A New Type of Dimension Polynomials of Inversive Difference Field Extensions

Alexander Levin
levin@cua.edu
The Catholic University of America
Washington, D. C. 20064, USA

ABSTRACT

We introduce a reduction of inversive difference polynomials that is associated with a partition of the basic set of automorphisms and uses a generalization of the concept of effective order of a difference polynomial. Then we develop the corresponding method of characteristic sets and apply it to prove the existence and obtain a method of computation of multivariate dimension polynomials that describe the transcendence degrees of intermediate fields of finitely generated inversive difference field extensions obtained by adjoining transforms of the generators whose orders with respect to the components of the partition of the basic set 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 its difference generators) than standard (univariate) difference dimension polynomials. We also show how the obtained results can be applied to the equivalence problem for systems of algebraic difference equations.

CCS CONCEPTS

• **Computing methodologies → Symbolic and algebraic manipulation**.

KEYWORDS

Inversive difference polynomial; dimension polynomial; reduction; effective order; characteristic set

ACM Reference Format:

Alexander Levin. 2024. A New Type of Dimension Polynomials of Inversive Difference Field Extensions. In *International Symposium on Symbolic and Algebraic Computation (ISSAC '24), July 16–19, 2024, Raleigh, NC, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3666000.3669683

1 INTRODUCTION

The role of difference dimension polynomials in difference algebra is similar to the role of Hilbert polynomials in commutative algebra and algebraic geometry, as well as to the role of Kolchin differential dimension polynomials in the study of differential field extensions and algebraic differential equations. In particular, as it is shown in [7] (see also [8, Chapter 7]), the univariate difference dimension polynomial of a system of algebraic difference equations expresses its A. Einstein's strength, that is, the difference counterpart of the concept of strength of a system of partial differential equations introduced in [3]. Furthermore, the important role of difference dimension polynomials is determined by at least three more factors. First, a difference dimension polynomial of a finitely generated difference field extension (or of a system of algebraic difference equations defining such an extension) carries certain invariants, i.e., characteristics of the extension that do not change when we switch to another system of difference generators (with the corresponding change of the defining equations), see [5, Chapter 6] and [8, Chapter 4]. In this connection, one should mention the results on multivariate difference dimension polynomials associated with partitions of the basic set of translations, see [7], [10], and [8, Chapter 3]. They carry more invariants than their univariate counterparts. (See also [2], [12], [15], and [18] where the results on difference dimension polynomials are generalized to the difference-differential case.) Second, properties of difference dimension polynomials associated with prime difference polynomial ideals give a powerful tool in the dimension theory of difference algebras, see [5, Chapter 7], [8, Section 4.6], [11] and [17]. Finally, the results on difference dimension polynomials can be naturally extended to algebraic and differential algebraic structures with a finitely generated commutative group action, see [9], [13], [14] and [16].

In this paper we introduce a reduction of inversive difference polynomials that is associated with a fixed partition of the set of basic translations and takes into account the effective orders of the 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 of inversive difference polynomials that are associated with the introduced reduction and use their properties to prove the existence of a multivariate dimension polynomial of a finitely generated inversive 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 partition lie between 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, i. e., numerical characteristics of the extension that are carried by any its dimension polynomials and that do not depend on the system of difference generators the polynomial is associated with. Our Theorem 4.2 shows that the introduced dimension polynomials carry more invariants of the corresponding inversive difference field extensions than the univariate difference dimension polynomials introduced in [6] and their multivariate counterparts defined in [10]. Note that while the study of difference algebraic structures deals with power products

ISSAC '24, July 16–19, 2024, Raleigh, NC, USA

ACM ISBN 979-8-4007-0696-7/24/07
https://doi.org/10.1145/3666000.3669683

of translations with nonnegative exponents, inversive difference rings are considered together with the free commutative group generated by basic automorphisms. Therefore, while the dimension theory of difference rings and modules is close to its differential counterpart, the study of inversive difference algebraic structures (including the study of their dimensional characteristics) encounters many problems caused by the fact that one has to consider negative powers of translations.

2 PRELIMINARIES

Throughout the paper, $\mathbb{N}$, $\mathbb{Z}_{\leq 0}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{Q}[t_1, \dots, t_p]$ denote the sets of all non-negative integers, non-positive integers, integers, rational numbers, real numbers, and the ring of polynomials in variables $t_1, \dots, t_p$ over $\mathbb{Q}$, respectively. As usual, $\binom{t+i}{i}$ will denote the polynomial $(t+i)(t+i-1)\dots(t+1)/i! \in \mathbb{Q}[t]$. If S is a finite set, then $\operatorname{Card} S$ denotes the number of its elements. If $m \in \mathbb{N}$, $m > 0$, then, $\leq_P$ 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 $i = 1, \dots, m$. The lexicographic order will be denoted by $\leq_{\text{lex}}$.

By a *difference ring* we mean a commutative ring R with unity together with a finite set $\sigma = \{\alpha_1, \dots, \alpha_m\}$ of mutually commuting injective endomorphisms of R called *translations* (every ring homomorphism is unitary, that is, it maps unity to unity). 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, every field is supposed to have characteristic zero. If all translations of R are automorphisms, we set $\sigma^* = \{\alpha_1, \dots, \alpha_m, \alpha_1^{-1}, \dots, \alpha_m^{-1}\}$ and say that R is an *inversive difference ring* or a σ^*-ring. In this case, Γ will denote the free commutative group of all power products $\gamma = \alpha_1^{k_1} \dots \alpha_m^{k_m}$ where $k_i \in \mathbb{Z}$ $(1 \leq i \leq m)$. The *order* of γ is defined as $\operatorname{ord} \gamma = \sum_{i=1}^{m} |k_i|$; furthermore, for every $r \in \mathbb{N}$, we set $\Gamma(r) = \{\gamma \in \Gamma \mid \operatorname{ord} \gamma \leq r\}$. If a difference (respectively, inversive difference) ring R is a field, it is called a *difference* (or σ-) field (respectively, an *inversive difference* (or σ^*-) field).

A subring (ideal) R_0 of a σ-ring R is said to be a difference (or σ-) subring of R (respectively, difference (or σ-) ideal of R) if R_0 is closed with respect to the action of any $\alpha_i \in \sigma$. A σ-ideal I of R is called *reflexive* if the inclusion $\alpha_i(a) \in I$ $(a \in R,\ \alpha_i \in \sigma)$ implies that $a \in I$. (If R is a σ^*-ring, it means that I is closed with respect to every automorphism from σ^*). If a prime ideal P of R is also a σ-ideal, it is called a *prime difference* (or σ-) *ideal* of R. If R is a σ^*-ring and P is reflexive, it is referred to as a prime σ^*-ideal of R.

If R is a σ-ring and $S \subseteq R$, then the intersection I of all σ-ideals of R containing the set S is the smallest σ-ideal of R containing S; it is denoted by $[S]$. If the set S is finite, $S = \{a_1, \dots, a_r\}$, we say that the σ-ideal I is finitely generated (we write this as $I = [a_1, \dots, a_r]$) and call $a_1, \dots, a_r$ difference (or σ-) generators of I. If R is inversive, then the smallest σ^*-ideal I of R containing a subset S of R is denoted by $[S]^*$. Elements of the set S are called σ^*-generators of this ideal; if $S = \{a_1, \dots, a_r\}$, we write $I = [a_1, \dots, a_r]^*$, say that the σ^*-ideal I is finitely generated and call $a_1, \dots, a_r$ its σ^*-generators. Clearly, $[S]^*$ is generated, as an ideal, by the set $\{\gamma(a) \mid a \in S,\ \gamma \in \Gamma\}$. (In what follows we will often write γa instead of $\gamma(a)$.)

If R is a σ^*-ring, then an expression of the form $\sum_{\gamma \in \Gamma} a_\gamma \gamma$, where $a_\gamma \in R$ for any $\gamma \in \Gamma$ and only finitely many elements a_γ are different from 0, is called a σ^**-operator* over R. It is an endomorphism of the additive group of R; if $C = \sum_{\gamma \in \Gamma} a_\gamma \gamma$ and $f \in R$, then $C(f) = \sum_{\gamma \in \Gamma} a_\gamma \gamma(f)$. Two σ^*-operators $\sum_{\gamma \in \Gamma} a_\gamma \gamma$ and $\sum_{\gamma \in \Gamma} b_\gamma \gamma$ are considered to be equal if and only if $a_\gamma = b_\gamma$ for any $\gamma \in \Gamma$. The set of all σ^*-operators over R will be denoted by $\mathcal{E}_R$. This set, which has a natural structure of an R-module generated by Γ, becomes a ring if one sets $\gamma a = \gamma(a)\gamma$ for any $a \in R$, $\gamma \in \Gamma$ and extends this rule to the multiplication of any two σ^*-operators by distributivity. The resulting ring $\mathcal{E}_R$ 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 $C_1, \dots, C_q \in \mathcal{E}_R$.

