^{(i)} \notin P$. Since the σ-ideal P is reflexive, $\tau(I_q^{(i)}) \notin P$ for any $\tau \in T$. (Note that if no $I_k^{(i)}$, $0 \leq k \leq d_i$, contains v_i, then $u_i = v_i$; in this case $I_{d_i}^{(i)} \in K$ and therefore $\tau(I_{d_i}^{(i)}) \notin P$ for any $\tau \in T$.)

Now, if we apply τ' to both sides of (4.2), the resulting equality will show that the element $\tau' u_i(\eta) = \tau\eta_k$ is algebraic over the field $K(\{\tilde{\tau}\eta_l \mid s \leq \operatorname{ord}\tilde{\tau} \leq r, \tilde{\tau} y_l < \tau' u_i\})$. Now, the induction on the well-ordered set of terms TY completes the proof of the fact that the set $U_\eta(r, s)$ is a transcendence basis of the field $K(W_\eta(r, s))$ over K.

In order to evaluate the size of $U_\eta(r, s)$ we are going to evaluate the sizes of the sets $U'_\eta(r, s)$ and $U''_\eta(r, s)$, that is, the sizes of the sets $U'(r, s)$ and $U''(r, s)$. For every $k = 1, \ldots, n$, let

$$A_k = \{(i_1, \ldots, i_m) \in \mathbb{N}^m \mid \alpha_1^{i_1} \ldots \alpha_m^{i_m} y_k \quad \text{is the leader of some element of} \quad \mathcal{A}\}.$$

Applying Theorem 2.1, we obtain that there exists a numerical polynomial $\omega_k(t)$ such that $\omega_k(r) = \operatorname{Card} V_{A_k}(r)$ for all sufficiently large $r \in \mathbb{N}$. It follows that if we set $\omega(t) = \sum_{k=1}^{n} \omega_k(t)$, then there exist $r_0, s_1 \in \mathbb{N}$ such that for all $r, s \in \mathbb{N}$ with $r \geq r_0$ and $s_1 \leq s \leq r - s_0$, $\operatorname{Card} U'(r, s) = \omega(r) - \omega(s)$. Furthermore, $\deg\omega \leq m$, and $\deg\omega = m$ if and only if at least one of the sets A_k $(1 \leq k \leq n)$ is empty.

In order to evaluate $\operatorname{Card} U''(r, s)$ note that this set consists of all terms τu_i $(\tau \in T, 1 \leq i \leq p)$ such that $s \leq \operatorname{ord}(\tau u_i) \leq r$ and $\operatorname{ord}(\tau v_i) < s$. For every fixed i, the number N_i of such terms is equal to $\operatorname{Card}\{\tau \in T \mid s - \operatorname{ord} u_i - 1 < \operatorname{ord}\tau \leq s - \operatorname{ord} v_i - 1\} = \binom{s - \operatorname{ord} v_i - 1 + m}{m} - \binom{s - \operatorname{ord} u_i - 1 + m}{m}$.
Applying the principle of inclusion and exclusion (taking into account terms that are multiples of more than one leader u_i), we obtain that $\operatorname{Card} U''(r, s)$ is an alternating sum of polynomials of the form $\binom{s - a + m}{m} - \binom{s - b + m}{m}$ where $a, b \in \mathbb{N}$, $a \leq b$. It follows that $\operatorname{Card} U''(r, s)$ is expressed by a numerical polynomial of s of degree at most $m - 1$. Denoting this polynomial by $\omega'(s)$ and setting $\psi_{\eta|K}^{(1)}(t_1) = \omega(t_1)$ and $\psi_{\eta|K}^{(2)}(t_2) = \omega(t_2) + \omega'(t_2)$, we obtain a numerical polynomial $\psi_{\eta|K}(t_1, t_2) = \psi_{\eta|K}^{(1)}(t_1) - \psi_{\eta|K}^{(2)}(t_2)$ that satisfies conditions (i) and (ii) of our theorem.

