Sharp Estimates for Triangular Sets

Xavier Dahan
Laboratoire STIX, FRE CNRS 2341
École polytechnique, 91128 Palaiseau, France
dahan@stix.polytechnique.fr

Éric Schost
Laboratoire STIX, FRE CNRS 2341
École polytechnique, 91128 Palaiseau, France
schost@stix.polytechnique.fr

ABSTRACT

We study the triangular representation of zero-dimensional varieties defined over the rational field (resp. a rational function field). We prove polynomial bounds in terms of intrinsic quantities for the height (resp. degree) of the coefficients of such triangular sets, whereas previous bounds were exponential. We also introduce a rational form of triangular representation, for which our estimates become linear. Experiments show the practical interest of this new representation.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algebraic Algorithms*

General Terms

Algorithms, Experimentation, Theory

Keywords

Polynomial systems, Triangular sets, Intrinsic bounds

1. INTRODUCTION

We start by defining the triangular representation of zero-dimensional varieties. Let k be a field, $V \subset \mathbb{A}^n(\overline{k})$ a zero-dimensional variety defined over k and $I \subset k[X_1, \ldots, X_n]$ the ideal of V. Our basic assumption is as follows.

ASSUMPTION 1. *For the lexicographic order $X_1 < \cdots < X_n$, the reduced Gröbner basis of the ideal I has the form*

$$\left|\begin{array}{l} T_n(X_1, \ldots, X_n) \\ \quad\vdots \\ T_2(X_1, X_2) \\ T_1(X_1), \end{array}\right.$$

where for $\ell \le n$, T_ℓ depends only on $X_1, \ldots, X_\ell$ and, when considered in $k[X_1, \ldots, X_{\ell-1}][X_\ell]$, T_ℓ is monic in X_ℓ. We also suppose that the extension $k \to k[V]$ is separable.

ISSAC'04, July 4–7, 2004, Santander, Spain.

Following the terminology introduced in [15], the polynomials $T_1, \ldots, T_n$ form a *triangular set*. This representation is well-suited to many practical problems (see some examples in [15, 3, 20, 24]), as meaningful informations are easily read off these triangular sets; however, many complexity questions remain unanswered in this model. To formulate such questions, we introduce suitable notation.

DEFINITION 1. *Let V be as in Assumption 1 and $\ell \le n$. We let d_ℓ be the degree of T_ℓ in X_ℓ and $V_\ell \subset \mathbb{A}^\ell(\overline{k})$ the image of V by the projection $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_\ell)$.*

Representing $T_1, \ldots, T_\ell$ then amounts to specifying at most $\ell d_1 \cdots d_\ell$ elements of k. If k bears no particular structure, we cannot say more in terms of complexity. New questions arise when k is endowed with a "size" function: then, the natural question is to relate the size of the coefficients in $T_1, \ldots, T_n$ to quantities associated to V. This is the case in the following two fundamental situations.

NUMBER FIELDS. If k is the rational field $\mathbb{Q}$ (or more generally a number field), we want to estimate the number of digits necessary to write the coefficients of $T_1, \ldots, T_n$. Here, the interesting quantity to refer to is the *height* of V, which is a measure of its arithmetic complexity.

FUNCTION FIELDS. Here k is the rational function field $\mathfrak{K}(Y_1, \ldots, Y_m)$ over a field $\mathfrak{K}$. This situation typically arises when studying parametric polynomial systems: $Y_1, \ldots, Y_m$ are the parameters, and $T_1, \ldots, T_n$ describe the *generic solutions* of such systems. Then, we want to estimate the degrees of the numerators and denominators of the coefficients of $T_1, \ldots, T_n$ and the interesting quantity to refer to is a suitable *geometric degree*.

Up to now, in the function field case, the best bounds for the coefficients of $T_1, \ldots, T_n$ were in [20]. These bounds are *exponential*, as the number n of variables appears as an exponent. It is expected that similar methods would yield similar bounds in the case $k = \mathbb{Q}$.

The optimality of these bounds is a crucial question: If these exponential bounds were sharp, triangular representations might become difficult to compute and potentially impossible to use for large problems. The question is all the more important as for other representations (e.g., with primitive elements, see below), polynomial bounds are known.

Our first contribution is to settle this issue, proving *polynomial*, and more precisely quadratic, bounds for the triangular representation, with respect to the above quantities, height and degree. Our results cover both the number field and function field cases.

Rational representations. To obtain estimates better than quadratic (*i.e.*, linear), it is necessary to modify the representation. To motivate our discussion, we first present an important special case.

Suppose that X_1 is a primitive element for the extension $k \to k[V]$. Then there exist univariate polynomials $P_2, \dots, P_n$ such that $(T_1, \dots, T_n)$ have the following shape:

$$\left|\begin{array}{l} T_n = X_n - P_n(X_1) \\ \quad\vdots \\ T_2 = X_2 - P_2(X_1) \\ T_1(X_1). \end{array}\right.$$

Suppose now that $k = \mathbb{Q}$ (the discussion is the same in the function field case). Then, it is known [19] that the bit-size of the coefficients of $P_2, \dots, P_n$ is (up to minor correcting terms) bounded by the product of the height of V by the cardinality of V, *i.e.* it has a quadratic behavior. If V is defined by polynomials of degree d, with integer coefficients of bit-size h, this quantity is bounded by (essentially) nhd^{2n}.

Is is well known that one can improve this by switching to the following equivalent *rational representation*

$$\left|\begin{array}{lcl} \tau_n & = & X_n - \frac{Q_n(X_1)}{T_1'(X_1)} \\ & \vdots & \\ \tau_2 & = & X_2 - \frac{Q_2(X_1)}{T_1'(X_1)} \\ \tau_1 & = & T_1(X_1), \end{array}\right. \tag{1}$$

where for $i \geq 2$, $Q_i = P_i T_1' \bmod T_1$. Indeed, the bit-size of the coefficients of $Q_2, \dots, Q_n$ is now (up to small correcting terms) bounded by solely the height of V [19]. If V is defined by polynomials of degree d, with integers coefficients of bit-size h, this quantity is bounded by (essentially) nhd^n, *i.e.*, much less than above.

From the practical point of view, it was already noticed in [1] that using the rational representation (1) quite frequently brings dramatic reductions in terms of bit-size. Nowadays, such representations bear the name Rational Univariate Representation [18], or Kronecker representation [9].

When X_1 is not a separating variable, we will apply similar ideas, by defining a triangular representation with rational function coefficients that generalizes Equations (1): let V as in Assumption 1 and $T_1, \dots, T_n$ the corresponding triangular set. Recall that for $\ell \leq n$, $T_1, \dots, T_\ell$ form a reduced Gröbner basis; for a polynomial A, $A \mod (T_1, \dots, T_\ell)$ denotes the normal form of A modulo $(T_1, \dots, T_\ell)$.

Definition 2. *Let $D_1 = 1$ and $N_1 = \tau_1 = T_1$. For ℓ in $2, \dots, n$, define*

$$\begin{aligned} D_\ell &= \prod_{1 \leq i \leq \ell-1} \frac{\partial T_i}{\partial X_i} \mod (T_1, \dots, T_{\ell-1}), \\ N_\ell &= D_\ell T_\ell \mod (T_1, \dots, T_{\ell-1}). \\ \tau_\ell &= \frac{N_\ell}{D_\ell} \in k(X_1, \dots, X_{\ell-1})[X_\ell]. \end{aligned}$$

Note that $D_\ell \in k[X_1, \dots, X_{\ell-1}]$, $N_\ell \in k[X_1, \dots, X_{\ell-1}, X_\ell]$, and D_ℓ is the leading coefficient of N_ℓ in X_ℓ. Due to the separability assumption, D_ℓ is invertible modulo $(T_1, \dots, T_{\ell-1})$, so τ_ℓ equals T_ℓ modulo $(T_1, \dots, T_{\ell-1})$.