If L is a σ-field and its subfield K is also a σ-subring of L, then K is said to be a σ-subfield of L; L, in turn, is called a σ-field extension or a σ-overfield of K. We also say that we have a σ-field extension L/K. If L is inversive and $\alpha(K) \subseteq K$ for any $\alpha \in \sigma^*$, we say that K is an inversive difference (or σ^*-) subfield of L or that we have a σ^*-field extension L/K. In the last case, if $S \subseteq L$, then the smallest σ^*-subfield of L containing K and S is denoted by $K\langle S\rangle^*$. S is said to be the set of σ^**-generators* of $K\langle S\rangle^*$ over K. If the set S is finite, $S = \{\eta_1, \dots, \eta_n\}$, we say that L/K is a finitely generated σ^*-field extension. As a field, $L\langle S\rangle^* = K(\{\gamma a \mid \gamma \in \Gamma,\ a \in S\})$.

Let R and R' 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 R' 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 $\phi : R \longrightarrow R'$ is called a *difference* (or σ-) *homomorphism* if $\phi(\alpha a) = \alpha\phi(a)$ for any $\alpha \in \sigma$, $a \in R$. Clearly, the kernel of such a mapping is a reflexive difference ideal of R.

In what follows we deal with inversive difference (σ^*-) rings and fields. If R is such a ring and $Y = \{y_1, \dots, y_n\}$ is a finite set of symbols, we can consider the polynomial ring $R[\Gamma Y]$, where ΓY denotes the set of symbols $\{\gamma y_j | \gamma \in \Gamma, 1 \leq j \leq n\}$, as a σ^*-ring containing R as its σ^*-subring. The corresponding σ^*-ring extension is defined by setting $\alpha(\gamma y_j) = (\alpha\gamma) y_j$ for any $\alpha \in \sigma^*$, $\gamma \in \Gamma$, $1 \leq j \leq n$; it is denoted by $R\{y_1, \dots, y_n\}^*$ and called the ring of inversive difference (or σ^*-) polynomials in σ-indeterminates $y_1, \dots, y_n$ over R. A σ^*-ideal of $R\{y_1, \dots, y_n\}^*$ is called *linear* if it is generated (as a σ^*-ideal) by homogeneous linear σ^*-polynomials, that is, σ^*-polynomials of the form $\sum_{i=1}^{d} a_i \gamma_i y_{k_i}$ $(a_i \in R,\ \gamma_i \in \Gamma,$ $1 \leq k_i \leq n$ for $i = 1, \dots, d)$. It is shown in [8, Proposition 2.4.9] that if R is a σ^*-field, then a linear σ^*-ideal of $R\{y_1, \dots, y_n\}^*$ is prime.

If K is a σ^*-field, $f \in K\{y_1, \dots, y_n\}^*$ and $\eta = (\eta_1, \dots, \eta_n)$ is an n-tuple with coordinates in a σ^*-overfield of K, then $f(\eta)$ (or $f(\eta_1, \dots, \eta_n)$) denotes the result of the replacement of every entry γy_i in f with $\gamma\eta_i$ $(\gamma \in \Gamma,\ 1 \leq i \leq n)$. 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 $P = \operatorname{Ker} \pi$ is a prime σ^*-ideal of R called the *defining ideal* of the extension L/K. In this case, L is isomorphic to the σ-field $\operatorname{qf}(R/P)$, 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 in some σ^*-overfield of K. We say that $\mathcal{U}$ is σ*-algebraically dependent* over K, if the family $\Gamma\mathcal{U} = \{\gamma(u) \mid \gamma \in \Gamma,\ u \in \mathcal{U}\}$ is algebraically dependent over K. Otherwise, the family $\mathcal{U}$ is said to be σ*-algebraically independent* over K. If L is a σ^*-overfield of 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 $K\langle B\rangle^*$ (that is, the set $\{\gamma a \mid \gamma \in \Gamma\}$ is algebraically dependent over $K\langle B\rangle^*$). 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 [8, 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 σ-tr. $\deg_K L$.

The following theorem, whose prove can be found in [5, Section 6.4], introduces the (univariate) dimension polynomial of a finitely generated inversive difference field extension.

Theorem 2.1. *Let $L = K\langle \eta_1, \dots, \eta_n\rangle^*$ be a σ^*-field extension of a σ^*-field K generated by a finite set $\eta = \{\eta_1, \dots, \eta_n\}$. Then there exists a polynomial $\phi_{\eta|K}(t) \in \mathbb{Q}[t]$ such that*

(i) *$\phi_{\eta|K}(r) = \text{tr.}\deg_K K(\{\gamma\eta_j \mid \gamma \in \Gamma(r), 1 \le j \le n\})$ for all sufficiently large $r \in \mathbb{N}$;*

(ii) *$\deg \phi_{\eta|K} \le m$, where $m = \operatorname{Card}\sigma$, and $\phi_{\eta|K}(t)$ can be written as $\phi_{\eta|K}(t) = \sum_{i=0}^{m} a_i\binom{t+i}{i}$ where $a_0, \dots, a_m \in \mathbb{Z}$ and $2^m | a_m$.*

(iii) *$d = \deg \phi_{\eta|K}$, a_m and a_d do not depend on the set of σ^*-generators η (if $d < m$, $a_d \ne a_m$). Moreover, $\dfrac{a_m}{2^m} = \sigma\text{-tr.}\deg_K L$.*

(iv) *If the elements $\eta_1, \dots, \eta_n$ are σ-algebraically independent over K, then $\phi_{\eta|K}(t) = n\sum_{k=0}^{m}(-1)^{m-k}2^k\binom{n}{k}\binom{t+k}{k}$.*

The polynomial $\phi_{\eta|K}(t)$ is called the σ^*-*dimension polynomial* of the σ^*-field extension L/K associated with the system of σ^*-generators η. Methods and algorithms for computation of such polynomials can be found in [5].

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

In what follows we give some results on numerical polynomials associated with subsets of $\mathbb{Z}^m$ (m is a positive integer). The proofs of the corresponding statements can be found in [5, Chapter 2].

Definition 2.2. *A polynomial $f(t_1, \dots, t_p) \in \mathbb{Q}[t_1, \dots, t_p]$ is called* **numerical** *if $f(r_1, \dots, r_p) \in \mathbb{Z}$ for all sufficiently large $(r_1, \dots, r_p) \in \mathbb{N}^p$. (That is, there exist $s_1, \dots, s_p \in \mathbb{N}$ such that $f(r_1, \dots, r_p) \in \mathbb{Z}$ for all $(r_1, \dots, r_p) \in \mathbb{N}^p$ with $r_1 \ge s_1, \dots, r_p \ge s_p$.)*

Polynomials in $\mathbb{Z}[t_1, \dots, t_p]$ and polynomials $\prod_{i=1}^{p}\binom{t_i}{m_i}$ with $m_1, \dots, m_p \in \mathbb{N}$ are examples of numerical polynomials in p variables. The following theorem proved in [5, Chapter 2] gives the "canonical" representation of such polynomials.

Theorem 2.3. *Let $f(t_1, \dots, t_p)$ be a numerical polynomial in p variables and $m_i = \deg_{t_i} f$ $(1 \le i \le p)$. Then this polynomial can be represented in the form*

$$f(t_1, \dots t_p) = \sum_{i_1=0}^{m_1} \dots \sum_{i_p=0}^{m_p} a_{i_1\dots i_p}\binom{t_1+i_1}{i_1}\dots\binom{t_p+i_p}{i_p} \qquad (1)$$

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

In what follows we deal with subsets of $\mathbb{Z}^m$. Also, we fix a partition of the set $\mathbb{N}_m = \{1, \dots, m\}$ into p disjoint subsets ($p \ge 1$):

$$\mathbb{N}_m = \Delta_1 \cup \Delta_2 \cup \dots \Delta_p \qquad (2)$$

where $\Delta_1 = \{1, \dots, m_1\}$, $\Delta_2 = \{m_1{+}1, \dots, m_1{+}m_2\}, \dots, \Delta_p = \{m_1 + \dots + m_{p-1}{+}1, \dots, m\}$ ($m_i = \operatorname{Card}\Delta_i$ for $i = 1, \dots, p$; $m_1 + \dots + m_p = m$). If $a = (a_1, \dots, a_m) \in \mathbf{Z}^m$, 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 $\operatorname{ord}_1 a, \dots, \operatorname{ord}_p a$, respectively; $\operatorname{ord}_k a$ $(1 \le k \le p)$ is called the *order of a with respect to Δ_k*). Furthermore, we consider the set $\mathbb{Z}^m$ as the union

$$\mathbb{Z}^m = \bigcup_{1 \le j \le 2^m} \mathbb{Z}_j^{(m)} \qquad (3)$$

where $\mathbb{Z}_1^{(m)}, \dots, \mathbb{Z}_{2^m}^{(m)}$ are all distinct Cartesian products of m sets each of which is either $\mathbb{N}$ or $\mathbb{Z}_{\le 0}$. We assume that $\mathbb{Z}_1^{(m)} = \mathbb{N}$ and call $\mathbb{Z}_j^{(m)}$ the j*th orthant* of $\mathbb{Z}^m$ $(1 \le j \le 2^m)$.

