



Generalized characteristic sets and new multivariate difference dimension polynomials

Alexander Levin¹

Received: 31 December 2022 / Revised: 19 August 2023 / Accepted: 19 August 2023 /
Published online: 28 October 2023

© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2023

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 and a partition of the basic set of translations σ . Using properties of these characteristic sets, we prove the existence and outline a method of computation of a multivariate 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 with respect to the components of the partition of σ are bounded by two sequences of natural numbers. We show that such dimension polynomials carry essentially more invariants (that is, characteristics of the extension that do not depend on the set of its difference generators) than previously known difference dimension polynomials. In particular, a dimension polynomial of the new type associated with a system of algebraic difference equations gives more information about the system than the classical univariate difference dimension polynomial.

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

1 Introduction

Hilbert-type dimension polynomials of difference field extensions, difference modules and prime difference ideals play the same role in difference algebra as Hilbert and Hilbert-Samuel polynomials play in commutative algebra and algebraic geometry. In particular, a system of algebraic difference equations can be characterized by its associated difference dimension polynomials; these polynomials are of primary

✉ Alexander Levin
levin@cua.edu

¹ Department of Mathematics, The Catholic University of America, 620 Michigan Avenue, Washington, DC 20064, USA

importance for the problem of equivalence of such systems and for the comparative analysis of systems of algebraic difference equations arisen from systems of PDEs. Univariate difference dimension polynomials introduced in [6] and [7] characterize difference modules and difference field extensions in the same way as Hilbert polynomials characterize the corresponding structures in commutative algebra and algebraic geometry. A similar concept of differential dimension polynomial introduced in [3] plays an important role in the study of finitely generated differential field extensions, differential modules and algebras. An important property of dimension polynomials is the fact that they carry certain invariants of the corresponding difference or differential algebraic structure, that is, elements which do not depend on the choice of the system of its generators. The above mentioned results were generalized to the case of an arbitrary partition of the basic set of operators (derivations or/and translations) and the corresponding multivariate filtrations of difference (as well as differential) modules and field extensions, see [10, 11], and [12]. It was shown that multivariate dimension polynomials whose existence was proved in these papers carry more invariants of the corresponding difference or differential algebraic structures than their univariate counterparts. The following theorem proved in [9, Section 4.2] presents a multivariate dimension polynomial of a finitely generated difference field extension associated with a partition of the basic set of translations.

Theorem 1.1 *Let K be a difference field of characteristic zero with a basic set $\sigma = \{\alpha_1, \dots, \alpha_m\}$, that is, a field considered together with the action of elements σ as mutually commuting endomorphisms of the field (they are called translations). Let T be the free commutative semigroup generated by σ and let a partition of the set σ into a disjoint union of its subsets be fixed:*

$$\sigma = \sigma_1 \cup \dots \cup \sigma_p \quad (1.1)$$

where $p \in \mathbb{N}$. Let $\text{Card } \sigma_i = m_i$ and for any $\tau = \alpha_1^{k_1} \dots \alpha_m^{k_m} \in T$, let $N_i = \{j \mid \alpha_j \in \sigma_i\}$ and $\text{ord}_i \tau = \sum_{j \in N_i} k_j$ ($1 \leq i \leq p$). Furthermore, let $T(r_1, \dots, r_p) = \{\tau \in T \mid \text{ord}_1 \tau \leq r_1, \dots, \text{ord}_p \tau \leq r_p\}$ for any $r_1, \dots, r_p \in \mathbb{N}$.

Let $L = K\langle \eta_1, \dots, \eta_s \rangle$ be a difference (with respect to σ) field extension of K generated by a finite set $\eta = \{\eta_1, \dots, \eta_n\}$. (As a field, $L = K(\{\tau(\eta_i) \mid \tau \in T, 1 \leq i \leq n\})$.) Then there exists a polynomial $\chi_{\eta|K}(t_1, \dots, t_p)$ in p variables with rational coefficients such that

(i) $\chi_{\eta|K}(r_1, \dots, r_p) = \text{trdeg}_K K(\{\tau\eta_j \mid \tau \in T(r_1, \dots, r_p), 1 \leq j \leq n\})$ for all sufficiently large $(r_1, \dots, r_p) \in \mathbb{N}^p$ (that is, there exist $r_1^{(0)}, \dots, r_p^{(0)} \in \mathbb{N}$ such that the equality holds for all $(r_1, \dots, r_p)$ with $r_i \geq r_i^{(0)}, 1 \leq i \leq p$).

(ii) $\deg_{t_i} \chi_{\eta|K} \leq m_i$ and the polynomial $\chi_{\eta|K}(t_1, \dots, t_p)$ can be represented as

$$\chi_{\eta|K}(t_1, \dots, t_p) = \sum_{i_1=0}^{m_1} \dots \sum_{i_p=0}^{m_p} a_{i_1 \dots i_p} \binom{t_1 + i_1}{i_1} \dots \binom{t_p + i_p}{i_p}$$

where $a_{i_1 \dots i_p} \in \mathbb{Z}$ for all $i_1, \dots, i_p$.

(iii) For any permutation $(j_1, \dots, j_p)$ of the set $\{1, \dots, p\}$, let $<_{j_1, \dots, j_p}$ denote the lexicographic order on $\mathbb{N}^p$ such that $(r_1, \dots, r_p) <_{j_1, \dots, j_p} (s_1, \dots, s_p)$ if and only if either $r_{j_1} < s_{j_1}$ or there exists $k \in \mathbb{N}$, $1 < k \leq p$, such that $r_{j_v} = s_{j_v}$ for $v = 1, \dots, k-1$ and $r_{j_k} < s_{j_k}$. Let $E_{\eta|K} = \{(i_1, \dots, i_p) \in \mathbb{N}^p \mid 0 \leq i_k \leq m_k \text{ for } k = 1, \dots, p \text{ and } a_{i_1 \dots i_p} \neq 0\}$ and let $E'_{\eta|K}$ denote the set of all $e \in E_{\eta|K}$ that are maximal elements of $E_{\eta|K}$ with respect to one of the $p!$ orders $<_{j_1, \dots, j_p}$. Then $d = \deg \chi_{\eta|K}$, $a_{m_1 \dots m_p}$, p -tuples $(j_1, \dots, j_p) \in E'_{\eta|K}$, the corresponding coefficients $a_{j_1 \dots j_p}$, and the coefficients of the terms of total degree d do not depend on the choice of the system of σ -generators η of L over K . Furthermore, $a_{m_1 \dots m_p} = \sigma\text{-tr.deg}_K L$ where $\sigma\text{-tr.deg}_K L$ denoted the maximal number of elements $\xi_1, \dots, \xi_k \in L$ such that the set $\{\tau \xi_i \mid \tau \in T, 1 \leq i \leq k\}$ is algebraically independent over K .

The polynomial $\chi_{\eta|K}$ is called the σ -dimension polynomial of L/K associated with the set of σ -generators $\eta = \{\eta_1, \dots, \eta_n\}$ and partition (1.1). (If $p = 1$, the last theorem gives a “standard” univariate difference dimension polynomial introduced in [6].) Theorem 1.1 allows one to assign dimension polynomials to prime difference ideals of finitely generated difference algebras over difference fields (these are dimension polynomials of the quotient fields of the corresponding factor rings). Using properties of difference dimension polynomials, one can efficiently study Krull-type dimension of difference rings, local difference algebras, and extensions of difference fields (see, for example, [5, Chapter 7], [9, Chapter 4], and [15]). Furthermore, as it is shown in [16] and [9, 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 [2]. (See [9, Section 7.7] for the description of the relationship between difference dimension polynomials and Einstein’s strength of systems of equations in finite differences. The discussion of this relationship in the multivariate case associated with a fixed partition of the set of translations can be found in [8].)

In this paper we introduce a reduction of difference polynomials associated with a fixed partition of the set of basic translations. This reduction takes into account the effective orders of difference polynomials with respect to the elements of the partition (we generalize the concept of the effective order of an ordinary difference polynomial defined in [1, Chapter 2, Section 4]). We consider a new type of characteristic sets that are associated with this reduction and use their properties to prove the existence of a multivariate 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 with respect to the elements of the given partitions lie between two given natural numbers. This dimension polynomial is a polynomial in $2p$ variables where p is the number of subsets in the partition of the basic set of translations. We determine invariants of such polynomials, that is, numerical characteristics of the extension that are carried by any its dimension polynomial and that do not depend on the system of difference generators the polynomial is associated with. Furthermore, we show (see Examples 2 and 3 in section 4) that the introduced multivariate difference dimension polynomials carry essentially more invariants of the corresponding difference field extensions than any previously known difference dimension polynomials, including such polynomials defined in Theorem 1.1 and bivariate difference dimension polynomials introduced in [13] (the corresponding bivariate difference dimension polynomials for finitely generated difference modules are defined in [14]). Given a finitely generated difference field extension, the latter dimension polynomial describes the transcendence degrees of intermediate fields obtained by adjoining transforms of the generators whose (total) orders lie between two natural numbers. By considering a partition of the basic set of translations, generalizing the concept of effective order of a difference polynomial and developing the corresponding method of characteristic sets, we obtain much stronger results than those of [13]. The fact that the multivariate difference dimension polynomial introduced in this paper carries extra invariants of the corresponding difference field extension allows one to apply our results to the equivalence problem for systems of algebraic difference equations. At the end of section 4, we give an example where we use the introduced dimension polynomials to show that two algebraic difference equations are not equivalent even though their invariants carried by the associated univariate and bivariate dimension polynomials defined in [13] coincide.

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. For any positive integer m , $\leq_p$ will denote the product order on $\mathbb{N}^m$, that is, a partial order such that $(a_1, \dots, a_m) \leq_p (a'_1, \dots, a'_m)$ if and only if $a_i \leq a'_i$ for $i = 1, \dots, m$.

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. $\mathbb{Q}[t_1, \dots, t_p]$ will denote the ring of polynomials in variables $t_1, \dots, t_p$ over $\mathbb{Q}$.