Example. Let us take $k = \mathbb{Q}$ and consider the variety

$$V \subset \mathbb{A}^2(\overline{\mathbb{Q}}) = \big\{(1,1), (1,2), (2,3), (2,4)\big\}.$$

This variety satisfies Assumption 1; the corresponding triangular set is

$$\left|\begin{array}{l} T_2 = X_2^2 + (-4X_1 + 1)X_2 + 10X_1 - 8, \\ T_1 = X_1^2 - 3X_1 + 2. \end{array}\right.$$

Our definitions give $D_2 = T_1' = 2X_1 - 3$ and

$$N_2 = (2X_1 - 3)X_2^2 + (-10X_1 + 13)X_2 + 14X_1 - 16.$$

Then we associate to V the representation

$$\left|\begin{array}{l} \tau_2 = X_2^2 + \frac{-10X_1+13}{2X_1-3} X_2 + \frac{14X_1-16}{2X_1-3}, \\ \tau_1 = X_1^2 - 3X_1 + 2. \end{array}\right.$$

Our second contribution is the introduction and the study of the polynomials N_ℓ. Whereas our complexity estimates for the coefficients of the polynomials T_ℓ are quadratic, those for N_ℓ will turn out to be *linear* (note that this trivially implies similar bounds for the polynomials τ_ℓ). Again, our results cover both the number field and function field cases.

From these estimates, it is expected that in practice, the coefficients of N_ℓ should be smaller than those of T_ℓ. Our experiments confirm these expectations: for a large class of examples, both over $\mathbb{Q}$ or a rational function field, the coefficients in N_ℓ are significantly smaller than those of T_ℓ.

2. MAIN RESULTS

To state our results, we need new definitions, that are used throughout this paper. Let k be a field and $V \subset \mathbb{A}^n(\overline{k})$ a zero-dimensional variety defined over k. The *Chow form* $\mathcal{C}_V$ of V is the polynomial in $\overline{k}[X_0, X_1, \dots, X_n]$ given by

$$\mathcal{C}_V = \prod_{\alpha \in V} (X_0 - \alpha_1 X_1 - \cdots - \alpha_n X_n)$$

(a different sign convention is sometimes used, but this has no consequence whatsoever for what follows). $\mathcal{C}_V$ is homogeneous of degree the cardinality of V, denoted by $\#V$. If $k \to k[V]$ is separable, $\mathcal{C}_V$ has coefficients in k. Finally, note that $\mathcal{C}_{V \cup V'} = \mathcal{C}_V \mathcal{C}_{V'}$ if V and V' are disjoint.

Our second set of definitions is used to denote some terms that appear in the complexity estimates. Given V that satisfies Assumption 1 and $\ell \leq n$, we will write

$$\begin{aligned} \mathsf{G}_\ell &= 1 + 2\sum\nolimits_{i \leq \ell-1} (d_i - 1) \\ \mathsf{H}_\ell &= 5\log(\ell+3) \sum\nolimits_{i \leq \ell} d_i \\ \mathsf{I}_\ell &= \mathsf{H}_\ell + 3\log(2) \sum\nolimits_{i \leq \ell-1} d_i(d_i - 1). \end{aligned}$$

Since $\prod_i d_i > \sum_i (d_i - 1)$, G_ℓ and H_ℓ are in $O(\log(\ell)(\ell + \#V_\ell))$: we think of them as linear in $\#V_\ell$, overlooking the dependence in ℓ. Since $d_i^2 \geq d_i(d_i-1) + 1$ we get $\prod_i d_i^2 > \sum_i d_i(d_i - 1)$, so I_ℓ is in $O(\log(\ell)(\#V_\ell + \ell) + (\#V_\ell + \ell)^2) = O((\#V_\ell + \ell)^2)$: we see it as a quadratic quantity.

The number field case. We now recall some basic definitions of height theory over the field $k = \mathbb{Q}$.

We first introduce the (global) height of polynomials with coefficients in $\mathbb{Q}$, as a means to estimate their size in binary representation. Let P in $\mathbb{Q}[X_1, \dots, X_m]$, and $c \in \mathbb{N}$ the lcm of the denominators of its coefficients. Let next C be the set of the coefficients of cP and C^+ the set of their absolute values; note that $C \subset \mathbb{Z}$ and $C^+ \subset \mathbb{N}$. Then the *height* of P is $h(P) = \log \max(\{c\} \cup C^+)$; thus, $h(P)$ is up to a factor $\log(2)$ equal to the bit-size of the coefficients of P.

Let next $W \subset \mathbb{A}^m(\overline{\mathbb{Q}})$ be a zero-dimensional variety defined over $\mathbb{Q}$. We now define its height $h(W)$ as a measure of its bit complexity (we are deliberately brief here, as all details are given in Section 4):

$$h(W) = \sum_{p \text{ prime}} h_p(\mathcal{C}_W) + m(\mathcal{C}_W; S_{m+1}) + \#W \sum_{i=1}^{m} \frac{1}{2i},$$

where $\mathcal{C}_W$ is the Chow form of W, $h_p(\,.\,)$ denotes the p-adic height of polynomials, and $m(\,.\,; S_{m+1})$ denotes the Mahler measure on the complex sphere S_{m+1}. This quantity was initially introduced in [17], and used in effective algebra in [22, 10, 13, 5]. This height is especially useful in positive dimension, but also fits quite naturally in our subsequent developments. It is polynomially equivalent to the Weil height and to the heights of Bost *et al.* [4] and Giusti *et al.* [8]; see for instance [22].

With these notions at hand, let V be a zero-dimensional variety defined over $\mathbb{Q}$ that satisfies Assumption 1. The following theorem gives upper bound on the heights of the polynomials $T_1, \ldots, T_n$ and $N_1, \ldots, N_n$.

THEOREM 1. *For $\ell \leq n$, we have the inequalities*

$$h(N_\ell) \leq h(V_\ell) + \mathsf{H}_\ell, \quad h(T_\ell) \leq \mathsf{G}_\ell\, h(V_\ell) + \mathsf{I}_\ell.$$

As announced, the bound on N_ℓ is *linear* in $h(V_\ell)$ and $\#V_\ell$; that on T_ℓ is linear in $h(V_\ell)\#V_\ell$ and $(\#V_\ell)^2$: we can say it is *quadratic* in quantities intrinsic to V. Both bounds on N_ℓ and T_ℓ are polynomial.

If V is given as the zero-set of a polynomial system F, we deduce extrinsic bounds by means of an arithmetic Bézout theorem [13]. Suppose indeed that all polynomials in F have total degree at most d, and integer coefficients which all satisfy $\log|x| \leq h$. Then the height of all varieties V_ℓ satisfies $h(V_\ell) \leq (nh+(2n+3)\log(n+1))d^n$. Further, $\#V_\ell = d_1 \cdots d_\ell$ is bounded by d^n. From this, it is easy to deduce that the bit-size of the coefficients of T_ℓ grows at most like nhd^{2n}, whereas the coefficients of N_ℓ have bit-size controlled by the smaller quantity nhd^n.

The function field case. Here we first describe the geometric context (see [20] for a more detailed presentation).

Let $\mathfrak{K}$ be a field and $\mathfrak{V} \subset \mathbb{A}^{m+n}(\overline{\mathfrak{K}})$ an m-equidimensional variety defined over $\mathfrak{K}$. We make the following geometric assumption: *the projection of $\mathfrak{V}$ on the space of the first m coordinates is Zariski-dense.*

Let us denote by $Y = Y_1, \ldots, Y_m$ the first m coordinates, by $X = X_1, \ldots, X_n$ the last n ones and by $\mathfrak{I}$ the radical ideal in $\mathfrak{K}[Y, X]$ defining $\mathfrak{V}$. The underlying idea is that $\mathfrak{V}$ is the zero-set of a parametric polynomial system in $\mathfrak{K}[Y, X]$, where Y play the role of parameters; the assumption says that for a generic value of the parameters, the system has a finite, non-zero, number of solutions.

