Bivariate Dimension Quasi-polynomials of Difference-Differential Field Extensions with Weighted Basic Operators

Alexander Levin

The Catholic University of America
Washington, D. C. 20064

23rd Conference on Applications of Computer Algebra

Jerusalem, July 18, 2017

Let K be a difference-differential field of zero characteristic with basic sets of derivations $\Delta = \{\delta_1, \dots, \delta_m\}$ and automorphisms $\sigma = \{\alpha_1, \dots, \alpha_n\}$ (any two mapping from the set $\Delta \cup \sigma$ commute) and let every δ_i, $1 \le i \le m$ (respectively, every α_j, $1 \le j \le n$) be assigned a positive integer weight v_i (respectively, w_j). Let $V = \{v_1, \dots, v_m\},\ W = \{w_1, \dots, w_n\}$.

Let T be the free commutative semigroup generated by the set $\Delta \cup \sigma$, that is, the semigroup of all power products

$$\tau = \delta_1^{k_1} \dots \delta_m^{k_m} \alpha_1^{l_1} \dots \alpha_n^{l_n} \ (k_i, l_j \in \mathbb{N}).\ \text{The numbers}$$

$$\operatorname{ord}_\Delta \tau = \sum_{i=1}^{m} v_i k_i \ \text{ and } \ \operatorname{ord}_\sigma \tau = \sum_{j=1}^{n} w_j l_j$$

are called the *orders* of τ with respect to Δ and σ (and with respect to the given weights).

Furthermore, for every $r, s \in \mathbb{N}$, we set

$$T(r, s) = \{\tau \in T \mid \text{ord}_\Delta \tau \leq r, \text{ ord}_\sigma \tau \leq s\}.$$

In what follows, we will often use the prefix Δ-σ- instead of the adjective "difference-differential".

If $\eta = \{\eta_1, \dots, \eta_q\}$ is a finite subset of a Δ-σ-field extension of K, we write $K\langle\eta_1, \dots, \eta_q\rangle$ for the Δ-σ-field extension of K generated by the set η. (As a field, it coincides with $K(\{\tau(\eta_i) \mid \tau \in T, 1 \leq i \leq q\})$.)

Dimension quasi-polynomials of subsets of $\mathbb{N}^p$

A function $f : \mathbb{Z} \to \mathbb{Q}$ is called a (univariate) **quasi-polynomial** of period q if there exist q polynomials $g_i(x) \in \mathbb{Q}[x]$ $(0 \leq i \leq q-1)$ such that

$$f(n) = g_i(n) \ \text{ whenever } \ n \in \mathbb{Z}, \ \text{ and } \ n \equiv i \, (mod \ q).$$

An equivalent way of introducing quasi-polynomials is as follows.
A **rational periodic number** $U(n)$ is a function $U : \mathbb{Z} \to \mathbb{Q}$ with the property that there exists (a period) $q \in \mathbb{N}$ such that

$$U(n) = U(n') \ \text{ whenever } \ n \equiv n' \, (mod \ q).$$

A rational periodic number can be represented by a list of q its possible values enclosed in square brackets:

$$U(n) = [a_0, \ldots, a_{q-1}]_n.$$

Example 1. $U(n) = \left[\frac{1}{2}, \frac{3}{4}, 1\right]_n$ is a periodic number with period 3 such that $U(n) = \frac{1}{2}$ if $n \equiv 0\,(mod\ 3)$,

$U(n) = \frac{3}{4}$ if $n \equiv 1\,(mod\ 3)$, and $U(n) = 1$ if $n \equiv 2\,(mod\ 3)$.

A (univariate) **quasi-polynomial** of degree d is a function $f : \mathbb{Z} \to \mathbb{Q}$ such that

$$f(n) = c_d(n)n^d + \cdots + c_1(n)n + c_0(n) \quad (n \in \mathbb{Z})$$

where $c_i(n)$'s are rational periodic numbers and $c_d(n) \neq 0$.

