Reduction with Respect to the Effective Order and a New Type of Dimension Polynomials of Difference Modules

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

ABSTRACT

We introduce a new type of reduction in a free difference module over a difference field that uses a generalization of the concept of effective order of a difference polynomial. Then we define the concept of a generalized characteristic set of such a module, establish some properties of these characteristic sets and use them to prove the existence, outline a method of computation and find invariants of a dimension polynomial in two variables associated with a finitely generated difference module. As a consequence of these results, we obtain a new type of bivariate dimension polynomials of finitely generated difference field extensions. We also explain the relationship between these dimension polynomials and the concept of Einstein's strength of a system of difference equations.

CCS CONCEPTS

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

KEYWORDS

Difference module; effective order, characteristic set, dimension polynomial

ACM Reference Format:
Alexander Levin. 2022. Reduction with Respect to the Effective Order and a New Type of Dimension Polynomials of Difference Modules. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation (ISSAC'22), July 4–7, 2022, Lille, France.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3476446.3535497

1 INTRODUCTION

Difference dimension polynomials play the same role in difference algebra, as Hilbert polynomials play in commutative algebra and algebraic geometry. (A similar role in differential algebra is played by differential dimension polynomials introduced by E. Kolchin in [4]; see also [5, Chapter 2].) Several applications of difference dimension polynomials to the study of difference algebraic structures are based on the fact that if P is a prime reflexive difference ideal in a ring of difference polynomials $R = K\{y_1, \ldots, y_n\}$ over a difference field K, then the quotient field of R/P is a difference field extension of K generated by the images of y_i in R/P. The dimension polynomial of this extension, therefore, characterizes the ideal P; assigning such polynomials to prime reflexive difference polynomial ideals has led to a number of new results on dimension of difference varieties (see [3] and [14]) and on the Krull-type dimension of difference algebras (see [13], [6, Section 7.2], and [11, Section 4.6]) and difference field extensions (see [12]). Another important application of difference dimension polynomials is based on the fact that the univariate difference dimension polynomial of a system of algebraic difference equations (defined as the dimension polynomial of the difference field extension associated with the system) expresses the A. Einstein's strength of this system (see [9] and [11, Chapter 7]). In this connection, the study of difference dimension polynomials and methods of their computation is of primary importance for the qualitative theory of difference equations. One should also mentioned that a number of results on difference dimension polynomials were generalized to the case of difference fields and modules where one considers a partition of the basic set of translations. The corresponding study (see [8] and [10]) resulted in theorems on multivariate dimension polynomials of difference modules and difference field extensions that carry more invariants (i. e., characteristics of a difference module or a difference field extension that do not depend on the set of generators) than their univariate counterparts.

In this paper we introduce a reduction in a free difference module F over a difference field K that takes into account the effective order of elements of the module (we generalize the concept of the effective order of an ordinary difference polynomial defined in [1, Chapter 2, Section 4] to the partial case) and consider a new type of characteristic sets that are associated with this reduction (they are called $\mathcal{E}$-characteristic sets). Then we use properties of $\mathcal{E}$-characteristic sets to prove the existence of a bivariate dimension polynomial of a finitely generated difference K-module M that describes the dimension of intermediate K-vector spaces generated by the transforms of the module generators whose orders lie between two given natural numbers. We also determine invariants of such dimension polynomials, and apply them to the study of the isomorphism problem for difference modules. As an application, we obtain a bivariate dimension polynomial of a finitely generated difference field extension that describes the transcendence degrees of intermediate fields obtained by adjoining transforms of the generators whose orders are bounded above and below. We determine invariants of these polynomials and discuss their relationship with the concept of Einstein's strength of a system of algebraic difference equations.

ISSAC'22, July 4–7 2022, Lille, France

ACM ISBN 978-1-4503-8688-3/22/07…$15.00
https://doi.org/10.1145/3476446.3535497

2 PRELIMINARIES

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

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

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

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

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

A subring (respectively, 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 in σ to R_0 is denoted by the same symbol. If a prime ideal P of R is closed with respect to the action of σ, it is called a *prime 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 σ-field extension or a σ-overfield of K (we also say that we have a σ-field extension L/K). The maximal number of elements $\zeta_1, \ldots, \zeta_k \in L$ such that the set $\{\tau(\zeta_i) \mid \tau \in T, 1 \leq i \leq k\}$ is algebraically independent over K is called the *σ-transcendence degree* of L over K; it is denoted by $\sigma\text{-tr.deg}_K L$. 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 a finite subset of L, $S = \{\eta_1, \ldots, \eta_n\}$, then L is said to be a finitely generated σ-field extension of K with the set of σ-generators $\{\eta_1, \ldots, \eta_n\}$. In this case we write $L = K\langle \eta_1, \ldots, \eta_n \rangle$. It is easy to see that $K\langle \eta_1, \ldots, \eta_n \rangle$ coincides with the field $K(\{\tau\eta_i \mid \tau \in T, 1 \leq i \leq n\})$. (Here and below we often write $\tau\eta$ for $\tau(\eta)$ where $\tau \in T$, $\eta \in L$.)

A difference (σ-) field K is said to be *inversive* if the elements of σ are automorphisms of K. As it is shown in [11, Proposition 2.1.7], any σ-field K has an inversive closure, that is, an inversive σ-overfield K^* of K with the property that for any $a \in K^*$, there exists $\tau \in T$ such that $\tau(a) \in K$.

Let K be a difference field with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_m\}$. With the above notation, 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 K. 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 K will be denoted by $\mathfrak{D}$. This set, which has a natural structure of a K-vector space with a basis T, becomes a ring if one sets $\tau a = \tau(a)\tau$ for any $a \in K$, $\tau \in T$ and extends this rule to the multiplication of any two σ-operators by distributivity. The resulting ring $\mathfrak{D}$ is called the ring of σ-operators over K. A left $\mathfrak{D}$-module is called a *difference K-module* or a *σ-K-module*. In other words, a K-vector space M is a difference (or σ-) K-module, if the elements of σ act on M in such a way that $\alpha(x + y) = \alpha(x) + \alpha(y)$, $\alpha(\beta x) = \beta(\alpha x)$, and $\alpha(ax) = \alpha(a)\alpha(x)$ for any $x, y \in M$; $\alpha, \beta \in \sigma$; $a \in K$.

If M is a σ-K-module and $S \subseteq M$, then the $\mathfrak{D}$-submodule of M generated by S is denoted by $[S]$. A σ-K-module is said to be finitely generated (respectively, free) if it is finitely generated (respectively, free) as a left $\mathfrak{D}$-module. If M and N are two σ-K-modules, then a homomorphism of $\mathfrak{D}$-modules $\phi : M \to N$ is said to be a difference (or σ-) homomorphism if $\phi(\alpha x) = \alpha\phi(x)$ for any $x \in M$, $\alpha \in \sigma$.

If M is a σ-K-module, then the maximal number of elements $e_1, \ldots, e_k \in M$ such that the set $\{\tau e_i \mid \tau \in T, 1 \leq i \leq k\}$ is linearly independent over K is called the difference (or σ-) dimension of M over K; it is denoted by $\sigma\text{-dim}_K M$.

The following theorem proved in [6, Section 6.2] establishes the existence of a Hilbert-type dimension polynomial associated with a finite system of generators of a σ-K-module.