The set $\mathbb{Z}^m$ will be considered as a partially ordered set with the order $\trianglelefteq$ such that $(e_1, \dots, e_m) \trianglelefteq (e'_1, \dots, e'_m)$ if and only if $(e_1, \dots, e_m)$ and $(e'_1, \dots, e'_m)$ lie in the same orthant and $(|e_1|, \dots, |e_m|) \le_P (|e'_1|, \dots, |e'_m|)$.

If $A \subseteq \mathbb{Z}^m$, then W_A will denote the set of all elements of $\mathbb{Z}^m$ that do not exceed any element of A with respect to $\trianglelefteq$. Furthermore, for any $r_1, \dots, r_p \in \mathbb{N}$, $A(r_1, \dots, r_p)$ will denote the set of all elements $x = (x_1, \dots, x_m) \in A$ such that $\operatorname{ord}_i x \le r_i$ $(i = 1, \dots, p)$.

Theorem 2.4. *[5, Theorem 2.5.5] Let $A \subseteq \mathbb{Z}^m$ and let partition (2) of the set $\mathbb{N}_m$ be fixed. Then there exists a numerical polynomial in p variables $\phi_A(t_1, \dots, t_p)$ such that*

(i) *$\phi_A(r_1, \dots, r_p) = \operatorname{Card} W_A(r_1, \dots, r_p)$ for all sufficiently large p-tuples $(r_1, \dots, r_p) \in \mathbb{N}^p$.*

(ii) *$\deg \phi_A \le m$ and $\deg_{t_i}\phi_A \le m_i$ $(1 \le i \le p)$. Furthermore, if $\phi_A(t_1, \dots, t_p)$ is written in the form (1), then $2^m | a_{m_1\dots m_p}$.*

(iii) *If $A = \emptyset$, then*

$$\phi_A(t_1, \dots, t_p) = \prod_{j=1}^{p}\left[\sum_{i=0}^{m_j}(-1)^{m_j-i}2^i\binom{m_j}{i}\binom{t_j+i}{i}\right]. \qquad (4)$$

The polynomial $\phi_A(t_1, \dots, t_p)$ is called the *dimension polynomial* of the set $A \subseteq \mathbb{Z}^m$ associated with partition (2) of $\mathbb{N}_m$. Algorithms for computing such polynomials can be found in [5, Chapter 2].

3 E-REDUCTION OF INVERSIVE DIFFERENCE POLYNOMIALS. E-CHARACTERISTIC SETS

Let K be an inversive difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_m\}$. Let us fix a partition of the set σ into p disjoint subsets ($p \ge 1$):

$$\sigma = \sigma_1 \bigcup \dots \bigcup \sigma_p \qquad (5)$$

where $\sigma_1 = \{\alpha_1, \dots, \alpha_{m_1}\}$, $\sigma_2 = \{\alpha_{m_1+1}, \dots, \alpha_{m_1+m_2}\}, \dots,$ $\sigma_p = \{\alpha_{m_1+\dots+m_{p-1}+1}, \dots, \alpha_m\}$ $(m_1 + \dots + m_p = m)$.

The order of an element $\gamma = \alpha_1^{k_1}\dots\alpha_m^{k_m} \in \Gamma$ with respect to σ_i $(1 \le i \le p)$ is defined as $\sum_{\nu=m_1+\dots+m_{i-1}+1}^{m_1+\dots+m_i}|k_\nu|$; it is denoted by $\operatorname{ord}_i\gamma$. If $i = 1$, the sum is $\sum_{\nu=1}^{m_1}|k_\nu|$. For any $r_1, \dots, r_p \in \mathbf{N}$, we set $\Gamma(r_1, \dots, r_p) = \{\gamma \in \Gamma \mid \operatorname{ord}_i\gamma \le r_i \ (1 \le i \le p)\}$.

Let us consider p total orderings $<_1, \dots, <_p$ of the group Γ such that $\gamma = \alpha_1^{k_1}\dots\alpha_m^{k_m} <_i \gamma' = \alpha_1^{k'_1}\dots\alpha_m^{k'_m}$ $(1 \le i \le p)$ if and only if the $(2m+p)$-tuple $(\operatorname{ord}_i\gamma, \operatorname{ord}_1\gamma, \dots, \operatorname{ord}_{i-1}\gamma, \operatorname{ord}_{i+1}\gamma, \dots, \operatorname{ord}_p\gamma,$ $|k_{m_1+\dots+m_{i-1}+1}|, \dots, |k_{m_1+\dots+m_i}|, k_{m_1+\dots+m_{i-1}+1}, \dots, k_{m_1+\dots+m_i},$ $|k_1|, \dots, |k_{m_1+\dots+m_{i-1}}|, |k_{m_1+\dots+m_i+1}, \dots, |k_m|, k_1, \dots, k_{m_1+\dots+m_{i-1}},$ $k_{m_1+\dots+m_i+1}, \dots, k_m)$ is less than the corresponding $(2m+p)$-tuple for γ' with respect to the lexicographic order on $\mathbb{Z}^{2m+p}$.

Two elements $\gamma_1 = \alpha_1^{k_1}\dots\alpha_m^{k_m}$ and $\gamma_2 = \alpha_1^{l_1}\dots\alpha_m^{l_m}$ are called *similar* if $(k_1, \dots, k_m)$ and $(l_1, \dots, l_m)$ lie in the same orthant of $\mathbb{Z}^m$.

Then we write $\gamma_1 \sim \gamma_2$. We say that γ_1 *divides* γ_2 (or γ_2 is a *multiple* of γ_1) and write $\gamma_1|\gamma_2$ if $\gamma_1 \sim \gamma_2$ and $\gamma_2 = \gamma\gamma_1$ for some $\gamma \in \Gamma$, $\gamma \sim \gamma_1$.

Let $R = K\{y_1, \dots, y_n\}^*$ be the algebra of σ^*-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 $\Gamma Y = \{\gamma y_i \mid \gamma \in \Gamma, 1 \le i \le n\}$ whose elements are called *terms*. We define the order of a term $u = \gamma y_i$ with respect to σ_j (denoted by $\mathrm{ord}_j\, u$) as $\mathrm{ord}_j\, \gamma$. Furthermore, considering representation (3) of $\mathbb{Z}^m$, we set $\Gamma_j = \{\alpha_1^{k_1} \dots \alpha_m^{k_m} \in \Gamma \mid (k_1, \dots, k_m) \in \mathbb{Z}_j^{(m)}\}$ and $\Gamma_j Y = \{\gamma y_i \mid \gamma \in \Gamma_j, 1 \le i \le n\}$.

Terms $u = \gamma y_i$ and $v = \gamma' y_j$ are called *similar* if $\gamma \sim \gamma'$; in this case we write $u \sim v$. If $u = \gamma y_i$ is a term and $\gamma' \in \Gamma$, we say that u is similar to γ' and write $u \sim \gamma'$ if $\gamma \sim \gamma'$. Clearly, if $u \in \Gamma Y$, $\gamma \in \Gamma$ and $\gamma \sim u$, then $\mathrm{ord}_j(\gamma u) = \mathrm{ord}_j\, \gamma + \mathrm{ord}_j\, u$ for $j = 1, \dots, p$. Furthermore, if $u, v \in \Gamma Y$, we say that u *divides* v (or v is a *transform* or a *multiple* of u) and write $u \mid v$, if $u = \gamma' y_i$, $v = \gamma'' y_i$ for some y_i and $\gamma'|\gamma''$. (If $\gamma'' = \gamma\gamma'$ for some $\gamma \in \Gamma$, $\gamma \sim \gamma'$, we write $\frac{v}{u}$ for γ.)

We consider p orders $<_1, \dots, <_p$ on the set ΓY that correspond to the orders on the group Γ (we use the same symbols for the orders on Γ and ΓY). These orders are defined as follows: $\gamma y_j <_i \gamma' y_k$ if and only if $\gamma <_i \gamma'$ in Γ or $\gamma = \gamma'$ and $j < k$ $(1 \le i \le p,\ 1 \le j, k \le n)$.

Definition 3.1. *Let $f \in K\{y_1, \dots, y_n\}^* \setminus K$ and $1 \le k \le p$. Then the greatest with respect to $<_k$ term 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 3.2. *Let $f \in K\{y_1, \dots, y_n\} \setminus K$ and let $u_f^{(k)}$ and $v_f^{(k)}$ be the k-leader and k-coleader of f, respectively $(1 \le k \le p)$. Then the nonnegative integer $\mathrm{ord}_k\, u_f^{(k)} - \mathrm{ord}_k\, v_f^{(k)}$ is called the k**th effective order** of f; it is denoted by $\mathrm{Eord}_k\, f$.*

Definition 3.3. *Let $f, g \in K\{y_1, \dots, y_n\}^*$. We say that f* has lower rank than g *and write* $\mathrm{rk}\ f < \mathrm{rk}\ g$ *if either $f \in K$, $g \notin K$, or*

$$(u_f^{(1)}, \deg_{u_f^{(1)}} f, \mathrm{ord}_2\, u_f^{(2)}, \dots, \mathrm{ord}_p\, u_f^{(p)}, \mathrm{Eord}_1\, f, \dots, \mathrm{Eord}_p\, f) <_{\mathrm{lex}}$$
$$(u_g^{(1)}, \deg_{u_g^{(1)}} f, \mathrm{ord}_2\, u_g^{(2)}, \dots, \mathrm{ord}_p\, u_g^{(p)}, \mathrm{Eord}_1\, g, \dots, \mathrm{Eord}_p\, g) \tag{6}$$

($u_f^{(1)}$ and $u_g^{(1)}$ are compared with respect to the order $<_1$ on ΓY). If the two $(2p+1)$-tuples are equal (or $f, g \in K$) we say that f and g are of the same rank and write $\mathrm{rk}\, f = \mathrm{rk}\, g$.