One of the main applications of the theory of quasi-polynomials is its application to the problem of counting integer points in polytopes.

Recall that a **rational polytope** in $\mathbb{R}^d$ is the convex hall of finitely many points (vertices) in $\mathbb{Q}^d$.
Equivalently, a rational polytope $P \subseteq \mathbb{R}^d$ is the set of solutions of a finite system of linear inequalities

$$A\mathbf{x} \leq \mathbf{b},$$

where A is an $m \times d$-matrix with integer entries (m is a positive integer) and $\mathbf{b} \in \mathbb{Z}^m$, provided that the solution set is bounded.

Let $P \subseteq \mathbb{R}^d$ be a rational polytope. (We assume that P has dimension d, that is, P is not contained in a proper affine subspace of $\mathbb{R}^d$.) Then a polytope

$$rP = \{r\mathbf{x} \mid \mathbf{x} \in P\}$$

($r \in \mathbb{N}$, $r \geq 1$) is called the rth dilate of P.

Clearly, if $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are all vertices of P, then rP is the convex hall of $r\mathbf{v}_1, \ldots, r\mathbf{v}_k$.

In what follows, $L(P, r)$ denotes the number of integer points (that is, points with integer coordinates) in rP. In other words,

$$L(P, r) = \mathrm{Card}(rP \cap \mathbb{Z}^d).$$

Theorem 1 (Ehrhart, 1962)

$L(P, r)$ is a degree d quasi-polynomial of r whose leading coefficient is equal to the Euclidean volume of P.

The main tools for computation of Ehrhart quasi-polynomials are Alexander Barvinok's polynomial time algorithm and its modifications, see

[A. I. Barvinok. Computing the Ehrhart polynomial of a convex lattice polytope, Discrete Comput. Geom. 12 (1994), 35–48] and

[A. I. Barvinok and J. E. Pommersheim, An algorithmic theory of lattice points in polyhedra, New Perspectives in Algebraic Combinatorics. Math. Sci. Res. Inst. Publ., vol. 38, Cambridge Univ. Press, 1999, 91–147].

Let $\mathbf{p} = (p_1, \ldots, p_k)$ be a k-dimensional parameter vector. A *k-dimensional periodic number* (on $p_1, \ldots, p_k$) $U(\mathbf{p})$ is a function $U : \mathbb{Z}^k \to \mathbb{Q}$ such that there exists a k-tuple $\mathbf{q} = (q_1, \ldots, q_k) \in \mathbb{N}^k$, $q_i > 0$, with the property

$$U(p_1, \ldots, p_k) = U(p'_1, \ldots, p'_k) \text{ if } p_i \equiv p'_i \,(mod\, q_i),\ 1 \le i \le k.$$

$\mathbf{q} = (q_1, \ldots, q_k)$ is called a *multi-period* of U.

Say, $[[1, \frac{1}{2}]_{p_2}, [0, \frac{3}{2}]_{p_2}, [-1, \frac{1}{4}]_{p_2}]_{p_1}$ is a 2-dimensional periodic number with a 2-period $\mathbf{q} = (3, 2)$.

A polynomial in k variables $p_1, \ldots, p_k$, where each coefficient is a multidimensional periodic number on a subset of $\{p_1, \ldots, p_k\}$, is called a **multivariate quasi-polynomial** (in $p_1, \ldots, p_k$).

Let $m, n \in \mathbb{N}$, $A \subseteq \mathbb{N}^{m+n}$ and let

$X_A = \{\mathbf{x} = (x_1, \dots, x_{m+n}) \,|\, \mathbf{x}$ is not greater than or equal to any $\mathbf{a} \in A$ with respect to the product order $<_P$ on $\mathbb{N}^{m+n}\}$.

($(a_1, \dots, a_{m+n}) <_P (x_1, \dots, x_{m+n})$ iff $a_i < x_i$ for $i = 1, \dots, m+n$.)