In order to prove the last statement of the theorem, suppose that $L = K\langle\eta_1, \ldots, \eta_n\rangle = K\langle\zeta_1, \ldots, \zeta_k\rangle$. Then there exists $q \in \mathbb{N}$ such that $\eta_i \in K(T(q)\zeta_1 \cup \cdots \cup T(q)\zeta_k)$ and $\zeta_j \in K(T(q)\eta_1 \cup \cdots \cup T(q)\eta_n)$ $(1 \leq i \leq n, 1 \leq j \leq k)$. It follows that for all sufficiently large $r, s \in \mathbb{N}$ with $s_1 \leq s \leq r - s_0$, one has

$$\psi_{\eta|K}(r, s) \leq \psi_{\zeta|K}(r + q, s) \quad \text{and} \quad \psi_{\zeta|K}(r, s) \leq \psi_{\eta|K}(r + q, s). \tag{4.3}$$

Furthermore, the proof of the first part of the theorem shows that $\psi_{\eta|K}^{(1)}(t_1) = \phi_{\eta|K}(t_1)$ (the univariate σ-dimension polynomial of L/K associated with the set of σ-generators η) and similarly $\psi_{\zeta|K}^{(1)}(t_1) = \phi_{\zeta|K}(t_1)$. It follows from Theorem 1.1 that the coefficients of t_1^m in the polynomials $\psi_{\eta|K}$ and $\psi_{\zeta|K}$ are equal to $\sigma\text{-tr.deg}_K L$, $\deg_{t_1}\psi_{\eta|K} = \deg_{t_1}\psi_{\zeta|K}$, and if this common degree is denoted by d, then $\psi_{\zeta|K}$ and $\psi_{\zeta|K}$ have the same coefficient a_d before $\binom{t_1 + d}{d}$ in the representation (4.1).

If $\deg \psi^{(1)}_{\eta|K} < \deg \psi^{(2)}_{\eta|K}$, then setting $s = r - s_0$ we would have $\psi_{\eta|K}(r, r - s_0) < 0$ for sufficiently large r, a contradiction. Therefore, $\deg \psi^{(1)}_{\eta|K} \geq \deg \psi^{(2)}_{\eta|K}$.

The evaluation of Card $U''(r, s)$ in the proof of the first part of the theorem shows that this number is expressed by a polynomial of s of degree at most $m - 1$. Suppose that $\deg \psi^{(1)}_{\eta|K} = \psi^{(2)}_{\eta|K} = e < m$. Then setting $t_1 = r$ and $t_2 = r - s_0$ in the representations of the form (4.1) for $\psi_{\eta|K}(t_1, t_2)$ and $\psi_{\zeta|K}(t_1, t_2)$ and using (4.3), we obtain that the coefficient of r^e in the resulting polynomials of r are the same, $a_e - b_e$. Since a_e is an invariant of the extension L/K, so is b_e. □

As it follows from the proof of the last theorem, the computation of the bivariate dimension polynomial $\psi_{\eta|K}(t_1, t_2)$ can be reduced to the computation of the numbers of elements of the sets $U'(r, s)$ and $U''(r, s)$ where $r, s \in \mathbb{N}$, $s < r$. It is shown above that Card $U''(r, s)$ depends only on s and it is a certain alternating sum of binomial coefficients of the form $\binom{s-a-1+m}{m}$ where the values of a are the orders of the leaders and coleaders of elements the E-characteristic set $\mathcal{A}$ of the defining σ-ideal of the extension L/K. Thus, the main problem in obtaining $\psi_{\eta|K}(t_1, t_2)$ is the computation of the numerical polynomial that expresses Card $U'(r, s)$ for all sufficiently large $r, s \in \mathbb{N}$ $(s < r)$ satisfying the conditions of the theorem. As it is shown in the proof, Card $U'(r, s) = \omega(r) - \omega(s)$ where $\omega(t)$ is the sum of the Kolchin polynomials of the sets $A_k = \{(i_1, \ldots, i_m) \in \mathbb{N}^m \mid \alpha_1^{i_1} \ldots \alpha_m^{i_m} y_k$ is the leader of some element of $\mathcal{A}\}$ $(k = 1, \ldots, n)$. Algorithms for computing Kolchin polynomials and their complexity evaluation can be found in [11, Section 2.3].

Example Let K be a difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$. Let $L = K\langle\eta\rangle$ be a σ-field extension of k with the defining equation

$$\alpha_1^a \alpha_2^b \eta + \alpha_1^b \eta + \alpha_2^a \eta = 0, \tag{4.4}$$

where a and b are positive integers, $a \leq b$. Since every linear difference ideal in the ring of σ-polynomials $K\{y\}$ is prime (see [15, Proposition 2.4.9]), the difference ideal $P = [f]$, where $f = \alpha_1^a \alpha_2^b y + \alpha_1^b y + \alpha_2^a y$, is the defining ideal of the extension L/K. It follows from Corollary 3.12 that $\{f\}$ is a characteristic set of P. With the notation of the proof of Theorem 4.1, we have $u_f = \alpha_1^a \alpha_2^b y$, $v_f = \alpha_2^a y$, Eord $f = (a + b) - a = b$, and $\mathcal{E}ord(f) = (b, a, b - a)$. Furthermore, if s is sufficiently large and $s \leq r - b$, then

$$U'(r, s) = \{\alpha_1^i \alpha_2^j y \in TY \mid s \leq i + j \leq r \quad \text{and} \quad (a, b) \not\leq_P (i, j)\}.$$