THEOREM 2.1. *Let K be a difference field of characteristic zero with a basic set $\sigma = \{\alpha_1, \ldots, \alpha_m\}$, $\mathfrak{D}$ the ring of σ-operators over K, and M a finitely generated σ-K-module with generators $x_1, \ldots, x_n$ (that is, $M = \sum_{i=1}^{n} \mathfrak{D}x_i$). For any $r \in \mathbb{N}$, let M_r denote the K-vector space generated by all elements of the form τx_i ($\tau \in T$, $1 \leq i \leq n$) with $\operatorname{ord} \tau \leq r$. Then there exists a polynomial $\phi(t) \in \mathbb{Q}[t]$ with the following properties.*

(i) *$\phi(r) = \dim_K M_r$ for all sufficiently large $r \in \mathbb{N}$ (that is, there exists $r_0 \in \mathbb{N}$ such that the last equality holds for all integers $r \geq r_0$).*

(ii) *$\deg \phi(t) \leq m$ and the polynomial $\phi(t)$ can be written as $\phi(t) = \sum_{i=0}^{m} c_i \binom{t+i}{i}$ where $c_0, c_1, \ldots, c_m \in \mathbb{Z}$. (As usual, $\binom{t+i}{i}$ denotes the polynomial $(t+i)(t+i-1)\ldots(t+1)/i! \in \mathbb{Q}[t]$ that takes integer values for all sufficiently large integer values of t.)*

(iii) *The integers $d = \deg \phi(t)$, c_m and c_d (if $d < m$) do not depend on the choice of the system of generators of M over $\mathfrak{D}$. Furthermore, $c_m = \sigma\text{-dim}_K M$.*

The polynomial $\phi(t)$ is called a *σ-dimension polynomial* of the σ-K-module M associated with the system of σ-generators $x_1, \ldots, x_n$.

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

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

Of course, every polynomial with integer coefficients is numerical. As an example of a numerical polynomial in p variables with non-integer coefficients ($p \geq 1$) one can consider $\prod_{i=1}^{p} \binom{t_i}{m_i}$ where $m_1, \ldots, m_p \in \mathbb{N}$. Note that the σ-dimension polynomial $\phi(t)$ introduced in Theorem 2.1 is a univariate numerical polynomial.

As it is shown in [6, Chapter 2], a numerical polynomial in p variables has a "canonical" representation as

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

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

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

The following theorem about a univariate numerical polynomial associated with a subset of $\mathbb{N}^m$ is due to E. Kolchin, see [5, Chapter 0, Lemma 16].

Theorem 2.2. *Let $A\subseteq\mathbb{N}^m$. Then there exists a numerical polynomial $\omega_A(t)$ such that*

(i) $\omega_A(r)=\operatorname{Card}V_A(r)$ *for all sufficiently large* $r\in\mathbb{N}$.

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

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

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

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

Note that if $A\subseteq\mathbb{N}^m$ and A' is the set of all minimal elements of A with respect to the product order on $\mathbb{N}^m$, then the set A' is finite (it follows from [5, 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 [6, Chapter 2] gives an explicit formula for the Kolchin polynomial of a finite subset of $\mathbb{N}^m$.

Theorem 2.3. *Let $A=\{a_1,\dots,a_n\}$ be a finite subset of $\mathbb{N}^m$ and let $a_k=(a_{k1},\dots,a_{km})$ $(1\le k\le n)$. For any $l\in\mathbb{N}$, $0\le l\le n$, let $\Gamma(l,n)$ denote the set of all l-element subsets of the set $\mathbb{N}_n=\{1,\dots,n\}$. Let $\bar a_{0j}=0$ and for any $\gamma\in\Gamma(l,n)$, $\gamma\ne\emptyset$, let $\bar a_{\gamma j}=\max\{a_{ij}\mid i\in\gamma\}$ $(1\le j\le m)$. Then*

$$\omega_A(t)=\sum_{l=0}^{n}(-1)^l\sum_{\gamma\in\Gamma(l,n)}\binom{t+m-\sum_{j=1}^{m}\bar a_{\gamma j}}{m} \qquad (2)$$

3 $\mathcal{E}$-REDUCTION AND $\mathcal{E}$-GRÖBNER BASES IN FREE DIFFERENCE MODULES

Let K be a difference field with a basic set $\sigma=\{\alpha_1,\dots,\alpha_m\}$ and F a free σ-K-module with free generators $f_1,\dots,f_n$ (i. e., these generators form a basis of the free left module F over the ring of σ-operators $\mathfrak{D}$ over K). Then the elements of the form τf_ν ($\tau\in T, 1\le\nu\le n$) are called *terms*; the set of all terms is denoted by Tf. It is easy to see that this set is a basis of F treated as a vector space over the field K.

The order of a term $u=\tau f_i$ (denoted by $\operatorname{ord}u$) is defined as the order of τ. As usual, if $\tau,\tau'\in T$, we say that τ divides τ' (and write $\tau\mid\tau'$) if $\tau'=\tau\tau''$ for some $\tau''\in T$. If $u=\tau f_i$ and $v=\tau' f_j$ are two terms in Tf, we say that u divides v (and write $u|v$) if $i=j$ and $\tau|\tau'$. In this case we also say that v is a *transform* of u.

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

(i) $u\le\tau u$ for any $u\in Tf,\tau\in T$. (We denote the ordering of Tf by the usual symbol $\le$ and write $u<v$ or $v>u$ if $u\le v$ and $u\ne v$.)

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

A ranking is said to be *orderly* if the inequality $\operatorname{ord}u<\operatorname{ord}v$ $(u,v\in Tf)$ implies $u<v$. In what follows, we assume that the following orderly ranking $\le$ on Tf is fixed: if $u_1=\alpha_1^{k_1}\dots\alpha_m^{k_m}f_i, u_2=\alpha_1^{l_1}\dots\alpha_m^{l_m}f_j\in Tf$, then $u_1\le u_2$ if and only if

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

($\le_{lex}$ denotes the lexicographic order on $\mathbb{N}^{m+2}$). In this case we set $\mu(u_2,u_1)=(\operatorname{ord}u_2-\operatorname{ord}u_1,l_1-k_1,\dots,l_m-k_m,j-i)\in\mathbb{N}\times\mathbb{Z}^{m+1}$.

Remark 3.1. *Note that for every $r=1,\dots,m$, $|l_r-k_r|\le l_r+k_r\le\operatorname{ord}u_1+\operatorname{ord}u_2$. It follows that there is no infinite sequences of terms $u_1,u_2,\dots,v_1,v_2,\dots$ such that $\mu(u_1,v_1)>_{lex}\mu(u_2,v_2)>_{lex}\dots$.*

Since the set Tf is a basis of the vector K-space F, every nonzero element $f\in F$ has a unique (up to the order of the terms in the sum) representation in the form

$$g=a_1\tau_1f_{i_1}+\dots+a_p\tau_pf_{i_p} \qquad (3)$$

where $\tau_1f_{i_1},\dots,\tau_pf_{i_p}$ are distinct elements of Tf $(1\le i_1,\dots,i_p\le n)$ and $a_1,\dots,a_p$ are nonzero elements of K.

Definition 3.2. *Let g be an element of the free σ-K-module F written in the form (3) and let $\tau_rf_{i_r}$ and $\tau_sf_{i_s}$ $(1\le r,s\le p)$ be the greatest and the smallest terms in the set $\{\tau_1f_{i_1},\dots,\tau_lf_{i_l}\}$, respectively, relative to the introduced order on Tf. Then the terms $\tau_rf_{i_r}$ and $\tau_sf_{i_s}$ are called, respectively, the* **leader** *and* **coleader** *of the element g; they are denoted by u_g and v_g, respectively. The coefficient of u_g is called the* **leading coefficient** *of g; it is denoted by* $\operatorname{lc}(g)$.