By a *difference ring* we mean a commutative ring R considered together with a finite set $\sigma = \{\alpha_1, \dots, \alpha_m\}$ of mutually commuting injective endomorphisms of R called *translations*. 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. (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 $\tau = \alpha_1^{k_1} \dots \alpha_m^{k_m}$ ($k_i \in \mathbb{N}$). Furthermore, we fix representation (1.1) of the set σ as the union of p disjoint subsets $\sigma_1, \dots, \sigma_p$ ($p \geq 1$): where

$$\sigma_1 = \{\alpha_1, \dots, \alpha_{m_1}\}, \dots, \sigma_p = \{\alpha_{m_1+\dots+m_{p-1}+1}, \dots, \alpha_m\}$$

($m_1 + \dots + m_p = m$). If $\tau = \alpha_1^{k_1} \dots \alpha_m^{k_m} \in T$ ($k_i \in \mathbb{N}$), then the *order* of τ with respect to a set σ_i ($1 \leq i \leq p$) is defined as $\sum_{v=m_1+\dots+m_{i-1}+1}^{m_1+\dots+m_i} k_v$; it is denoted by $\text{ord}_i \tau$. (If $i = 1$, the last sum is replaced by $k_1 + \dots + k_{m_1}$.) If $r_1, \dots, r_p \in \mathbb{N}$, we set

$$T(r_1, \dots, r_p) = \{\tau \in T \mid \text{ord}_i \tau \leq r_i \text{ for } i = 1, \dots, p\}.$$

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 $\alpha_i \in \sigma$ to R_0 is denoted by the same symbol α_i . 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, $S = \{\eta_1, \dots, \eta_n\}$, then we say that L is a finitely generated σ -field extension of K with the set of σ -generators $\{\eta_1, \dots, \eta_n\}$ and write $L = K\langle \eta_1, \dots, \eta_n \rangle$. Clearly, this field 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, $F = \{f_1, \dots, f_k\}$, we say that the σ -ideal $I = [F]$ is finitely generated, write $I = [f_1, \dots, f_k]$ 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 $a \in I$).

If R is a σ -ring, then an expression of the form $\sum_{\tau \in T} a_\tau \tau$, where $a_\tau \in R$ for any $\tau \in T$ and only finitely many elements a_τ are different from 0, is called a σ -operator over R . It is an endomorphism of the additive group of R ; if $C = \sum_{\tau \in T} a_\tau \tau$ and $f \in R$, then $C(f) = \sum_{\tau \in T} a_\tau \tau(f)$. Two σ -operators $\sum_{\tau \in T} a_\tau \tau$ and $\sum_{\tau \in T} b_\tau \tau$ are considered to be equal if and only if $a_\tau = b_\tau$ for any $\tau \in T$. The set of all σ -operators over R will be denoted by $\mathfrak{D}_R$. This set, which has a natural structure of an R -module generated by T , becomes a ring if one sets $\tau a = \tau(a)\tau$ for any $a \in R, \tau \in T$ and extends this rule to the multiplication of any two σ -operators by distributivity. The resulting ring $\mathfrak{D}_R$ is called the ring of σ -operators over R . Clearly, if I is a σ -ideal of R , $I = [f_1, \dots, f_k]$, then every element of I is of the form $\sum_{i=1}^q C_i(f_i)$ ($q \in \mathbb{N}$) where $C_1, \dots, C_q \in \mathfrak{D}_R$.

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). A ring homomorphism $\phi : R \rightarrow S$ is called a *difference* (or σ -) *homomorphism* if $\phi(\alpha a) = \alpha \phi(a)$ for any $\alpha \in \sigma$, $a \in R$. The notions of σ -epimorphism, σ -monomorphism and σ -isomorphism are defined accordingly.

If K is a difference (σ -) field and $Y = \{y_1, \dots, y_n\}$ is a finite set of symbols, then one can consider a countable set of symbols $TY = \{\tau y_j \mid \tau \in T, 1 \leq j \leq n\}$ and the polynomial ring $R = K[\{\tau y_j \mid \tau \in T, 1 \leq j \leq n\}]$ 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 $\tau, \tau' \in T$, $1 \leq j \leq n$, 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 $y_1, \dots, y_n$ over K . This ring is denoted by $K\{y_1, \dots, y_n\}$ and its elements are called difference (or σ -) polynomials. A σ -polynomial is called linear if it is linear as a polynomial in the variables τy_i ($\tau \in T$, $1 \leq i \leq n$).

If $f \in K\{y_1, \dots, y_n\}$ and $\eta = (\eta_1, \dots, \eta_n)$ is an n -dimensional vector with coordinates in some σ -overfield of K , then $f(\eta)$ (or $f(\eta_1, \dots, \eta_n)$) 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 $\pi : R = K\{y_1, \dots, y_n\} \rightarrow L = K\langle \eta_1, \dots, \eta_n \rangle$ is a natural σ -homomorphism ($\pi(a) = a$ for any $a \in K$ and $y_i \mapsto \eta_i$), then $P = \text{Ker } \pi$ 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 $\text{qf}(R/P)$, the quotient field of R/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 $K(B)$ (it means that the set $\{\tau a \mid \tau \in T\}$ is algebraically dependent over the field $K(B)$). 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 [9, 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 $\sigma\text{-tr.deg}_K L$.

Multivariate 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 membership $f(r_1, \dots, r_p) \in \mathbb{Z}$ holds for all $(r_1, \dots, r_p) \in \mathbb{N}^p$ with $r_1 \geq s_1, \dots, r_p \geq s_p$).

It is clear that every polynomial with integer coefficients is numerical. As an example of a numerical polynomial in p variables with non-integer coefficients ($p \in \mathbb{N}, p \geq 1$) one can consider a polynomial $\prod_{i=1}^p \binom{t_i}{m_i}$ where $m_1, \dots, m_p \in \mathbb{N}$. (As usual, $\binom{t}{k}$ ($k \in \mathbb{Z}, k \geq 1$) denotes the polynomial $\frac{t(t-1)\dots(t-k+1)}{k!}$ in one variable t , $\binom{t}{0} = 1$, and $\binom{t}{k} = 0$ if k is a negative integer.) The following theorem proved in [5, Chapter 2] gives the "canonical" representation of a numerical polynomial in several variables.

Theorem 2.1 *Let $f(t_1, \dots, t_p)$ be a numerical polynomial in p variables $t_1, \dots, t_p$, and let $\deg_{t_i} f = m_i$ ($1 \leq i \leq p$) where $m_1, \dots, m_p \in \mathbb{N}$. Then the polynomial $f(t_1, \dots, t_p)$ can be represented in the form*

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

with integer coefficients $a_{i_1 \dots i_p}$ ($0 \leq i_k \leq m_k$ for $k = 1, \dots, p$) that are uniquely defined by the numerical polynomial.

In what follows (until the end of the section), we deal with subsets of the set $\mathbb{N}^m$ (m is a positive integer). Furthermore, we fix a partition of the set $\mathbb{N}_m = \{1, \dots, m\}$ into p disjoint subsets ($p \geq 1$):

$$\mathbb{N}_m = \Delta_1 \cup \Delta_2 \cup \dots \cup \Delta_p \quad (2.2)$$

where $\Delta_1 = \{1, \dots, m_1\}$, $\Delta_2 = \{m_1 + 1, \dots, m_1 + m_2\}$, $\dots$, $\Delta_p = \{m_1 + \dots + m_{p-1} + 1, \dots, m\}$ ($m_i = \text{Card } \Delta_i$ for $i = 1, \dots, p$; $m_1 + \dots + m_p = m$).

If $a = (a_1, \dots, a_m) \in \mathbb{N}^m$, we denote the numbers $\sum_{i=1}^{m_1} a_i$, $\sum_{i=m_1+1}^{m_1+m_2} a_i$, $\dots$, $\sum_{i=m_1+\dots+m_{p-1}+1}^m a_i$, by $\text{ord}_1 a$, $\dots$, $\text{ord}_p a$, respectively.

In what follows, if A is a subset of $\mathbb{N}^m$, 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 $r_1, \dots, r_p \in \mathbb{N}$, we set $A(r_1, \dots, r_p) = \{a \in A \mid \text{ord}_i a \leq r_i \text{ for } i = 1, \dots, p\}$.

The following theorem proved in [5, Chapter 2] generalizes the well-known Kolchin's result on the univariate numerical polynomial associated with a subset of $\mathbb{N}^m$ (see [4, Chapter 0, Lemma 17]).

Theorem 2.2 *Let A be a subset of $\mathbb{N}^m$ and let partition (2.2) of $\mathbb{N}_m$ be fixed ($m = m_1 + \dots + m_p$ for some nonnegative integers $m_1, \dots, m_p$, $p \geq 1$). Then there exists a numerical polynomial $\omega_A(t_1, \dots, t_p)$ with the following properties:*

(i) $\omega_A(r_1, \dots, r_p) = \text{Card } V_A(r_1, \dots, r_p)$ for all sufficiently large p -tuples $(r_1, \dots, r_p) \in \mathbb{N}^p$.

(ii) The total degree of the polynomial ω_A does not exceed m and $\deg_{t_i} \omega_A \leq m_i$ for all $i = 1, \dots, p$.

(iii) $\deg \omega_A = m$ if and only if $A = \emptyset$. Then $\omega_A(t_1, \dots, t_p) = \prod_{i=1}^p \binom{t_i + m_i}{m_i}$.

(iv) ω_A is a zero polynomial if and only if $(0, \dots, 0) \in A$.

The polynomial $\omega_A(t_1, \dots, t_p)$ is called the *dimension polynomial* of the set $A \subseteq \mathbb{N}^m$ associated with the given partition of $\mathbb{N}_m$. If $p = 1$, the corresponding univariate numerical polynomial $\omega_A(t)$ is called the *Kolchin polynomial* of A .

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 [4, 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 [5, Chapter 2] gives an explicit formula for the dimension polynomial of a finite subset of $\mathbb{N}^m$ associated with a partition of $\mathbb{N}_m$ into the union of p disjoint subsets.

Theorem 2.3 Let $A = \{a_1, \dots, a_n\}$ be a finite subset of $\mathbb{N}^m$, where n is a positive integer, and let partition (2.2) of $\mathbb{N}_m$ be fixed ($m = m_1 + \dots + m_p$ for some nonnegative integers $m_1, \dots, m_p$, $p \geq 1$). Let $a_i = (a_{i1}, \dots, a_{im})$ ($1 \leq i \leq n$) and for any $l \in \mathbb{N}$, $0 \leq l \leq n$, let $\Gamma(l, n)$ denote the set of all l -element subsets of $\mathbb{N}_n$. Furthermore, for any $\sigma \in \Gamma(l, n)$, let $\bar{a}_{\sigma j} = \max\{a_{ij} \mid i \in \sigma\}$ ($1 \leq j \leq m$) and $b_{\sigma j} = \sum_{h \in \Delta_j} \bar{a}_{\sigma h}$ ($j = 1, \dots, p$). Then

$$\omega_A(t_1, \dots, t_p) = \sum_{l=0}^n (-1)^l \sum_{\sigma \in \Gamma(l, n)} \prod_{j=1}^p \binom{t_j + m_j - b_{\sigma j}}{m_j}. \quad (2.3)$$

Remark 2.1 It is well known (see for example [5, Chapter 2]) that the number of solutions $(x_1, \dots, x_m) \in \mathbb{N}^m$ of the inequality $x_1 + \dots + x_m \leq r$ ($r \in \mathbb{N}$) is $\binom{r+m}{m}$. It follows that if $r_1, \dots, r_p, s_1, \dots, s_p \in \mathbb{N}$, $s_i < r_i$ ($1 \leq i \leq p$), and $A = \{a = (a_1, \dots, a_m) \in \mathbb{N}^m \mid s_i \leq a_i \leq r_i \text{ for } i = 1, \dots, p\}$, then

$$\text{Card } A = \prod_{i=1}^p \left[\binom{r_i + m_i}{m_i} - \binom{s_i + m_i - 1}{m_i} \right]$$

(as before we consider partition (2.2) of $\mathbb{N}_m$). We will use this observation in the proof of Theorem 4.1.