Let us fix two sets of positive integers $V = \{v_1, \dots, v_m\}$ and $W = \{w_1, \dots, w_n\}$ ("weights") and define the orders of an $(m+n)$-tuple $\mathbf{a} = (a_1, \dots, a_{m+n}) \in \mathbb{N}^{m+n}$ with respect to these sets as

$$\operatorname{ord}_V \mathbf{a} = \sum_{i=1}^{m} v_i a_i \quad \text{and} \quad \operatorname{ord}_W \mathbf{a} = \sum_{i=m+1}^{m+n} w_i a_i, \text{ respectively.}$$

Furthermore, for any set $A \subseteq \mathbb{N}^{m+n}$ and any $r, s \in \mathbb{N}$, let

$$A(r, s) = \{\mathbf{a} \in A \,|\, \operatorname{ord}_V \mathbf{a} \le r, \operatorname{ord}_W \mathbf{a} \le s\}.$$

Theorem 2

With the above notation, there exists a bivariate quasi-polynomial $\phi_{V,W}(t_1, t_2)$ *such that*

(i) $\phi_{V,W}(r,s) = \mathrm{Card}\, X_A(r,s)$ *for all sufficiently large* $(r,s) \in \mathbb{N}^2$. *(It means that there is* $(r_0, s_0) \in \mathbb{N}^2$ *such that the equality holds for all integers* $r \geq r_0$, $s \geq s_0$*.)*

(ii) $\deg_{t_1} \phi_{V,W} \leq m$ *and* $\deg_{t_2} \phi_{V,W} \leq n$*.*

(iii) $\deg \phi_{V,W} = m + n$ *if and only if* $A = \emptyset$

(iv) $\phi_{V,W}(t_1, t_2) = 0$ *if and only if* $(0, \ldots, 0) \in A$*.*

Sketch of the proof of Theorem 2

Let $A \subseteq \mathbb{N}^{m+n}$ and $X_A = \{\mathbf{x} = (x_1, \dots, x_{m+n}) \in \mathbb{N}^{m+n} \,|\, a \nleq_P \mathbf{x}$ for any $a \in A\}$.

Clearly, if one replaces A with the finite set of all its minimal points with respect to $\leq_P$, this replacement does not change X_A. Therefore, we can assume that A is finite:

$A = \{a^{(1)}, \dots, a^{(d)}\}$ where $a^{(i)} = (a_{i,1}, \dots, a_{i,m+n}),\ \ 1 \leq i \leq d$.

We prove the theorem by induction on n and $\gamma(A) = \sum_{i=1}^{d} \sum_{j=1}^{m+n} a_{i,j}$.

If $n = 0$, the statement is true by [A. Levin. Difference Dimension Quasi-polynomials. To appear in Advances in Appl.Math., 89, (August 2017), pp. 1-17. arXiv:1609.08544v1].

Let $n \geq 1$. If $\mathbf{x} = (x_1, \ldots, x_m, y_1, \ldots, y_n) \in X_A(r, s)$, then either

$y_n = 0$ and $\sum_{i=1}^{n} w_i y_i \leq s$ or $y_n = y'_n + 1$

with $y'_n \in \mathbb{N}$ and $\sum_{i=1}^{n-1} w_i y_i + w_n y'_n \leq s - w_n$. Let $A_0 =$

$\{(a_1, \ldots, a_m, b_1, \ldots, b_{n-1}) \,|\, (a_1, \ldots, a_m, b_1, \ldots, b_{n-1}, 0) \in A\}$,
$(A_0 \in \mathbb{N}^{m+n-1})$ and

$A_1 = \{a = (a_1, \ldots, a_m, b_1, \ldots, b_{n-1}, b'_n) \in \mathbb{N}^{m+n} \,|$
$(a_1, \ldots, a_m, b_1, \ldots, b_{n-1}, b'_n + 1) \in A$ or $b'_n = 0$ and
$(a_1, \ldots, a_m, b_1, \ldots, b_{n-1}, 0) \in A\}$.