To obtain an analogue of the results given in the number field case, we introduce suitable projections of $\mathfrak{V}$. For ℓ in $1, \ldots, n$, let $\mathfrak{V}_\ell$ denote the projection of $\mathfrak{V}$ on the space of coordinates $Y, X_1, \ldots, X_\ell$. We denote $\deg \mathfrak{V}_\ell$ its degree.

Let us finally define the *generic solutions* V of $\mathfrak{V}$ as the zeros of the extended ideal $I = \mathfrak{I} \cdot \mathfrak{K}(Y)[X]$. Our assumption says that V has dimension zero over $k = \mathfrak{K}(Y)$. Let us furthermore suppose that V satisfies Assumption 1. In this case, the polynomials T_ℓ and N_ℓ belong to $k[X] = \mathfrak{K}(Y)[X]$, that is, they have rational functions coefficients.

To give complexity estimates, we will adopt a language similar to the one used in the number field case, introducing a notion of *(global) height* of polynomials in this context. Let P a polynomial with coefficients in $\mathfrak{K}(Y)$ and $c \in \mathfrak{K}[Y]$ the lcm of the denominators of its coefficients. Let next C denote the set of the coefficients of cP; note that $C \subset \mathfrak{K}[Y]$. Then the height of P is defined as $h(P) = \max\{\deg(x) \mid x \in \{c\} \cup C\}$. In particular, $h(P)$ bounds the degree of the numerators and denominators of all coefficients of P.

As an illustration of this notion, let us note the following proposition, which is a restatement of [21, Lemma 3]. It will be used in the proof of the subsequent theorem.

PROPOSITION 1. *For $\ell \leq n$, let $\mathcal{C}_\ell \in \mathfrak{K}(Y)[X_0, \ldots, X_\ell]$ be the Chow form of V_ℓ. Then $h(\mathcal{C}_\ell) \leq \deg \mathfrak{V}_\ell$.*

Then, the main result is the following.

THEOREM 2. *For $\ell \leq n$, we have the inequalities*

$$h(N_\ell) \leq \deg(\mathfrak{V}_\ell), \quad h(T_\ell) \leq \mathsf{G}_\ell \deg(\mathfrak{V}_\ell).$$

As announced, the bound for N_ℓ is linear in the degree of $\mathfrak{V}_\ell$. As for T_ℓ, note that $\Pi_{i \leq \ell} d_i \leq \deg(\mathfrak{V}_\ell)$, and thus G_ℓ is bounded by $2\deg(\mathfrak{V}_\ell)$. This implies the bound $h(T_\ell) \leq 2\deg(\mathfrak{V}_\ell)^2$. If $\mathfrak{V}$ is the zero-set of polynomials of total degree at most d, then the Bézout inequality of [11] implies $\deg \mathfrak{V}_\ell \leq d^n$. Thus, the coefficients of T_ℓ have degree at most $2d^{2n}$, whereas those of N_ℓ have degree at most d^n, which is much smaller.

Related work. Our definition of triangular sets in dimension zero comes from [15]. There exists a vast literature on the subject, with extensions in arbitrary dimension, see notably [2] and [12] for a comprehensive overview. However, fewer articles focus on the complexity-theoretic questions: previous upper bounds were given in [6, 23, 20] in the function field case. To give a comparison with our results, we use again the notation of Theorem 2.

The results in [6, 23] show that $h(T_\ell) \leq n^{O(n)} d^{O(n^2)}$ if $\mathfrak{V}$ is defined by polynomials of degree at most d. Those in [20] are intrinsic; they show that $h(T_\ell) \leq n^{O(n)} \deg(\mathfrak{V}_\ell)^{O(n)}$, which is exponential in n. If $\mathfrak{V}$ is defined by polynomials of degree at most d, the Bézout bound implies estimates that are slightly better that those of [6, 23], but still in the class $n^{O(n)} d^{O(n^2)}$. Thus, the bounds for T_ℓ in Theorem 2 significantly improve all previously known results. For the number field case, we are not aware of similar results.

The introduction of the polynomials N_ℓ is inspired by the approach of [1, 18] for primitive element representations over $\mathbb{Q}$, where the practical interest of using rational representations is already underlined, and estimates are given in terms of a suitable multiplication tensor. Polynomial-type bounds were also given for such representations in [8, 22, 19]. It should be noted that our estimates are a faithful extension of these results to triangular representations.

A first generalization of the approach of [1, 18] is in [5], based on a study of the Chow for of V and its successive derivatives. However, the bounds in [5] are not as good as the ones given here.

Strategy of proof and outline of the paper. We will deduce Theorems 1 and 2 as particular cases of a more general theorem applicable to a wide class of fields (containing $\mathbb{Q}$ and $\mathfrak{K}(Y)$). A field k in this class has a family of *valuations* which verifies the so-called *product formula*. These valuations allow to develop a theory of *heights* of varieties and polynomials defined over k. In the particular case $k = \mathbb{Q}$, we recover the notions of height defined in the previous paragraphs. In the case $k = \mathfrak{K}(Y)$, this justifies our introduction of the notion of "height of polynomials".

The first step of the proof consists in rewriting the polynomials T_ℓ and N_ℓ by means of a generalization of Lagrange interpolation: this enables us to relate these polynomials to suitable Chow forms. This is done in Section 3, and involves no valuation theory. Next, we recall the necessary valuation and height-theoretic definitions in Section 4. They enable us to use the results of Section 3 to obtain a general theorem on the heights in a triangular set, in Section 5, from which Theorems 1 and 2 follow easily.

The last section presents practical experiments over $k = \mathbb{Q}$, where we compare the bit-size of the coefficients of the representations T_ℓ and N_ℓ for various systems. These results show the interest of using the polynomials N_ℓ.

3. INTERPOLATION FORMULAS

In this section, we give interpolation formulas which are the basis of the estimates in Section 5. The main ingredient is the introduction of polynomials (to be denoted by E_α) that, up to constant factors, form a complete set of orthogonal idempotents modulo $T_1, \ldots, T_\ell$.

Notation and definitions. For $1 \le i \le j \le n$, we define

$$\begin{array}{cccc} \pi_i^j: & V_j & \to & V_i \\ & (x_1, \ldots, x_j) & \mapsto & (x_1, \ldots, x_i) \end{array}$$

Then Assumption 1 implies that all fibers of π_i^j have cardinality $d_{i+1} \cdots d_j$, see [3] for more explanations.

Let next K be a finite extension of k that contains all coordinates of all points of V; e.g., K can be the splitting field of the minimal polynomial of a primitive element for V. The field K is our base field in what follows.

Let ℓ be a fixed integer in $1, \ldots, n-1$; we now give interpolation formulas for the polynomials $T_{\ell+1}$ and $N_{\ell+1}$ (this shift of one unit in the index aims at simplifying the presentation). To this effect, let $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ in V_ℓ. Associated with α, we define the varieties $V_\alpha^1, \ldots, V_\alpha^{\ell+1} \subset V_{\ell+1}$ by

$$V_\alpha^i = \{\alpha' = (\alpha_1, \ldots, \alpha_{i-1}, \alpha'_i, \ldots \alpha'_{\ell+1}) \in V_{\ell+1} \mid \alpha'_i \ne \alpha_i\}$$

for $1 \le i \le \ell$, and $V_\alpha^{\ell+1} = \{(\alpha_1, \ldots, \alpha_\ell, \alpha'_{\ell+1}) \in V_{\ell+1}\}$. These sets form a partition of $V_{\ell+1}$. In terms of cardinality, $\#V_\alpha^i = (d_i - 1)d_{i+1} \cdots d_{\ell+1}$ for $i \le \ell$ and $\#V_\alpha^{\ell+1} = d_{\ell+1}$. Other interesting objects are the projections of the varieties V_α^i, defined by $v_\alpha^i = \pi_i^{\ell+1}(V_\alpha^i) \subset V_i$ for $i \le \ell$. In terms of cardinality, we have $\#v_\alpha^i = d_i - 1$.

