数理解析研究所講究録
第 1759 巻 2011 年 26-42

On bit-size estimates of triangular systems

Xavier Dahan *
九州大学 数理学研究院
FACULTY OF MATHEMATICS, KYŪSHŪ UNIVERSITY †

Abstract

When solving polynomial equations over an infinite field like $\mathbb{Q}$, in an exact manner, that is without approximation, coefficients usually become very large. This survey presents some upper-bounds on the size of coefficients of some specific Gröbner bases. They concern still quite limited families of such systems, but are among the first of this kind. A special emphasize is put on the elementary presentation of a main tool, *height theory* for measuring the complexity in term of space of a polynomial system.

1 Introduction

System of polynomial equations in several indeterminates arise nowadays in several contexts of concrete applications, that are in need for an efficient solving process. A standard method consists in computing Gröbner bases. It is well-known that they can often require prohibitive memory size, limiting their computations drastically, although the several recent important improvements. The size of the coefficients of such Gröbner bases can indeed be very large (and also can be the number of such coefficients !). It is widely experimentally observed that it is for lexicographic orders that this problem is the worth.

This suggests the following question:

How large can the coefficients can become when computing a lexicographic Gröbner basis of a given input polynomial system ?

This is a quite general problem that has not been studied much when "large" means "number of digitis" of integers or rational coefficients. If the coefficients are themselves parameters (polynomial or rational fractions in one or several indeterminates), then a few previous results exist, with not very satisfactory bounds. In both cases, the works [5, 3] gave new results or improvements on this matter. However, somewhat quite strong restrictive hypotheses are still in order.

Triangular sets We will call a polynomial system a *triangular set* any family T of polynomials $T_1, \ldots, T_n$ that are in the following ("triangular") shape:

$$T \left| \begin{array}{l} T_n(X_1, X_2, \cdots, X_{n-1}, X_n) = X_n^{d_n} + \cdots \\ T_{n-1}(X_1, \ldots, X_{n-1}) = X_{n-1}^{d_{n-1}} + \cdots \\ \quad \vdots \\ T_1(X_1) = X_1^{d_1} + \cdots \end{array} \right.$$

*GCOE project Maths-for-industry
†dahan@math.kyushu-u.ac.jp

The degree d_i is denoted $\deg_{X_i}(T_i)$. It is also required that T is a *reduced* lexicographic Gröbner basis (necessarily for the monomial order $X_1 < \cdots < X_n$). This family is then a regular sequence, hence it generates a *0-dimensional* ideal.

The method we have used to get upper-bounds in [5, 3] requires the classical algebra/geometry dictionary, so it is assumed that the output triangular system to be *radical.* The input polynomial system may not be radical, but then consists of as many polynomials as the number of indeterminates n, *i.e.* is a square system, and the solutions are those where the Jacobian determinant does not vanish. By the *Jacobian criterion*, these solutions are indeed simple. Let V be this set of solutions over the algebraic closure $\bar{k}$ of the field of definition k[1)]

Assumption 1. V is finite, and there exists a triangular set $T_1(X_1), \ldots, T_n(X_1, \ldots, X_n)$ such that $V = Z(\langle T_1, \ldots, T_n \rangle)$.

Since we are with lexicographic orders, the *elimination* property fully holds. On the geometric side, this implies good properties under *projections*, and it is possible to rewrite the polynomials of a triangular set in a Lagrange interpolation formulation. Let us denote by π_j the projection on the coordinate space spanned by $X_1, \ldots, X_j$. That is, given a point $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{C}^n$, $\pi_j(\gamma) = (\gamma_1, \ldots, \gamma_j)$. We also denote by X_i the i-th coordinate function, defined by $X_i(\gamma) := \gamma_i$ The set $X_i(V)$ is therefore equal to $\{b \in \mathbb{C} \mid \exists(\gamma_1, \ldots, \gamma_n) \in V \text{ s.t. } X_i(\gamma) = \gamma_i = b\}$, that is the projection of V on the X_i-axis.