If for any $B \subset \mathbb{N}^{m+n}$ and $r, s \in \mathbb{N}$, we set $N_B(r,s) = \mathrm{Card}\{\mathbf{x} = (x_1, \ldots, x_m, y_1, \ldots, y_n) \in X_B \mid \sum_{i=1}^{m} v_i x_i \leq r, \sum_{j=1}^{n} w_j x_j \leq s\}$, then

$$N_A(r,s) = N_{A_0}(r,s) + N_{A_1}(r, s - w_n).$$

Since $|A_1| < |A|$ and $A_0 \subseteq \mathbb{N}^{m+n-1}$, $N_{A_0}(r,s)$ and $N_{A_1}(r, s - w_m)$ are expressed by bivariate quasi-polynomials $\phi_0(t_1, t_2)$ and $\phi_1(t_1, t_2)$ with $\deg_{t_1} \phi_0 \leq m$, $\deg_{t_2} \phi_0 \leq n - 1$, $\deg_{t_1} \phi_1 \leq m$, and $\deg_{t_2} \phi_1 \leq n$. It follows that $N_A(r,s)$ is expressed by a bivariate quasi-polynomial satisfying the conditions of Theorem 2.

Example 2.

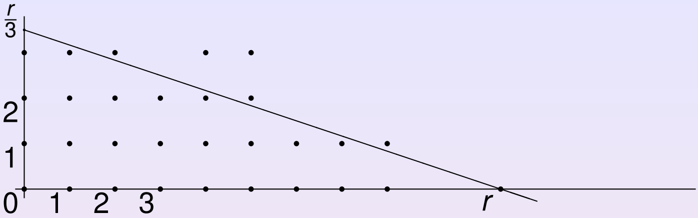
Let $m = 2$, $n = 1$, $A = \{(2,1,1),(0,2,1)\} \subseteq \mathbb{N}^3$ and $v_1 = 1$, $v_2 = 3$, $w_1 = 2$.

Then $A_0 = \emptyset \subseteq \mathbb{N}^2$ and $A_1 = \{(2,1,0),(0,2,0)\} \subseteq \mathbb{N}^3$. In this case $N_A(r,s) = N_{A_0}(r,s) + N_{A_1}(r,s-2)$ where

$N_{A_0}(r,s) = \mathrm{Card}\{(x,y) \in \mathbb{N}^2 \mid x + 3y \leq r\}$ and

$N_{A_1}(r,s-2) = \mathrm{Card}\{(x,y,z) \in \mathbb{N}^3 \mid (2,1,0) \not\leq_P (x,y,z),\ (0,2,0) \not\leq_P (x,y,z) \text{ and } x + 3y \leq r,\ 2z \leq s-2\}$.

Clearly, $N_{A_0}(r,s) = N_{A_0}(r)$ is the number of integer points in the closed triangle $\triangle_r$ with vertices $(0,0)$, $(r,0)$, and $(0,r/3)$.



Applying the Ehrhart's theorem (the area of the triangle $\triangle_1$ is $1/6$), we obtain that

$$N_{A_0}(r) = \frac{1}{6}r^2 + [a, b, c]_r r + [d, e, f]_r$$

for some $a, b, c, d, e, f \in \mathbb{Z}$. In order to find these integers, we can count the number of integer points in the triangles $\triangle_r$ with $r = 0, 1, 2, 3, 4$, and 5 and get

$$N_{A_0}(0) = d = 1,$$
$$N_{A_0}(1) = \frac{1}{6} + b + e = 2,$$
$$N_{A_0}(2) = \frac{2}{3} + 2c + f = 3,$$
$$N_{A_0}(3) = \frac{3}{2} + 3a + d = 5,$$
$$N_{A_0}(4) = \frac{8}{3} + 4b + e = 7,$$
$$N_{A_0}(5) = \frac{25}{6} + 5c + f = 9.$$

It follows that $a = b = c = \frac{5}{6}$, $d = e = 1$, and $f = \frac{2}{3}$, so

$$N_{A_0}(r, s) = N_{A_0}(r) = \frac{1}{6}r^2 + \frac{5}{6}r + [1, 1, \frac{2}{3}]_r$$

for all $r \in \mathbb{N}$.

