ISSN 0012-9593

quatrième série - tome 46 fascicule 4 juillet-août 2013

ANNALES SCIENTIFIQUES de L'ÉCOLE NORMALE SUPÉRIEURE

Carlos D'ANDREA & Teresa KRICK & Martín SOMBRA

Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Ann. Scient. Éc. Norm. Sup.
4 e série, t. 46, 2013, p. 549 à 627

HEIGHTS OF VARIETIES IN MULTIPROJECTIVE SPACES AND ARITHMETIC NULLSTELLENSÄTZE

BY Carlos D'ANDREA, Teresa KRICK AND Martín SOMBRA

Abstract. – We present bounds for the degree and the height of the polynomials arising in some problems in effective algebraic geometry including the implicitization of rational maps and the effective Nullstellensatz over a variety. Our treatment is based on arithmetic intersection theory in products of projective spaces and extends to the arithmetic setting constructions and results due to Jelonek. A key role is played by the notion of canonical mixed height of a multiprojective variety. We study this notion from the point of view of resultant theory and establish some of its basic properties, including its behavior with respect to intersections, projections and products. We obtain analogous results for the function field case, including a parametric Nullstellensatz.

Résumé. – Nous présentons des bornes pour les degrés et hauteurs des polynômes apparaissant dans certains problèmes de géométrie algébrique effective, dont l'implicitation d'applications rationnelles et le Nullstellensatz effectif sur une variété. Notre traitement est basé sur la théorie de l'intersection arithmétique dans un produit d'espaces projectifs. Il étend au cadre arithmétique des constructions et résultats dus à Jelonek. Un rôle central est joué par la notion de hauteur canonique mixte d'une variété multiprojective. Nous étudions cette notion à l'aide de la théorie des résultants et nous montrons quelques-unes de ses propriétés de base, y compris son comportement par rapport aux intersections, projections et produits. Nous obtenons aussi des résultats analogues dans le cas d'un corps de fonctions, dont un Nullstellensatz paramétrique.

D'Andrea was partially supported by the research project MTM2010-20279 (Spain). Krick was partially supported by the research projects ANPCyT 3671/05, UBACyT X-113 2008-2010 and CONICET PIP 2010-2012 (Argentina). Sombra was partially supported by the research projects MTM2009-14163-C02-01 and MTM2012-38122-C03-02 (Spain) and by a MinCyT Milstein fellowship (Argentina).

Introduction

In 1983, Serge Lang wrote in the preface to his book [20]:

> *It is legitimate, and to many people an interesting point of view, to ask that the theorems of algebraic geometry from the Hilbert Nullstellensatz to the more advanced results should carry with them estimates on the coefficients occurring in these theorems. Although some of the estimates are routine, serious and interesting problems arise in this context.*

Indeed, the main purpose of the present text is to give bounds for the degree and the size of the coefficients of the polynomials in the Nullstellensatz.

Let $f_1, \dots, f_s \in \mathbb{Z}[x_1, \dots, x_n]$ be polynomials without common zeros in the affine space $\mathbb{A}^n(\overline{\mathbb{Q}})$. The Nullstellensatz says then that there exist $\alpha \in \mathbb{Z} \setminus \{0\}$ and $g_1, \dots, g_s \in \mathbb{Z}[x_1, \dots, x_n]$ satisfying a Bézout identity

$$\alpha = g_1 f_1 + \cdots + g_s f_s.$$

As for many central results in commutative algebra and in algebraic geometry, it is a non-effective statement. By the end of the 1980s, the estimation of the degree and the height of polynomials satisfying such an identity became a widely considered question in connection with problems in computer algebra and Diophantine approximation. The results in this direction are generically known as *arithmetic Nullstellensätze* and they play an important role in number theory and in theoretical computer science. In particular, they apply to problems in complexity and computability [16, 1, 9], to counting problems over finite fields or over the rationals [4, 34], and to effectivity in existence results in arithmetic geometry [17, 3].