Definition 3.3. *If $0\ne g\in F, u_g=\alpha_1^{k_1}\dots\alpha_m^{k_m}f_i, v_g=\alpha_1^{l_1}\dots\alpha_m^{l_m}f_j$, then the nonnegative integer $\operatorname{Eord}(g)=\operatorname{ord}u_g-\operatorname{ord}v_g$ is called the* **effective order** *of g. The $(m+2)$-tuple $\mu(u_g,v_g)\in\mathbb{Z}^{m+2}$ is said to be the* **full effective order** *of g; it is denoted by $\mathcal{E}\operatorname{ord}(g)$.*

It follows from the last definition that for any $g\in F$ and for any $\tau\in T$, $\operatorname{Eord}(\tau g)=\operatorname{Eord}(g)$ and $\mathcal{E}ord(\tau g)=\mathcal{E}\operatorname{ord}(g)$. Furthermore, if $g,h\in F$ and $\operatorname{Eord}(g)<\operatorname{Eord}(h)$, then $\mu(u_g,v_g)<\mu(u_h,v_h)$ (with respect to the lexicographic order on $\mathbb{Z}^{m+2}$), that is, $\mathcal{E}\operatorname{ord}(g)<\mathcal{E}\operatorname{ord}(h)$ (we will always compare the full effective orders of elements of F by the lexicographic order).

Definition 3.4. *Let $g,h\in F$. We say that g is $\mathcal{E}$-reduced with respect to h if g does not contain any τu_h $(\tau\in T)$ such that $\tau v_h\ge v_g$. If $S\subseteq F$, then an element $g\in F$ is said to be $\mathcal{E}$-reduced with respect to S of g is $\mathcal{E}$-reduced with respect to every element of S.*

Definition 3.5. *Let $g,h\in F$. Then g is said to have lower rank than h (we write* $\operatorname{rk}g<\operatorname{rk}h$*) if either $g=0, h\ne0$ or*

$$(\mathcal{E}\operatorname{ord}(g),u_g)<_{lex}(\mathcal{E}\operatorname{ord}(h),u_h).$$

If the pairs are equal, we say that g and h are of the same rank and write $\operatorname{rk}g=\operatorname{rk}h$.

Remark 3.6. *If $g, h \in F$ and $\operatorname{rk} g < \operatorname{rk} h$, then g is $\mathcal{E}$-reduced with respect to h. Indeed, if it is not so, then g contains τu_h for some $\tau \in T$ such that $\tau v_h \geq v_g$. Since $u_g \geq \tau u_h \geq u_h$ and $\mathcal{E}\operatorname{ord}(h) = \mathcal{E}\operatorname{ord}(\tau h)$, we obtain that $\mathcal{E}\operatorname{ord}(g) \geq \mathcal{E}\operatorname{ord}(h)$ and the last inequality becomes an equality if and only if $\tau = 1$, $u_g = u_h$, and $v_g = v_h$, that is, $\operatorname{rk} g = \operatorname{rk} h$, a contradiction.*

Definition 3.7. *A set of $\mathcal{A} \subseteq F$ is said to be $\mathcal{E}$-**autoreduced** if either it is empty or every element of $\mathcal{A}$ is $\mathcal{E}$-reduced with respect to all other elements of the set $\mathcal{A}$.*

Lemma 3.8. *Every $\mathcal{E}$-autoreduced set is finite.*

Proof. Note first that two elements of an $\mathcal{E}$-autoreduced set cannot have the same leader (if $u_g = u_h$ for some $g, h \in F$, then either $v_h \geq v_g$ or $v_g \geq v_h$, so one of these two elements is not reduced with respect to the other one). Suppose that there is an infinite $\mathcal{E}$-autoreduced set $\mathcal{A}$. It follows from [5, Chapter 0, Lemma 15] that $\mathcal{A}$ contains a sequence of elements $\{g_1, g_2, \dots\}$ such that $u_{g_i} | u_{g_{i+1}}$ for $i = 1, 2, \dots$. Let $u_{g_{i+1}} = \tau_i u_{g_i}$ $(i = 1, 2, \dots)$. Since the set $\mathcal{A}$ is $\mathcal{E}$-autoreduced, it follows that for every $i = 1, 2, \dots$, g_{i+1} is $\mathcal{E}$-reduced with respect to g_i, hence $\tau_i v_{g_i} < v_{g_{i+1}}$ and $\mathcal{E}\operatorname{ord}(\tau g_i) = \mathcal{E}\operatorname{ord}(g_i) > \mathcal{E}\operatorname{ord}(g_{i+1})$. Thus, we obtain a strictly decreasing sequence $\mathcal{E}\operatorname{ord}(g_1) > \mathcal{E}ord(g_2) > \dots$, a contradiction (see Remark 3.1). □

Example 3.9. Let $\sigma = \{\alpha_1, \alpha_2\}$ and F a free σ-K-module with one free generator f. Let $\mathcal{A} = \{g_1, g_2\} \subseteq F$ where

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

Then $\mathcal{E}ord(g_1) = (1, 2, -1, 0) <_{lex} \mathcal{E}ord(g_2) = (2, 2, 0, 0)$, hence $\operatorname{rk} g_1 < \operatorname{rk} g_2$ and therefore g_1 is $\mathcal{E}$-reduced with respect to g_2. Since g_2 contains no transform of $u_{g_1} = \alpha_1^2\alpha_2 y$, g_2 is reduced with respect to g_1, so the set $\mathcal{A}$ is $\mathcal{E}$-autoreduced. However, since g_1 contains a transform of u_{g_2}, the set $\mathcal{A}$ is not autoreduced in the usual sense (where h is said to be reduced with respect to g if h does not contain any (τu_g) $(\tau \in T)$, see [6, Section 4.1] or [11, Section 2.4]).

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

Definition 3.10. *Let $\mathcal{A} = \{g_1, \dots, g_s\}$ and $\mathcal{B} = \{h_1, \dots, h_t\}$ be two nonempty $\mathcal{E}$-autoreduced sets in a finitely generated free σ-K-module F. Then $\mathcal{A}$ is said to have lower rank than $\mathcal{B}$, written as $\operatorname{rk}\mathcal{A} < \operatorname{rk}\mathcal{B}$, if one of the following two cases holds:*

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

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

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

Proposition 3.11. *In every nonempty family of $\mathcal{E}$-autoreduced sets in a finitely generated free σ-K-module F there exists an $\mathcal{E}$-autoreduced set of lowest rank.*

Proof. Let $\mathcal{M}$ be a nonempty family of $\mathcal{E}$-autoreduced sets in F. Let us inductively define an infinite descending chain of subsets of $\mathcal{M}$ as follows: $\mathcal{M}_0 = \mathcal{M}$, $\mathcal{M}_1 = \{\mathcal{A} \in \mathcal{M}_0 \mid \mathcal{A}$ contains at least one element and the first element of $\mathcal{A}$ is of lowest possible rank$\}, \dots, \mathcal{M}_k = \{\mathcal{A} \in \mathcal{M}_{k-1} \mid \mathcal{A}$ contains at least k elements and the kth element of $\mathcal{A}$ is of lowest possible rank$\}, \dots$. It is clear that if f and g are the ith elements in two $\mathcal{E}$-autoreduced sets in the same set $\mathcal{M}_k$ $(1 \leq i \leq k)$, then $\mathcal{E}\operatorname{ord}(f) = \mathcal{E}\operatorname{ord}(g)$ and $u_f = u_g$ (hence $v_f = v_g$). Therefore, if all sets $\mathcal{M}_k$ are nonempty, then the set $\{f_k \mid f_k$ is the kth element of some $\mathcal{E}$-autoreduced set in $\mathcal{M}_k\}$ would be an infinite $\mathcal{E}$-autoreduced set, and this would contradict Lemma 3.8. Thus, there is the smallest positive integer k such that $\mathcal{M}_k = \emptyset$. Clearly, every element of $\mathcal{M}_{k-1}$ is an $\mathcal{E}$-autoreduced set of lowest rank in the family $\mathcal{M}$. □