The direct computation of the number of integer points in $X_{A_1}(r, s-2)$ gives

$$N_{A_1}(r, s-2) = \frac{1}{2}rs + \left[0, -\frac{1}{2}\right]_s r + \frac{3}{2}s + \left[0, -\frac{3}{2}\right]_s$$

whence

$$N_A(r, s) = \frac{1}{6}r^2 + \frac{1}{2}rs + \left[\frac{5}{6}, \frac{1}{3}\right]_s r + \frac{3}{2}s + \left[0, 0, -\frac{1}{3}\right]_r + \left[1, -\frac{1}{2}\right]_s.$$

Thus,

$$\phi_{V,W}(t_1, t_2) = \frac{1}{6}t_1^2 + \frac{1}{2}t_1 t_2 + \left[\frac{5}{6}, \frac{1}{3}\right]_{t_2} t_1 + \frac{3}{2}t_2 + \left[0, 0, -\frac{1}{3}\right]_{t_1} + \left[1, -\frac{1}{2}\right]_{t_2}.$$

Theorem 3

Let K be a Δ-σ-field and let $L = K\langle \eta_1, \dots, \eta_p \rangle$ be a Δ-σ-field extension of K generated by a finite set $\eta = \{\eta_1, \dots, \eta_p\}$. For any $r, s \in \mathbb{N}$, let $L_{r,s} = K(\{\tau(\eta_i) \mid \tau \in T(r,s),\ 1 \leq i \leq p\})$. Then there exists a bivariate quasi-polynomial $\Phi_{\eta|K}^{(V,W)}(t_1, t_2)$ such that

(i) $\Phi_{\eta|K}^{(V,W)}(r,s) = \operatorname{tr.deg}_K L_{rs}$ *for all sufficiently large* $(r,s) \in \mathbb{N}^2$.

(ii) $\deg_{t_1} \Phi_{\eta|K}^{(V,W)} \leq m = \text{Card } \Delta$ *and* $\deg_{t_2} \Phi_{\eta|K}^{(V,W)} \leq n = \text{Card } \sigma$.

(iii) $\Phi_{\eta|K}^{(V,W)}$ *is an alternating sum of bivariate quasi-polynomials of the form $g(t_1)h(t_2)$ where $g(t_1)$ and $h(t_2)$ are (univariate) Ehrhart quasi-polynomials associated with rational conic polytopes.*

(iv) *The total degree and the coefficient of $t_l^m t_2^n$ of $\Phi_{\eta|K}^{(V,W)}(t_1, t_2)$ are constants that do not depend on the set of difference-differential generators η of the extension L/K.*

This theorem generalizes the result on a bivariate difference-differential dimension polynomial proved in [A. Levin, *Reduced Gröbner bases, free difference-differential modules and difference-differential dimension polynomials*, J. Symb. Comput., 29 (2000), 1–26] and also allows one to assign a bivariate quasi-polynomial to a system of algebraic difference-differential (Δ-σ-) equations with weighted basic derivations and translations

$$f_i(y_1, \dots, y_p) = 0 \qquad (i = 1, \dots, q) \tag{1}$$

($f_i \in R = K\{y_1, \dots, y_p\}$ $(1 \leq i \leq q)$ where $K\{y_1, \dots, y_p\}$ is the ring of Δ-σ-polynomials in p variables over K) such that the Δ-σ-ideal P of R generated by $f_1, \dots, f_q$ is prime (e. g., to a system of linear difference-differential equations). Systems of this form arise in connection with systems of PDEs with weighted derivatives and their finite difference approximations.