3 Relative effective orders and E -reduction

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_m\}$ and $R = K\{y_1, \dots, y_n\}$ the algebra of difference polynomials in σ -indeterminates $y_1, \dots, y_n$ over K . Then R can be viewed as a polynomial ring in the set of indeterminates $TY = \{\tau y_i \mid \tau \in T, 1 \leq i \leq n\}$ whose elements are called *terms*. As before, we fix partition (1.1) of the set σ and for every $j = 1, \dots, p$, define the order of a term $u = \tau y_i$ with respect to σ_j (denoted by $\text{ord}_j u$) as the corresponding order of τ (that is, $\text{ord}_j(\tau y_i) = \text{ord}_j \tau$ for any $i = 1, \dots, n, \tau \in T$). As usual, if $\tau, \tau' \in T$, we say that τ divides τ' (and write $\tau \mid \tau'$) if $\tau' = \tau \tau''$ for some element $\tau'' \in T$ denoted by $\frac{\tau'}{\tau}$. If $u = \tau y_i$ and $v = \tau' y_j$ are two terms in TY , we say that u divides v (and write $u \mid v$) if $i = j$ and $\tau \mid \tau'$. In this case we also say that v is a *transform* of u and define the ratio $\frac{v}{u}$ as $\frac{\tau'}{\tau}$.

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 $\tau \in T$.

If $\leq$ is a ranking on R and $f \in R$, then the greatest and smallest (with respect to $<$) terms in f are called the *leader* and *coleader* of f with respect to the ranking $\leq$.

Let us consider p total orderings $<_1, \dots, <_p$ of the set of power products T such that if $\tau = \alpha_1^{k_1} \dots \alpha_m^{k_m}, \tau' = \alpha_1^{l_1} \dots \alpha_m^{l_m} \in T$, then for any $i = 1, \dots, p$, $\tau <_i \tau'$ if and only if

$(\text{ord}_i \tau, \text{ord}_1 \tau, \dots, \text{ord}_{i-1} \tau, \text{ord}_{i+1} \tau, \dots, \text{ord}_p \tau, k_{m_1+\dots+m_{i-1}+1}, \dots, k_{m_1+\dots+m_i}, k_1, \dots, k_{m_1+\dots+m_{i-1}}, k_{m_1+\dots+m_{i+1}}, \dots, k_m)$ is less than the corresponding $(m+p)$ -tuple for τ' with respect to the lexicographic order on $\mathbb{N}^{m+p}$. Furthermore, we consider p orders $<_1, \dots, <_p$ on the set of terms TY that correspond to the introduced orders on T . They are defined as follows: $\tau y_j <_i \tau' y_k$ if and only if $\tau <_i \tau'$ in T or $\tau = \tau'$ and $j < k$ ($1 \leq i \leq p, 1 \leq j, k \leq n$). Clearly, these orders are rankings on $K\{y_1, \dots, y_n\}$.

If $f \in K\{y_1, \dots, y_n\} \setminus K$ and $1 \leq k \leq p$, then the greatest with respect to $<_k$ term that appears in f is called the k -*leader* of the σ -polynomial f ; it is denoted by $u_f^{(k)}$. The smallest with respect to $<_k$ term in f is called the k -*coleader* of f and is denoted by $v_f^{(k)}$.

Definition 3.1 Let $f \in K\{y_1, \dots, y_n\} \setminus K$ and let $u_f^{(k)} = \alpha_1^{k_1} \dots \alpha_m^{k_m} y_i$ and $v_f^{(k)} = \alpha_1^{l_1} \dots \alpha_m^{l_m} y_j$ be the k -leader and k -coleader of f , respectively ($1 \leq k \leq p$). Then

for every $k = 1, \dots, p$, the nonnegative integer $\text{ord}_k u_f^{(k)} - \text{ord}_k v_f^{(k)}$ is called the k th **effective order** of f ; it is denoted by $\text{Eord}_k f$.

It follows from the last definition that for any $f \in K\{y_1, \dots, y_n\}$ and for any $\tau \in T$, $\text{Eord}_k(\tau f) = \text{Eord}_k(f)$ for $k = 1, \dots, p$.

Definition 3.2 Let f and g be two σ -polynomials in the ring $K\{y_1, \dots, y_n\}$. We say that f has lower rank than g and write $\text{rk } f < \text{rk } g$ if either $f \in K$, $g \notin K$, or

$$(\text{Eord}_1(f), \dots, \text{Eord}_p(f), u_f^{(1)}, \deg_{u_g^{(1)}} f) <_{\text{lex}} (\text{Eord}_1(g), \dots, \text{Eord}_p(g), u_g^{(1)}, \deg_{u_g^{(1)}} g)$$

(the comparison of $u_f^{(1)}$ and $u_g^{(1)}$ in this lexicographic order is made with respect to the order $<_1$ on the set of terms TY). If the last two $(p+2)$ -tuples are equal (or $f, g \in K$) we say that f and g are of the same rank and write $\text{rk } f = \text{rk } g$.

Definition 3.3 Let $f, g \in K\{y_1, \dots, y_n\}$ and let $d = \deg_{u_g^{(1)}} g$. We say that f is E -reduced with respect to g if one of the following two conditions holds.

- (i) f does not contain any $(\tau u_g^{(1)})^e$ ($\tau \in T$) such that $e \geq d$;
- (ii) f contains $(\tau u_g^{(1)})^e$ with $e \geq d$ for some $\tau \in T$, but in this case either there exists $k \in \mathbb{N}_p$, $k \geq 2$, such that $\text{ord}_k(\tau u_g^{(k)}) > \text{ord}_k(u_f^{(k)})$ or there exists $j \in \mathbb{N}_p$ such that $\text{ord}_j(\tau v_g^{(j)}) < \text{ord}_j(v_f^{(j)})$. (The “or” here is inclusive, that is, the case when both conditions hold is included.)

Thus, f is not E -reduced with respect to g if f contains some $(\tau u_g^{(1)})^e$ ($\tau \in T$) with $e \geq d = \deg_{u_g^{(1)}} g$ and also $\text{ord}_k(\tau u_g^{(k)}) \leq \text{ord}_k(u_f^{(k)})$ for $k = 2, \dots, p$ and $\text{ord}_j(\tau v_g^{(j)}) \geq \text{ord}_j(v_f^{(j)})$ for $j = 1, \dots, p$.

Proposition 3.1 If $\text{rk } f < \text{rk } g$, then f is E -reduced with respect to g .

Proof Suppose that f is not E -reduced with respect to g . Then f contains some $(\tau u_g^{(1)})^e$ ($\tau \in T$) such that $e \geq d = \deg_{u_g^{(1)}} g$, $\text{ord}_k(\tau u_g^{(k)}) \leq \text{ord}_k(u_f^{(k)})$ for $k = 2, \dots, p$ and $\text{ord}_j(\tau v_g^{(j)}) \geq \text{ord}_j(v_f^{(j)})$ for $j = 1, \dots, p$. Then $u_f^{(1)} \geq \tau u_g^{(1)} = u_{\tau g}^{(1)} \geq u_g^{(1)}$, hence $\text{ord}_1 u_f^{(1)} \geq \text{ord}_1(\tau u_g^{(1)})$. Since $\text{ord}_1(v_f^{(1)}) \leq \text{ord}_1(\tau v_g^{(1)}) = \text{ord}_1(v_{\tau g}^{(1)})$, we have $\text{Eord}_1(f) \geq \text{Eord}_1(\tau g) = \text{Eord}_1(g)$. Also, for any $k = 2, \dots, p$, $\text{Eord}_k(f) = \text{ord}_k u_f^{(k)} - \text{ord}_k v_f^{(k)} \geq \text{ord}_k(\tau u_g^{(k)}) - \text{ord}_k(\tau v_g^{(k)}) = \text{Eord}_k(\tau g) = \text{Eord}_k(g)$. Therefore, $\text{rk } f \geq \text{rk } g$ according to Definition 3.2, so we have arrived at a contradiction. $\square$

Proposition 3.2 Let $\mathcal{A} = \{g_1, \dots, g_t\}$ be a finite set of σ -polynomials in the ring $R = K\{y_1, \dots, y_n\}$, let $u_k^{(i)}$ and $v_k^{(i)}$ denote the i -leader and i -coleader of g_k , respectively ($1 \leq k \leq t$, $1 \leq i \leq p$). Let $d_k = \deg_{u_k^{(1)}} g_k$ and I_k denote the coefficient of $(u_k^{(1)})^{d_k}$

when g_k is written as a polynomial in $u_k^{(1)}$ ($1 \leq k \leq t$). Furthermore, let $I(\mathcal{A}) = \{B \in R \mid \text{either } B = 1 \text{ or } B \text{ is a product of finitely many } \sigma\text{-polynomials of the form } \tau(I_k) \text{ } (\tau \in T, k = 1, \dots, t)\}$. Then for any $h \in R$, there exist σ -polynomials $J \in I(\mathcal{A})$ and $h^* \in R$ such that h^* is E -reduced with respect to $\mathcal{A}$ and $Jh \equiv h^* \pmod{[\mathcal{A}]}$ (that is, $Jh - h^* \in [\mathcal{A}]$).