Definition 3.12. *Let N be any σ-K-submodule of a finitely generated free σ-K-module F (that is, N is a left $\mathfrak{D}$-submodule of F). Since the set of all $\mathcal{E}$-autoreduced subsets of N is not empty (if $f \in N$, then $\{f\}$ is an $\mathcal{E}$-autoreduced subset of N), the last statement shows that N contains an $\mathcal{E}$-autoreduced subset of lowest rank. Such an $\mathcal{E}$-autoreduced set is called an $\mathcal{E}$-**characteristic set** of the σ-K-submodule N.*

Proposition 3.13. *Let $\mathcal{A} = \{g_1, \dots, g_d\}$ be an $\mathcal{E}$-characteristic set of a σ-K-submodule N of a finitely generated free σ-K-module F. Then an element $h \in N$ is $\mathcal{E}$-reduced with respect to the set $\mathcal{A}$ if and only if $h = 0$.*

Proof. Suppose that a nonzero element $h \in N$ is $\mathcal{E}$-reduced with respect to $\mathcal{A}$. First of all, note that if $\operatorname{rk} h < \operatorname{rk} g_1$, then $\operatorname{rk}\{h\} < \operatorname{rk}\mathcal{A}$ that contradicts the fact that $\mathcal{A}$ is an $\mathcal{E}$-characteristic set of N. Let $\operatorname{rk} h > \operatorname{rk} g_1$ (if $\operatorname{rk} h = \operatorname{rk} g_1$, then h is not reduced with respect to g_1, contrary to our assumption) and let $g_1, \dots, g_j$ $(1 \leq j \leq d)$ be all elements of $\mathcal{A}$ whose rank is lower that the rank of h. Then the set $\mathcal{A}' = \{g_1, \dots, g_j, h\}$ is $\mathcal{E}$-autoreduced. Indeed, since the set $\mathcal{A}$ is $\mathcal{E}$-autoreduced, elements $g_1, \dots, g_j$ are $\mathcal{E}$-reduced with respect to each other, and h is $\mathcal{E}$-reduced with respect to the set $\{g_1, \dots, g_j\}$ by our assumption. Furthermore, each g_i $(1 \leq i \leq j)$ is $\mathcal{E}$-reduced with respect to h because $\operatorname{rk} g_i < \operatorname{rk} g$. Since $\operatorname{rk}\mathcal{A}' < \operatorname{rk}\mathcal{A}$, $\mathcal{A}$ is not an $\mathcal{E}$-characteristic set of N, a contradiction. □

Proposition 3.14. *Let $\mathcal{A} = \{g_1, \dots, g_d\}$ be a subset of a finitely generated free $\mathfrak{D}$-module F and let $h \in F$. Then there exists an element $h^* \in F$ such that*

$$h - h^* = \sum_{i=1}^{d} C_i g_i$$

for some $C_1, \dots, C_d \in \mathfrak{D}$ and h^* is $\mathcal{E}$-reduced with respect to $\mathcal{A}$.

Proof. If h is $\mathcal{E}$-reduced with respect to $\mathcal{A}$, the statement is obvious (one can set $h^* = h$). Suppose that h is not $\mathcal{E}$-reduced with respect to $\mathcal{A}$. In what follows, a term w_t, that appears in a non-$\mathcal{E}$-reduced element $t \in F$, will be called the $\mathcal{A}$-leader of t if w_t is the greatest term among all terms τu_{g_j} $(\tau \in T, 1 \leq j \leq d)$ that appear in t and satisfy the condition $\tau v_{g_j} \geq v_t$.

Let w_h be the $\mathcal{A}$-leader of the element h and let c_h be the coefficient of w_h in h. Then $w_h = \tau u_{g_j}$ for some $\tau \in T$ and for some j $(1 \leq j \leq d)$ such that $\tau v_{g_j} \geq v_h$. Let us choose such j that corresponds to the maximum leader u_{g_j} in the set of all leaders of elements of $\mathcal{A}$ and let us consider the element $h' = h - \frac{c_h}{\tau(\operatorname{lc}(g_j))}\tau g_j$. Obviously, h' does not contain w_h and $u_{h'} \leq u_h$. Furthermore, h' cannot contain any term of the form $\tau' u_{g_i}$ $(\tau' \in T, 1 \leq i \leq d)$ that is greater than w_h and satisfies the condition $\tau' v_{g_i} \geq v_{h'}$. Indeed, since $v_{h'} \geq v_h$, such a term $\tau' u_{g_i}$ cannot appear in h. Such a term

cannot appear in τg_j either, since $u_{\tau g_j} = \tau u_{g_j} = w_h < \tau' u_{g_i}$. Thus, the $\mathcal{A}$-leader of h' is strictly less than the $\mathcal{A}$-leader of h. Applying the same procedure to the element h' and continuing in the same way, we obtain an element $h^* \in F$ such that $h - h^*$ is a linear combination of elements $g_1, \dots, g_d$ with coefficients in $\mathfrak{D}$ and h^* is $\mathcal{E}$-reduced with respect to $\mathcal{A}$. □

The process of reduction described in the proof of the last proposition can be realized by the following algorithm.

Algorithm 3.15. *$(h, d, g_1, \dots, g_d; h^*)$*

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

Output: Element $h^* \in F$ and elements $C_1, \dots, C_d \in \mathfrak{D}$ such that $h = C_1 g_1 + \cdots + C_d g_d + h^*$ and h^* is $\mathcal{E}$-reduced with respect to $\mathcal{A}$

Begin

$C_1 := 0, \dots, C_d := 0, h^* := h$

While there exist i, $1 \leq i \leq d$, and a term w, that appears in h^* with a (nonzero) coefficient c_w, such that $u_{g_i} | w$ and $\frac{w}{u_{g_i}} v_{g_i} \geq v_{h^*}$ **do**

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

$j :=$ the smallest number i for which u_{g_i} is the greatest leader of an element of $\mathcal{A}$ such that $u_{g_i} | z$ and $\frac{z}{u_{g_i}} v_{g_i} \geq v_{h^*}$

$\tau := \frac{z}{u_{g_j}}$

$C_j := C_j + \frac{c_z}{\tau(\mathrm{lc}(g_j))} \tau$ *where* c_z is the coefficient of z *in* h^*

$h^* := h^* - \frac{c_z}{\tau(\mathrm{lc}(g_j))} g_j$

End

Corollary 3.16. *If $\mathcal{A}$ is an $\mathcal{E}$-characteristic set of a σ-K-submodule N of a finitely generated free σ-K-module F, then $\mathcal{A}$ generates N as a left $\mathfrak{D}$-module.*

Proof. By Proposition 3.14, if $h \in N$, then there exists an element $g \in N$ such that g is a linear combination of elements of $\mathcal{A}$ with coefficients in $\mathfrak{D}$ and $h - g$ is $\mathcal{E}$-reduced with respect to $\mathcal{A}$. By Proposition 3.13, $h - g = 0$, hence $h \in \mathfrak{D}\mathcal{A}$. □

Proposition 3.17. *Let $N = [g]$ be a cyclic $\mathfrak{D}$-submodule of the free σ-K-module F. Then $\{g\}$ is an $\mathcal{E}$-characteristic set of N.*