The first non-trivial result on this problem was obtained by Philippon, who got a bound on the minimal size of the denominator α in a Bézout identity as above [28]. Berenstein and Yger achieved the next big progress, producing height estimates for the polynomials g_i's with techniques from complex analysis (integral formulae for residues of currents) [2]. Later on, Krick, Pardo and Sombra [19] exhibited sharp bounds by combining arithmetic intersection theory with the algebraic approach in [18] based on duality theory for Gorenstein algebras. Recall that the height of a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, denoted by $\mathrm{h}(f)$, is defined as the logarithm of the maximum of the absolute value of its coefficients. Then, Theorem 1 in [19] reads as follows: if $d = \max_j \deg(f_j)$ and $h = \max_j \mathrm{h}(f_j)$, there is a Bézout identity as above satisfying

$$\deg(g_i) \leq 4\, n\, d^n, \quad \mathrm{h}(\alpha), \mathrm{h}(g_i) \leq 4\, n\, (n+1)\, d^n \big(h + \log s + (n+7)\, \log(n+1)\, d\big).$$

We refer the reader to the surveys [38, 6] for further information on the history of the effective Nullstellensatz, main results and open questions.

One of the main results of this text is the arithmetic Nullstellensatz over a variety below, which is a particular case of Theorem 4.28. For an affine equidimensional variety $V \subset \mathbb{A}^n(\overline{\mathbb{Q}})$, we denote by $\deg(V)$ and by $\widehat{\mathrm{h}}(V)$ the degree and the canonical height of the closure of V with respect to the standard inclusion $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$. The degree and the height of a variety are measures of its geometric and arithmetic complexity, see §2.3 and the references therein for details. We say that a polynomial relation holds on a variety if it holds for every point in it.

THEOREM 1. – *Let $V \subset \mathbb{A}^n(\overline{\mathbb{Q}})$ be a variety defined over $\mathbb{Q}$ of pure dimension r and $f_1, \dots, f_s \in \mathbb{Z}[x_1, \dots, x_n] \setminus \mathbb{Z}$ a family of $s \le r+1$ polynomials without common zeros in V. Set $d_j = \deg(f_j)$ and $h_j = \mathrm{h}(f_j)$ for $1 \le j \le s$. Then there exist $\alpha \in \mathbb{Z} \setminus \{0\}$ and $g_1, \dots, g_s \in \mathbb{Z}[x_1, \dots, x_n]$ such that*

$$\alpha = g_1 f_1 + \cdots + g_s f_s \quad \text{on } V$$

with

- $\deg\big(g_i f_i\big) \le \Big(\prod_{j=1}^{s} d_j\Big) \deg(V)$,
- $\mathrm{h}(\alpha), \mathrm{h}(g_i) + \mathrm{h}(f_i) \le \Big(\prod_{j=1}^{s} d_j\Big)\Big(\widehat{\mathrm{h}}(V) + \deg(V)\Big(\sum_{\ell=1}^{s} \frac{h_\ell}{d_\ell} + (4r+8)\log(n+3)\Big)\Big)$.

For $V = \mathbb{A}^n$, this result gives the bounds

$$\deg\big(g_i f_i\big) \le \prod_{j=1}^{s} d_j\,, \quad \mathrm{h}(\alpha), \mathrm{h}(g_i) + \mathrm{h}(f_i) \le \sum_{\ell=1}^{s}\Big(\prod_{j\ne\ell} d_j\Big) h_\ell + (4n+8)\log(n+3)\prod_{j=1}^{s} d_j.$$

These bounds are substantially sharper than the previously known. Moreover, they are close to optimal in many situations. For instance, let $d_1, \dots, d_{n+1}, H \ge 1$ and set

$$f_1 = x_1 - H,\ f_2 = x_2 - x_1^{d_2},\ \dots,\ f_n = x_n - x_{n-1}^{d_n},\ f_{n+1} = x_n^{d_{n+1}}.$$