For $i \le \ell + 1$, recall that $T_i \in k[X_1, \ldots, X_i]$. We define $T_{\alpha,i} = T_i(\alpha_1, \ldots, \alpha_{i-1}, X_i)$. Next, for $i \le \ell$, we define

$$e_{\alpha,i} = \prod_{\alpha' \in v_\alpha^i} (X_i - \alpha'_i) \in K[X_i] \subset K[X_1, \ldots, X_\ell], \quad (2)$$

so that $T_{\alpha,i} = e_{\alpha,i}(X_i - \alpha_i)$. For further use, note also the equality

$$T_{\alpha,\ell+1} = \prod_{\alpha' \in V_\alpha^{\ell+1}} (X_{\ell+1} - \alpha'_{\ell+1}). \quad (3)$$

We now introduce

$$E_\alpha = \prod_{1 \le i \le \ell} e_{\alpha,i} \in K[X_1, \ldots, X_\ell].$$

Results. The following lemma shows that the polynomials E_α satisfy orthogonality conditions, which show them as analogues of Lagrange interpolation polynomials.

LEMMA 1. *Let $\alpha \in V_\ell$. Then $E_\alpha(\alpha) \ne 0$ and $E_\alpha(\alpha') = 0$ for $\alpha' \in V_\ell$, $\alpha' \ne \alpha$.*

PROOF. Our definitions imply that $e_{\alpha,i}(\alpha) \ne 0$ for all $i \le \ell$, from which the first point follows. Let next $\alpha' \ne \alpha$ in V_ℓ. Then, there exists $i \le \ell$ such that $\pi_i^\ell(\alpha') \in v_\alpha^i$. Then, $e_{\alpha,i}(\alpha') = 0$, concluding the proof. □

As a consequence, we deduce our interpolation formulas.

PROPOSITION 2. *The following equalities hold:*

$$T_{\ell+1} = \sum_{\alpha \in V_\ell} \frac{E_\alpha T_{\alpha,\ell+1}}{E_\alpha(\alpha)}, \quad (4)$$

$$N_{\ell+1} = \sum_{\alpha \in V_\ell} E_\alpha T_{\alpha,\ell+1}. \quad (5)$$

PROOF. All polynomials appearing in Equations (4) and (5) are reduced with respect to the Gröbner basis $T_1, \ldots, T_\ell$ in $k[X_1, \ldots, X_{\ell+1}]$. This is true by definition for $T_{\ell+1}$ and $N_{\ell+1}$; as for the right-hand sides, this comes from inspecting the degrees in all variables X_i, $i \le \ell$.

Thus, it suffices to prove that both sides of Equation (4) (resp. (5)) agree on V_ℓ. Due to Lemma 1, this is immediately checked for Equation (4). As for Equation (5), consider $\alpha \in V_\ell$. By Definition 2, the evaluation at α of $N_{\ell+1}$ is

$$\left(\prod_{1 \le i \le \ell} \frac{\partial T_i}{\partial X_i}(\alpha) \right) T_{\alpha,\ell+1} \in K[X_{\ell+1}].$$

Since $E_{\alpha'}(\alpha) = 0$ for $\alpha' \ne \alpha$, the right-hand side reduces to $E_\alpha(\alpha) T_{\alpha,\ell+1}$, so we are left to estimate the value $E_\alpha(\alpha)$. Recall that for $1 \le i \le \ell$, we have $T_{\alpha,i} = e_{\alpha,i}(X_i - \alpha_i)$, whence

$$e_{\alpha,i}(\alpha) = T'_{\alpha,i}(\alpha) = \frac{\partial T_i}{\partial X_i}(\alpha).$$

Taking the product on $i \le \ell$ proves the proposition. □

Let us define the constants

$$e_i = \prod_{\alpha \in V_i} e_{\alpha,i}(\alpha) \ \text{ for } i \le \ell \quad \text{and} \quad E_\ell = \prod_{1 \le i \le \ell} e_i.$$

Equation (4) is equivalent to write $T_{\ell+1}$ as the quotient of

$$\mathfrak{T}_{\ell+1} = \sum_{\alpha \in V_\ell} \frac{E_\alpha T_{\alpha,\ell+1} E_\ell}{E_\alpha(\alpha)} = E_\ell T_{\ell+1}$$

by E_ℓ. We now show that both quantities are defined over k; in Section 5, we will actually prove bounds on $\mathfrak{T}_{\ell+1}$, and deduce bounds for $T_{\ell+1}$.

LEMMA 2. *The polynomial $\mathfrak{T}_{\ell+1}$ is in $k[X_1, \ldots, X_{\ell+1}]$.*

PROOF. Since $T_{\ell+1}$ is defined over k, it suffices to prove that for $i \le \ell$, e_i is in k. Given α in V_i, we saw in the proof of Proposition 2 that $e_{\alpha,i}(\alpha) = \partial T_i / \partial X_i(\alpha)$. Thus, e_i is the determinant of the endomorphism of multiplication by $\partial T_i / \partial X_i$ modulo $T_1, \ldots, T_i$, so it is in k. □

We next relate the polynomials introduced above to suitable Chow forms. Let first be $\mathcal{C}_{\ell+1} \in k[X_0, X_1, \ldots, X_{\ell+1}]$

the Chow form of $V_{\ell+1}$. For α in V_ℓ, the partition $V^1_\alpha, \dots, V^{\ell+1}_\alpha$ of $V_{\ell+1}$ induces the factorization

$$\mathcal{C}_{\ell+1} = \prod_{1\le i\le \ell+1} \mathcal{C}_{\alpha,i}$$

in $K[X_0, X_1, \dots, X_{\ell+1}]$, where $\mathcal{C}_{\alpha,i}$ is the Chow form of V^i_α. The next lemma gives useful facts about these polynomials.

LEMMA 3. *For α in V_ℓ and $i \le \ell$, we have*

$$\mathcal{C}_{\alpha,i}(X_i, 0, \dots, 0, 1, 0, \dots, 0) = e_{\alpha,i}^{d_{i+1}\cdots d_{\ell+1}} \quad (6)$$

$$\mathcal{C}_{\alpha,\ell+1}(X_{\ell+1}, 0, \dots, 0, 1) = T_{\alpha,\ell+1}. \quad (7)$$

PROOF. For $i \le \ell$, let $c_{\alpha,i}$ be the Chow form of v^i_α. For $i \le \ell+1$ (resp. $i \le \ell$), we respectively have

$$\mathcal{C}_{\alpha,i} = \prod_{\alpha' \in V^i_\alpha} (X_0 - \alpha'_1 X_1 - \cdots - \alpha'_{\ell+1} X_{\ell+1}) \quad (8)$$

$$c_{\alpha,i} = \prod_{\alpha' \in v^i_\alpha} (X_0 - \alpha'_1 X_1 - \cdots - \alpha'_i X_i). \quad (9)$$

Since $v^i_\alpha = \pi^{\ell+1}_i(V^i_\alpha)$ and since all fibers have cardinality $d_{i+1}\cdots d_{\ell+1}$, we deduce

$$\mathcal{C}_{\alpha,i}(X_0, X_1, \dots, X_i, 0, \dots, 0) = c_{\alpha,i}^{d_{i+1}\cdots d_{\ell+1}}.$$

Equations (2) and (9) then imply Equation (6). Next, combining Equations (3) and (8) easily gives Equation (7). □

For further use, let us finally note useful equalities. The proofs are easy and left to the reader.