Proof. Let $0 \neq h \in N$, so that h can be written as $h = \sum_{i=1}^{s} c_i \tau_i g$ where $\tau_1, \dots, \tau_s \in T, c_1, \dots, c_s \in K$, $c_i \neq 0$ $(1 \leq i \leq s)$, and $\tau_1 < \cdots < \tau_s$. Then $u_h = \tau_s u_g$ and $\tau_s v_g \geq \tau_1 v_g = v_h$. Therefore, h is not $\mathcal{E}$-reduced with respect to g. Furthermore, for any $i = 1, \dots, s$, $u_h = \tau_s u_g \geq \tau_i u_g \geq u_g$ and $v_h = \tau_1 v_g \leq \tau_i v_g$, so $\mathcal{E}\,\mathrm{ord}(h) \geq \mathcal{E}\,\mathrm{ord}(\tau_i g) = \mathcal{E}\,\mathrm{ord}(g)$. It follows that $rk(g) \leq rk(h)$, and $rk(g) = rk(h)$ if and only if $\tau_i = 1$ for $i = 1, \dots, s$, that is, $h = cg$ for some $c \in K$. Thus, N does not contain elements reduced with respect to g, and g is the element of the lowest rank in N. It follows that if $\mathcal{A} = \{h_1, \dots, h_l\}$ is an $\mathcal{E}$-characteristic set of N, then $rk(g) = rk(h_1)$ and $l = 1$, whence $\{g\}$ is also an $\mathcal{E}$-characteristic set of N. □

Remark 3.18. *The concepts of $\mathcal{E}$-autoreduced and $\mathcal{E}$-characteristic sets in a finitely generated free σ-K-module with n free generators produce the corresponding notions for linear difference (σ-) ideals in the algebra of difference polynomials $R = K\{y_1, \dots, y_n\}$ in n σ-indeterminates over K (see [6, Section 3.3]). If one considers the free σ-K-module F generated by $y_1, \dots, y_n$ in R, then every $\mathcal{E}$-autoreduced set of F will be an autoreduced set (in the sense of [6, Definition 3.3.4]) of the σ-ideal of R generated F. Therefore, if F is a free σ-K-module with n free generators $f_1, \dots, f_n$, N a σ-K-submodule of F and $\mathcal{A}$ is an $\mathcal{E}$-characteristic set of N, then one can apply [6, Theorem 6.4.1] to the factor module F/N and obtain that there exists a numerical polynomial $\phi(t)$ of degree at most m such that $\phi(r) = \dim_K (F_r / N \bigcap F_r)$ for all sufficiently large $r \in \mathbb{N}$. ($F_r = \sum_{i=1}^{n} \mathfrak{D}_r f_i$ where $\mathfrak{D}_r$ is the K-vector space generated by $T(r)$.) Furthermore, this theorem shows that if A_j is the set of all m-tuples $(k_1, \dots, k_m) \in \mathbb{N}^m$ such that $\alpha_1^{k_1} \dots \alpha_m^{k_m} f_j$ $(1 \leq j \leq n)$ is a leader of an element of $\mathcal{A}$, then $\phi(t) = \sum_{j=1}^{n} \omega_{A_j}(t)$ where $\omega_{A_j}(t)$ is the Kolchin polynomial of the set A_j defined in Theorem 2.2.*

4 THE MAIN THEOREM AND ITS APPLICATIONS

The following theorem is the main result of the paper.

Theorem 4.1. *Let K be a difference field with a basic set $\sigma = \{\alpha_1, \dots, \alpha_m\}$ and M a finitely generated σ-K-module with generators $x_1, \dots, x_n$ (that is, $M = \sum_{i=1}^{n} \mathfrak{D} x_i$ where $\mathfrak{D}$ is the ring of difference (σ-) operators over K). For any $r, s \in \mathbb{N}$, let $M_{rs} = \sum_{i=1}^{n} \mathfrak{D}_{rs} x_i$ where $\mathfrak{D}_{rs}$ denotes the K-vector subspace of $\mathfrak{D}$ generated by all elements τx_i $(1 \leq i \leq n)$ with $\tau \in T(r, s)$. Then there exists a polynomial $\psi(t_1, t_2) \in \mathbb{Q}[t_1, t_2]$ and numbers $r_0, s_0, s_1 \in \mathbb{N}$ with $s_1 < r_0 - s_0$ such that*

(i) *$\psi(r, s) = \dim_K M_{rs}$ for all $(r, s) \in \mathbb{N}^2$ with $r \geq r_0$, $s_1 \leq s \leq r - s_0$.*

(ii) *$\psi(t_1, t_2) = \psi^{(1)}(t_1) - \psi^{(2)}(t_2)$ where $\deg \psi^{(i)}(t) \leq m$ $(i = 1, 2)$, so $\psi(t_1, t_2)$ can be written as*

$$\psi_(t_1, t_2) = \sum_{i=0}^{m} a_i \binom{t_1 + i}{i} - \sum_{j=0}^{m} b_j \binom{t_2 + j}{j} \tag{4}$$

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

(iii) *For all sufficiently large $r \in \mathbb{N}$, $\psi^{(1)}(r) = \phi(r)$ where $\phi(t)$ is the difference (σ-) dimension polynomial of M associated with the filtration $(M_r = \sum_{i=1}^{n} \mathfrak{D}_r x_i)_{r \in \mathbb{Z}}$ where $\mathfrak{D}_r$ denotes the K-vector subspace of $\mathfrak{D}$ generated by all elements τx_i $(1 \leq i \leq n)$ with $\tau \in T(r)$.*

(iv) *$a_m = b_m = \sigma\text{-}\dim_K M$. Furthermore, $d = \deg_{t_1} \psi$, and a_d are invariants of the σ-K-module M, that is, they do not depend on the finite system of σ-generators of M over K the polynomial $\psi(t_1, t_2)$ is associated with.*

(v) *$\deg \psi^{(1)} \geq \deg \psi^{(2)}$ and if $\deg \psi^{(1)} = \deg \psi^{(2)} = e < m$, then b_e is also an invariant of M.*

Definition 4.2. *The bivariate numerical polynomial $\psi(t_1, t_2)$ whose existence is established by Theorem 4.1 is called a σ-E-dimension polynomial of the σ-K-module M associated with the system of σ-K-generators $\{x_1, \dots, x_n\}$.*

We will start the proof of the theorem with the following lemma.

Lemma 4.3. *With the above notation, let F be a free $\mathfrak{D}$-module with a basis $f_1, \dots, f_n$, and $\pi : F \longrightarrow M$ the natural $\mathfrak{D}$-epimorphism of F onto M ($\pi(f_i) = x_i$ for $i = 1, \dots, n$). Let $N = \operatorname{Ker} \pi$ and let $\mathcal{A} = \{g_1, \dots, g_p\}$ be an $\mathcal{E}$-characteristic set of N. Let u_i and v_i denote the leader and coleader of g_i, respectively ($1 \le i \le p$). For any $r, s \in \mathbb{N}$ such that $s \le r$, let*

$$W(r,s) = \{w \in Tf \mid s \le \operatorname{ord} w \le r\}, \quad W_M(r,s) = \pi(W(r,s)),$$

$$U'(r,s) = \{u \in Tf \mid s \le \operatorname{ord} u \le r \ \text{ and } \ u_i \nmid u \ (i = 1, \dots, p)\}$$

$$U'_M(r,s) = \{\pi(u) \mid u \in U'(r,s)\},$$

$$U''(r,s) = \{u \in Tf \mid s \le \operatorname{ord} u \le r, \ \ u \text{ is divisible by some } u_i$$

($1 \le i \le p$) and whenever $u = \tau u_i$ for some $\tau \in T$, one has $\operatorname{ord}(\tau v_i) < s\}$, *and*

$$U''_M(r,s) = \{\pi(u) \mid u \in U''(r,s)\}.$$

Furthermore, let

$$U(r,s) = U'(r,s) \bigcup U''(r,s) \text{ and } U_M(r,s) = U'_M(r,s) \bigcup U''_M(r,s).$$

Then for every $(r,s) \in \mathbb{N}^2$, $s < r$, the set $U_M(r,s)$ is a basis of the K-vector space M_{rs}.