We now introduce the Lagrange basis built on the points in $\pi_{n-1}(V)$, in which we will rewrite the polynomial T_n (it is similar for the other polynomial T_ℓ, for $2 \leq \ell \leq n-1$, by considering the points in $\pi_{\ell-1}(V)$ instead). To $\alpha \in \pi_{n-1}(V)$ we associate the polynomial $E_\alpha(X_1, \ldots, X_{n-1})$ that verifies $E_\alpha(\alpha) = 1$ and $E_\alpha(\beta) = 0$ for any other point $\beta \in \pi_{n-1}(V)$.

$$E_\alpha(X_1, \ldots, X_{n-1}) := \prod_{i=1}^{n-1} \prod_{\substack{b \in X_i(V) \\ b \neq \alpha_i}} \frac{X_i - b}{\alpha_i - b}. \tag{1}$$

For further need, we introduce also this alternative form:

$$F_\alpha(X_1, \ldots, X_{n-1}) := \prod_{i=1}^{n-1} \prod_{\substack{b \in X_i(V) \\ b \neq \alpha_i}} X_i - b. \tag{2}$$

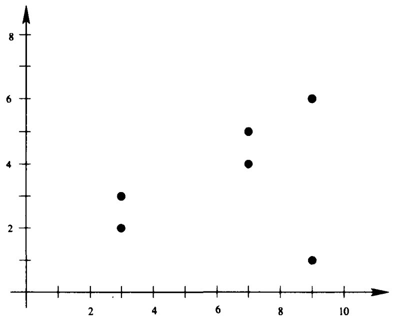
The expression of T_n in the Lagrange basis $\{E_\alpha,\ \alpha \in \pi_{n-1}(V)\}$ is:

$$T_n(X_1, \ldots, X_n) = \sum_{\alpha \in \pi_{n-1}(V)} \left(\prod_{y \in \pi_{n-1}^{-1}(\alpha) \cap V} X_n - y \right) E_\alpha(X_1, \ldots, X_{n-1}). \tag{3}$$

When $n = 2$, Figure 1 shows a simple example.

Primitive elements Leaving Assumption 1, it is also possible to give a parametrization of the coordinates of V, parallel with a randomly chosen hyperplane. This is the data of a "randomly" chosen linear

[1)]the focus will be on $k = \mathbb{Q}$ in this survey, and for convenience we will use $\mathbb{C}$ instead of $\overline{\mathbb{Q}}$. In the original papers [5, 3], fields of rational functions are also considered, and in the Ph.D. thesis of the author, number and function fields are treated, only in dimension 0 though.



$$
\begin{aligned}
q_3(Y) &= (Y-2)(Y-3) \\
q_7(Y) &= (Y-4)(Y-5) \\
q_9(Y) &= (Y-1)(Y-6).
\end{aligned}
$$

$$T_2(X,Y) = (q_3)\frac{(X-7)(X-9)}{(3-7)(3-9)} + (q_7)\frac{(X-3)(X-9)}{(7-3)(7-9)} + (q_9)\frac{(X-3)(X-7)}{(9-3)(9-7)}$$

$$N_2(X_1,X_2) = (q_3)(X-7)(X-9) + (q_7)(X-3)(X-9) + (q_9)(X-3)(X-7)$$

Figure 1: Lagrange interpolation

form $\Delta(X_1,\ldots,X_n)$ defining H, that almost always will be *separating* for V (that is $\Delta(\alpha) \neq \Delta(\beta)$ for all $\alpha \neq \beta$ in V) and a family of polynomials

$$(\ q(T)\ ,\ X_1 - v_1(T)\ ,\ \ldots\ ,\ X_n - v_n(T)\ ), \tag{4}$$

such that the roots of q are given by $\Delta(V)$, *i.e.* $q(t) = 0 \iff t = \Delta(\alpha)$ for a unique α in V. And, that $\alpha = (\alpha_1,\ldots,\alpha_n) = (v_1(t),\ldots,v_n(t))$. If $I(V)$ denotes the ideal of vanishing polynomials on V, we get:

$$q(\Delta(X_1,\ldots,X_1)) \equiv 0 \bmod I(V), \tag{5}$$

Relying on a projection (over a line here), this representation admits also a description through Lagrange polynomials.

$$v_i(T) = \sum_{\alpha\in V} \alpha_i \prod_{\beta\neq\alpha} \frac{T-\Delta(\alpha)}{\Delta(\beta)-\Delta(\alpha)}. \tag{6}$$