In this case,

$$\begin{aligned}\text{Card } U'(r, s) &= \left[\binom{r+2}{2} - \binom{r+2-(a+b)}{2}\right] - \left[\binom{(s-1)+2}{2} - \binom{(s-1)+2-(a+b)}{2}\right] \\ &= (a + b)r - (a + b)s + (a + b).\end{aligned}$$

Now,

$$\text{Card } U''(r, s) = \text{Card}\{\alpha_1^{k_1} \alpha_1^{k_2} (\alpha_1^a \alpha_2^b y) \mid k_1 + k_2 + a + b \geq s \quad \text{and} \quad k_1 + k_2 + a < s\} =$$

$$\text{Card}\{(k_1, k_2) \in \mathbb{N}^2 \mid s - (a + b) \leq k_1 + k_2 < s - a\} = \binom{s-(a+1)+2}{2} - \binom{s-(a+b+1)+2}{2} =$$

$$bs - \frac{b(2a + b - 1)}{2}. \quad \text{Thus,}$$

$$\text{Card } U(r, s) = \text{Card } U'(r, s) + \text{Card } U''(r, s) = (a + b)r - (a - 1)s - \frac{b^2 + 2ab - 3b - 2a}{2},$$

so we get the following expression for the bivariate dimension polynomial associated with the extension L/K.

$$\psi_{\eta|K}(t_1, t_2) = (a + b)t_1 - at_2 - \frac{b^2 + 2ab - 3b - 2a}{2}.$$

Note that the univariate σ-dimension polynomial $\phi_{\eta|K}(t)$ of the extension L/K associated with the σ-generator η (which is equal to the Kolchin polynomial of the set $\{(a, b)\} \subset \mathbb{N}^2$) is as follows.

$$\phi_{\eta|K}(t) = \binom{t+2}{2} - \binom{t+2-(a+b)}{2} = (a+b)t - \frac{(a+b)(a+b-3)}{2}.$$

Comparing bivariate and univariate dimension polynomials with the use of Theorems 1.1 and 4.1, we see that $\phi_{\eta|K}(t)$ carries two invariants of the extension L/K, $\deg \phi_{\eta|K} = 1$ and the leading coefficient $a + b$. At the same time, the bivariate dimension polynomial $\psi_{\eta|K}(t_1, t_2)$ carries three such invariants: $\deg_{t_1} \psi_{\eta|K} = 1$, $a + b$ (the coefficient of t_1), and $-a$ (the coefficient of t_2). Thus, $\psi_{\eta|K}(t_1, t_2)$ gives both parameters a and b of the defining Eq. (4.4) while $\phi_{\eta|K}(t)$ gives just the sum of the parameters.

Suppose that we have two systems of difference (σ-) algebraic equations in n σ-indeterminates over a σ-field K (i. e., equations of the form $f = 0$ where $f \in K\{y_1, \dots, y_n\}$) that are defining equations of finitely generated σ-field extensions L/K and L'/K (it means that they generate prime σ-ideals P and P' of the ring $R = K\{y_1, \dots, y_n\}$, respectively, such that L and L' are σ-isomorphic to $\mathrm{qf}(R/P)$ and $\mathrm{qf}(R/P')$, respectively). These systems are said to be *equivalent* if there is a σ-isomorphism between L and L' which is identity on K. The obtained bivariate σ-dimension polynomial allows one to figure out that two systems of σ-algebraic equations are not equivalent in the case when the corresponding σ-field extensions have the same univariate σ-dimension polynomial. As an example, consider the equations

$$\alpha_1^a \alpha_2^b y + \alpha_1^b y + \alpha_2^a y = 0 \tag{4.5}$$

and

$$\alpha_1^a \alpha_2^b y + \alpha_1^a y + y = 0. \tag{4.6}$$

The invariants of the univariate and bivariate σ-dimension polynomials for equation (4.5) were found in the last example; they are $\{1, a+b\}$ and $\{1, a, b\}$, respectively. Similar computation for the extension with defining equation (4.6) gives (with the above notation)