Proof. First, let us show that the set $U_M(r,s)$ is linearly independent over K. Indeed, suppose that $\sum_{i=1}^{k} a_i \pi(u_i) = 0$ for some $u_1, \dots, u_k \in U(r,s)$ and $a_1, \dots, a_k \in K$. Then $h = \sum_{i=1}^{k} a_i u_i$ is an element of N which is $\mathcal{E}$-reduced with respect to $\mathcal{A}$. Indeed, if a term $u = \tau f_j$ appears in h (so that $u = u_i$ for some i, $1 \le i \le k$), then either u is not a transform of any u_ν ($1 \le \nu \le p$) or $u = \tau u_\nu$ for some $\tau \in T$, $1 \le \nu \le p$, such that $\operatorname{ord}(\tau v_\nu) < s \le \operatorname{ord} v_h$, hence $\tau v_\nu < v_h$. Thus, h is $\mathcal{E}$-reduced with respect to the $\mathcal{E}$-characteristic set $\mathcal{A}$, hence (see Proposition 3.13) $h = 0$ and $a_1 = \dots = a_k = 0$.

Now let us prove that if $s \in \mathbb{N}$ and $s \le r - s_0$, where $s_0 = \max\{\operatorname{Eord} g_i \mid 1 \le i \le p\}$, then every element $\tau x_j \in W_M(r,s) \setminus U_M(r,s)$ ($\tau \in T$, $1 \le j \le n$) can be written as a finite linear combination of elements of $U_M(r,s)$ with coefficients in K. In this case $\tau f_j \notin U(r,s)$, hence τf_j is equal to some term of the form $\tau' u_i$ ($1 \le i \le p$) where $\tau' \in T$ and $\operatorname{ord}(\tau' v_i) \ge s$. Let us consider the element $g_i = c_i u_i + \dots$ ($c_i \in K, c_i \ne 0$), where dots are placed instead of the linear combination of terms that appear in g_i and that are less than u_i. Since $g_i \in N = \operatorname{Ker} \pi$, $\pi(g_i) = c_i \pi(u_i) + \dots = 0$, whence $\pi(\tau' g_i) = c_j \pi(\tau' u_i) + \dots = c_i \pi(\tau f_j) + \dots = c_i \tau x_j + \dots = 0$, so that τx_j is a finite linear combination with coefficients in K of some elements $\tilde{\tau} x_l$ ($1 \le l \le n$) such that $\tilde{\tau} \in T(r,s)$ and $\tilde{\tau} f_l < \tau' u_i$. Thus, we can apply the induction on the well-ordered set Tf and obtain that every element τx_i ($\tau \in T(r,s)$, $1 \le i \le n$) can be written as a finite linear combination of elements of the set $\pi(U(r,s))$ with coefficients in K. It follows that $U_M(r,s)$ is a basis of the K-vector space M_{rs}. □

Now we can prove the main theorem.

Proof. As above, let F be a free $\mathfrak{D}$-module with a basis $f_1, \dots, f_n$, N the kernel of the natural σ-epimorphism $\pi : F \to M$, and $\mathcal{A} = \{g_1, \dots, g_p\}$ an $\mathcal{E}$-characteristic set of N. Furthermore, let $U(r,s)$ and $U_M(r,s)$ be the sets defined in the proof of the Lemma 4.3 ($s, r \in \mathbb{N}, s \le r$). By this lemma, for any $r, s \in \mathbb{N}$, $s \le r$, $U_M(r,s)$ is a basis of the K-vector space M_{rs}. Therefore, $\dim_K M_{rs} = \operatorname{Card} U_M(r,s) = \operatorname{Card} U(r,s)$. (It was shown in the second part of the proof of Lemma 4.3 that the restriction of the mapping π on $U(r,s)$ is bijective.)

In order to evaluate the size of $U(r,s)$ we are gong to evaluate the sizes of the sets $U'(r,s)$ and $U''(r,s)$. For every $k = 1, \dots, n$, let

$$A_k = \{(i_1, \dots, i_m) \in \mathbb{N}^m \mid \alpha_1^{i_1} \dots \alpha_m^{i_m} f_k \ \text{ is the leader of some}$$

element of $\mathcal{A}\}$.

Applying Theorem 2.2, we obtain that there exists a numerical polynomial $\omega_k(t)$ such that $\omega_k(r) = \operatorname{Card} V_{A_k}(r)$ for all sufficiently large $r \in \mathbb{N}$. It follows that if we set $\omega(t) = \sum_{k=1}^{n} \omega_k(t)$, then there exist $r_0, s_1 \in \mathbb{N}$ such that for all $r, s \in \mathbb{N}$ with $r \ge r_0$ and $s_1 \le s \le r - s_0$, $\operatorname{Card} U'(r,s) = \omega(r) - \omega(s)$. Furthermore, $\deg \omega \le m$, and $\deg \omega = m$ if and only if at least one of the sets A_k ($1 \le k \le n$) is empty.

In order to evaluate $\operatorname{Card} U''(r,s)$ note that this set consists of all terms τu_i ($\tau \in T, 1 \le i \le p$) such that $s \le \operatorname{ord}(\tau u_i) \le r$ and $\operatorname{ord}(\tau v_i) < s$. For every fixed i, the number N_i of such terms is equal to $\operatorname{Card}\{\tau \in T \mid s - \operatorname{ord} u_i - 1 < \operatorname{ord} \tau \le s - \operatorname{ord} v_i - 1\} = \binom{s - \operatorname{ord} v_i - 1 + m}{m} - \binom{s - \operatorname{ord} u_i - 1 + m}{m}$.

Applying the principle of inclusion and exclusion (taking into account terms that are multiples of more than one leaders u_i), we obtain that $\operatorname{Card} U''(r,s)$ is an alternating sum of polynomials of the form $\binom{s-a+m}{m} - \binom{s-b+m}{m}$ where $a, b \in \mathbb{N}$, $a \le b$. It follows that $\operatorname{Card} U''(r,s)$ is expressed by a numerical polynomial of s of degree at most $m-1$. Denoting this polynomial by $\omega'(s)$ and setting $\psi^{(1)}(t_1) = \omega(t_1)$ and $\psi^{(2)}(t_2) = \omega(t_2) - \omega'(t_2)$, we obtain a numerical polynomial $\psi(t_1, t_2) = \psi^{(1)}(t_1) - \psi^{(2)}(t_2)$ that satisfies conditions (i) and (ii) of our theorem. Furthermore, it follows from Remark 3.18 that $\psi^{(1)}(t_1) = \phi(t_1)$ where $\phi(t)$ is the polynomial described in part (iii) of the theorem.

In order to prove the last two statements of the theorem, suppose that $\{z_1, \dots, z_k\}$ is another system of generators of M as a $\mathfrak{D}$-module and let $\bar{M}_{rs} = \sum_{i=1}^{k} \mathfrak{D}_{rs} z_i$ and $\bar{M}_r = \sum_{i=1}^{k} \mathfrak{D}_r z_i$ for any $r, s \in \mathbb{N}$. Then there exists $q \in \mathbb{N}$ such that $x_i \in \bar{M}_q$ and $z_j \in M_q$ ($1 \le i \le n, 1 \le j \le k$). It follows that if $\bar{\psi}(t_1, t_2)$ is the σ-E-dimension polynomial associated with the system of σ-K-generators $\{z_1, \dots, z_k\}$, then for all sufficiently large $r, s \in \mathbb{N}$ with $s_1 \le s \le r - s_0$ for certain $s_0, s_1 \in \mathbb{N}$, one has

$$\psi(r,s) \le \bar{\psi}(r+q, s) \ \text{ and } \ \bar{\psi}(r,s) \le \psi(r+q, s). \tag{5}$$

Furthermore, as we have proved, $\psi^{(1)}(t_1) = \phi(t_1)$ and $\bar{\psi}^{(1)}(t_1) = \bar{\phi}(t_1)$ where $\phi(t_1)$ and $\bar{\phi}(t_1)$ are σ-dimension polynomials of M associated with filtrations $(M_r = \sum_{i=1}^{n} \mathfrak{D}_r x_i)_{r \in \mathbb{Z}}$ and $(\bar{M}_r = \sum_{j=1}^{k} \mathfrak{D}_r z_j)_{r \in \mathbb{Z}}$, respectively. It follows from Theorem 2.1 that the coefficients of t_1^m in the polynomials ψ and $\bar{\psi}$ are equal to σ-$\dim_K M$, $\deg_{t_1} \psi = \deg_{t_1} \bar{\psi}$, and if this common degree is denoted by d, then ψ and $\bar{\psi}$ have the same coefficient a_d of the summand $\binom{t_1 + d}{d}$ in the representation (4).