Definition 3.4. *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 at least one of the following two conditions holds.*

(i) f does not contain $(\gamma u_g^{(1)})^e$ ($\gamma \in \Gamma$) with $\gamma \sim u_g^{(1)}$ and $e \ge d$;

(ii) f contains some $(\gamma u_g^{(1)})^e$ with $\gamma \in \Gamma$, $\gamma \sim u_g^{(1)}$, $e \ge d$, and either there is $k \in \mathbb{N}$, $2 \le k \le p$, such that $\mathrm{ord}_k\, u_{\gamma g}^{(k)} > \mathrm{ord}_k(u_f^{(k)})$ or there is $j \in \mathbb{N}$, $1 \le j \le p$, such that $\mathrm{ord}_j\, v_{\gamma g}^{(j)} < \mathrm{ord}_j(v_f^{(j)})$.

Thus, f is not E-reduced with respect to g if f contains some $(\gamma u_g^{(1)})^e$ such that $\gamma \in \Gamma$, $\gamma \sim u_g^{(1)}$, $e \ge \deg_{u_g^{(1)}} g$, $\mathrm{ord}_k\, u_{\gamma g}^{(k)} \le \mathrm{ord}_k(u_f^{(k)})$ $(2 \le k \le p)$, and $\mathrm{ord}_j\, v_{\gamma g}^{(j)} \ge \mathrm{ord}_j(v_f^{(j)})$ for $j = 1, \dots p$.

Remark 3.5. *If $f, g \in K\{y_1, \dots, y_n\}^*$ then f is reduced with respect to g in the sense of [5, Definition 3.4.22] with respect to the term ordering $<_1$, if condition (i) of the last definition holds. Clearly, in this case f is E-reduced with respect to g as well.*

Remark 3.6. *It follows from [18, Lemma 3.3] that for all $f \in R = K\{y_1, \dots, y_n\}^*$, $j \in \{1, \dots, 2^m\}$ and $k \in \{1, \dots, p\}$, there exist terms u_{fjk} and v_{fjk} in f such that for all elements $\gamma = \alpha_1^{k_1} \dots \alpha_m^{k_m} \in \Gamma_j$ with sufficiently large $(|k_1|, \dots, |k_m|) \in \mathbb{N}^m$ (in the sense of Definition 2.2), one has $u_{\gamma f}^{(k)} = \gamma u_{fjk}$ and $v_{\gamma f}^{(k)} = \gamma v_{fjk}$. Therefore, if $f \in R$ and $u_f^{(1)} = \gamma_1 y_k$ where $\gamma_1 \in \Gamma_j$ $(1 \le j \le 2^m)$, then there exist $a_{if}, b_{kf} \in \mathbb{Z}$ $(2 \le i \le p, 1 \le k \le p)$ such that for any such $\gamma \in \Gamma_j$, $\mathrm{ord}_i\, u_{\gamma f}^{(i)} = \mathrm{ord}\, \gamma + a_{if}$ and $\mathrm{ord}_k\, v_{\gamma f}^{(k)} = \mathrm{ord}\, \gamma + b_{kf}$.*

Proposition 3.7. *If $f, g \in K\{y_1, \dots, y_n\}^*$ and $\mathrm{rk}\, f < \mathrm{rk}\, g$, 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 $(\gamma u_g^{(1)})^e$ where $\gamma \in \Gamma$, $\gamma \sim u_g^{(1)}$, $e \ge d = \deg_{u_g^{(1)}} g$ (hence $\gamma = 1$, since otherwise $u_g^{(1)} <_1 \gamma u_g^{(1)} \le_1 u_f^{(1)}$ that contradicts the condition (6) for $\mathrm{rk}\, f < \mathrm{rk}\, g$), and also $\mathrm{ord}_k\, u_g^{(k)} \le \mathrm{ord}_k\, u_f^{(k)}$ for $k = 2, \dots, p$ and $\mathrm{ord}_k\, v_g^{(k)} \ge \mathrm{ord}_k\, v_f^{(k)}$ for $k = 1, \dots, p$. Then $\mathrm{Eord}_k\, g \le \mathrm{Eord}_k\, f$ $(1 \le k \le p)$, contrary to the inequality $\mathrm{rk}\, f < \mathrm{rk}\, g$. Therefore, f is E-reduced with respect to g. □

Proposition 3.8. *Let $\mathcal{A} = \{g_1, \dots, g_t\}$ be a finite set of σ^*-polynomials in the ring $R = K\{y_1, \dots, y_n\}^*$ and let $u_k^{(i)}$ denote the i-leader of g_k $(1 \le k \le t, 1 \le i \le p)$. Let $d_k = \deg_{u_k^{(1)}} g_k$ and let I_k be the coefficient of $(u_k^{(1)})^{d_k}$ when g_k is written as a polynomial in $u_k^{(1)}$ $(1 \le k \le t)$. Furthermore, let $I(\mathcal{A}) = \{f \in R \mid$ either $f = 1$ or f is a product of finitely many σ^*-polynomials of the form $\gamma(I_k)$ $(\gamma \in \Gamma, k = 1, \dots, t)\}$. Then for any $h \in R$, there exist $J \in I(\mathcal{A})$ and $\overline{h} \in R$ such that $\overline{h}$ is E-reduced with respect to $\mathcal{A}$ and $Jh \equiv \overline{h} (mod\ [\mathcal{A}]^*)$ (that is, $Jh - \overline{h} \in [\mathcal{A}]^*$).*

Proof. If h is E-reduced with respect to $\mathcal{A}$, one can set $\overline{h} = h$. 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 $\gamma u_{g_k}^{(1)}$ with $\gamma \in \Gamma, \gamma \sim u_{g_k}^{(1)}$, $(1 \le k \le t)$ such that f contains $(\gamma u_k^{(1)})^e$ with $e \ge d_k$, $\mathrm{ord}_i\, u_{\gamma g_k}^{(i)} \le \mathrm{ord}_i\, u_f^{(i)}$ for $i = 2, \dots, p$, and $\mathrm{ord}_j\, v_{\gamma g_k}^{(i)} \ge \mathrm{ord}_j\, v_f^{(j)}$ 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 $w_h = \gamma u_k^{(1)}$ for some $k \in \{1, \dots, t\}$ and $\gamma \in \Gamma$ such that $\gamma \sim u_{g_k}^{(1)}$, $d \ge d_k$, $\mathrm{ord}_i\, u_{\gamma g_k}^{(i)} \le \mathrm{ord}_i\, u_h^{(i)}$ $(2 \le i \le p)$, and $\mathrm{ord}_j\, v_{\gamma g_k}^{(j)} \ge \mathrm{ord}_j\, v_h^{(j)}$ $(1 \le j \le p)$. Let us choose such k that corresponds to the maximum (with respect to $<_1$) 1-leader $u_i^{(1)}$ $(1 \le i \le t)$ and consider the σ^*-polynomial $h' = \gamma(I_k)h - c_h w_h^{d-d_k}(\gamma g_k)$. Clearly, $\deg_{w_h} h' < \deg_{w_h} h$ and h' does not contain any $\mathcal{A}$-leader $\gamma' u_\nu^{(1)}$ $(\gamma' \in \Gamma, 1 \le \nu \le t)$ that is greater than w_h with respect to $<_1$ (such a term cannot appear in $\gamma(I_k)h$ or γg_k, since $u^{(1)}_{\gamma g_k} = \gamma u^{(1)}_{g_k} = w_h$). Applying the same procedure to h' and continuing in the same way, we will arrive at a σ-polynomial $\overline{h} \in R$ such that $\overline{h}$ is E-reduced with respect to $\mathcal{A}$ and $Jh - \overline{h} \in [\mathcal{A}]^*$ for some $J \in I(\mathcal{A})$. □

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

Algorithm 3.9. *$(h, t, g_1, \dots, g_t;\ \overline{h})$*

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

Begin

$C_1 := 0, \dots, C_t := 0, \overline{h} := h$

While *there exist k, $1 \le k \le t$, and a term w that appears in $\overline{h}$ with a (nonzero) coefficient c_w, such that $u^{(1)}_{g_k} \mid w$, $\deg_{u^{(1)}_{g_k}} g_k \le \deg_w \overline{h}$, $\mathrm{ord}_i(\gamma_{kw} u^{(i)}_{g_k}) \le \mathrm{ord}_i\, u^{(i)}_{\overline{h}}$ for $i = 2, \dots, p$, where $\gamma_{kw} = \frac{w}{u^{(1)}_{g_k}}$, and $\mathrm{ord}_j(\gamma_{kw} v^{(j)}_{g_k}) \ge \mathrm{ord}_j\, v^{(j)}_{\overline{h}}$ 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 $u^{(1)}_{g_k}$ is the greatest (with resect to $<_1$) 1-leader of an element of $\mathcal{A}$ such that $u^{(1)}_{g_k} \mid z$, $\deg_{u^{(1)}_{g_k}} g_k \le \deg_z \overline{h}$, $\mathrm{ord}_i(\gamma_{kz} u^{(i)}_{g_k}) \le \mathrm{ord}_i\, u^{(i)}_{\overline{h}}$ for $i = 2, \dots, p$, where $\gamma_{kz} = \frac{z}{u^{(1)}_{g_k}}$, and $\mathrm{ord}_j(\gamma_{kz} v^{(j)}_{g_k}) \ge \mathrm{ord}_j\, v^{(j)}_{\overline{h}}$ for $j = 1, \dots, p$,

$J := \gamma(I_l)J$, $C_l := C_l + c_z z^{d-d_l}\gamma_{lz}$ where $d = \deg_z \overline{h}$, $d_l = \deg_{u^{(1)}_{g_l}} g_l$, and c_z is the coefficient of z^d when $\overline{h}$ is written as a polynomial in z.