$$\mathrm{Card}\, U'(r, s) = (a+b)r - (a+b)s + (a+b)$$

(the same as the corresponding value for (4.5)) and

$$\mathrm{Card}\, U''(r, s) = (a+b)s - \frac{(a+b)(a+b-1)}{2},$$

so the univariate and bivariate dimension σ-polynomials for the equation (4.6) are

$$\phi(t) = (a+b)t - \frac{(a+b)(a+b-3)}{2} \quad \text{and} \quad \psi(t_1, t_2) = (a+b)t_1 - \frac{(a+b)(a+b-1)}{2},$$

respectively. Therefore, the invariants of the univariate and bivariate σ-dimension polynomials for equation (4.3) are $\{1, a+b\}$ and $\{1, a+b, 0\}$, respectively. Thus, the systems (4.5) and (4.6) are not equivalent, even though the corresponding σ-field extensions have the same univariate σ-dimension polynomial.

References

1. Blinkov, Y.A., Gerdt, V., Lyakhov, D.A., Michels, D.L.: On the consistency analysis of finite difference approximations. J. Math. Sci. **240**(5), 665–677 (2019)
2. Cohn, R.M.: Difference Algebra. Interscience, New York (1965)
3. Einstein, A.: The Meaning of Relativity. Appendix II (Generalization of Gravitation Theory), 4th edn., Princeton, pp. 133–165
4. Gerdt, V., Blinkov, Y., Mozzhilkin, V.: Gröbner Bases and Generation of Difference Schemes for Partial Differential Equations. Symmetry, Integrability and Geometry: Methods and Applications, vol. 2, paper 051, 26 pp (2006)
5. Gerdt, V., Robertz, D.: Consistency of finite difference approximations for linear PDE systems and its algorithmic verification. In: Proceedings of ISSAC 2010. ACM Press, New York, pp. 53–59 (2010)
6. Gerdt, V., Robertz, D.: Computation of difference Gröbner bases. Comput. Sci. J. Moldova **20**(2), 203–226 (2012)

7. Gerdt, V., Robertz, D.: Algorithmic approach to strong consistency analysis of finite difference approximations to PDE systems. In: Proceedings of ISSAC 2019, ACM Press, New York, pp. 163–170 (2019)
8. Hrushovski, E.: The Elementary Theory of the Frobenius Automorphisms. arXiv:math/0406514v1, 2004, pp. 1–135. The updated version (2012). www.ma.huji.ac.il/ehud/FROB.pdf
9. Kolchin, E.R.: The notion of dimension in the theory of algebraic differential equations. Bull Am. Math. Soc. **70**, 570–573 (1964)
10. Kolchin, E.R.: Differential Algebra and Algebraic Groups. Acad Press, New York (1973)
11. Kondrateva, M.V., Levin, A.B., Mikhalev, A.V., Pankratev, E.V.: Differential and Difference Dimension Polynomials, Kluwer Acad. Publ. (1998)
12. Levin, A.B.: Characteristic polynomials of filtered difference modules and of difference field extensions. Russ. Math. Surv. **33**(3), 165–166 (1978)
13. Levin, A.B.: Characteristic polynomials of inversive difference modules and some properties of inversive difference dimension. Russ. Math. Surv. **35**(1), 217–218 (1980)
14. Levin, A.B.: Type and dimension of inversive difference vector spaces and difference algebras. VINITI (Moscow, Russia) **1606–82**, 1–36 (1982)
15. Levin, A.B.: Difference Algebra. Springer, New York (2008)
16. Levin, A.: Bivariate dimension polynomials of non-reflexive prime difference-differential ideals. The case of one translation. In: Proceedings of ISSAC 2018. ACM Press, New York, pp. 255–262 (2018)
17. Levin, A.: Bivariate Kolchin-type dimension polynomials of non-reflexive prime difference-differential ideals: the case of one translation. J. Symb. Comput. **102**, 173–188 (2021)
18. Levin, A.B., Mikhalev, A.V.: Type and dimension of finitely generated G-algebras. Contemp. Math. **184**, 275–280 (1995)
19. Mikhalev, A.V., Pankratev, E.V.: Differential dimension polynomial of a system of differential equations. In: Algebra (collection of papers), Moscow State Univ. Press, pp. 57–67 (1980)
20. Wibmer, M.: Algebraic Difference Equations. Lecture Notes, University of Pennsylvania. http://www.mmrc.iss.ac.cn/mm2015/notes/wibmer1.pdf