LEMMA 4. *For $\alpha \in V_\ell$, the following equality holds:*

$$\frac{E_\ell}{E_\alpha(\alpha)} = \prod_{1\le i\le \ell} \prod_{\substack{\alpha' \in V_i \\ \alpha' \ne \pi^\ell_i(\alpha)}} e_{\alpha',i}(\alpha'). \quad (10)$$

For $i \le \ell$, the following equality holds:

$$\prod_{\alpha' \in V_i} e_{\alpha',i}(X_i - \alpha'_i)^{d_i - 1} = \prod_{\alpha' \in V_i} (X_i - \alpha'_i)^{2d_i-2}. \quad (11)$$

4. VALUATED FIELDS AND HEIGHTS

We now recall the definitions and properties of absolute values and heights. Our references are [14, 16, 17, 22, 10, 13]; our presentation is strongly inspired by [13].

4.1 Absolute values

Let k be a field. An *absolute value* v on k is a multiplicative map $k \to \mathbb{R}^+$, such that $v(a) = 0$ iff $a = 0$, and $\forall a, b \in k^2$, $v(a+b) \le v(a) + v(b)$. If the stronger inequality $v(a+b) \le \max(v(a), v(b))$ holds $\forall a, b \in k^2$, v is called *non-Archimedean*, and *Archimedean* otherwise.

A family M_k of absolute values verifies the *product formula* (with multiplicities 1) if for every $x \in k^*$, there are only a finite number of v in M_k such that $v(x) \ne 1$, and the equality $\prod_{v\in M_k} v(x) = 1$ holds. In this case, we denote by A_k and NA_k the Archimedean and non-Archimedean absolute values in M_k, and write $M_k = (A_k, NA_k)$. A_k is then necessarily finite; we write its cardinality $\#A_k$.

We now introduce two basic examples of valuated fields, which respectively underlie the proofs of Theorems 1 and 2.

Case 1: $k = \mathbb{Q}$. Let $\mathcal{P}$ be the set of prime numbers, so that each x in $\mathbb{Q}^*$ has the unique factorization

$$x = \pm \prod_{p\in\mathcal{P}} p^{\mathrm{ord}_p(x)}.$$

For each prime p, $x \mapsto |x|_p = p^{-\mathrm{ord}_p(x)}$ defines a non-Archimedean absolute value. Denoting $x \mapsto |\ .\ |_\infty$ the usual Archimedean absolute value, we let $M_{\mathbb{Q}} = \{ |\ .\ |_p \}_{p\in\mathcal{P}} \cup \{ |\ .\ |_\infty \}$. Note that $\#A_{\mathbb{Q}} = 1$.

Case 2: $k = \mathfrak{K}(Y)$, with $Y = Y_1, \dots, Y_m$ and $\mathfrak{K}$ a field. Let $\mathcal{P}$ be a set of irreducible polynomials in $\mathfrak{K}[Y]$, such that each x in k^* has the unique factorization

$$x = c \prod_{p\in\mathcal{P}} p^{\mathrm{ord}_p(x)}, \quad c \in \mathfrak{K}.$$

Then each p in $\mathcal{P}$ defines a non-Archimedean absolute value $x \mapsto |x|_p = e^{-\deg p \ \mathrm{ord}_p(x)}$. An additional non-Archimedean absolute value is given by $x \mapsto |x|_\infty = e^{\deg x}$, where $\deg x$ is defined as $\deg n - \deg d$, with $n, d \in \mathfrak{K}[Y]$ and $x = n/d$. We define $M_{\mathfrak{K}(Y)} = \{ |\ .\ |_p \}_{p\in\mathcal{P}} \cup \{ |\ .\ |_\infty \}$, so that $\#A_{\mathfrak{K}(Y)} = 0$.

We easily check that $M_{\mathbb{Q}}$ and $M_{\mathfrak{K}(Y)}$ satisfy the product formula.

4.2 Heights of polynomials

Let k be a field and M_k a set of absolute values on k that satisfies the product formula. We now define the notion of *height* over k, and more generally on polynomial rings over k.

Let $m \ge 0$ and $f = \sum_\beta f_\beta X_1^{\beta_1} \dots X_m^{\beta_m}$ in $k[X_1, \dots, X_m]$. For v in M_k, define the *v-adic local height* of f by

$$h_v(f) = \log\max\{1, \max_\beta\{v(f_\beta)\}\} \ge 0.$$

In the two special cases seen above, $k = \mathbb{Q}$ and $k = \mathfrak{K}(Y)$, we defined in Section 2 a notion of (global) height of polynomials in $k[X_1, \dots, X_m]$. This notion fits nicely into the setting of valuated fields through the following general definition. Define the *(global) height* of f by

$$h(f) = \sum_{v\in M_k} h_v(f). \quad (12)$$

In the above particular cases, this definition coincides with that of Section 2: see [13] when $k = \mathbb{Q}$; the proof for $\mathfrak{K}(Y)$ is the same and both follow simply from the product formula.

Mahler measures. Archimedean local heights are not additive; this shortcoming will prevent us from using them to define heights of varieties. We now introduce Mahler measures, which are closely related to Archimedean local heights, but possess the additivity property.

Let v an Archimedean absolute value over k. Then there exists a isometric injection σ_v from k to $\mathbb{C}$ endowed with its usual norm. Extending σ_v to the polynomial rings over k, we define the *S_n-Mahler measure* associated to v as

$$m_v(f; S_n) = \int_{S_n} \log|\sigma_v(f)|\,\mu_n$$

for $f \in k[X_1, \dots, X_n]$, where μ_n is the Haar measure of mass 1 over the complex sphere S_n of dimension n. We also use the more "classical" Mahler measure, given by

$$m_v(f) = \int_0^1 \dots \int_0^1 \log|\sigma_v(f)(e^{2i\pi t_1}, \dots, e^{2i\pi t_n})| dt_1 \dots dt_n.$$

It is immediately seen that both quantities are additive.

Useful inequalities. We conclude by giving basic inequalities for local heights and Mahler measures. Let $f_1, \dots, f_s$ be in $K[X_0, \dots, X_n]$, f in $K[X_1]$, and assume that each f_i has *at least one coefficient equal to 1* (this simplifying assumption is satisfied in the sequel). If v is an Archimedean absolute value on K, we have:

$\mathbf{A_1}$ $m(f_i) \geq 0$ if $\deg(f_i) = 1$.
$\mathbf{A_2}$ $h_v(f_i) \leq m_v(f_i) + \log(n+2)\deg(f_i)$.
$\mathbf{A_3}$ $h_v(f_1 \cdots f_s) \leq \sum_{i=1}^s h_v(f_i) + \log(n+2)\sum_{i=1}^s \deg(f_i)$.
$\mathbf{A_4}$ $\sum_{i=1}^s h_v(f_i) \leq h_v(f_1 \cdots f_s) + 2\log(n+2)\sum_{i=1}^s \deg(f_i)$.
$\mathbf{A_5}$ $h_v(f_1 + \cdots + f_s) \leq \max_{i \leq s} h_v(f_i) + \log s$.
$\mathbf{A_6}$ $m_v(f_i) \leq m_v(f_i; S_{n+1}) + \deg(f_i)\left(\sum_{i=1}^n \frac{1}{2i}\right)$.
$\mathbf{A_7}$ $h_v(f(x)) \leq h_v(f) + \deg(f)(h_v(x) + \log(2))$ for $x \in K$.
$\mathbf{A_8}$ $m_v(f_i(X_0, \ldots, X_{n-1}, 0)) \leq m_v(f_i)$.