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

End

Definition 3.10. *A set $\mathcal{A} \subseteq K\{y_1, \dots, y_n\}^*$ is said to be E-* **autoreduced** *if either it is empty or $\mathcal{A} \bigcap K = \emptyset$ and every element of $\mathcal{A}$ is E-reduced with respect to all other elements of the set $\mathcal{A}$.*

Example 3.11. *Let K be an inversive 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 $\mathcal{A} = \{g, h\} \subseteq K\{y\}^*$ (the ring of σ^*-polynomials in one σ^*-indeterminate y) where*

$$g = \alpha_1^3\alpha_2^{-2}y + \alpha_2^3 y + \alpha_2 y, \qquad h = \alpha_1^2\alpha_2^{-1}y + \alpha_1^{-1}\alpha_2^2 y + \alpha_1\alpha_2 y.$$

Then $u^{(1)}_g = \alpha_1^3\alpha_2^{-2}y$, $v^{(1)}_g = v^{(2)}_g = \alpha_2 y$, $u^{(2)}_g = \alpha_2^3 y$, $u^{(1)}_h = \alpha_1^2\alpha_2^{-1}y$, $v^{(1)}_h = v^{(2)}_h = \alpha_1\alpha_2 y$, and $u^{(2)}_h = \alpha_1^{-1}\alpha_2^2 y$. We see that $u^{(1)}_g$ is a transform of $u^{(1)}_h$, $u^{(1)}_g = \gamma u^{(1)}_h$ where $\gamma = \alpha_1\alpha_2^{-1} \sim u^{(1)}_h$. Furthermore, $\gamma h = \alpha_1^3\alpha_2^{-2}y + \alpha_1^2 y + \alpha_2 y$, so $u^{(1)}_{\gamma h} = u^{(2)}_{\gamma h} = \alpha_1^3\alpha_2^{-2}y$, $v^{(1)}_{\gamma h} = \alpha_2 y$, and $v^{(2)}_{\gamma h} = \alpha_1^2 y$. Thus, $\mathrm{ord}_2\, u^{(2)}_{\gamma h} = 2 < \mathrm{ord}_2\, u^{(2)}_g = 3$, $\mathrm{ord}_1\, v^{(1)}_{\gamma h} = 0 = \mathrm{ord}_1\, v^{(1)}_g$, but $\mathrm{ord}_2\, v^{(2)}_{\gamma h} = 0 < \mathrm{ord}_2\, v^{(2)}_g = 1$. Therefore, g is E-reduced with respect to h. Since h is clearly E-reduced with respect to g, $\mathcal{A} = \{g, h\}$ is an E-autoreduced set. At the same time, this set is not autoreduced in the sense of [5] where an analog of Definition 3.4 does not assume option (ii) of our definition.

Proposition 3.12. *Every E-autoreduced set is finite.*

Proof. Suppose that there is an infinite E-autoreduced set $\mathcal{A}$. Since every infinite sequence of elements of Γ contains an infinite subsequence whose elements are similar to each other (there are only finitely many orthants of $\mathbb{Z}^m$), it follows from [4, Chapter 0, Section 17] that $\mathcal{A}$ contains a sequence of σ^*-polynomials $\{f_1, f_2, \dots\}$ such that $u^{(1)}_{f_i} \mid u^{(1)}_{f_{i+1}}$ for $i = 1, 2, \dots$. Moreover, we can assume that all leaders and coleaders of σ^*-polynomials in this sequence are similar to each other. Since the sequence $\{\deg_{u^{(1)}_{f_i}} f_i\}$ cannot have an infinite decreasing subsequence, without loss of generality we can assume that $\deg_{u^{(1)}_{f_i}} f_i \le \deg_{u^{(1)}_{f_{i+1}}} f_{i+1}$ $(i = 1, 2, \dots)$.

Let $k_{ij} = \mathrm{ord}_j\, u^{(1)}_{f_i}$, $l_{ij} = \mathrm{ord}_j\, u^{(j)}_{f_i}$, $n_{ij} = \mathrm{ord}_j\, v^{(j)}_{f_i}$ $(1 \le j \le p)$. Obviously, $l_{ij} \ge k_{ij} \ge n_{ij}$ $(i = 1, 2, \dots; j = 1, \dots, p)$, 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 [4, Chapter 0, Section 17], there exists an infinite sequence $i_1 < i_2 < \dots$ such that

$$(l_{i_1 2} - k_{i_1 2}, \dots, l_{i_1 p} - k_{i_1 p}) \le_P (l_{i_2 2} - k_{i_2 2}, \dots, l_{i_2 p} - k_{i_2 p}) \le_P \dots, \quad (7)$$

$$(k_{i_1 1} - n_{i_1 1}, \dots, k_{i_1 p} - n_{i_1 p}) \le_P (k_{i_2 1} - n_{i_2 1}, \dots, k_{i_2 p} - n_{i_2 p}) \le_P \dots. \quad (8)$$

Then for $j = 2, \dots, p$ and for $\gamma_{12} = \dfrac{u^{(1)}_{f_{i_2}}}{u^{(1)}_{f_{i_1}}}$, we have (using (7)) $\mathrm{ord}_j\, u^{(j)}_{\gamma_{12} f_{i_1}} \le \mathrm{ord}_j\, \gamma_{12} + \mathrm{ord}_j\, u^{(j)}_{f_{i_1}} = k_{i_2 j} - k_{i_1 j} + l_{i_1 j} \le k_{i_2 j} + l_{i_2 j} - k_{i_2 j} = \mathrm{ord}_j\, u^{(j)}_{f_{i_2}}$. Similar arguments with the use of (8) give $\mathrm{ord}_j(\gamma_{12} v^{(j)}_{f_{i_1}}) \ge \mathrm{ord}_j\, v^{(j)}_{f_{i_2}}$ $(2 \le j \le p)$. Thus, f_{i_2} is not E-reduced with respect to f_{i_1} contrary to the fact that $\mathcal{A}$ is an E-autoreduced set. □

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

Definition 3.13. *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 $\mathrm{rk}\, \mathcal{A} < \mathrm{rk}\, \mathcal{B}$, if one of the following two cases holds:*

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

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

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

The proof of the following statement can be obtained by mimicking the proof of the corresponding theorem for differential polynomial, see [5, Proposition 3.3.37].

Proposition 3.14. *Every nonempty family of E-autoreduced sets of σ^*-polynomials contains an E-autoreduced set of lowest rank.*

Let J be any nonzero σ^*-ideal of $K\{y_1, \dots, y_n\}^*$. Since the set of all E-autoreduced subsets of J is not empty (if $0 \neq f \in J$, 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 3.15. *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. If $g \neq 0$ and rk $g <$ rk f_1, then rk $\{g\} <$ rk $\mathcal{A}$ that contradicts $\mathcal{A}$ being an E-characteristic set of J. Let rk $g >$ rk f_1 and let $f_1, \dots, f_j$ $(1 \leq j \leq d)$ be all elements of $\mathcal{A}$ whose rank is lower that the rank of g. Then $\mathcal{A}' = \{f_1, \dots, f_j, g\}$ is an E-autoreduced set and rk $\mathcal{A}' <$ rk $\mathcal{A}$, a contradiction. Thus, $g = 0$. □

The proof of the following statement can be obtained by mimicking the proof of [5, Theorem 6.5.3 and Corollary 6.5.4].