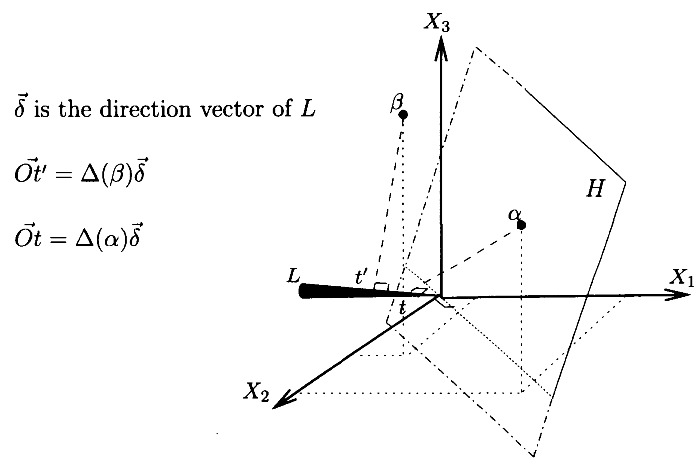


Figure 2: The orthogonal projection along H of two points α and β over L

Alternative representation: decrease of the coefficients size From the Lagrange formulas (6) and (3) we define 2 alternative representations.

Rational Univariate Representation: instead of considering the data of ($q(T)$, $X_1 - v_1(T)$, ... , $X_n - v_n(T)$) like in (4), it consists of choosing rather ($q(T)$, $q'(T)X_1 - w_1(T)$, ... , $q'(T)X_n - w_n(T)$), where:

$$w_i(T) = \sum_{\alpha \in V} \alpha_i \prod_{\beta \neq \alpha} T - \Delta(\alpha). \tag{7}$$

It is easy to see that $w_i(T) \equiv q'(T)v_i(T) \bmod q(T)$ (the mod $q(T)$ means taking the remainder of the Euclidean division by $q(T)$). The RUR is equivalent to the data of (4) since both parametrize the same set of points. It was introduced by Alonso *et al.* [1], as they remark the smaller coefficients [2]. Rouillier developed further the use of this representation, and renamed it Rational Univariate Representation [11]. By a different method, Giusti *et al.* [6] got an algorithm called *geometric resolution* to compute the same representation.

As for triangular sets, a similar transformation is possible and leads to the same nice decrease of the coefficients. Using the polynomial F_α in (2) instead of the E_α in (1):

$$N_n(X_1, \ldots, X_n) = \sum_{\alpha \in \pi_{n-1}(V)} \left(\prod_{y \in \pi_{n-1}^{-1}(\alpha) \cap V} X_n - y \right) F_\alpha(X_1, \ldots, X_{n-1}). \tag{8}$$

Statements of the results There are two kinds of upper-bounds: the *intrinsic* one, depending only on quantities attached to the solutions[3] and not of a particular system of equations. And the non-intrinsic ones, that depends on a specified system of equations (the input). The bounds from this last kind of measure are always deduced from the intrinsic ones, using a version of the "geometric-arithmetic" intersection theorem (the standard and the Arithmetic Bézout theorem (10)).

In dimension 0. Let V be the set of solutions in an algebraic closure of a field k of a given family of polynomials. We assume V finite. We let h_V be the height of V (Cf. § 2.2 for a definition) and d_V be its degree, that corresponds here to the cardinal of V. We get the following:

Primitive element: We let Δ be a separating linear form for V and we let $(q, q'X_1 - w_1, \ldots, q'X_n - w_n)$ be the associated RUR (7). Then:

$$h(w_i) \leq h_V + d_V h(\Delta) + d_V \log(n+2) + (n+1) \log d_V$$

Triangular set: We assume that V verfies Assumption 1:

$$h(T_n) \leq d_V \left(h_V + 5 \log(n+3) + 4 d_V \right)$$

Alternative triangular polynomial systems: With the same assumption as above, the polynomials $(N_1, \ldots, N_n)$ defined in Equation (8) verifies:

$$h(N_n) \leq h_V + 5 d_V \log(n+3) \tag{9}$$

The alternative representations have *linear* sized bounds with respect to the degree $\deg(V) := d_V$ and the height h_V, while the corresponding lexicographic Gröbner bases have *quadratic* sized bound. This better behavior is neatly observed experimentally.

In positive dimension. New results in this case are available in [3] but require several other notations to be stated. We have postponed this to § 4.

[2] but was already known by Kronecker

[3] seen as an algebraic variety

2 Height theory

This is a fundamental tool in our work. It comes from the theory of "Diophantine geometry" in mathematics. Several definitions have emerged, one of them developed mainly by Philippon, is using explicitly Elimination theory [9]. View our context, it is natural to choose this one. For any further details, we refer rather to the paper of Krick *et al.* [7] instead, because their presentation is closer to applications relevant to the community of "effective mathematicis".

2.1 Overview

There are two levels of measure with height theory: one concerning the algebraic numbers, the polynomials with coefficients of those, and one concerning algebraic varieties. In any case, the viewpoint lies in the parallel with the degree:

Polynomials We start with the definition of the height of a polynomial. The *algebraic complexity* is measured by the degree.