Proof If h is E -reduced with respect to $\mathcal{A}$, the statement is obvious (one can set $h^* = h$). Suppose that h is not E -reduced with respect to $\mathcal{A}$. In what follows, if a σ -polynomial $f \in R$ is not E -reduced with respect to $\mathcal{A}$, then a term w_f that appears in f will be called the $\mathcal{A}$ -leader of f if w_f is the greatest (with respect to $<_1$) term among all terms of the form $\tau u_{g_k}^{(1)}$ ($\tau \in T, 1 \leq k \leq t$) such that f contains $(\tau u_k^{(1)})^e$ with $e \geq d_k$, $\text{ord}_i(\tau u_k^{(i)}) \leq \text{ord}_i u_h^{(i)}$ for $i = 2, \dots, p$, and $\text{ord}_j(\tau v_k^{(j)}) \geq \text{ord}_j v_h^{(j)}$ for $j = 1, \dots, p$. Let w_h be the $\mathcal{A}$ -leader of the element h , $d = \deg_{w_h} h$, and c_h the coefficient of w_h^d when h is written as a polynomial in w_h . Then $w_h = \tau u_k^{(1)}$ for some $\tau \in T$ and for some k ($1 \leq k \leq t$) such that $d \geq d_k$, $\text{ord}_i(\tau u_k^{(i)}) \leq \text{ord}_i u_h^{(i)}$ ($2 \leq i \leq p$), and $\text{ord}_j(\tau v_k^{(j)}) \geq \text{ord}_j v_h^{(j)}$ ($1 \leq j \leq p$). Let us choose such k that corresponds to the maximum (with respect to $<_1$) 1-leader $u_k^{(1)}$ in the set of all 1-leaders of elements of $\mathcal{A}$, and let us consider the σ -polynomial $h' = \tau(I_k)h - c_h w_h^{d-d_k}(\tau g_k)$. Clearly, $\deg_{w_h} h' < \deg_{w_h} h$ and h' does not contain any $\mathcal{A}$ -leader $\tau' u_v^{(1)}$ ($\tau' \in T, 1 \leq v \leq t$) that is greater than w_h with respect to $<_1$ (such a term cannot appear in $\tau(I_k)h$ or τg_k). Applying the same procedure to h' and continuing in the same way, we will arrive at a σ -polynomial $h^* \in R$ such that h^* is E -reduced with respect to $\mathcal{A}$ and $Jh - h^* \in [\mathcal{A}]$ for some $J \in I(\mathcal{A})$. $\square$

The process of reduction described in the proof of the last proposition can be realized by the following algorithm. (Recall that $\mathfrak{D}_R$ denotes the ring of σ -operators over the σ -ring $R = K\{y_1, \dots, y_n\}$.)

Algorithm 1 ($h, t, g_1, \dots, g_t; h^*$)

Input: $h \in R$, a positive integer t , $\mathcal{A} = \{g_1, \dots, g_t\} \subseteq R$ where $g_i \neq 0$ for $i = 1, \dots, t$

Output: Element $h^* \in R$, elements $C_1, \dots, C_t \in \mathfrak{D}_R$ and $J \in I(\mathcal{A})$ such that $Jh = \sum_{i=1}^t C_i(g_i) + h^*$ and h^* is E -reduced with respect to $\mathcal{A}$

Begin

$C_1 := 0, \dots, C_t := 0, h^* := h, J := 1$

While there exist $k, 1 \leq k \leq t$, and a term w that appears in h^* with a (nonzero) coefficient c_w , such that $u_{g_k}^{(1)} \mid w$, $\deg_{u_{g_k}^{(1)}} g_k \leq \deg_w h^*$, $\text{ord}_i \left(\frac{w}{u_{g_k}^{(1)}} u_{g_k}^{(i)} \right) \leq \text{ord}_i v_{h^*}^{(i)}$ for $i = 2, \dots, p$, and $\text{ord}_j \left(\frac{w}{u_{g_k}^{(1)}} v_{g_k}^{(j)} \right) \geq \text{ord}_j v_{h^*}^{(j)}$ for $j = 1, \dots, p$, **do**

$z :=$ the greatest of the terms w that satisfy the above conditions.

$l :=$ the smallest number k for which $u_{g_k}^{(1)}$ is the greatest (with respect to $<_1$) 1-leader of an element of $\mathcal{A}$ such that $u_{g_k}^{(1)} \mid z$, $\deg_{u_{g_k}^{(1)}} g_k \leq \deg_z h^*$,

$$\text{ord}_i \left(\frac{z}{u_{g_k}^{(1)}} u_{g_k}^{(i)} \right) \leq \text{ord}_i u_{h^*}^{(i)} \quad \text{for } i = 2, \dots, p, \quad \text{and} \quad \text{ord}_j \left(\frac{z}{u_{g_k}^{(1)}} v_{g_k}^{(j)} \right) \geq \text{ord}_j v_{h^*}^{(j)} \quad \text{for } j = 1, \dots, p,$$

$$\tau := \frac{z}{u_{g_l}^{(1)}}$$

$J := \tau(I_l)J$, $C_l := C_l + c_z z^{d-d_l} \tau$ where $d = \deg_z h^*$, $d_l = \deg_{u_{g_l}^{(1)}} g_l$, and c_z is the coefficient of z^d when h^* is written as a polynomial in z

$$h^* := \tau(I_l)h^* - c_z z^{d-d_l} (\tau g_l)$$

End

Definition 3.4 A set $\mathcal{A} \subseteq K\{y_1, \dots, y_n\}$ is said to be *E-autoreduced* if either it is empty or $\mathcal{A} \cap K = \emptyset$ and every element of $\mathcal{A}$ is *E-reduced* with respect to all other elements of the set $\mathcal{A}$.

We are going to show that every *E-autoreduced* sets is finite. The proof of the following lemma can be found in [4, Chapter 0, Section 17].

Lemma 3.1 Let A be any infinite subset of the set $\mathbb{N}^m \times \mathbb{N}_n$ ($m, n \in \mathbb{N}$, $n \geq 1$). Then there exists an infinite sequence of elements of A , strictly increasing relative to the product order, in which every element has the same projection on $\mathbb{N}_n$.

This lemma immediately implies the following statement that will be used below.

Lemma 3.2 Let S be any infinite set of terms τy_j ($\tau \in T$, $1 \leq j \leq n$) in the ring $K\{y_1, \dots, y_n\}$. Then there exists an index j ($1 \leq j \leq n$) and an infinite sequence of terms $\tau_1 y_j, \tau_2 y_j, \dots, \tau_k y_j, \dots$ such that $\tau_k \mid \tau_{k+1}$ for every $k = 1, 2, \dots$

Proposition 3.3 Every *E-autoreduced* set is finite.

Proof Suppose that there is an infinite *E-autoreduced* set $\mathcal{A}$. It follows from Lemma 3.2 that $\mathcal{A}$ contains a sequence of σ -polynomials $\{f_1, f_2, \dots\}$ such that $u_{f_i}^{(1)} \mid u_{f_{i+1}}^{(1)}$ for $i = 1, 2, \dots$. Since the sequence of non-negative integers $\{\deg_{u_{f_i}^{(1)}} f_i\}$ cannot have an infinite decreasing subsequence, without loss of generality we can assume that $\deg_{u_{f_i}^{(1)}} f_i \leq \deg_{u_{f_{i+1}}^{(1)}} f_{i+1}$ ($i = 1, 2, \dots$).

Let $k_{ij} = \text{ord}_j u_{f_i}^{(1)}$, $l_{ij} = \text{ord}_j u_{f_i}^{(j)}$, $n_{ij} = \text{ord}_j v_{f_i}^{(j)}$ ($1 \leq j \leq p$). Obviously, $l_{ij} \geq k_{ij} \geq n_{ij}$ ($i = 1, 2, \dots$; $j = 1, \dots, p$), so $\{(l_{i1} - k_{i1} = 0, l_{i2} - k_{i2}, \dots, l_{ip} - k_{ip}) \mid i = 1, 2, \dots\} \subseteq \mathbb{N}^p$ and $\{(k_{i1} - n_{i1}, k_{i2} - n_{i2}, \dots, k_{ip} - n_{ip}) \mid i = 1, 2, \dots\} \subseteq \mathbb{N}^p$. By Lemma 3.1, there exists an infinite sequence of indices $i_1 < i_2 < \dots$ such that

$$(l_{i_1 2} - k_{i_1 2}, \dots, l_{i_1 p} - k_{i_1 p}) \leq_P (l_{i_2 2} - k_{i_2 2}, \dots, l_{i_2 p} - k_{i_2 p}) \leq_P \dots \quad (3.1)$$

and

$$(k_{i_1 1} - n_{i_1 1}, \dots, k_{i_1 p} - n_{i_1 p}) \leq_P (k_{i_1 1} - n_{i_1 1}, \dots, k_{i_2 p} - n_{i_2 p}) \leq_P \dots \quad (3.2)$$

Then for any $j = 2, \dots, p$, we have
 $\text{ord}_j \left(\frac{u_{f_2}^{(1)}}{u_{f_1}^{(1)}} u_{f_1}^{(j)} \right) = k_{i_2 j} - k_{i_1 j} + l_{i_1 j} \leq k_{i_2 j} - l_{i_2 j} - k_{i_1 j} = l_{i_2 j} = \text{ord}_j u_{f_2}^{(j)}$, so that f_{i_2} contains a term $\tau u_{f_1}^{(1)} = u_{f_2}^{(1)}$ such that $\tau \neq 1$ and $\text{ord}_j(\tau u_{f_1}^{(j)}) \leq \text{ord}_j u_{f_2}^{(j)}$ for $j = 2, \dots, p$. Similar arguments with the use of (3.2) show that $\text{ord}_j(\tau v_{f_1}^{(j)}) \geq \text{ord}_j v_{f_2}^{(j)}$ for $j = 2, \dots, p$. Thus, the σ -polynomial f_{i_2} is not reduced with respect to f_{i_1} that contradicts the fact that $\mathcal{A}$ is an E -autoreduced set. $\square$

Example 1 Let K be a difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ considered with a partition $\sigma = \sigma_1 \cup \sigma_2$ where $\sigma_1 = \{\alpha_1\}$ and $\sigma_2 = \{\alpha_2\}$. Let $\mathcal{A} = \{g_1, g_2\} \subseteq K\{y\}$ (the ring of σ -polynomials in one σ -indeterminate y) where

$$g_1 = \alpha_1^3 \alpha_2 y + \alpha_1^2 y + \alpha_2^3 y + y, g_2 = \alpha_1^2 \alpha_2 y + \alpha_2^2 y + 1.$$

Then $(\text{Eord}_1(g_1), \dots, \text{Eord}_p(g_1), u_{g_1}^{(1)}, \deg_{u_{g_1}^{(1)}} g_1) = (3 - 2, 3 - 1, \alpha_1^3 \alpha_2 y, 1) <_{\text{lex}} (2, 2 - 1, \alpha_1^2 \alpha_2 y, 1) = (\text{Eord}_1(g_2), \dots, \text{Eord}_p(g_2), u_{g_2}^{(1)}, \deg_{u_{g_2}^{(1)}} g_2)$, so $\text{rk } g_1 < \text{rk } g_2$. By Proposition 3.1, g_1 is E -reduced with respect to g_2 . Since g_2 contains no transform of $u_{g_1}^{(1)} = \alpha_1^3 \alpha_2 y$, 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 $\alpha_1 u_{g_2}^{(1)}$ is equal to the degree of g_2 with respect to $u_{g_2}^{(1)}$, the set $\mathcal{A}$ is not autoreduced in the usual sense (where one considers an orderly ranking of terms in $K\{y\}$ and f is said to be reduced with respect to g if f does not contain any $(\tau u_g)^e$ ($\tau \in T$, u_g is the leader of g with respect to the given ranking) such that $e \geq d = \deg_{u_g} g$, see [5, Section 3.3]) or [9, 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 3.5 Let $\mathcal{A} = \{g_1, \dots, g_s\}$ and $\mathcal{B} = \{h_1, \dots, h_t\}$ be two E -autoreduced sets in the ring $K\{y_1, \dots, y_n\}$. Then $\mathcal{A}$ is said to have lower rank than $\mathcal{B}$, written as $\text{rk } \mathcal{A} < \text{rk } \mathcal{B}$, if one of the following two cases holds:

(1) $\text{rk } g_1 < \text{rk } h_1$ or there exists $k \in \mathbb{N}$ such that $1 < k \leq \min\{s, t\}$, $\text{rk } g_i = \text{rk } h_i$ for $i = 1, \dots, k - 1$ and $\text{rk } g_k < \text{rk } h_k$.