If v is a non-Archimedean absolute value on K, we have:

$\mathbf{N_1}$ $h_v(f_1 \cdots f_s) = h_v(f_1) + \cdots + h_v(f_s)$.
$\mathbf{N_2}$ $h_v(f_1 + \cdots + f_s) \leq \max_{i \leq s} h_v(f_i)$.
$\mathbf{N_3}$ $h_v(f(x)) \leq h_v(f) + \deg(f)h_v(x)$ for $x \in k$.

If we drop the assumption that each f_i has one coefficient equal to 1, we still have, for any absolute value v:

$\mathbf{E}$ $h_v(xf_i) \leq h_v(x) + h_v(f_i)$ for $x \in K$.

4.3 Heights of varieties

Let $M_k = (A_k, NA_k)$ be absolute values over k, which satisfy the product formula. We now use these absolute values to define heights of zero-dimensional varieties.

Let $V \subset \mathbb{A}^n(\overline{k})$ be a zero-dimensional variety defined over k, and suppose that $k \to k[V]$ is separable, so that the Chow form $\mathcal{C}_V$ of V has coefficients in k. We use the local heights and Mahler measures of $\mathcal{C}_V$ to define the height $h(V)$ of V as

$$\sum_{v \in NA_k} h_v(\mathcal{C}_V) + \sum_{v \in \mathrm{A}_k} m_v(\mathcal{C}_V; S_{n+1}) + \#A_k \#V \sum_{i=1}^n \frac{1}{2i}.$$

This quantity is additive: $h(V \cup V') = h(V) + h(V')$ if V and V' are disjoint zero-dimensional varieties.

Let us inspect the content of this definition in the two special cases we are primarily interested in. If $k = \mathbb{Q}$, this definition does coincide with the one given in Section 2, since $\#A_{\mathbb{Q}} = 1$. If k is the rational function field $\mathfrak{K}(Y)$, there are no Archimedean absolute values in $M_{\mathfrak{K}(Y)}$, so the height of V equals the global height of its Chow form.

5. MAIN THEOREM

Let k be a field, with a family of absolute values $M_k = (A_k, NA_k)$ that satisfies the product formula; let $V \subset \mathbb{A}^n(\overline{k})$ a variety defined over k that satisfies Assumption 1. We now prove a general result that relates the height of the polynomials T_ℓ and N_ℓ associated to V to the height of V, and deduce Theorems 1 and 2 as special cases. We actually take ℓ in $0, \ldots, n-1$, and consider the polynomials $N_{\ell+1}$, $T_{\ell+1}$ (compared to Theorems 1 and 2, we shift the indices of one unit for convenience).

Theorem 3. *Let $(\mathsf{G}_\ell)_\ell$, $(\mathsf{H}_\ell)_\ell$ and $(\mathsf{I}_\ell)_\ell$ be as in Section 2. Then for $0 \leq \ell \leq n-1$, the following inequalities holds:*

$$h(N_{\ell+1}) \leq h(V_{\ell+1}) + \#A_k \mathsf{H}_{\ell+1}.$$

$$h(T_{\ell+1}) \leq \mathsf{G}_{\ell+1}\, h(V_{\ell+1}) + \#A_k \mathsf{I}_{\ell+1}.$$

Taking these results for granted, we deduce our main theorems. Theorem 1 is merely the special case $k = \mathbb{Q}$, with the set of absolute values $M_{\mathbb{Q}}$ of Subsection 4.1. Theorem 2 corresponds to the case $k = \mathfrak{K}(Y)$ with the set of absolute values $M_{\mathfrak{K}(Y)}$: in this case, all absolute values are non-Archimedean, so $\#A_k = 0$. We saw in Subsection 4.3 that the height of V_ℓ then equals the height of its Chow form, so Proposition 1 concludes the proof of Theorem 2.

Thus, we can now concentrate on proving Theorem 3. The core of the proof is the following lemma, which involves the polynomials $\mathfrak{T}_{\ell+1}$ of Section 3.

Lemma 5. *Let $0 \leq \ell \leq n-1$. For $v \in NA_k$ we have $h_v(N_{\ell+1}) \leq h_v(\mathcal{C}_{\ell+1})$, and $h_v(\mathfrak{T}_{\ell+1}) \leq \mathsf{G}_{\ell+1}\, h_v(\mathcal{C}_{\ell+1})$.*

For $v \in A_k$, we have $h_v(N_{\ell+1}) \leq m_v(\mathcal{C}_{\ell+1}) + \mathsf{H}_{\ell+1}$ and $h_v(\mathfrak{T}_{\ell+1}) \leq \mathsf{G}_{\ell+1}\, m_v(\mathcal{C}_{\ell+1}) + \mathsf{I}_{\ell+1}$.

Let us show how to derive Theorem 3. Plugging the estimates for $N_{\ell+1}$ in Equation (12) gives

$$h(N_{\ell+1}) \quad \leq \quad \sum_{v \in NA_k} h_v(\mathcal{C}_{\ell+1}) + \sum_{v \in A_k} (m_v(\mathcal{C}_{\ell+1}) + \mathsf{H}_{\ell+1})$$

and the first part of Theorem 3 follows from inequality $\mathbf{A_6}$. Similar arguments apply to $\mathfrak{T}_{\ell+1}$ and yield the bound

$$h(\mathfrak{T}_{\ell+1}) \leq \mathsf{G}_{\ell+1}\, h(V_{\ell+1}) + \#A_k \mathsf{I}_{\ell+1}.$$

Now, recall that $T_{\ell+1}$ is obtained by dividing out $\mathfrak{T}_{\ell+1}$ by its leading coefficient in $X_{\ell+1}$. By the product formula, this operation lowers the global height, whence Theorem 3 follows. Thus, we can now focus on proving the lemma, using freely the notation of Section 3.

In what follows, we consider ℓ in $1, \ldots, n-1$. The case $\ell = 0$ follows along the same lines, by noting that $T_1 = N_1$ is obtained by a suitable specialization of the Chow form $\mathcal{C}_1$ of V_1. The easy details are left to the reader.

Let then K be a finite extension of k that contains all coordinates of all points in V. Let $v \in M_k$ and w an absolute value on K that coincides with v on k. If v is Archimedean (resp. non-Archimedean), w is Archimedean (resp. non-Archimedean) as well: for the existence of such w, see [14, 16]. Let finally α in V_ℓ.

Specializing indeterminates at zero decreases height, so $h_w(\mathcal{C}_{\alpha,i}(X_0, 0, \ldots, 0, X_i, 0, \ldots, 0)) \leq h_w(\mathcal{C}_{\alpha,i})$ for $i \leq \ell$. Since $\mathcal{C}_{\alpha,i}(X_0, 0, \ldots, 0, X_i, 0, \ldots, 0)$ is homogeneous, its local height coincides with that of $\mathcal{C}_{\alpha,i}(X_i, 0, \ldots, 0, 1, 0, \ldots, 0)$. Then, Equations (6) and (7) finally give

$$h_w(e_{\alpha,i}^{d_{i+1}\cdots d_{\ell+1}}) \quad \leq \quad h_w(\mathcal{C}_{\alpha,i}) \quad \text{for } i \leq \ell \tag{13}$$
$$h_w(T_{\alpha,\ell+1}) \quad \leq \quad h_w(\mathcal{C}_{\alpha,\ell+1}). \tag{14}$$

Case 1: w is non-Archimedean. We use equality $\mathbf{N_1}$ and Equations (13) and (14) to give

$$\begin{aligned} h_w(E_\alpha T_{\alpha,\ell+1}) &= \sum_{i \leq \ell} h_w(e_{\alpha,i}) + h_w(T_{\alpha,\ell+1}) \\ &\leq \sum_{i \leq \ell} h_w(\mathcal{C}_{\alpha,i}) + h_w(\mathcal{C}_{\alpha,\ell+1}) = h_w(\mathcal{C}_{\ell+1}). \end{aligned}$$

Summing on all α, we deduce $h_w(N_{\ell+1}) \leq h_w(\mathcal{C}_{\ell+1})$ by inequality $\mathbf{N_2}$. Since both polynomials have coefficients in k, and w extends v, this proves the first part of Lemma 5.