Proposition 3.16. *Let $\leq$ be a preorder on $K\{y_1, \dots, y_n\}^*$ such that $f \leq g$ if and only if $u_g^{(1)}$ is a transform of $u_f^{(1)}$. Let f be a linear σ^*-polynomial in $K\{y_1, \dots, y_n\}^* \setminus K$. Then the set of all minimal with respect to $\leq$ elements of the set $\{\gamma f \mid \gamma \in \Gamma\}$ is an E-characteristic set of the σ^*-ideal $[f]^*$.*

4 A NEW TYPE OF DIMENSION POLYNOMIALS OF σ^*-FIELD EXTENSIONS

In this section we use properties of E-characteristic sets to obtain the following result that generalizes Theorem 2.1 and introduces a new type of multivariate dimension polynomials of finitely generated σ^*-field extensions that carry more invariants than the standard (univariate) difference dimension polynomials. (By an invariant of a σ^*-field extension we mean a numerical characteristic that does not depend on the set of its σ^*-generators.) We still deal with a σ^*-field K and partition (5) of its basic set σ. 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

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

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 $s_i^{(1)} < r_i^{(0)} - s_i^{(0)}$ such that $\Phi_{\eta\,|\,K}(r_1, \dots, r_p, s_1, \dots, s_p) =$*

tr. $\deg_K K(\{\gamma\eta_j \mid \gamma \in \Gamma(r_1, \dots, r_p; s_1, \dots, s_p), 1 \leq j \leq n\})$

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 $\mathcal{A} = \{f_1, \dots, f_q\}$ an E-characteristic set of P. For any $\bar{r} = (r_1, \dots, r_p), \bar{s} = (s_1, \dots, s_p) \in \mathbb{N}^p$ with $\bar{s} \leq_P \bar{r}$, let
$W(\bar{r}, \bar{s}) = \{w \in \Gamma Y \mid s_i \leq \text{ord}_i\, w \leq r_i \text{ for } i = 1, \dots, p\}$,
$W_\eta(\bar{r}, \bar{s}) = \{w(\eta) \mid w \in W(\bar{r}, \bar{s})\}$,
$U'(\bar{r}, \bar{s}) = \{u \in \Gamma Y \mid s_i \leq \text{ord}_i\, u \leq r_i$ $(1 \leq i \leq p)$ and u is not a transform of any $u_{f_j}^{(1)}$ $(1 \leq j \leq q)\}$, $U'_\eta(\bar{r}, \bar{s}) = \{u(\eta) \mid u \in U'(\bar{r}, \bar{s})\}$,
$U''(\bar{r}, \bar{s}) = \{u \in \Gamma Y \mid s_i \leq \text{ord}_i\, u \leq r_i$ $(1 \leq i \leq p)$ and whenever $u = \gamma u_{f_j}^{(1)}$ $(\gamma \in \Gamma, \gamma \sim u_{f_j}^{(1)})$, there exists $k \in \{2, \dots, p\}$ such that $\text{ord}_k(u_{\gamma f_j}^{(k)}) > r_k$ or there exists $i \in \{1, \dots, p\}$ such that $\text{ord}_i\, v_{\gamma f_j}^{(i)} < s_i$ ("or" is inclusive)$\}$,
$U''_\eta(\bar{r}, \bar{s}) = \{u(\eta) \mid u \in U''(\bar{r}, \bar{s})\}$,
$U(\bar{r}, \bar{s}) = U'(\bar{r}, \bar{s}) \cup U''(\bar{r}, \bar{s})$ and $U_\eta(\bar{r}, \bar{s}) = U'_\eta(\bar{r}, \bar{s}) \cup U''_\eta(\bar{r}, \bar{s})$.

We will 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 $K(U_\eta(\bar{r}, \bar{s}))$ over K. First, note that $U_\eta(\bar{r}, \bar{s})$ is algebraically independent over K. Indeed, if $f(w_1(\eta), \dots, w_k(\eta)) = 0$ for some $w_1, \dots, w_k \in U(\bar{r}, \bar{s})$, 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 $w = \gamma u_{f_j}^{(1)}$, with $\gamma \sim u_{f_j}^{(1)}$, $\deg_w f \geq \deg_{u_{f_j}^{(1)}} f_j$, then $w \in U''(\bar{r}, \bar{s})$, so there exists $k \in \{2, \dots, q\}$ such that $\text{ord}_k\, u_{\gamma f_j}^{(k)} > r_k \geq \text{ord}_k\, u_f^{(k)}$ or there exists $i \in \{1, \dots, p\}$ such that $\text{ord}_i\, v_{\gamma f_j}^{(i)} < s_i \leq \text{ord}_i\, v_f^{(i)}$; "or" is inclusive). Then f is E-reduced with respect to $\mathcal{A}$.) By Proposition 3.15, $f = 0$, 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 $s_i^{(0)} = \max\{\text{Eord}_i\, f_j \mid 1 \leq j \leq q\}$ $(1 \leq i \leq p)$, then every element $\gamma\eta_k \in W_\eta(\bar{r}, \bar{s}) \setminus U_\eta(\bar{r}, \bar{s})$ $(\gamma \in \Gamma, 1 \leq k \leq n)$ is algebraic over the field $K(U_\eta(\bar{r}, \bar{s}))$. In this case, since $\gamma y_k \notin U(\bar{r}, \bar{s})$, γy_k is equal to some term $\gamma' u_{f_j}^{(1)}$ $(1 \leq j \leq q)$ where $\gamma' \in \Gamma$, $\gamma' \sim \gamma' u_j^{(1)}$, $\text{ord}_i\, u_{\gamma' f_j}^{(i)} \leq r_i$ $(2 \leq i \leq p)$, and $\text{ord}_l\, v_{\gamma' f_j}^{l} \geq s_l$ for $l = 1, \dots, p$.

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

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

where $I_0^{(j)}, I_1^{(j)}, \dots I_{d_j}^{(j)}$ do not contain $u_{f_j}^{(1)}$ (therefore, all their terms are lower than $u_{f_j}^{(1)}$ with respect to $<_1$). Since $f_j \in P$,

$$I_{d_j}^{(j)}(\eta)(u_{f_j}^{(1)}(\eta))^{d_j} + \dots + I_1^{(j)}(\eta) u_{f_j}^{(1)}(\eta) + I_0^{(j)}(\eta) = 0. \quad (9)$$

Note that $I_{d_j}^{(j)}(\eta) \neq 0$. Indeed, since rk $I_{d_j}^{(j)} <$ rk f_j, the equality $I_{d_j}^{(j)}(\eta) = 0$ would imply that $I_{d_j}^{(j)} \in P$. Then the family of all f_l with rk $f_l <$ rk $I_{d_j}^{(j)}$ and $I_{d_j}^{(j)}$ would form an E-autoreduced set in P whose rank is lower than the rank of $\mathcal{A}$, contrary to the fact that $\mathcal{A}$ is an E-characteristic set of P. Similarly, $I_\nu^{(j)} \notin P$ for $0 \leq \nu < d_j$ (and any $j = 1, \dots, q$), and since P is a σ^*-ideal, $\gamma(I_\nu^{(j)}) \notin P$ for any $I_\nu^{(j)}$, $\gamma \in \Gamma$. Therefore, if we apply γ' to both sides of (9), the resulting equality will show that the element $\gamma' u_{f_j}^{(1)}(\eta) = \gamma\eta_k$ is algebraic over the field $K(\{\tilde{\gamma}\eta_l \mid s_i \leq \text{ord}_i\, \tilde{\gamma} \leq r_i \ (1 \leq i \leq p), \tilde{\gamma} y_l <_1 \gamma' u_{f_j}^{(1)}\})$. (Note that if $I = I_\nu^{(j)}$ for some $j \in \{1, \dots, q\}$ and $\nu \in \{0, \dots, d_j\}$, then $\text{ord}_i(\gamma' u_I^{(i)}) \leq \text{ord}_i\, u_{\gamma' I}^{(i)} \leq r_i$ $(2 \leq i \leq p)$ and $\text{ord}_k(\gamma' v_I^{(k)}) \geq \text{ord}_k\, v_{\gamma' I}^{(k)} \geq s_k$ $(1 \leq k \leq p)$). By induction on the well-ordered (with respect to $<_1$) set ΓY we obtain that $U_\eta(\bar{r}, \bar{s})$ 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 $U'_\eta(\bar{r}, \bar{s})$ 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

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

By Theorem 2.4, there exists a numerical polynomial $\omega_k(t_1, \dots, t_p)$ such that $\omega_k(r_1, \dots, r_p) = \text{Card}\, W_{A_k}(r_1, \dots, r_p)$ for all sufficiently large $(r_1, \dots, r_p) \in \mathbb{N}^p$. Therefore, if we set $\psi_{\eta|K}(t_1, \dots, t_p) = \sum_{k=1}^{n} \omega_k(t_1, \dots, t_p)$, then there exist $r_i^{(0)}, s_i^{(0)}, s_i^{(1)} \in \mathbb{N}$ $(1 \leq i \leq p)$ with $s_i^{(1)} < r_i^{(0)} - s_i^{(0)}$ 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

$$\operatorname{Card} U_\eta(\bar{r}, \bar{s}) = \psi_{\eta|K}(r_1, \dots, r_p) - \psi_{\eta|K}(s_1 - 1, \dots, s_p - 1). \quad (10)$$

Furthermore, $\deg \psi_{\eta|K} \leq m$, and $\deg \psi_{\eta|K} = m$ if and only if at least one of the sets A_k $(1 \leq k \leq n)$ is empty.