(2) $s > t$ and $\text{rk } g_i = \text{rk } h_i$ for $i = 1, \dots, t$.

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

Proposition 3.4 *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 $K\{y_1, \dots, y_n\}$. Let us inductively define an infinite descending chain of subsets of $\mathcal{M}$ as follows: $\mathcal{M}_0 = \mathcal{M}$, $\mathcal{M}_1 = \{\mathcal{A} \in \mathcal{M}_0 \mid \mathcal{A} \text{ contains at least one element and the first element of } \mathcal{A} \text{ is of lowest possible rank}\}$, $\dots$, $\mathcal{M}_k = \{\mathcal{A} \in \mathcal{M}_{k-1} \mid \mathcal{A} \text{ contains at least } k \text{ elements and the } k\text{th element of } \mathcal{A} \text{ is of lowest possible rank}\}$, $\dots$. It is clear that if $\mathcal{A}$ and $\mathcal{B}$ are any two E -autoreduced sets in $\mathcal{M}_k$ and f and g are their l th σ -polynomials ($l \geq k$), then $\text{rk } f = \text{rk } g$. Therefore, if all sets $\mathcal{M}_k$ are nonempty, then the set $\{A_k \mid A_k \text{ is the } k\text{th element of some } E\text{-autoreduced set in } \mathcal{M}_k\}$ would be an infinite autoreduced set, and this would contradict Proposition 3.3. 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 $\mathcal{M}$. $\square$

Let J be any ideal of the ring $K\{y_1, \dots, y_n\}$. Since the set of all E -autoreduced subsets of J is not empty (if $f \in J$, 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 3.5 *Let $\mathcal{A} = \{f_1, \dots, f_d\}$ be an E -characteristic set of a σ -ideal J of the ring $K\{y_1, \dots, y_n\}$. 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 $\text{rk } g < \text{rk } f_1$, then $\text{rk } \{g\} < \text{rk } \mathcal{A}$ that contradicts the fact that $\mathcal{A}$ is a E -characteristic set of the ideal J . Let $\text{rk } g > \text{rk } f_1$ (if $\text{rk } g = \text{rk } f_1$, then g is not reduced with respect to f_1 , contrary to the assumption that g is E -reduced with respect to $\mathcal{A}$). Let $f_1, \dots, f_j$ ($1 \leq j \leq d$) be all elements of $\mathcal{A}$ whose rank is lower than the rank of g . Then the set $\mathcal{A}' = \{f_1, \dots, f_j, g\}$ is E -autoreduced. Indeed, by the conditions of the theorem, σ -polynomials $f_1, \dots, f_j$ are reduced with respect to each other and g is reduced with respect to the set $\{f_1, \dots, f_j\}$. Furthermore, each f_i ($1 \leq i \leq j$) is reduced with respect to g because $\text{rk } f_i < \text{rk } g$. Since $\text{rk } \mathcal{A}' < \text{rk } \mathcal{A}$, $\mathcal{A}$ is not an E -characteristic set of J that contradicts the conditions of the proposition. Thus, $g = 0$. $\square$

Proposition 3.6 *Let $\leq$ be a ranking on the ring $R = K\{y_1, \dots, y_n\}$ and let $f_1, \dots, f_s$ ($s \geq 2$) be linear σ -polynomials in R . For every $i = 1, \dots, s$, let u_i and v_i denote, respectively, the leader and coleader of f_i with respect to $\leq$, and let $u_1 > u_2 > \dots > u_s$ and $v_1 > v_2 > \dots > v_s$. Suppose that*

$$g = h_1 f_1 + \dots + h_s f_s \quad (3.3)$$

where $0 \neq h_i \in R$ ($1 \leq i \leq s$) and that g cannot be represented as a linear combination of any proper subset of $\{f_1, \dots, f_s\}$ with coefficients in R . Then g contains u_1 and v_s .

Proof Without loss of generality we can assume that the coefficient of u_1 in f_1 is 1. Dividing each h_i ($2 \leq i \leq s$) by f_1 with respect to u_1 , we obtain that $h_i = h'_i f_1 + h''_i$ where the σ -polynomial h''_i does not contain u_1 . Thus, $g = (h_1 + h'_2 f_1 + \dots + h'_s f_1) f_1 + h''_2 f_2 + \dots + h''_s f_s$ where the σ -polynomial $h''_2 f_2 + \dots + h''_s f_s$ does not contain u_1 . Since $h_1 + h'_2 f_1 + \dots + h'_s f_1 \neq 0$ (otherwise, g is a linear combination of $f_2, \dots, f_s$ that contradicts our assumption), g contains u_1 .

Similarly, writing each h_j with $1 \leq j \leq s-1$ as $h_j = h^*_j f_s + h^{**}_j$ where h^{**}_j does not contain v_s , we obtain (using the fact that g cannot be written as a linear combination of elements of any proper subset of $\{f_1, \dots, f_s\}$) that g contains v_s . $\square$

Proposition 3.7 *Let f be a linear σ -polynomial in $R = K\{y_1, \dots, y_n\}$. Then $\{f\}$ is an E -characteristic set of the σ -ideal $[f]$.*

Proof Let $g \in [f]$. Then one can represent g in the form

$$g = h_1(\tau_1 f) + \dots + h_s(\tau_s f)$$

where $0 \neq h_i \in R$, $\tau_i \in T$ ($1 \leq i \leq s$), $\tau_i \neq \tau_j$ whenever $i \neq j$, and s is the smallest positive integer for which such a representation of g exists. (In particular, g cannot be written as a linear combination with coefficients in R of elements of any proper subset of $\{\tau_1 f, \dots, \tau_s f\}$.) Since the elements $\tau_1, \dots, \tau_s$ are all distinct, for every $k = 1, \dots, p$, there exists a permutation π_k of the set $\{1, \dots, s\}$ such that $\tau_{\pi_k(s)} <_k \dots <_k \tau_{\pi_k(1)}$. By Proposition 3.6, g contains the k -leader of $\tau_{\pi_k(1)} f$ and the k -coleader of $\tau_{\pi_k(s)} f$ (clearly, the latter term cannot be smaller than $v_g^{(k)}$ with respect to $<_k$). Therefore, g is not E -reduced with respect to $\{f\}$ and $\text{rk } g \geq \text{rk } f$. Thus, no element of $[f]$ is E -reduced with respect to $\{f\}$ and f has the smallest rank among all σ -polynomials in $[f]$. It follows that $\{f\}$ is an E -characteristic set of the σ -ideal $[f]$. $\square$

4 A new type of multivariate difference dimension polynomials

In this section we use properties of E -characteristic sets to obtain the following result that generalizes Theorem 1.1 and introduces a new type of multivariate dimension polynomials of difference field extensions that carry more invariants than any previously known difference dimension polynomials. (By an invariant of a finitely generated difference field extension we mean a numerical characteristic that is carried by a difference dimension polynomial of such an extension and that does not depend on the choice of the finite set of its difference generators.) As before, K denotes a difference (σ -) field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_m\}$ considered together with its partition (1.1) into the union of p disjoint subsets σ_i , $\text{Card } \sigma_i = m_i$ ($1 \leq i \leq p$). Furthermore, for any two p -tuples $(r_1, \dots, r_p), (s_1, \dots, s_p) \in \mathbb{N}^p$ with $s_i \leq r_i$ for $i = 1, \dots, p$, we set

$$T(r_1, \dots, r_p; s_1, \dots, s_p) = \{\tau \in T \mid s_i \leq \text{ord}_i \tau \leq r_i \text{ for } i = 1, \dots, p\}.$$

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 $\phi_{\eta|K}(t_1, \dots, t_{2p})$ in $2p$ variables with rational coefficients and numbers $r_i^{(0)}, s_i^{(0)}, s_i^{(1)} \in \mathbb{N}$ ($1 \leq i \leq p$) with $s_i^{(0)} < r_i^{(0)}$ and $s_i^{(1)} < r_i^{(0)} - s_i^{(0)}$ such that

$$\phi_{\eta|K}(r_1, \dots, r_p, s_1, \dots, s_p) = \text{tr.deg}_K K(\{\tau \eta_j \mid \tau \in T(r_1, \dots, r_p; s_1, \dots, s_p), 1 \leq j \leq n\})$$

for all $(r_1, \dots, r_p, s_1, \dots, s_p) \in \mathbb{N}^{2p}$ with $r_i \geq r_i^{(0)}$, $s_i^{(1)} \leq s_i \leq r_i - s_i^{(0)}$. Furthermore, $\deg \phi_{\eta|K} \leq m$, $\deg_{t_i} \phi_{\eta|K} \leq m_i$ for $i = 1, \dots, p$ and $\deg_{t_j} \phi_{\eta|K} \leq m_{j-p}$ for $j = p+1, \dots, 2p$.