Next, we consider $\mathfrak{T}_{\ell+1}$. Inequality $\mathbf{E}$ yields

$$h_w\left(\frac{E_\alpha T_{\alpha,\ell+1} E_\ell}{E_\alpha(\alpha)}\right) \leq h_w(E_\alpha T_{\alpha,\ell+1}) + h_w\left(\frac{E_\ell}{E_\alpha(\alpha)}\right). \tag{15}$$

The term $h_w(E_\alpha T_{\alpha,\ell+1})$ was dealt with above. As to the other term, inequality $\mathbf{E}$ and Equation (10) show that

$$h_w\left(\frac{E_\ell}{E_\alpha(\alpha)}\right) \leq \sum_{1 \leq i \leq \ell} \sum_{\alpha' \in V_i} h_w(e_{\alpha',i}(\alpha')), \tag{16}$$

since the positivity of height enables us to complete the product in Equation (10). Then inequality $\mathbf{N_3}$ gives the upper bound

$$\sum_{1\le i\le \ell}\ \sum_{\alpha'\in V_i} \left(h_w(e_{\alpha',i}) + (d_i-1)h_w(\alpha_i')\right).$$

Note that $h_w(\alpha_i') = h_w(X_i - \alpha_i')$, so by equality $\mathbf{N_1}$, the innermost term is $h_w(e_{\alpha',i}(X_i-\alpha_i')^{d_i-1})$. Using Equation (11), the inner sum is then bounded from above by

$$\sum_{\alpha'\in V_i} h_w(e_{\alpha',i}(X_i-\alpha_i')^{d_i-1}) = h_w\Big(\prod_{\alpha'\in V_i}(X_i-\alpha_i')^{2d_i-2}\Big).$$

This quantity can be bounded from above by $2(d_i-1)h_w(\mathcal{C}_i)$. Note that $h_w(\mathcal{C}_i) \le h_w(\mathcal{C}_{\ell+1})$; summing on $i\le \ell$ and introducing the constant $\mathsf{G}_{\ell+1}$ gives the second point in Lemma 5.

Case 2: w is Archimedean. Let m_v and m_w be the Mahler measures associated to v and w; they coincide on polynomials with coefficients in k.

For $i\le\ell$, since $\mathcal{C}_{\alpha,i}$ has degree $(d_i-1)d_{i+1}\cdots d_{\ell+1}$, inequality $\mathbf{A_2}$ gives

$$h_w(\mathcal{C}_{\alpha,i}) \le m_w(\mathcal{C}_{\alpha,i}) + (d_i-1)d_{i+1}\cdots d_{\ell+1}\log(\ell+2).$$

Thus, we deduce from inequality $\mathbf{A_4}$ and Equation (13)

$$\begin{aligned} h_w(e_{\alpha,i}) &\le \frac{h_w(\mathcal{C}_{\alpha,i})}{d_{i+1}\cdots d_{\ell+1}} + 2(d_i-1)\log(\ell+2)\\ &\le \frac{m_w(\mathcal{C}_{\alpha,i})}{d_{i+1}\cdots d_{\ell+1}} + 3(d_i-1)\log(\ell+2)\end{aligned}$$

Using $(d_{i+1}\cdots d_{\ell+1})\ge 1$ and inequality $\mathbf{A_3}$, we obtain

$$h_w(E_\alpha) \le \sum_{i\le\ell} m_w(\mathcal{C}_{\alpha,i}) + 4\log(\ell+2)\sum_{i\le\ell}(d_i-1).$$

We next deduce from Equation (14) and inequality $\mathbf{A_2}$

$$h_w(T_{\alpha,\ell+1}) \le m_w(\mathcal{C}_{\alpha,\ell+1}) + \log(\ell+3)d_{\ell+1}.$$

Now, $m_w(\mathcal{C}_{\ell+1}) = m_w(\mathcal{C}_{\alpha,\ell+1}) + \sum_{i\le\ell} m_w(\mathcal{C}_{\alpha,i})$, so applying inequality $\mathbf{A_3}$ yields

$$h_w(E_\alpha T_{\alpha,\ell+1}) \le m_w(\mathcal{C}_{\ell+1}) + 4\log(\ell+3)\sum_{i\le\ell+1} d_i.$$

Summing over α and using inequality $\mathbf{A_5}$, we finally get

$$h_w(N_{\ell+1}) \le m_w(\mathcal{C}_{\ell+1}) + 4\log(\ell+3)\sum_{i\le\ell+1} d_i + \log(d_1\cdots d_{\ell+1}).$$

Next, we use the inequality $\log(d_i)\le d_i$ for all i. With the introduction of the constant $\mathsf{H}_{\ell+1}$, this finishes the proof of the third point in Lemma 5, since $N_{\ell+1}$ and $\mathcal{C}_{\ell+1}$ both have coefficients in k.

As for the last point of that lemma, note first that inequalities (15) and (16) hold in the Archimedean case as well; we now only have to bound the rightmost term of Equation (16).

Using inequalities $\mathbf{A_7}$ and $\mathbf{A_3}$ and Equation (11), an easy check proves that for $i\le\ell$, the sum $\sum_{\alpha'\in V_i} h_w(e_{\alpha',i}(\alpha'))$ is bounded from above by

$$2(d_i-1)m_w\Big(\prod_{\alpha\in V_i}(X_i-\alpha_i)\Big) + 3d_i(d_i-1)\log(2).$$

Now, we remark that $m_w(X_i-\alpha_i) = m_w(X_0-\alpha_iX_i)$. Using the additivity of the Mahler measure, we deduce that the above quantity equals

$$2(d_i-1)m_w(\mathcal{C}_i(X_0,0,\dots,0,X_i,0,\dots,0)) + 3d_i(d_i-1)\log(2).$$

Inequality $\mathbf{A_8}$ now shows that this can be bounded from above by $2(d_i-1)m_w(\mathcal{C}_i) + 3d_i(d_i-1)\log(2)$. Noticing that $m_w(\mathcal{C}_i)\le m_w(\mathcal{C}_{\ell+1})$ and using the above estimates yields

$$\begin{aligned} h_w\left(\frac{E_\alpha T_{\alpha,\ell+1}E_\ell}{E_\alpha(\alpha)}\right) &\le m_w(\mathcal{C}_{\ell+1})\Big(1+2\sum_{i\le\ell}(d_i-1)\Big)\\ &+ 4\log(\ell+3)\sum_{i\le\ell+1} d_i\\ &+ 3\log(2)\sum_{i\le\ell} d_i(d_i-1).\end{aligned}$$

Summing on all α and using inequality $\mathbf{A_5}$ as above, we conclude the proof of Lemma 5.

6. EXPERIMENTAL RESULTS

In this last section, we compare the representations by the polynomials T_ℓ and N_ℓ (or equivalently τ_ℓ) from a practical viewpoint. We set $k=\mathbb{Q}$ and compare the bit-size of the coefficients of these polynomials for various systems. In our experiments, the second representation always leads to smaller coefficients, sometimes by an important factor.

For our first examples, we fix n, some integers $[d_1,\dots,d_n]$, select random points in n-space and with rational coefficients, such that the variety formed by their reunion satisfies Assumption 1 with degrees $d_1,\dots,d_n$; then we use the interpolation formulas (4) and (5) to construct the polynomials $T_1,\dots,T_n$ and $N_1,\dots,N_n$.