This is a system of polynomials without common zeros. Hence, the above result implies that there is a Bézout identity $\alpha = g_1 f_1 + \cdots + g_{n+1} f_{n+1}$ which satisfies $\mathrm{h}(\alpha) \le d_2 \cdots d_{n+1}(\log(H) + (4n+8)\log(n+3))$. On the other hand, specializing any such identity at the point $(H, H^{d_2}, \dots, H^{d_2\cdots d_n})$, we get

$$\alpha = g_{n+1}(H, H^{d_2}, \dots, H^{d_2\cdots d_n}) H^{d_2\cdots d_{n+1}}.$$

This implies the lower bound $\mathrm{h}(\alpha) \ge d_2 \cdots d_{n+1}\log(H)$ and shows that the height bound in Theorem 1 is sharp in this case. More examples can be found in §4.3.

It is important to mention that all previous results in the literature are limited to the case when V is a complete intersection and cannot properly distinguish the influence of each individual f_j, due to the limitations of the methods applied. Hence, Theorem 1 is a big progress as it holds for an arbitrary variety and gives bounds depending on the degree and height of each f_j. This last point is more important than it might seem at first. Indeed, by using Rabinowicz' trick one can show that the weak Nullstellensatz implies its strong version. However, this reduction yields good bounds for the strong Nullstellensatz only if the corresponding weak version can correctly differentiate the influence of each f_j, see Remark 4.27. Using this observation, we obtain in §4.3 the following arithmetic version of the strong Nullstellensatz over a variety.

THEOREM 2. – *Let $V \subset \mathbb{A}^n(\overline{\mathbb{Q}})$ be a variety defined over $\mathbb{Q}$ of pure dimension r and $g, f_1, \dots, f_s \in \mathbb{Z}[x_1, \dots, x_n]$ such that g vanishes on the common zeros of $f_1, \dots, f_s$ in V. Set $d_j = \deg(f_j)$ and $h = \max_j \mathrm{h}(f_j)$ for $1 \le j \le s$. Assume that $d_1 \ge \cdots \ge d_s \ge 1$ and set $D = \prod_{j=1}^{\min\{s,r+1\}} d_j$. Set also $d_0 = \max\{1, \deg(g)\}$ and $h_0 = \mathrm{h}(g)$. Then there exist $\mu \in \mathbb{N}$, $\alpha \in \mathbb{Z} \setminus \{0\}$ and $g_1, \dots, g_s \in \mathbb{Z}[x_1, \dots, x_n]$ such that*

$$\alpha\, g^\mu = g_1 f_1 + \cdots + g_s f_s \quad \text{on } V$$

with

- $\mu \leq 2D\deg(V)$,
- $\deg(g_i f_i) \leq 4d_0 D\deg(V)$,
- $\mathrm{h}(\alpha), \mathrm{h}(g_i) + \mathrm{h}(f_i) \leq 2d_0 D\Big(\widehat{\mathrm{h}}(V) + \deg(V)\Big(\frac{3h_0}{2d_0} + \sum_{\ell=1}^{\min\{s,r+1\}} \frac{h}{d_\ell} + c(n,r,s)\Big)\Big)$,

where $c(n,r,s) \leq (6r+17)\log(n+4) + 3(r+1)\log(\max\{1, s-r\})$.

Our treatment of this problem is the arithmetic counterpart of Jelonek's approach to produce bounds for the degrees in the Nullstellensatz over a variety [14]. To this end, we develop a number of tools in arithmetic intersection and elimination theory in products of projective spaces. A key role is played by the notion of canonical mixed heights of multiprojective varieties, which we study from the point of view of resultants. Our presentation of mixed resultants of cycles in multiprojective spaces is mostly a reformulation of the theory developed by Rémond in [32, 33] as an extension of Philippon's theory of eliminants of homogeneous ideals [27]. We also establish new properties of them, including their behavior under projections (Proposition 1.41) and products (Proposition 1.45).