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

The evaluation of $\operatorname{Card} U''(r,s)$ in the proof of the first part of the theorem shows that this number is expressed by a polynomial of s of degree at most $m-1$. Suppose that $\deg \psi^{(1)} = \deg \psi^{(2)} = e < m$. Then setting $t_1 = r$ and $t_2 = r - s_0$ in the representations of the form (4) for $\psi(t_1, t_2)$ and $\bar{\psi}(t_1, t_2)$ and using (5), we obtain that the coefficients of r^e in the resulting polynomials of r are the same, $a_e - b_e$. Since a_e is an invariant of the module M , so is b_e. □

Example 4.4. Let K be a difference field with a basic set $\sigma = \{\alpha_1, \alpha_2\}$ and let M be a σ-K-module with one generator x over the ring of σ-operators $\mathfrak{D}$ and with the defining equation

$$\alpha_1^a \alpha_2^b x + \alpha_1^b x + \alpha_2^a x = 0. \tag{6}$$

where a and b are positive integers, $1 \leq a \leq b$. In other words, if F denotes the free $\mathfrak{D}$-module with free generator $f$and $g = \alpha_1^a \alpha_2^b f + \alpha_1^b f + \alpha_2^a f \in F$, then $N = [g]$ is the kernel of the natural σ-epimorphism $F \to M$ $(f \mapsto x)$. By Proposition 3.17, $\{g\}$ is an $\mathcal{E}$-characteristic set of N. With the notation of Section 3 we have $u_g = \alpha_1^a \alpha_2^b f$, $v_g = \alpha_2^a f$, $\operatorname{Eord}(g) = (a + b) - a = b$, and $\mathcal{E}\operatorname{ord}(g) = (b, a, b - a, 0)$. Furthermore, with the notation of the proof of Lemma 4.3, if s is sufficiently large and $s \leq r - b$, then

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

Then

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

Now,

$$\operatorname{Card} U''(r,s) = \operatorname{Card}\{\alpha_1^{k_1}\alpha_1^{k_2}(\alpha_1^a\alpha_2^b y) \mid k_1 + k_2 + a + b \geq s \text{ and } k_1 + k_2 + a < s\} = \operatorname{Card}\{(k_1,k_2) \in \mathbb{N}^2 \mid s - (a+b) \leq k_1 + k_2 < s - a\}$$
$$= \binom{s-(a+1)+2}{2} - \binom{s-(a+b+1)+2}{2} = bs - \frac{b(2a+b-1)}{2}.$$

We obtain that

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

so that the σ-E-dimension polynomial of M associated with the generator x is as follows:

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

By Remark 3.18, the univariate σ-dimension polynomial $\phi(t)$ of the σ-K-module M associated with the generator x is equal to the Kolchin polynomial of the set $\{(a,b)\} \subset \mathbb{N}^2$. By Theorem 2.3,

$$\phi(t) = \binom{t+2}{2} - \binom{t+2-(a+b)}{2} = (a+b)t - \frac{(a+b)(a+b-3)}{2}.$$

Comparing this polynomial with the bivariate σ-E-dimension polynomial $\psi(t_1, t_2)$, we see that $\phi(t)$ carries two invariants of the module M, $\deg \phi(t) = 1$ and the leading coefficient $a + b$. At the same time, $\psi(t_1, t_2)$ carries three such invariants: $\deg_{t_1} \psi = 1$, $a + b$ (the coefficient of t_1), and $-a$ (the coefficient of t_2). Thus, $\psi(t_1, t_2)$ gives both parameters a and b of the defining equation (6) while $\phi(t)$ gives just the sum of the parameters.

The last example illustrates an important application of the obtained results to the isomorphism problem for difference modules. The example shows that it is possible that two non-isomorphic finitely generated σ-K-modules have the same invariants carried by the univariate σ-dimension polynomial, but have different invariants carried by their bivariate σ-E-dimension polynomials. Therefore, the fact that two finitely generated σ-K-modules are not isomorphic can be proved by comparing the corresponding σ-E-dimension polynomials computed from the corresponding $\mathcal{E}$-characteristic sets while the test based on consideration of invariants of univariate σ-dimension polynomials is inconclusive.

To justify the last observation, let us consider a cyclic σ-K-module $M' = \mathfrak{D}y$ with defining equation

$$\alpha_1^a \alpha_2^b y + y = 0.$$

Proceeding as in Example 4.4, we get (with the above notation)

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

(the same as the corresponding value in Example 4.4) and

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

so the univariate σ-dimension and bivariate σ-E-dimension polynomials for M' associated with the generator y are

$$\phi'(t) = (a+b)t - \frac{(a+b)(a+b-3)}{2} \quad \text{and}$$
$$\psi'(t_1,t_2) = (a+b)t_1 - \frac{(a+b)(a+b-1)}{2},$$

respectively. Thus, the σ-dimension polynomials of M (see Example 4.4) and M' carry the same invariants, $\deg \phi(t) = \deg \phi'(t) = 1$ and $a + b$. At the same time, the sets of invariants of the σ-E-dimension polynomials $\psi(t_1, t_2)$ and $\psi'(t_1, t_2)$ are $\{\deg_{t_1} \psi = 1, a + b, -a\}$ and $\{\deg_{t_1} \psi' = 1, a + b, 0\}$, respectively. Therefore, M and M' are not isomorphic (as $\mathfrak{D}$-modules) even though they have the same invariants carried by their univariate σ-dimension polynomials.

Theorem 4.1 implies the following result about difference fields.

Theorem 4.5. *Let $L = K\langle \eta_1, \ldots, \eta_n \rangle$ be a σ-field extension generated by a set $\eta = \{\eta_1, \ldots, \eta_n\}$. (As before, $\sigma = \{\alpha_1, \ldots, \alpha_m\}$.) Then there exists a polynomial $\psi_{\eta|K}(t_1, t_2) \in \mathbb{Q}[t_1, t_2]$ and $r_0, s_0, s_1 \in \mathbb{N}$ with $s_1 < r_0 - s_0$ such that*

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

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

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

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

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

Proof. Let L^* be the inversive closure of L and let $\Omega_{L^*|K}$ be the module of Kähler differentials of the extension L^*/K. By [11, Lemma 4.2.8], $\Omega_{L^*|K}$ has a natural structure of an inversive difference (σ-) L^*-module, that is, $\Omega_{L^*|K}$ is an L^*-vector space on which elements of the set $\sigma^* = \{\alpha_1, \dots, \alpha_m, \alpha_1^{-1}, \dots, \alpha_m^{-1}\}$ act in such a way that $\alpha(x+y) = \alpha x + \alpha y$, $\alpha(\beta x) = \beta(\alpha x)$, $\alpha(ax) = \alpha(a)\alpha(x)$, and $\alpha(\alpha^{-1}x) = x$ for any $\alpha, \beta \in \sigma^*$; $x, y \in \Omega_{L^*|K}$; $a \in L^*$. Furthermore, $\alpha(d\zeta) = d\alpha(\zeta)$ for any $\zeta \in L^*$ ($d : L^* \to \Omega_{L^*|K}$ is the universal K-linear derivation). In particular, $\Omega_{L^*|K}$ is a $\mathfrak{D}$-module, where $\mathfrak{D}$ is the ring of σ-operators over L^*, and we can consider a $\mathfrak{D}$-submodule $M = \sum_{i=1}^{n} \mathfrak{D} d\eta_i$ of $\Omega_{L^*|K}$. For any $r, s \in \mathbb{N}$, let $M_{rs} = \sum_{i=1}^{n} \mathfrak{D}_{rs} d\eta_i$ where $\mathfrak{D}_{rs}$ is the L^*-vector subspace of $\mathfrak{D}$ generated by the set $T(r,s)$. It follows from [11, Proposition 1.7.13] that $\dim_{L^*} M_{rs} = \text{tr. deg}_K K(\{\tau\eta_j \mid \tau \in T(r,s), 1 \le j \le n\})$, so all statements of our theorem follow from Theorem 4.1. □

The bivariate polynomial $\psi_{\eta|K}(t_1, t_2)$ is called a *σ-E-dimension polynomial* of the σ-field extension L/K associated with the system of generators η.