In this case, the reflexive closure P^* of the Δ-σ-ideal P is also prime, so one can consider the quotient field of R/P^* as a finitely generated Δ-σ-field extension of K: $L = K\langle \eta_1, \dots, \eta_p \rangle$ where η_i is the canonical image of y_i in R/P^*.

The corresponding bivariate dimension quasi-polynomial $\Phi_{\eta|K}^{(V,W)}(t_1, t_2)$ can be viewed as the Einstein's strength of the system (1) in the sense of the corresponding concepts for systems of partial differential and difference equations (see [A. V. Mikhalev, E. V. Pankratev, *Differential dimension polynomial of a system of differential equations*, in *Algebra*, Collection of papers. Moscow State Univ., 1980, 57–67] and Section 7.7 of [A.Levin, *Difference Algebra*. Springer, 2008] for detail descriptions of these concepts and their expressions as dimension polynomials).

Sketch of the proof of the main result (Theorem 3)

Let K be a difference-differential (Δ-σ-) field, $\Delta = \{\delta_1, \dots, \delta_m\}$, $\sigma = \{\alpha_1, \dots, \alpha_n\}$. Let T be the free commutative semigroup generated by $\Delta \bigcup \sigma$, and $R = K\{y_1, \dots, y_p\}$ the algebra of Δ-σ-polynomials. (R can be viewed as a polynomial ring in the set of indeterminates $TY = \{\tau y_i | \tau \in T, 1 \le i \le p\}$ over K with the natural extension of the actions of δ_i and α_j; elements of the set TY are called **terms**.) As before, if

$\tau = \delta_1^{k_1} \dots \delta_m^{k_m} \alpha_1^{l_1} \dots \alpha_n^{l_n} \in T$ (k_i, $l_j \in \mathbb{N}$), then the numbers

$$\operatorname{ord}_\Delta \tau = \sum_{i=1}^{m} v_i k_i \quad \text{and} \quad \operatorname{ord}_\sigma \tau = \sum_{j=1}^{n} w_j l_j$$

are said to be the *orders* of τ with respect to Δ and σ, respectively. We also set $\tau_\Delta = \delta_1^{k_1} \dots \delta_m^{k_m}$ and $\tau_\sigma = \alpha_1^{l_1} \dots \alpha_n^{l_n}$.

Consider two well-orderings $<_\Delta$ and $<_\sigma$ of T such that

$$\tau = \delta_1^{k_1} \dots \delta_m^{k_m} \alpha_1^{l_1} \dots \alpha_n^{l_n} <_\Delta \tau' = \delta_1^{k_1'} \dots \delta_m^{k_m'} \alpha_1^{l_1'} \dots \alpha_n^{l_n'} \text{ iff}$$

$$(\mathrm{ord}_\Delta \tau, \mathrm{ord}_\sigma \tau, k_1, \dots, k_m, l_1, \dots, l_n)$$

is less than the corresponding $(m+n+2)$-tuple for τ' with respect to the lexicographic order on $\mathbb{N}^{m+n+2}$. The order $<_\sigma$ is defined in the same way.

The orders $<_\Delta$ and $<_\sigma$ on the set T induce similar well-orderings of the set of terms TY (denoted by the same symbols): if $\tau y_i, \tau' y_j \in TY$, then $\tau y_i <_\Delta$(respectively, $<_\sigma$) $\tau' y_j$ iff $\tau <_\Delta$(respectively, $<_\sigma$) τ' or $\tau = \tau'$ and $i < j$.

If $A \in K\{y_1, \ldots, y_p\} \setminus K$, then the highest terms of A with respect to $<_\Delta$ and $<_\sigma$ are called the Δ-*leader* and σ-*leader* of A, respectively; they are denoted by u_A and v_A, respectively.