- total degree in $k[X_1, \dots, X_m] - \{0\}$.
- extended to $k(Y_1, \dots, Y_m)$ (taking maximum: if $\gcd(A, B) = 1$, $\mathrm{tdeg}(\frac{A}{B}) := \max\{\mathrm{tdeg}A, \mathrm{tdeg}(B)\}$)
- extended to $k(Y_1, \dots, Y_m)[X_1, \dots, X_n]$ (reducing to the same denominator, then taking the maximum of each coefficient in $k(Y_1, \dots, Y_m)$)

The height of a polynomial concerns its *arithmetic complexity*. We start by defining the height of a rational number.

- For $\frac{a}{b} \in \mathbb{Q}$ with $\gcd(a, b) = 1$, it is defined by $h(\frac{a}{b}) = \log\max\{|a|, |b|\}$.

  Formal definition: Let p be a prime.

  $h_p(\frac{a}{b}) = \log\max\{1, p^{v_p(b)-v_p(a)}\}$, $h_p(\frac{a}{b}) \neq 0 \iff p \nmid a$, and $p|b$.

  $h_\infty(\frac{a}{b}) = \log\max\{1, |\frac{a}{b}|\}$, $h_\infty(\frac{a}{b}) \neq 0 \iff |a| > |b|$

  Height of a rational: $h(\frac{a}{b}) = \sum_{p \text{ prime}} h_p(\frac{a}{b}) + h_\infty(\frac{a}{b}) = \log\max\{|a|, |b|\}$.
- extended to $\mathbb{Q}[X_1, \dots, X_n]$ in the following way: Let $F = \sum_{\mathbf{i}\in\mathbb{N}^n} f_{\mathbf{i}} X_1^{i_1} \cdots X_n^{i_n}$.

  Let $c = \mathrm{LCM}\{$ denom. of $f_{\mathbf{i}}\}$. Then $cF \in \mathbb{Z}[X_1, \dots, X_n]$, and define $h(F) = \log\max\{|c|, h_\infty(cF)\}$.

  Formal definition: For $v = p$, or $v = \infty$, let $h_v(F) = \log\max\{1, \max_{\mathbf{i}\in\mathbb{N}^n}\{h_v(f_{\mathbf{i}})\}\}$, then,

  height of a polynomial: $h(F) = \sum_{p \text{ prime}} h_p(F) + h_\infty(F)$.

Varieties The corresponding notion of height is more sophisticated to define. A convenient way to introduce it is the parallel with the *degree* seen as the algebraic complexity:

- V equidimensional: generic number of intersection points with a linear space of complementary dimension.
- Additivity: if $V_1 \cap V_2 = \emptyset$, then $\deg(V_1) + \deg(V_2) = \deg(V_1 \cup V_2)$

- Affine version of Bézout theorem: $\deg(V \cap W) \leq \deg(V)\deg(W)$.
- is well-defined for varieties defined over any field, not only $\mathbb{Q}$ or number fields.

As for polynomials, the height of a variety is a measure of its arithmetic complexity. The following points are to be compared with the above ones that concerned the degree.

- V equidimensional: its height, $h(V)$ is (almost) height of the *Chow form* (Cf. next paragraph).
- additive: $h(V_1 \cup V_2) = h(V_1) + h(V_2)$.
- arithmetic Bézout theorem: if $V \not\subset Z(f)$,

$$h(V \cap Z(f)) \leq \deg(f)h_V + d_V h(f) + \log(n+1)\deg(f). \tag{10}$$

- for varieties defined over $\mathbb{Q}$ (more generally, over a number fields).

The detailed definitions are given in the two next paragraphs.

2.2 Chow form

This is a polynomial attached to a given variety V that contains all the information of it (but has many more variables).

Let $V \subset \mathbb{C}^{m+n}$ be an equidimensional variety of dimension m, $\overline{V} \subset \mathbb{P}^{n+m}(\mathbb{C})$ its projective closure with Y_0 as homogenizing new variable.