Proof Let $P \subseteq R = K\{y_1, \dots, y_n\}$ be the defining σ -ideal of the extension L/K and let $\mathcal{A} = \{f_1, \dots, f_q\}$ be an E -characteristic set of P . Let $u_j^{(i)}$ and $v_j^{(i)}$ denote the i -leader and i -coleader of f_j , respectively ($1 \leq j \leq q$, $1 \leq i \leq p$). For any $\bar{r} = (r_1, \dots, r_p)$, $\bar{s} = (s_1, \dots, s_p) \in \mathbb{N}^p$ such that $\bar{s} \leq_p \bar{r}$ (that is, $s_i \leq r_i$ for $i = 1, \dots, p$), let

$$W(\bar{r}, \bar{s}) = \{w \in TY \mid s_i \leq \text{ord}_i w \leq r_i \text{ for } i = 1, \dots, p\},$$

$$W_\eta(\bar{r}, \bar{s}) = \{w(\eta) \mid w \in W(\bar{r}, \bar{s})\},$$

$$U'(\bar{r}, \bar{s}) = \left\{ u \in TY \mid s_i \leq \text{ord}_i u \leq r_i \text{ for } i = 1, \dots, p \text{ and } u_j^{(1)} \mid u (1 \leq j \leq q) \right\},$$

$$U'_\eta(\bar{r}, \bar{s}) = \{u(\eta) \mid u \in U'(\bar{r}, \bar{s})\},$$

$$U''_\eta(\bar{r}, \bar{s}) = \{u \in TY \mid s_i \leq \text{ord}_i u \leq r_i (1 \leq i \leq p)\},$$

u is divisible by the 1-leader of some f_j ($1 \leq j \leq q$) and whenever $u = \tau u_j^{(1)}$ for some $\tau \in T$, $1 \leq j \leq q$, either $\text{ord}_1(\tau v_j^{(1)}) < s_1$ or there exist $k \in \{2, \dots, p\}$, $i \in \{1, \dots, p\}$ such that $\text{ord}_k(\tau u_j^{(k)}) > r_k$ or $\text{ord}_i(\tau v_j^{(i)}) < s_i$ ("or" is inclusive),

$$\text{and } U''_\eta(\bar{r}, \bar{s}) = \{u(\eta) \mid u \in U''(\bar{r}, \bar{s})\}.$$

Furthermore, let

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

We are going to prove that for every $\bar{r}, \bar{s} \in \mathbb{N}^p$ with $\bar{s} <_p \bar{r}$, the set $U_\eta(\bar{r}, \bar{s})$ is a transcendence basis of the field $K(W_\eta(\bar{r}, \bar{s}))$ over K . First, one can see that this set is algebraically independent over K . Indeed, if $f(w_1(\eta), \dots, w_k(\eta)) = 0$ for some elements $w_1, \dots, w_k \in U(\bar{r}, \bar{s})$, 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 $w = \tau u_j^{(1)}$, $1 \leq i \leq q$, $\tau \in T$, such that $\deg_w f \geq \deg_{u_j^{(1)}} f$, then $w \in U''(\bar{r}, \bar{s})$, so either $\text{ord}_1(\tau v_j^{(1)}) < s_1 \leq \text{ord}_1 v_j^{(1)}$ or there exist $k \in \{2, \dots, q\}$, $i \in \{1, \dots, p\}$ such that $\text{ord}_i(\tau u_i^{(k)}) > r_k \geq \text{ord}_i u_i^{(i)}$ or

$\text{ord}_i(\tau v_k^{(i)}) < s_i \leq \text{ord}_i v_f^{(i)}$ ("or" is inclusive). It follows that f is E -reduced with respect to $\mathcal{A}$.) By Proposition 3.5, $f = 0$, so the set $U_\eta(\bar{r}, \bar{s})$ is algebraically independent over K .

Now let us prove that if $0 \leq s_i \leq r_i - s_i^{(0)}$, where $s_i^{(0)} = \max\{\text{Eord } f_j \mid 1 \leq j \leq q\}$ ($1 \leq i \leq p$), then every element $\tau \eta_k \in W_\eta(\bar{r}, \bar{s}) \setminus U_\eta(\bar{r}, \bar{s})$ ($\tau \in T$, $1 \leq k \leq n$) is algebraic over the field $K(U_\eta(\bar{r}, \bar{s}))$. In this case $\tau y_k \notin U(\bar{r}, \bar{s})$, therefore τy_k is equal to some term of the form $\tau' u_j^{(1)}$ ($1 \leq j \leq q$) where $\tau' \in T$, $\text{ord}_1(\tau' u_j^{(i)}) \leq r_i$ for $i = 2, \dots, p$, and $\text{ord}_l(\tau' v_j^{(l)}) \geq s_l$ for $l = 1, \dots, p$.

Let us represent f_j as a polynomial in $u_j^{(1)}$:

$$f_j = I_{d_j}^{(j)}(u_j^{(1)})^{d_j} + \dots + I_1^{(j)} u_j^{(1)} + I_0^{(j)}$$

where $I_0^{(j)}, I_1^{(j)}, \dots, I_{d_j}^{(j)}$ do not contain $u_j^{(1)}$ (therefore, all terms in these σ -polynomials are lower than $u_j^{(1)}$ with respect to $<_1$). Since $f_j \in P$, $f_j(\eta) = 0$, that is,

$$I_{d_j}^{(j)}(\eta)(u_j^{(1)}(\eta))^{d_j} + \dots + I_1^{(j)}(\eta)u_j^{(1)}(\eta) + I_0^{(j)}(\eta) = 0. \quad (4.1)$$

Note that $I_{d_j}^{(j)}(\eta) \neq 0$. Indeed, since $\text{rk } I_{d_j}^{(j)} < \text{rk } f_j$, the equality $I_{d_j}^{(j)}(\eta) = 0$ would imply that $I_{d_j}^{(j)} \in P$. In this case, the family of all f_i with $\text{rk } f_i < \text{rk } I_{d_j}^{(j)}$ and $I_{d_j}^{(j)}$ would form an E -autoreduced set in P (see Proposition 3.1) whose rank is lower than the rank of $\mathcal{A}$. This contradicts the fact that $\mathcal{A}$ is an E -characteristic set of P . Since the σ -ideal P is reflexive, $\tau(I_q^{(j)}) \notin P$ for any $\tau \in T$. Therefore, if we apply τ' to both sides of (4.1), the resulting equality will show that the element $\tau' u_j^{(1)}(\eta) = \tau \eta_k$ is algebraic over the field $K(\{\tilde{\tau} \eta_l \mid s_i \leq \text{ord}_i \tilde{\tau} \leq r_i (1 \leq i \leq p), \tilde{\tau} y_l <_1 \tau' u_j^{(1)}\})$. Now, the induction on the well-ordered (with respect to $<_1$) set of terms TY completes the proof of the fact that the set $U_\eta(\bar{r}, \bar{s})$ is a transcendence basis of the field $K(W_\eta(\bar{r}, \bar{s}))$ over K .

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

$$A_k = \{(i_1, \dots, i_m) \in \mathbb{N}^m \mid \alpha_1^{i_1} \dots \alpha_m^{i_m} y_k \text{ is the 1-leader of some element of } \mathcal{A}\}.$$

Applying Theorem 2.1, we obtain that there exists a numerical polynomial $\omega_k(t_1, \dots, t_p)$ in p variables with rational coefficients such that $\omega_k(r_1, \dots, r_p) = \text{Card } V_{A_k}(r_1, \dots, r_p)$ for all sufficiently large $(r_1, \dots, r_p) \in \mathbb{N}^p$. It follows that if we set $\chi_{\eta|K}(t_1, \dots, t_p) = \sum_{k=1}^n \omega_k(t_1, \dots, t_p)$, then there exist $r_i^{(0)}, s_i^{(0)}, s_i^{(1)} \in \mathbb{N}$ ($1 \leq i \leq p$) with $s_i^{(0)} < r_i^{(0)}$ and $s_i^{(1)} < r_i^{(0)} - s_i^{(0)}$ such that for all $\bar{r} = (r_1, \dots, r_p), \bar{s} = (s_1, \dots, s_p) \in \mathbb{N}^p$ with $r_i \geq r_i^{(0)}, s_i^{(1)} \leq s_i \leq r_i - s_i^{(0)}$, one has

$$\text{Card } U_\eta(\bar{r}, \bar{s}) = \chi_{\eta|K}(r_1, \dots, r_p) - \chi_{\eta|K}(s_1 - 1, \dots, s_p - 1). \quad (4.2)$$

Furthermore, $\deg \chi_{\eta|K} \leq m$, and $\deg \chi_{\eta|K} = m$ if and only if at least one of the sets A_k ($1 \leq k \leq n$) is empty. Note that $\chi_{\eta|K}$ is the σ -dimension polynomial of the extension

L/K associated with the set of σ -generators η and partition (1.1) of σ , as it is shown in the proof of Theorem 1.1 given in [9, Section 4.2].

In order to evaluate $\text{Card } U''(\bar{r}, \bar{s})$, note that this set consists of all terms $\tau u_j^{(1)}$ ($\tau \in T, 1 \leq j \leq q$) such that $s_i \leq \text{ord}_i(\tau u_j) \leq r_i$ and either $\text{ord}_1(\tau v_j^{(1)}) < s_1$ or there exist $k \in \{2, \dots, p\}, i \in \{1, \dots, p\}$ such that $\text{ord}_k(\tau u_j^{(k)}) > r_k$ or $\text{ord}_i(\tau v_j^{(i)}) < s_i$ (“or” is inclusive). It follows from Remark 2.1 that for every fixed j , the number N_j of such terms satisfying the conditions $\text{ord}_i(\tau v_j^{(i)}) < s_i$ for $i \in \{k_1, \dots, k_d\} \subseteq \{1, \dots, p\}$, $\text{ord}_i(\tau v_j^{(i)}) \geq s_i$ for $i \in \{1, \dots, p\}, i \neq k_v$ ($1 \leq v \leq d$) and $\text{ord}_i(\tau u_j^{(i)}) \leq r_i$ for $i = 1, \dots, p$ is equal to

$$\prod_{1 \leq i \leq p, i \neq k_v, (1 \leq v \leq d)} \left[\binom{r_i + m_i}{m_i} - \binom{s_i + m_i - 1}{m_i} \right] \cdot \prod_{v=1}^d \left[\binom{s_{k_v} - \text{ord}_{k_v} v_{k_v}^{(k_v)} - 1 + m_{k_v}}{m_{k_v}} - \binom{s_{k_v} - \text{ord}_{k_v} u_{k_v}^{(1)} - 1 + m_{k_v}}{m_{k_v}} \right].$$

By Remark 2.1, a similar formula holds for the number of terms satisfying the conditions $\text{ord}_i(\tau u_j^{(i)}) > r_i$ for $i \in \{l_1, \dots, l_e\} \subseteq \{2, \dots, p\}$, $\text{ord}_i(\tau v_j^{(i)}) \geq s_i$ for $i \in \{1, \dots, p\}$ and $\text{ord}_i(\tau u_j^{(i)}) \leq r_i$ for $i \neq l_v$ ($1 \leq v \leq e$).