In the following table, 4 examples are given, one for each of the last 4 columns. The first line gives the degrees of $[T_1,\dots,T_n]$ (thus the number of variables is the cardinal of the list). The second (resp. the third) line returns the lists of the maximum number of digits of the numerators (resp. denominators) of the coefficients of $[T_1,\dots,T_n]$. The last two lines give the same informations for the list of polynomials $[N_1,\dots,N_n]$. As $N_1=T_1$, the first number is the same in each column at lines 2-4 and 3-5.

d_ℓ	2,3,4,5	4,5,6,7	4,1,2,3,4	8,8,8,8
h_{num} T_ℓ	4,16 63,225	10,63, 286,1080	9,44, 91,123,157	28,324, 1813,9588
h_{den} T_ℓ	2,46, 62,220	9,59, 280,1076	7,45, 88,118,152	27,316, 1798,9567
h_{num} N_ℓ	4,13, 43,169	10,44, 150,357	9,32, 61,84,119	28,181, 831,2815
h_{den} N_ℓ	2,13, 43,137	9,41, 145,346	7,30, 58,80,115	27,176, 821,2802

We observe a diminution of the size of the coefficients, which corroborates the better bound for $h(N_\ell)$ in Theorem 1. The ratio is however smaller than what could be expected from Theorem 1; this is partly due to the simplifications we made along the proof.

Next, we experiment on systems coming from applications. These systems, called Bershenko, P19, Hawes and J1J2J3, together with background information, are given in [19, Annexe E]. The second line of the following table gives the number n of variables of the system, the third returns the lists of degrees $[d_1,\dots,d_n]$ of the polynomials $[T_1,\dots,T_n]$; the next lines are as above. In the third column, the dots denote six occurrences of the number 1560.

Syst.	P19	Bersh.	Hawes	J1J2J3
Var.	5	4	7	4
Deg. d_ℓ	31,1,2,1,1	12,2, 1,1	30,4,1,1, 1,1,1	5,2, 3,1
h_{num} T_ℓ	90,1444,1029, 1444,1467	15,58, 57,72	77,1560,... ...,1560	13,25, 24,39
h_{den} T_ℓ	30,1448,1031, 1450,1483	5,57, 57,70	46,1560,... ...,1560	19,24, 25,39
h_{num} N_ℓ	90,94,117, 117,117	15,17, 17,29	77,80,78,78, 79,118,80	13,17, 21,17
h_{den} N_ℓ	30,28,44, 44,62	5,5, 5,18	46,48,47, 46,46,85,47	19,2, 8,5

Again, we observe a systematic diminution of the size of the coefficients, which is sometimes quite important: our conclusion is that using the polynomials N_ℓ is a good choice in practice. For $k = \mathfrak{K}(Y)$, experiments on parametric systems are possible, measuring the degrees of the coefficients of the polynomials T_ℓ and N_ℓ. The results are similar.

7. CONCLUSION

We proved quadratic estimates for the representation by means of the triangular sets T_ℓ, improving all previous, exponential, bounds. We introduced an alternative representation by means of the polynomials N_ℓ, for which we are able to obtain linear bounds. We treated the cases $k = \mathbb{Q}$ and $k = \mathfrak{K}(Y)$ in a uniform manner. Our experiments showed the interest of using the new representation N_ℓ, since we observed a systematic reduction of the size of coefficients when switching from the data of T_ℓ to the data of N_ℓ.

The next question to answer is that of lower bounds, for both representations. It is expected that the first family of examples used in the previous section might yield such lower bounds when $k = \mathfrak{K}(Y)$, using points with generic and algebraically independent coordinates.

A last question is that of algorithms: in practice, it is certainly not interesting to compute first the polynomials T_ℓ and then deducing the polynomials N_ℓ: efficient algorithms should compute the polynomials N_ℓ only.

An answer is Hensel lifting for triangular sets, as presented in [20] (see also the references therein). Let us describe how such techniques apply over $k = \mathbb{Q}$. First the polynomials T_ℓ are computed modulo some prime p; then, by Hensel lifting, we can compute the polynomials T_ℓ modulo arbitrary powers p^κ, from which we can deduce N_ℓ at precision p^κ. We stop the lifting when the coefficients of N_ℓ can be reconstructed from their reduction modulo p^k: this way, we avoid computing the larger coefficients of the polynomials T_ℓ. This strategy is used for $k = \mathfrak{K}(Y)$ in [7].

Acknowledgements. We thank all referees for their detailed and accurate remarks.

8. REFERENCES

[1] M. E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. In *MEGA'94*, volume 142 of *Prog. in Math.*, pages 1–15. Birkhäuser, 1996.

[2] P. Aubry, D. Lazard, and M. M. Maza. On the theories of triangular sets. *J. Symb. Comp*, 28(1,2):45–124, 1999.

[3] P. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symb. Comp*, 30(6):635–651, 2000.

[4] J.-B. Bost, H. Gillet, and C. Soulé. Heights of projective varieties and positive Green forms. *J. Amer. Math. Soc.*, 7(4):903–1027, 1994.

[5] X. Dahan. Bornes de hauteur pour la représentation triangulaire de variétés présentant des symétries. `www.stix.polytechnique.fr/~dahan`, 2003.

[6] G. Gallo and B. Mishra. Efficient algorithms and bounds for Wu-Ritt characteristic sets. In *MEGA'90*, volume 94 of *Prog. in Math.*, pages 119–142. Birkhäuser, 1990.

[7] P. Gaudry and É. Schost. Construction of secure random curves of genus 2 over prime fields. 2003.

[8] M. Giusti, K. Hägele, J. Heintz, J. E. Morais, J. L. Montaña, and L. M. Pardo. Lower bounds for Diophantine approximations. *J. Pure Appl. Algebra*, 117–118:277–317, 1997.

[9] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.

[10] K. Hägele, J.-E. Morais, L.-M. Pardo, and M. Sombra. On the intrinsic complexity of the arithmetic Nullstellensatz. *J. Pure. Appl. Alg.*, 146:103–183, 2000.

[11] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3):239–277, 1983.

[12] É. Hubert. Notes on triangular sets and triangulation decomposition algorithms I: Polynomial systems. In *Symbolic and Numerical Scientific Computations*, volume 2630 of *LNCS*. Springer, 2003.

[13] T. Krick, L.-M. Pardo, and M. Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Math. J.*, 109(3):521–598, 2001.

[14] S. Lang. *Diophantine geometry*. Tracts in Pure and Applied Mathematics, No. 11. Interscience, 1962.

[15] D. Lazard. Solving zero-dimensional algebraic systems. *J. Symb. Comp*, 13(2):117–133, 1992.

[16] P. J. McCarthy. *Algebraic extensions of fields*. Dover Publications Inc., New York, 1991.

[17] P. Philippon. Sur des hauteurs alternatives. III. *J. Math. Pures Appl. (9)*, 74(4):345–365, 1995.

[18] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):433–461, 1999.

[19] É. Schost. *Sur la résolution des systèmes polynomiaux à paramètres*. PhD thesis, École polytechnique, 2000.

[20] É. Schost. Complexity results for triangular sets. *J. Symb. Comp*, 36(3–4):555–594, 2003.

[21] É. Schost. Computing parametric geometric resolutions. *Appl. Algebra Engrg. Comm. Comput.*, 13(4):349–393, 2003.

[22] M. Sombra. *Estimaciones para el teorema de ceros de Hilbert*. PhD thesis, U. de Buenos Aires, 1998.

[23] A. Szanto. *Computation with polynomial systems*. PhD thesis, Cornell Univ., 1999.

[24] D. Wang. *Elimination Methods*, volume XIII of *Texts and monographs in symbolic computation*. Springer-Verlag, 2001.