Let $\boldsymbol{n} = (n_1, \dots, n_m) \in \mathbb{N}^m$ and set $\mathbb{P}^{\boldsymbol{n}} = \mathbb{P}^{n_1}(\overline{\mathbb{Q}}) \times \cdots \times \mathbb{P}^{n_m}(\overline{\mathbb{Q}})$ for the corresponding multiprojective space. For a cycle X of $\mathbb{P}^{\boldsymbol{n}}$ of pure dimension r and a multi-index $\boldsymbol{c} = (c_1, \dots, c_m) \in \mathbb{N}^m$ of length $r+1$, the mixed Fubini-Study height $\mathrm{h}_{\boldsymbol{c}}(X)$ is defined as an alternative Mahler measure of the corresponding mixed resultant (Definition 2.40). The canonical mixed height is then defined by a limit process as

$$\widehat{\mathrm{h}}_{\boldsymbol{c}}(X) := \lim_{\ell \to \infty} \ell^{-r-1} \mathrm{h}_{\boldsymbol{c}}([\ell]_* X),$$

where $[\ell]$ denotes the ℓ-power map of $\mathbb{P}^{\boldsymbol{n}}$ (Proposition-Definition 2.45).

To handle mixed degrees and heights, we introduce a notion of extended Chow ring of $\mathbb{P}^{\boldsymbol{n}}$ (Definition 2.50). It is an arithmetic analogue of the Chow ring of $\mathbb{P}^{\boldsymbol{n}}$ and can be identified with the quotient ring $\mathbb{R}[\eta, \theta_1, \dots, \theta_m]/(\eta^2, \theta_1^{n_1+1}, \dots, \theta_m^{n_m+1})$. We associate to the cycle X an element in this ring, denoted by $[X]_{\mathbb{Z}}$, corresponding under this identification to

$$\sum_{\boldsymbol{c}} \widehat{\mathrm{h}}_{\boldsymbol{c}}(X)\, \eta\, \theta_1^{n_1-c_1} \cdots \theta_m^{n_m-c_m} + \sum_{\boldsymbol{b}} \deg_{\boldsymbol{b}}(X)\, \theta_1^{n_1-b_1} \cdots \theta_m^{n_m-b_m},$$

the sums being indexed by all $\boldsymbol{b}, \boldsymbol{c} \in \mathbb{N}^m$ of respective lengths r and $r+1$ such that $\boldsymbol{b}, \boldsymbol{c} \leq \boldsymbol{n}$. Here, $\deg_{\boldsymbol{b}}(X)$ denotes the mixed degree of X of index $\boldsymbol{b}$. This element contains the information of all non-trivial mixed degrees and canonical mixed heights of X, since $\deg_{\boldsymbol{b}}(X)$ and $\widehat{\mathrm{h}}_{\boldsymbol{c}}(X)$ are zero for any other $\boldsymbol{b}$ and $\boldsymbol{c}$.

The extended Chow ring of $\mathbb{P}^{\boldsymbol{n}}$ turns out to be a quite useful object which allows to translate geometric operations on multiprojective cycles into algebraic operations on rings and classes. In particular, we obtain the following multiprojective arithmetic Bézout's inequality, see also Theorem 2.58. For a multihomogeneous polynomial $f \in \mathbb{Z}[\boldsymbol{x}_1, \dots, \boldsymbol{x}_m]$, where $\boldsymbol{x}_i$ is a group of $n_i + 1$ variables, we denote by $||f||_{\sup}$ its sup-norm (Definition 2.29) and consider the element $[f]_{\sup}$ in the extended Chow ring corresponding to the element $\sum_{i=1}^m \deg_{\boldsymbol{x}_i}(f)\theta_i + \log||f||_{\sup}\,\eta$.