Applying the principle of inclusion and exclusion (taking into account terms that are multiples of more than one 1-leaders), we obtain that $\text{Card } U''(\bar{r}, \bar{s})$ is an alternating sum of polynomials in $r_1, \dots, r_p, s_1, \dots, s_p$ that are products of k terms of the form $\binom{r_i - a_i + m_i}{m_i} - \binom{s_i - b_i + m_i}{m_i}$ with $a_i, b_i \in \mathbb{N}$ ($1 \leq i < p$) and $p - k$ terms of the form either $\binom{m_i - c_i + m_i}{m_i} - \binom{m_i - d_i + m_i}{m_i}$ or $\binom{r_i - c_i + m_i}{m_i} - \binom{r_i - d_i + m_i}{m_i}$ with $c_i, d_i \in \mathbb{N}$, $c_i < d_i$. Since each such a polynomial has total degree at most $m - 1$ and its degree with respect to r_i or s_i ($1 \leq i \leq p$) does not exceed m_i , we obtain that $\text{Card } U''(\bar{r}, \bar{s}) = \psi(r_1, \dots, r_p, s_1, \dots, s_p)$ where $\psi(t_1, \dots, t_{2p})$ is a numerical polynomial in $2p$ variables such that $\deg \psi < m$ and $\deg_{t_i} \psi \leq m_i$, $\deg_{t_j} \psi \leq m_{j-p}$ for $i = 1, \dots, p, j = p + 1, \dots, 2p$. It follows that the numerical polynomial

$$\phi_{\eta|K}(t_1, \dots, t_{2p}) = \chi_{\eta|K}(t_1, \dots, t_p) - \chi_{\eta|K}(t_{p+1} - 1, \dots, t_{2p} - 1) + \psi(t_1, \dots, t_{2p})$$

satisfies conditions of our theorem. $\square$

Definition 4.1 The numerical polynomial $\phi_{\eta|K}(t_1, \dots, t_{2p})$ whose existence is established by Theorem 2.3 is called the $2p$ -variate σ -dimension polynomial of the σ -field extension L/K associated with the system of σ -generators η and partition (1.1) of the set σ .

The following theorem describes some invariants of a $2p$ -variate σ -dimension polynomial of a finitely generated σ -field extension L/K with partition (1.1) of σ ,

that is, characteristics of the extension that do not depend on the set of σ -generators of L over K . The formulation of the theorem uses the following notation. For any permutation $(j_1, \dots, j_{2p})$ of the set $\{1, \dots, 2p\}$, let $<_{j_1, \dots, j_{2p}}$ denote the lexicographic order on $\mathbb{N}^p$ such that $(k_1, \dots, k_{2p}) <_{j_1, \dots, j_{2p}} (l_1, \dots, l_{2p})$ if and only if either $k_{j_1} < l_{j_1}$ or there exists $q \in \mathbb{N}$, $2 \leq q \leq 2p$, such that $k_{j_v} = l_{j_v}$ for $v < q$ and $k_{j_q} < l_{j_q}$.

Theorem 4.2 *With the notation of Theorem 4.1, let $\phi_{\eta|K}(t_1, \dots, t_{2p})$ be the $2p$ -variate σ -dimension polynomial of the σ -field extension $L = K\langle \eta_1, \dots, \eta_n \rangle$. Since the degrees of $\phi_{\eta|K}$ with respect to t_i and t_{p+i} ($1 \leq i \leq p$) do not exceed $m_i = \text{Card } \sigma_i$ (see partition (1.1)), Theorem 2.1 shows that this polynomial can be written as*

$$\phi_{\eta|K} = \sum_{i_1=0}^{m_1} \dots \sum_{i_p=0}^{m_p} \sum_{i_{p+1}=0}^{m_1} \dots \sum_{i_{2p}=0}^{m_p} a_{i_1 \dots i_{2p}} \binom{t_1 + i_1}{i_1} \dots \binom{t_{2p} + i_{2p}}{i_{2p}}.$$

Let $E_\eta = \{(i_1, \dots, i_{2p}) \in \mathbb{N}^{2p} \mid 0 \leq i_k, i_{p+k} \leq m_k \ (k = 1, \dots, p) \text{ and } a_{i_1 \dots i_{2p}} \neq 0\}$. Then the total degree d of $\phi_{\eta|K}$ with respect to $t_1, \dots, t_p$ and the coefficients of the terms of total degree d in $\phi_{\eta|K}$ do not depend on the choice of the set of σ -generators η . Furthermore, if $(\mu_1, \dots, \mu_p)$ is any permutation of $\{1, \dots, p\}$ and $(v_1, \dots, v_p)$ is any permutation of $\{p+1, \dots, 2p\}$, then the maximal element of E_η with respect to the lexicographic order $<_{\mu_1, \dots, \mu_p, v_1, \dots, v_p}$ and the corresponding coefficient $a_{\mu_1, \dots, \mu_p, v_1, \dots, v_p}$ do not depend on the choice of a finite set of σ -generators of L/K either. Finally, $a_{m_1 \dots m_p, 0 \dots 0} = a_{0 \dots 0, m_1 \dots m_p} = \sigma\text{-tr.deg } K L$.

Proof Suppose that $\zeta = \{\zeta_1, \dots, \zeta_l\}$ is another system of σ -generators of L/K , that is, $L = K\langle \eta_1, \dots, \eta_n \rangle = K\langle \zeta_1, \dots, \zeta_l \rangle$. Let

$$\phi_{\zeta|K}(t_1, \dots, t_{2p}) = \sum_{i_1=0}^{m_1} \dots \sum_{i_p=0}^{m_p} \sum_{i_{p+1}=0}^{m_1} \dots \sum_{i_{2p}=0}^{m_p} b_{i_1 \dots i_{2p}} \binom{t_1 + i_1}{i_1} \dots \binom{t_{2p} + i_{2p}}{i_{2p}}$$

be the $2p$ -variate dimension polynomial of L/K associated with the system of generators ζ . Then there exist $h_1, \dots, h_p \in \mathbb{N}$ such that $\eta_i \in K(\bigcup_{j=1}^l T(h_1, \dots, h_p)\zeta_j)$ and $\zeta_k \in K(\bigcup_{j=1}^n T(h_1, \dots, h_p)\eta_j)$ for any $i = 1, \dots, n$ and $k = 1, \dots, l$. (If $T' \subseteq T$, then $T'\zeta_j$ denotes the set $\{\tau\zeta_j \mid \tau \in T'\}$.) It follows that there exist numbers $r_i^{(0)}, s_i^{(0)}, s_i^{(1)} \in \mathbb{N}$ ($1 \leq i \leq p$) with $s_i^{(1)} < r_i^{(0)} - s_i^{(0)}$ such that whenever $r_i \geq r_i^{(0)}$, $s_i^{(1)} \leq s_i \leq r_i - s_i^{(0)}$ ($1 \leq i \leq p$), one has

$$\phi_{\eta|K}(r_1, \dots, r_{2p}) \leq \psi_{\zeta|K}(r_1 + h_1, \dots, r_p + h_p, r_{p+1} - h_1, \dots, r_{2p} - h_p)$$

and

$$\phi_{\zeta|K}(r_1, \dots, r_{2p}) \leq \phi_{\zeta|K}(r_1 + h_1, \dots, r_p + h_p, r_{p+1} - h_1, \dots, r_{2p} - h_p).$$

Now the statement of the theorem follows from the fact that for any element $(k_1, \dots, k_{2p}) \in E'_\eta$, the term $\binom{t_1 + k_1}{k_1} \dots \binom{t_{2p} + k_{2p}}{k_{2p}}$ appears in $\phi_{\eta|K}(t_1, \dots, t_{2p})$ and $\phi_{\zeta|K}(t_1, \dots, t_{2p})$ with the same coefficient $a_{k_1 \dots k_{2p}}$. The equality of the coefficients of

the corresponding terms of total degree $d = \deg \phi_{\eta|K} = \deg \phi_{\zeta|K}$ in $\phi_{\eta|K}$ and $\phi_{\zeta|K}$ can be shown as in the proof of [9, Theorem 3.3.21].

In order to prove the last part of the theorem, note that the expression (4.3) and a similar expression corresponding to the condition with $\text{ord}_i(\tau u_j^{(i)}) > r_i$ for $i \in \{l_1, \dots, l_e\} \subseteq \{2, \dots, p\}$ (see the proof of Theorem 2.3) have the property that their total degrees with respect to $r_1, \dots, r_p$ and $s_1, \dots, s_p$ are less than m . It follows that the coefficients of the terms of total degree m in $t_1, \dots, t_p$ and terms of total degree m in $t_{p+1}, \dots, t_{2p}$ in the polynomial $\phi_{\eta|K}$ are equal to the corresponding coefficients in the polynomials $\chi_{\eta|K}(t_1, \dots, t_p)$ and $\chi_{\eta|K}(t_{p+1}, \dots, t_{2p})$, respectively (see (4.2)). It follows from Theorem 1.1 that $a_{m_1 \dots m_p 0 \dots 0} = a_{0 \dots 0 m_1 \dots m_p} = \sigma\text{-tr.deg}_K L$. $\square$

Example 2 Let K be a difference (σ -) field with a basic set of endomorphisms $\sigma = \{\alpha_1, \alpha_2, \alpha_3\}$ considered together with its partition $\sigma = \{\alpha_1\} \cup \{\alpha_2\} \cup \{\alpha_3\}$. Let $L = K\langle \eta \rangle$ be a σ -field extension with the defining equation

$$\alpha_1^a \alpha_2^b \eta + \alpha_1^a \eta + \alpha_2^b \eta + \alpha_3^c \eta = 0 \quad (4.4)$$

where $a, b, c \in \mathbb{N}$, $a > b > c > 0$. It means that the defining σ -ideal P of the extension L/K is a linear σ -ideal of the ring of σ -polynomials $K\{y\}$ generated by the linear σ -polynomial $f = \alpha_1^a \alpha_2^b y + \alpha_1^a y + \alpha_2^b y + \alpha_3^c y$.

By Proposition 3.7, $\{f\}$ is an E -characteristic set of P . Setting $\bar{r} = (r_1, r_2, r_3)$ and $\bar{s} = (s_1, s_2, s_3)$ and using the notation of the proof of Theorem 4.1, we obtain (applying (2.3)) that

$$\begin{aligned} \text{Card } U'(\bar{r}, \bar{s}) &= \text{Card } V_{\{a,b,0\}}(r_1, r_2, r_3) - \text{Card } V_{\{a,b,0\}}(s_1 - 1, s_2 - 1, s_3 - 1) \\ &= [a(r_2 + 1)(r_3 + 1) + b(r_1 + 1)(r_3 + 1) \\ &\quad - ab(r_3 + 1)] - [as_2s_3 + bs_1s_3 - abs_3] \end{aligned}$$

Furthermore,

$\text{Card } U''(\bar{r}, \bar{s}) = \text{Card } \{\alpha_1^{a+k_1} \alpha_2^{b+k_2} \alpha_3^{k_3} \mid s_1 \leq a + k_1 \leq r_1, s_2 \leq b + k_2 \leq r_2, s_3 \leq k_3 \leq r_3 \text{ and there are one or more of the inequalities } k_3 + c > r_3 \text{ or } k_1 + c < s_1 \text{ or } k_2 + c < s_2\}$.