In order to evaluate $\operatorname{Card} U''(\bar{r}, \bar{s})$, note that $U''(\bar{r}, \bar{s})$ consists of all terms $\gamma u_{f_j}^{(1)}$ $(\gamma \in \Gamma, \gamma \sim u_{f_j}^{(1)}, 1 \leq j \leq q)$ such that $s_i \leq \operatorname{ord}_i u_{\gamma f_j}^{(1)} \leq r_i$ and there exists $k \in \{2, \dots, p\}$ such that $\operatorname{ord}_k u_{\gamma f_j}^{(k)} > r_k$ or there exists $i \in \{1, \dots, p\}$ such that $\operatorname{ord}_i v_{\gamma f_j}^{(i)} < s_i$ ("or" is inclusive). It follows from Remark 3.6 and formula (4) that if we fix j, the number of such transforms $\gamma u_{f_j}^{(1)}$ of $u_{f_j}^{(1)}$ with the conditions $\operatorname{ord}_i v_{\gamma f_j}^{(i)} = \operatorname{ord} \gamma + b_{if_j} < s_i$, $\operatorname{ord}_i(\gamma u_{f_j}^{(1)}) = \operatorname{ord}_i \gamma + a_{1f_j} \geq s_i$ for $i \in \{k_1, \dots, k_d\} \subseteq \{1, \dots, p\}$, $\operatorname{ord}_i(v_{\gamma f_j}^{(i)}) = \operatorname{ord} \gamma + b_{if_j} \geq s_i$ for $i \in \{1, \dots, p\}$, $i \neq k_\nu$ $(1 \leq \nu \leq d)$ and $\operatorname{ord}_i u_{\gamma f_j}^{(i)} = \operatorname{ord} \gamma + a_{if_j} \leq r_i$ for $i = 1, \dots, p$ is $\prod\limits_{\substack{1 \leq i \leq p, \\ i \neq k_1, \dots, k_d}} \left[\sum\limits_{\mu=0}^{m_i} (-1)^{m_i - \mu} 2^\mu \binom{m_i}{\mu} \left(\binom{r_i - a_{if_j} + \mu}{\mu} - \binom{s_i - b_{if_j} + \mu - 1}{\mu} \right) \right] \cdot \prod\limits_{\nu=1}^{d} \left[\sum\limits_{\mu=0}^{m_{k_\nu}} (-1)^{m_{k_\nu} - \mu} 2^\mu \binom{m_{k_\nu}}{\mu} \cdot \right.$

$$\left. \left(\binom{s_{k_\nu} - b_{k_\nu f_j} - 1 + m_{k_\nu}}{m_{k_\nu}} - \binom{s_{k_\nu} - a_{1f_j} - 1 + m_{k_\nu}}{m_{k_\nu}} \right) \right] \quad (11)$$

and a similar formula holds for the number of terms with the conditions $\operatorname{ord}_i u_{\gamma f_j}^{(i)} > r_i$ for $i \in \{l_1, \dots, l_e\} \subseteq \{2, \dots, p\}$, $(\gamma \sim u_{f_j}^{(1)})$, $\operatorname{ord}_i v_{\gamma f_j}^{(i)} \geq s_i$ $(1 \leq i \leq p)$ and $\operatorname{ord}_i u_{\gamma f_j}^{(i)} \leq r_i$ for $i \neq l_\nu$ $(1 \leq \nu \leq e)$.

Applying the principle of inclusion and exclusion (taking into account terms that are multiples of more than one 1-leaders), we obtain that $\operatorname{Card} U''(\bar{r}, \bar{s})$ is an alternating sum of polynomials in $r_1, \dots, r_p, s_1, \dots, s_p$ that are products of k $(0 \leq k \leq p)$ 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 $\binom{s_i - c_i + m_i}{m_i} - \binom{s_i - d_i + m_i}{m_i}$ 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 $\operatorname{Card} U''(\bar{r}, \bar{s}) = \lambda(r_1, \dots, r_p, s_1, \dots, s_p)$ where $\lambda(t_1, \dots, t_{2p})$ is a numerical polynomial in $2p$ variables such that $\deg \lambda < m$ and $\deg_{t_i} \lambda \leq m_i$, $\deg_{t_j} \lambda \leq m_{j-p}$ for $i = 1, \dots, p$, $j = p+1, \dots, 2p$. It follows that the numerical polynomial

$$\Phi_{\eta \,|\, K} = \psi_{\eta \,|, K}(t_1, \dots, t_p) - \psi_{\eta \,|\, K}(t_{p+1} - 1, \dots, t_{2p} - 1) + \lambda(t_1, \dots, t_{2p})$$

satisfies conditions of our theorem. □

The numerical polynomial $\Phi_{\eta|K}(t_1, \dots, t_{2p})$ 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 (5) of the set σ. The following theorem describes some invariants of such a polynomial, that is, characteristics of the extension L/K that do not depend on the set of σ^*-generators of L/K. In what follows, 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 $\mathbb{N}^{2p}$ 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 $k_{j_\nu} = l_{j_\nu}$ for $\nu < q$ and $k_{j_q} < l_{j_q}$.

Theorem 4.2. *Let*

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

be the $2p$-variate σ^*-dimension polynomial of the σ^*-field extension $L = K\langle \eta_1, \dots, \eta_n \rangle^*$. Let $E_\eta = \{(i_1, \dots, i_{2p}) \in \mathbb{N}^{2p} \mid 0 \leq i_k, i_{p+k} \leq m_k$ $(k = 1, \dots, p)$ and $a_{i_1 \dots i_{2p}} \neq 0\}$. Then the total degree d of $\Phi_{\eta \,|\, K}$ and the coefficients of the terms of total degree d in $\Phi_{\eta \,|\, K}$ do not depend on the set of σ^*-generators η. Furthermore, if $(\mu_1, \dots, \mu_p)$ is any permutation of $\{1, \dots, p\}$ and $(\nu_1, \dots, \nu_p)$ is any permutation of $\{p+1, \dots, 2p\}$, then the maximal element of E_η with respect to the lexicographic order $<_{\mu_1, \dots, \mu_p, \nu_1, \dots, \nu_p}$ and the corresponding coefficient $a_{\mu_1, \dots, \mu_p, \nu_1, \dots, \nu_p}$ do not depend on the 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. Let $\zeta = \{\zeta_1, \dots, \zeta_l\}$ be another set 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

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

be the $2p$-variate dimension polynomial of the extension L/K associated with the system of σ^*-generators ζ. Then there exist $h_1, \dots, h_p \in \mathbb{N}$ such that $\eta_i \in K(\bigcup_{j=1}^{l} \Gamma(h_1, \dots, h_p)\zeta_j)$ and $\zeta_k \in K(\bigcup_{j=1}^{n} \Gamma(h_1, \dots, h_p)\eta_j)$, $1 \leq i \leq n$ and $1 \leq k \leq l$. (If $\Gamma' \subseteq \Gamma$, then $\Gamma'\zeta_j$ denotes the set $\{\gamma\zeta_j \mid \gamma \in \Gamma'\}$.) It follows that there exist $r_i^{(0)}, s_i^{(0)}, s_i^{(1)} \in \mathbb{N}$ $(1 \leq i \leq p)$ with $s_i^{(1)} < r_i^{(0)} - s_i^{(0)}$ such that whenever $r_i \geq r_i^{(0)}$, $s_i^{(1)} \leq s_i \leq r_i - s_i^{(0)}$ $(1 \leq i \leq p)$,

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

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

These inequalities immediately imply the statement of the theorem about the maximal elements of E_η with respect to the orders $<_{\mu_1, \dots, \mu_p, \nu_1, \dots, \nu_p}$ and the corresponding coefficients. 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 degree of the polynomial (11) is 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 $\psi_{\eta \,|\, K}(t_1, \dots, t_p)$ and $\psi_{\eta \,|\, K}(t_{p+1}, \dots, t_{2p})$, respectively (see the proof of Theorem 4.1). Now, using the fact that if elements $\eta_{i_1}, \dots, \eta_{i_k}$ $(i_1, \dots, i_k \in \{1, \dots, n\})$ are σ-algebraically independent over K, then $\operatorname{tr.}\deg_K K((\{\gamma\eta_{i_j} \mid \gamma \in \Gamma(r_1, \dots, r_p; s_1, \dots, s_p), 1 \leq j \leq k\}) = k \prod_{i=1}^{p} \left[\sum_{j=0}^{m_i} (-1)^{m_i - j} 2^j \binom{m_i}{j} \left(\binom{r_i + j}{j} - \binom{s_i + j - 1}{j} \right) \right]$ for any $r_i, s_i \in \mathbb{N}$ with $s_i \leq r_i$ $(1 \leq i \leq p)$, one can mimic the proof of [5, Theorem 6.4.8] to obtain that $a_{m_1 \dots m_p 0 \dots 0} = a_{0 \dots 0 m_1 \dots m_p} = \sigma\text{-tr.}\deg_K L$. □

Example 4.3. Let K be a σ^*-field with a basic set $\sigma = \{\alpha_1, \alpha_2, \alpha_3\}$ considered 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

$$\alpha_1^a \eta + \alpha_1^{-a} \eta + \alpha_2^b \eta + \alpha_3^c \eta = 0 \quad (12)$$

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 $K\{y\}^*$ generated by the linear σ^*-polynomial $f = \alpha_1^a y + \alpha_1^{-a} y + \alpha_2^b y + \alpha_3^c y$.