If A is written as a polynomial in u_A, $A = I_d(u_A)^d + I_{d-1}(u_A)^{d-1} + \cdots + I_0$, where all terms of $I_0, \ldots, I_d$ are less than u_A with respect to $<_\Delta$, then I_d and $\partial A/\partial u_A$ are called, respectively, the *initial* and *separant* of A; they are denoted by I_A and S_A, respectively.

If $A, B \in K\{y_1, \ldots, y_p\}$, then A is said to have lower rank than B (we write $rk\, A < rk\, B$) if either $A \in K$, $B \notin K$, or the vector $(u_A, \deg_{u_A} A, \operatorname{ord}_\sigma v_A)$ is less than $(u_B, \deg_{u_B} B, \operatorname{ord}_\sigma v_B)$ with respect to the lexicographic order (u_A and u_B are compared with respect to $<_\Delta$).
If the vectors are equal (or $A, B \in K$) we say that A and B are of the same rank and write $rk\, A = rk\, B$.

If $A, B \in K\{y_1, \dots, y_p\}$, then B is said to be reduced with respect to A if
(i) B does not contain terms τu_A such that $\tau_\Delta \neq 1$, and $\operatorname{ord}_\sigma(\tau v_A) \leq \operatorname{ord}_\sigma v_B$.

(ii) If B contains a term τu_A with $\tau_\Delta = 1$, then $\operatorname{ord}_\sigma v_B < \operatorname{ord}_\sigma(\tau v_A)$ or $\operatorname{ord}_\sigma(\tau v_A) \leq \operatorname{ord}_\sigma v_B$ and $\deg_{\tau u_A} B < \deg_{u_A} A$.

If $B \in K\{y_1, \dots, y_p\}$, then B is said to be *reduced with respect to a set* $\Sigma \subseteq K\{y_1, \dots, y_p\}$ if B is reduced with respect to every element of Σ.

A set $\Sigma \subseteq K\{y_1, \dots, y_p\}$ is called *autoreduced* if $\Sigma \bigcap K = \emptyset$ and every element of Σ is reduced with respect to any other element of this set.

Proposition 1

Every autoreduced set is finite.

In what follows, elements of an autoreduced set will be always arranged in order of increasing rank.

Proposition 2

Let $\mathcal{A} = \{A_1, \dots, A_d\}$ be an autoreduced set in the ring $R = K\{y_1, \dots, y_p\}$ and let I_k and S_k denote the initial and separant of A_k, respectively. Furthermore, let $I(\mathcal{A}) = \{X \in K\{y_1, \dots, y_p\} \mid X = 1$ or X is a product of finitely many elements of the form $\tau(I_k)$ and $\tau(S_k)$ where $\tau, \tau' \in T\}$. Then for any Δ-σ-polynomial B, there exist $B_0 \in K\{y_1, \dots, y_p\}$ and $J \in I(\mathcal{A})$ such that B_0 is reduced with respect to $\mathcal{A}$ and $JB \equiv B_0 \,(mod[\mathcal{A}])$ (that is, $JB - B_0 \in [\mathcal{A}]$).

With the notation of the last proposition, we say that the Δ-σ-polynomial *B reduces to B_0* modulo $\mathcal{A}$.

Let $\mathcal{A} = \{A_1, \dots, A_d\}$ and $\mathcal{A}' = \{B_1, \dots, B_e\}$ be two autoreduced sets in $K\{y_1, \dots, y_p\}$. We say that $\mathcal{A}$ has lower rank than $\mathcal{A}'$ if one of the following two cases holds:
(1) There exists $k \in \mathbb{N}$ such that $k \le \min\{d, e\}$, $rk\, A_i = rk\, B_i$ for $i = 1, \dots, k-1$ and $rk\, A_k < rk\, B_k$.
(2) $d > e$ and $rk\, A_i = rk\, B_i$ for $i = 1, \dots, e$.
If $d = e$ and $rk\, A_i = rk\, B_i$ for $i = 1, \dots, d$, then $\mathcal{A}$ is said to have the same rank as $\mathcal{A}'$.