Applying the combinatorial method of inclusion and exclusion, we obtain that

$$\begin{aligned} \text{Card } U''(\bar{r}, \bar{s}) &= c(r_1 - s_1 + 1)(r_2 - s_2 + 1) + (a - c)(r_2 - s_2 + 1)(r_3 - s_3 + 1) \\ &\quad + (b - c)(r_1 - s_1 + 1)(r_3 - s_3 + 1) - c(a - c)(r_2 - s_2 + 1) \\ &\quad - c(b - c)(r_1 - s_1 + 1) - (a - c)(b - c)(r_3 - s_3 + 1) + c(a - c)(b - c) \end{aligned}$$

Therefore, the dimension polynomial of the σ -field extension of L/K defined by the equation (4.4) on its σ -generator η , which expresses $\text{Card } U'(\bar{r}, \bar{s}) + \text{Card } U''(\bar{r}, \bar{s})$, is of the form

$$\begin{aligned} \phi_{\eta|K}(t_1, \dots, t_6) &= ct_1t_2 + (2b - c)t_1t_3 + (2a - c)t_2t_3 - ct_1t_5 - (b - c)t_1t_6 - ct_2t_4 - (a - c)t_2t_6 - \\ &\quad (b - c)t_3t_4 - (a - c)t_3t_5 + ct_4t_5 + (b - c)t_4t_6 + (a - c)t_5t_6 + \text{terms of degree} \leq 1. \end{aligned} \quad (4.5)$$

Note that the standard (univariate) σ -dimension polynomial $\omega_{\eta|K}(t)$ of the extension L/K associated with the σ -generator η (see [6] or [5, Theorem 6.4.1]), which is equal to the Kolchin polynomial of the set $\{(a, b)\} \subset \mathbb{N}^2$, is as follows.

$$\omega_{\eta|K}(t) = \binom{t+3}{3} - \binom{t+3-(a+b)}{2} = \frac{1}{2}(a+b)t^2 + \text{terms of degree} \leq 1.$$

This polynomial carries two invariants of the extension L/K , $\deg \omega_{\eta|K} = 2$ and the leading coefficient $a+b$. At the same time, according to Theorem 4.1, the numbers c , $2b-c$ and $2a-c$ are invariants of the dimension polynomial (4.5). Thus, the dimension polynomial (4.5) gives all three parameters a , b and c of the defining equation (4.4) while $\omega_{\eta|K}(t)$ gives just the sum $a+b$.

In [13], the author introduced a bivariate dimension polynomial $\psi_{\eta|K}(t_1, t_2)$ that describes the transcendence degrees of intermediate fields $K(\{\alpha_1^{k_1} \dots \alpha_m^{k_m} \eta_j \mid s \leq \sum_{i=1}^m k_i \leq r, 1 \leq j \leq n\})$ of the extension $K\langle \eta_1, \dots, \eta_n \rangle/K$ for all sufficiently large $r, s \in \mathbb{N}$ with $s < r$. The computation of this polynomial in the case of the σ -field extension $L = K\langle \eta \rangle$ with the defining equation (4.4) gives the following result (we use Theorem 4.1 of [13]):

$$\begin{aligned} \psi_{\eta|K}(t_1, t_2) &= \left[\binom{t_1+3}{3} - \binom{t_1+2-(a+b)}{3} \right] - \left[\binom{t_2+3}{3} - \binom{t_2+2-(a+b)}{3} \right] - \\ &\quad \left(\binom{t_2+3}{3} + \binom{t_2+2-c}{3} \right) = \frac{1}{2}(a+b+1)t_1^2 - \frac{1}{2}(c+1)t_2^2 + \text{terms of total degree at most 1.} \end{aligned}$$

By [13, Theorem 4.1], the polynomial $\psi_{\eta|K}(t_1, t_2)$ carries three invariants of the extension L/K , $\deg \psi_{\eta|K} = 2$, $a+b$, and c . We see that this polynomial does not give all the parameters a, b, c of the equation (4.4) while the polynomial $\phi_{\eta|K}(t_1, \dots, t_6)$ carries all these parameters.

The univariate difference dimension polynomial and the bivariate difference dimension polynomial introduced in [13] are defined without using partitions of the basic sets of translations. The multivariate σ -dimension polynomial given by Theorem 1.1 is associated with such a partition. The following example illustrates that in this case our $2p$ -dimension polynomial carries more invariants of the corresponding σ -field extension than the p -variate σ -dimension polynomial introduced by Theorem 1.1.

Example 3 Let K be a difference (σ -) field with a basic set of endomorphisms $\sigma = \{\alpha_1, \alpha_2\}$ considered together with its partition $\sigma = \{\alpha_1\} \cup \{\alpha_2\}$. Let $L = K\langle \eta \rangle$ be a σ -field extension with the defining equation

$$\alpha_1^a \eta + \alpha_2^b \eta + \alpha_1^c \eta = 0 \quad (4.6)$$

where $a, b, c \in \mathbb{N}$, $a > b > c > 0$. Then the computation of the bivariate σ -dimension polynomial $\chi_{\eta|K}(t_1, t_2)$ (see Theorem 1.1) using the method of [13] and the computation of the 4-variate σ -dimension polynomial $\phi_{\eta|K}(t_1, t_2, t_3, t_4)$ (using the evaluation of the set $\text{Card } U_{\eta}(\bar{r}, \bar{s})$, as it is done in the proof of Theorem 2.3 and in Example 2) give the following.

$$\chi_{\eta|K}(t_1, t_2) = bt_1 + at_2 + a + b - ab$$

and

$$\phi_{\eta|K}(t_1, t_2, t_3, t_4) = 2bt_1 + (a+c)t_2 - bt_3 - at_4 + b + c - bc.$$

Theorems 1.1 and 4.2 show that the polynomial $\chi_{\eta|K}$ carries two invariants of the extension L/K , a and b , while $\phi_{\eta|K}$ carries three such invariants, a , b and c , that is, all three parameters of the equation (4.6) (by Theorem 4.1, the coefficients of t_1 , t_2 and t_4 are invariants of the extension).

The fact that the $2p$ -dimension polynomial carry more invariants than all previously known difference dimension polynomials can be applied to the equivalence problem for algebraic difference equations. Suppose that we have two systems of algebraic σ -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 (that is, the left-hand sides of the systems 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 $\text{qf}(R/P)$ and $\text{qf}(R/P')$, respectively). These systems are said to be *equivalent* if there is a σ -isomorphism between L and L' which is identity on K . The σ -dimension polynomial introduced by Theorem 2.3 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 polynomials and the same bivariate dimension polynomials defined in [13]. As an example, consider the σ -equations

$$\alpha_1^a \alpha_2^b y + \alpha_1^a y + \alpha_2^b y + \alpha_3^c y = 0 \quad (4.7)$$

and

$$\alpha_1^d \alpha_2^e y + \alpha_1^d y + \alpha_2^e y + \alpha_3^c y = 0 \quad (4.8)$$

where $a, b, c, d, e \in \mathbb{N}$, $a > b > c > 0$, $d > e > c$, $a + b = d + e$, and $a \neq d$.

The invariants carried by standard (univariate) σ -dimension polynomials associated with these equations (the equation (4.7) is considered in Example 2) are the same, 2 and $a + b = d + e$. The invariants carried by the bivariate dimension polynomials defined in [13] are also the same, 2, $a + b = d + e$, and c (see Example 2). At the same time, the 6-variate dimension polynomials for these equations carry invariants a , b , c , and d , e , c , respectively (these 6-variate dimension polynomials are of the form (4.5)). Thus, the systems (4.7) and (4.8) are not equivalent, even though the corresponding σ -field extensions have the same invariants carried by the univariate and bivariate (in the sense of [13]) σ -dimension polynomials.

Acknowledgements This research was supported by the NSF grant CCF-2139462.

References

1. Cohn, R.M.: Difference Algebra. Interscience, New York (1965)

2. Einstein, A.: The Meaning of Relativity. Appendix II (Generalization of gravitation theory), 4th ed. Princeton, 133–165
3. Kolchin, E.R.: The notion of dimension in the theory of algebraic differential equations. *Bull. Am. Math. Soc.* **70**, 570–573 (1964)
4. Kolchin, E.R.: *Differential Algebra and Algebraic Groups*. Academic Press, Boston (1973)
5. Kondratyeva, M. V., Levin, A. B., Mikhalev, A. V., Pankratev, E. V.: *Differential and Difference Dimension Polynomials*, Kluwer Acad. Publ (1998)
6. Levin, A.B.: Characteristic polynomials of filtered difference modules and difference field extensions. *Russ. Math. Surv.* **33**(3), 165–166 (1978)
7. Levin, A.B.: Characteristic polynomials of inversive difference modules and some properties of inversive difference dimension. *Russ. Math. Surv.* **35**(1), 217–218 (1980)
8. Levin, A. B.: Computation of the Strength of Systems of Difference Equations via Generalized Gröbner Bases. In: *Gröbner Bases in Symbolic Analysis*, Walter de Gruyter. Berlin–New York, pp. 43–73 (2007)
9. Levin, A.B.: *Difference Algebra*. Springer, New York (2008)
10. Levin, A.B.: Multivariate dimension polynomials of inversive difference field extensions. *Lect. Notes Comput. Sci.* **8372**, 146–163 (2014)
11. Levin, A.B.: Multivariable difference dimension polynomials. *J. Math. Sci.* **131**(6), 6060–6082 (2005)
12. Levin, A.B.: Groebner bases with respect to several orderings and multivariable dimension polynomials. *J. Symb. Comput.* **42**, 561–578 (2007)
13. Levin, A.B.: A new type of difference dimension polynomials, *Math. Comput. Sci.*, 16, no. 4, article 20, 13 pp (2022)
14. Levin, A.B.: Reduction with respect to the effective order and a new type of dimension polynomials of difference modules. In: *Proceedings of ISSAC 2022*. ACM Press, New York, 55–62 (2022)
15. Levin, A.B., Mikhalev, A.V.: Type and dimension of finitely generated G-algebras. *Contemp. Math.* **184**, 275–280 (1995)
16. Mikhalev, A.V., Pankratev, E.V.: Differential dimension polynomial of a system of differential equations, *Algebra (collection of papers)*, Moscow State Univ. Press, 57–67 (1980)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.