By Proposition 3.16, the σ^*-polynomials f and $\alpha_1^{-1} f = \alpha_1^{-(a+1)} y + \alpha_1^{a-1} y + \alpha_1^{-1}\alpha_2^b y + \alpha_1^{-1}\alpha_3^c y$ form an E-characteristic set of P. Setting $\bar{r} = (r_1, r_2, r_3)$, $\bar{s} = (s_1, s_2, s_3)$ and using the notation of the proof of Theorem 4.1, we obtain (applying [5, Theorem 2.5.5]) that for all sufficiently large $(r_1, r_2, r_3, s_1, s_2, s_3) \in \mathbb{N}^6$,

$\mathrm{Card}\, U'_\eta(\bar{r}, \bar{s}) = \phi_{\{(a,0,0),(-a-1,0,0)\}}(r_1, r_2, r_3, s_1, s_2, s_3) = 2a(2r_2 - 2s_2 + 2)(2r_3 - 2s_3 + 2)$.

Furthermore, using the method of inclusion and exclusion (as it is indicated in the proof of Theorem 4.1), we get $\mathrm{Card}\, U''_\eta(\bar{r}, \bar{s}) = (2a+1)(2r_2 - 2s_2 + 2)(2r_3 - 2s_3 + 2) + 4b(r_1 - s_1 + 1)(2r_3 - 2s_3 + 2) + 4c(r_1 - s_1 + 1)(2r_2 - 2s_2 + 2) - 2b(2a+1)(2r_3 - 2s_3 + 2) - 2c(2a+1)(2r_2 - 2s_2 + 2) - 8bc(r_1 - s_1 + 1) + 8abc + 4bc$.

Since the 6-variate σ^*-dimension polynomial $\Phi_{\eta\,|\,K} t_1, \dots, t_6)$ expresses the number of elements of the set $U'_\eta(\bar{r}, \bar{s}) \cup U''_\eta(\bar{r}, \bar{s})$,

$$\Phi_{\eta\,|\,K} = 8ct_1t_2 + 8bt_1t_3 - 8ct_1t_5 - 8bt_1t_6 + 4(4a+1)t_2t_3 - 8ct_2t_4$$
$$-4(4a+1)t_2t_6 - 8bt_3t_4 - 4(4a+1)t_3t_5 + 8ct_4t_5 + 8bt_4t_6 + 4(4a+1)t_5t_6 +$$
$$\text{a linear combination of monomials of degree} \le 1. \tag{13}$$

By [5, Theorem 6.4.8], the univariate σ^*-dimension polynomial $\phi_{\eta\,|\,K}(t)$ (see Theorem 2.1) coincides with the dimension polynomial of the set $A = \{(a, 0, 0), (-a-1, 0, 0)\} \subset \mathbb{Z}^3$). Therefore

$\phi_{\eta\,|\,K} = 4at^2 +$ a linear combination of monomials of degree ≤ 1.

By Theorem 4.3, $\deg \Phi_{\eta\,|\,K} = 2$ and the coefficients of the terms t_it_j $(1 \le i, j \le 6)$ are invariants of the extension L/K. Therefore, the polynomial $\Phi_{\eta\,|\,K}(t_1, \dots, t_6)$ carries all three parameters a, b and c of the defining equation (12). At the same time, the univariate polynomial $\phi_{\eta\,|\,K}(t)$ carries only the parameter a.

The fact that the $2p$-variate σ^*-dimension polynomial carries more invariants than its univariate counterpart can be applied to the equivalence problem for systems of algebraic difference equations. Suppose we have two such systems over a σ^*-field K (i. e., systems $f_i = 0$ $(i \in I)$ where all f_i lie in some ring of σ^*-polynomials) that are defining systems of equations for σ^*-field extensions L/K and L'/K (that is, the left-hand sides of the systems generate prime σ^*-ideals P and P' in the corresponding rings of σ^*-polynomials R and R' (possibly of different numbers of σ^*-generators) 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 $2p$-variate σ^*-dimension polynomial given by Theorem 4.1 allows one to determine that two systems of algebraic difference equations are not equivalent even if the corresponding σ^*-field extensions have the same univariate σ^*-dimension polynomials. As an example, consider difference equations

$$\alpha_1^a\eta + \alpha_1^{-a}\eta + \alpha_2^b\eta + \alpha_3^c\eta = 0, \tag{14}$$
$$\alpha_1^a\eta + \alpha_1^{-a}\eta + \alpha_2^d\eta + \alpha_3^e\eta = 0 \tag{15}$$

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

The invariants carried by the univariate σ^*-dimension polynomials associated with these equations (the equation (14) was considered in the last Example) are the same, the degree 1 and a. At the same time, the 6-variate dimension polynomials for these equations (they are of the form (13)) carry invariants a, b, c, and a, d, e, respectively. Thus, the difference equations (14) and (15) are not equivalent, even though the corresponding σ^*-field extensions have the same invariants carried by the univariate σ^*-dimension polynomials. (Note that the problem of finding a complete system of invariants in our settings is still open.)

We conclude with a remark on an analytic interpretation of the obtained results. Consider a system of equations in finite differences with respect to n unknown functions in m independent variables $x_1, \dots, x_m$ over $\mathbb{R}$ and shifts of arguments $\alpha_i : x_i \mapsto x_i + h_i$ $(h_i \in \mathbb{R}$, $1 \le i \le m)$. Given a partition of the set of variables into p disjoint subsets, the σ^*-dimension polynomial introduced by Theorem 4.1 $(\sigma = \{\alpha_1, \dots, \alpha_m\})$ gives the maximal number of algebraically independent values the solution functions take at nodes of the $h_1 \times \cdots \times h_m$ grid in $\mathbb{R}^m$ whose orders with respect to the ith set of the partition lie between two given positive integers s_i and r_i, $1 \le i \le p$. (The orders of nodes are considered with respect to some fixed node (the origin), see [8, Section 7.7] for details.) It gives a more delicate characterization of the system than its Einstein-type strength discussed in [8, Section 7.7].

5 ACKNOWLEDGES

This research was supported by the NSF grant CCF−2139462.

REFERENCES

[1] R. M. Cohn. Difference Algebra, Interscience, New York, 1965.
[2] C. Doench. Bivariate difference-differential dimension polynomials and their computation in Maple. Technical report no. 09-19. RISC, Johannes Kepler Univ., Linz, Austria. ISSN 2791-4267 (online). 2009.
[3] A. Einstein. The Meaning of Relativity. Appendix II (Generalization of gravitation theory), 4th ed. Princeton, 133–165.
[4] E. R. Kolchin. Differential Algebra and Algebraic Groups, Acad. Press, 1973.
[5] M. V. Kondrateva, A. B. Levin, A. V. Mikhalev, E. V. Pankratev. Differential and Difference Dimension Polynomials, Kluwer Acad. Publ., 1998.
[6] A. B. Levin. Characteristic Polynomials of Inversive Difference Modules and Some Properties of Inversive Difference Dimension. Russian Mathematical Surveys, 35 (1980), no. 1, 217–218.
[7] A. B. Levin. Computation of the Strength of Systems of Difference Equations via Generalized Groebner Bases. In: *Groebner Bases in Symbolic Analysis*. Walter de Gruyter, 2007, 43–73.
[8] A. B. Levin. Difference Algebra. Springer, 2008.
[9] A. B. Levin. Dimension Polynomials of Intermediate Differential Fields and the Strength of a System of Differential Equations with Group Action. Journal of Mathematical Sciences, 163, no. 5 (2009), 554–562.
[10] A. B. Levin. Multivariate Dimension Polynomials of Inversive Difference Field Extensions. Lecture Notes in Comput. Sci., 8372 (2014), 146–163.
[11] A. B. Levin. Dimension polynomials of difference local algebras. Advances in Applied Mathematics, 72 (2016), 166–174.
[12] A. B. Levin. A. Multivariate Difference–Differential Dimension Polynomials. Mathematics in Computer Science, 14 (2020), 361–374.
[13] A. B. Levin, A. V. Mikhalev. Dimension polynomials of filtered G-modules and finitely generated G-field extensions. *Collection of Papers on Algebra*. Moscow State University, 1989, 74– 94.
[14] A. B. Levin, A. V. Mikhalev. Type and Dimension of Finitely Generated Vector G-spaces. *Moscow University Mathematics Bulletin*, 46, no. 4, 51–52.
[15] A. B. Levin, A. V. Mikhalev. Dimension Polynomials of Difference-Differential Modules and of Difference-Differential Field Extensions. *Abelian Groups and Modules*, no. 10 (1991), 56–82.
[16] A. B. Levin, A. V. Mikhalev. Dimension Polynomials of Filtered Differential G-modules and Extensions of Differential G-fields. Contemporary Mathematics, 131 (1992), Part 2, 469 – 489.
[17] A. B. Levin, A. V. Mikhalev. Type and Dimension of Finitely Generated G-algebras. Contemporary Mathematics, 184 (1995), 275–280.
[18] Zhou, M.; Winkler, F. Computing difference-differential dimension polynomials by relative Gröbner bases in difference-differential modules. *J. Symbolic Comput.*, 43 (10), 2008, 726–745.