Proposition 3

In every nonempty family of autoreduced sets of Δ-σ-polynomials there exists an autoreduced set of lowest rank.

Let J be any ideal of the ring $K\{y_1, \dots, y_p\}$. Since the set of all autoreduced subsets of J is not empty (if $A \in J$, then $\{A\}$ is an autoreduced subset of J), the last statement shows that the ideal J contains an autoreduced subset of lowest rank. Such an autoreduced set is called a **characteristic set** of the ideal J.

Proposition 4

Let $\mathcal{A} = \{A_1, \dots, A_d\}$ be a characteristic set of a Δ-σ-ideal J of the ring $R = K\{y_1, \dots, y_p\}$. Then an element $B \in J$ is reduced with respect to the set $\mathcal{A}$ if and only if $B = 0$.

Proposition 5

Let $L = K\langle \eta_1, \ldots, \eta_p \rangle$ *and* P *the defining* Δ*-*σ*-ideal of* L/K *(i. e.,* $P = \mathrm{Ker}(K\{y_1, \ldots, y_p\} \to L)$*,* $y_i \mapsto \eta_i$ *). Let* $\mathcal{A} = \{A_1, \ldots, A_d\}$ *be a characteristic set of* P *and for any* $r, s \in \mathbf{N}$*, let*

$U^{(1)}_{r,s} = \{u \in TY \mid \mathrm{ord}_\Delta u \le r, \mathrm{ord}_\sigma u \le s$ *and* $u \neq \tau u_{A_i}$ *for any* $\tau \in T, 1 \le i \le d\}$*,*

$U^{(2)}_{r,s} = \{u \in TY \mid \mathrm{ord}_\Delta u \le r, \mathrm{ord}_\sigma u \le s$ *and for every* $\tau \in T$*,* $A \in \mathcal{A}$ *such that* $u = \tau u_A$*, one has* $\mathrm{ord}_\sigma(\tau v_A) > s\}$*, and*

$$U_{r,s} = U^{(1)}_{r,s} \bigcup U^{(2)}_{r,s}.$$

Then $\bar{U}_{r,s} = \{u(\eta) | u \in U_{r,s}\}$ *is a transcendence basis of the field* $K(\bigcup_{j=1}^{n} T(r,s)\eta_j)$ *over* K*.*

Now, in order to prove the main theorem, one has to evaluate $\text{Card}\, U_{r,s} = U^{(1)}_{r,s} \bigcup U^{(2)}_{r,s}$. By Theorem 2, $\text{Card}\ U^{(1)}_{r,s}$ is expressed by a bivariate quasi-polynomial whose degrees with respect to r and s do not exceed m and n, respectively.
Furthermore, using the principle of inclusion and exclusion, one can express $\text{Card}\ U^{(2)}_{r,s}$ as an alternative sum of bivariate quasi-polynomials that describe the numbers of points $(k_1, \dots, k_m, l_1, \dots, l_n) \in \mathbb{N}^{m+n}$ satisfying the inequalities

$$\sum_{i=1}^{m} v_i k_i \leq r - a, \qquad s - b < \sum_{j=1}^{n} w_j l_j \leq s$$

where $a, b \in \mathbb{N}$. (a and b appear as the orders of the Δ- and σ-leaders of elements of the characteristic set $\mathcal{A}$ with respect to Δ and σ.) It follows that $\text{Card}\ U_{r,s} = \text{tr.}\deg_K K(\bigcup_{j=1}^{n} T(r,s)\eta_j)$ is expressed as a bivariate quasi-polynomial with the properties stated in Theorem 3.

Thanks!

beamer-tu-lo

beamer-ur-log