Note that the last theorem generalizes the theorem on univariate difference dimension polynomial of a difference field extension introduced in [7]. (With the notation of Theorem 4.5, this numerical polynomial gives $\text{tr. deg}_K K(\{\tau\eta_j \mid \tau \in T(r), 1 \le j \le n\})$ for all sufficiently large $r \in \mathbb{N}$). Applications of univariate dimension polynomials of difference field extensions to the study of difference rings, modules and systems of algebraic difference equations, as well as methods of computation of such polynomials, can be found in [6] and [11].

The σ-E-dimension polynomial has a natural interpretation in the spirit of Einstein's strength of a system of equations in finite differences (see [11, Section 7.7] for the description of this notion, which is a difference analog of Einstein's strength of a system of partial differential equations introduced in [2]). Let

$$A_i(f_1, \dots, f_n) = 0 \qquad (i = 1, \dots, p) \tag{7}$$

be a system of equations in finite differences with respect to n unknown grid functions $f_1, \dots, f_n$ in m real variables $x_1, \dots, x_m$ with coefficients in some functional field K. Suppose that the difference grid, whose nodes form the domain of considered functions, has equal cells of dimension $h_1 \times \cdots \times h_m$ ($h_1, \dots, h_m \in \mathbb{R}$) and fills the whole space $\mathbb{R}^m$. (As an example, one can consider a field K consisting of the zero function and fractions of the form u/v where u and v are grid functions defined almost everywhere and vanishing at a finite number of nodes.) Let us fix some node $\mathcal{P}$ and say that *a node Q has order i* (with respect to $\mathcal{P}$) if the shortest path from $\mathcal{P}$ to Q along the edges of the grid consists of i steps (by a step we mean a path from a node of the grid to a neighbor node along the edge between these two nodes). Let us consider the values of the unknown grid functions $f_1, \dots, f_n$ at the nodes whose orders lie between s and r inclusively ($r, s \in \mathbb{N}$, $s \le r$). If $f_1, \dots, f_n$ should not satisfy any system of equations (or any other condition), their values at nodes of any order can be chosen arbitrarily. Because of the system in finite differences (and equations obtained from the equations of the system by transformations of the form $f_j(x_1, \dots, x_m) \mapsto f_j(x_1 + k_1 h_1, \dots, x_m + k_m h_m)$ with $k_1, \dots, k_m \in \mathbb{N}$, $1 \le j \le m$), the number of independent values of the functions $f_1, \dots, f_n$ at the nodes of order $\le r$ decreases. This number, which is a function of r and s, can be viewed as a generalized "measure of strength" of the system in finite differences (in the sense of A. Einstein). We denote it by S_{rs}. (The direct difference counterpart of Einstein's strength expresses the number of independent values of unknown functions at nodes of order at most r, $r \in \mathbb{N}$.)

Considering the field of coefficients K as a difference field with a set of m translation $\sigma = \{\alpha_1, \dots, \alpha_m\}$ such that

$$\alpha_j f(x_1, \dots, x_m) = f(x_1, \dots, x_{j-1}, x_j + h_j, \dots, x_m)$$

($1 \le j \le m$) and assuming that the left-hand sides of equations (7) are polynomials in f_i's and their transforms, we can treat system (7) as a system of algebraic difference equations $A_i(y_1, \dots, y_n) = 0$ ($1 \le i \le n$) in the ring of difference (σ-) polynomials $R = K\{y_1, \dots, y_n\}$. Suppose that the reflexive difference ideal P generated by $A_1, \dots, A_p$ in R is prime (in this case the system (7) is said to be prime) and L is the difference field of fractions of R/P. Then $L = K\langle\eta_1, \dots, \eta_n\rangle$, where η_i denotes the canonical image of y_i in L ($1 \le i \le n$), and one can consider the σ-E-dimension polynomial $\psi_{\eta|K}(t_1, t_2)$ of the σ-field extension L/K associated with the system of generators η. This polynomial is said to be the σ-E-dimension polynomial of system (7). In the considered case, $\psi_{\eta|K}(r, s) = S_{rs}$ for sufficiently large values of r and s (and with $s \le r - s_0$ for some $s_0 \in \mathbb{N}$), so the σ-E-dimension polynomial of a prime system of difference equations can be viewed as a generalized measure of strength of such a system. In this connection, Example 4.4 can be viewed as computation of the strength of equation (6); equations of this type arise from finite difference approximations to heat, wave and many other PDEs of mathematical physics.

5 ACKNOWLEDGES

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

REFERENCES

[1] Cohn, R. M. *Difference Algebra.* Interscience, New York, 1965.

[2] A. Einstein. The Meaning of Relativity. *Appendix II (Generalization of gravitation theory).* Princeton University Press, Princeton, NJ, 1953, 153–165.

[3] Hrushovski, E. The Elementary Theory of the Frobenius Automorphisms. arXiv:math/0406514v1, 2004, 1–135. The updated version (2012): www.ma.huji.ac.il/ehud/FROB.pdf.

[4] E. R. Kolchin. The notion of dimension in the theory of algebraic differential equations. *Bull. Amer. Math. Soc.*, 70 (1964), 570–573.

[5] E. R. Kolchin. *Differential Algebra and Algebraic Groups.* Academic Press, 1973.

[6] M. V. Kondrateva, A. B. Levin, A. V. Mikhalev, and E. V. Pankratev. *Differential and Difference Dimension Polynomials.* Kluwer Acad. Publ., 1999.

[7] A. B. Levin. Characteristic polynomials of filtered difference modules and of difference field extensions. *Russian Math. Surveys*, 33 (1978), no.3, 165–166.

[8] A. B. Levin. Multivariable Difference Dimension Polynomials. *Journal of Mathematical Sciences*, 131, no. 6 (2005), 6060–6082.

[9] A. B. Levin Computation of the Strength of Systems of Difference Equations via Generalized Gröbner Bases. *Grobner Bases in Symbolic Analysis*, Walter de Gruyter, 2007, 43–73.

[10] A. B. Levin. Gröbner bases with respect to several orderings and multivariable dimension polynomials. *J. Symbolic Comput.*, 42 (2007), 561–578.

[11] A. B. Levin *Difference Algebra.* Springer, 2008.

[12] A. B. Levin. Dimension Polynomials of Intermediate Fields of Inversive Difference Field Extensions. *Lect. Notes in Comp. Sci.*, 9582 (2016), 362–376.

[13] A. B. Levin and A. V. Mikhalev. Type and Dimension of Finitely Generated G-algebras. *Contemporary Mathematics*, 184 (1995), 275–280.

[14] Wibmer, M. Algebraic Difference Equations. *Lecture Notes*, University of Pennsylvania. http://www.mmrc.iss.ac.cn/mm2015/notes/wibmer1.pdf