We introduce $m+1$ generic linear forms L_i, $i = 0, \ldots, m$, with generic coordinates represented by $(n+m+1)(m+1)$ new variables: $\mathbf{U}_i = U_{i,0}, \ldots, U_{i,m+n}$

$$L_i^h = U_{i,0}Y_0 + U_{i,1}Y_1 + \cdots + U_{i,m}Y_m + U_{i,m+1}X_1 + \cdots + U_{i,m+n}X_n. \tag{11}$$

The *incidence variety* W is by definition:

$$W = \overline{V} \cap Z(L_0^h, \ldots, L_m^h) \subset \overline{V} \times \underbrace{\mathbb{P}^{m+n}(\mathbb{C}) \times \cdots \times \mathbb{P}^{m+n}(\mathbb{C})}_{m+1}$$

The Zariski closure of the projection of W on $\mathbb{P}^{m+n}(\mathbb{C}) \times \cdots \times \mathbb{P}^{m+n}(\mathbb{C})$ is a hypersurface. A *Chow form* is a square-free polynomial that defines this hypersurface. Here are simple remarks:

Fact 0: All Chow forms Ch_V are defined up to a constant factor.

Fact 1: The Chow forms are polynomials in $(m+1)$ groups $\mathbf{U}_i$ of $(m+n+1)$ variables, multi-homogeneous w.r.t. each groups.

If $V \subset \mathbb{C}^{m+n}$ is defined over $\mathbb{Z} \subset R \subset \mathbb{C}$, then:

$$Ch_V(\mathbf{U}_0, \mathbf{U}_1, \ldots, \mathbf{U}_m) \in R[\mathbf{U}_0, \ldots, \mathbf{U}_m]$$

In this survey, $R = \mathbb{Z}$.

Fact 2: If V is an irreducible variety, then Ch_V is an irreducible polynomial.

If $V = V_1 \cap V_2$, with $\dim(V_1) = \dim(V_2) = m$, $V_1 \cap V_2 = \emptyset$, then the product $Ch_{V_1}Ch_{V_2}$ is a Chow form of V.

A more geometric interpretation The m groups of $(m+n+1)$ variables $\mathbf{U}_1, \ldots, \mathbf{U}_m$ are used to parametrize m hyperplanes in $\mathbb{P}^{m+n}(\mathbb{C})$. For *almost all* values $\mathbf{U}_i \leftarrow \mathbf{u}_i = (u_{i,0}, \ldots, u_{i,m+n+1}) \in \mathbb{Q}^{m+n+1}$, let H_i be the hyperplane defined by the linear form L_i of (11) evaluated at $\mathbf{u}_i$:

$$H_i := Z(L_i(u_{i,0}, u_{i,1}, \ldots, u_{i,m}, u_{i,m+1}, \ldots, u_{i,m+n})).$$

Remark: H_i is an affine hyperplane, its projective closure is $\overline{H_i} := Z(L_i^h(\mathbf{u}_i))$. By the property of the degree of V, then:

$$V_0 := V \cap H_1 \cdots \cap H_m \qquad \text{is finite, of cardinal } \leq d_V,$$

and for almost all choices of the evaluation points $\{u_{i,j},\ 0 \leq j \leq m+n+1,\ 1 \leq i \leq m\}$, $\#V_0$ is equal to d_V.

The first group of $m+n$ variables $U_{0,1}, \ldots, U_{0,m}$ of $\mathbf{U}_0$ parametrizes the *affine hyperplanes* in $\mathbb{A}^{m+n}(\bar{\mathbb{Q}})$ going though 0, leaving one variable $U_{0,0}$ free. Let $\mathbf{u}_0' := (u_{0,1}, \ldots, u_{0.m+n}) \in \mathbb{Q}^{m+n}$.

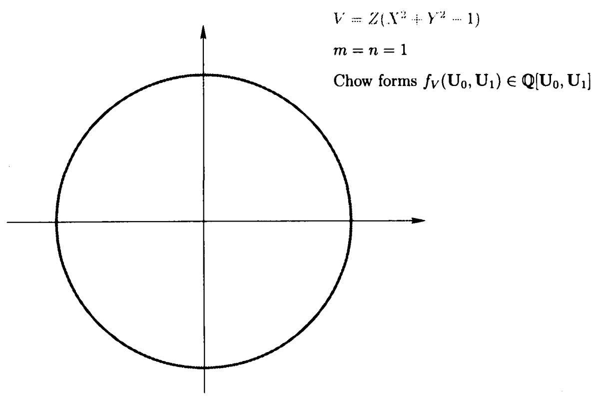
$$\text{homogeneous linear form} \quad L_0 := u_{0,1}Y_1 + \cdots + u_{0,m}Y_m + u_{0,m+1}X_1 + \cdots + u_{0,m+n}X_n$$

Let $H_0 = Z(L_0)$ be the corresponding hyperplane going through 0. The Chow form of V verifies the following property.

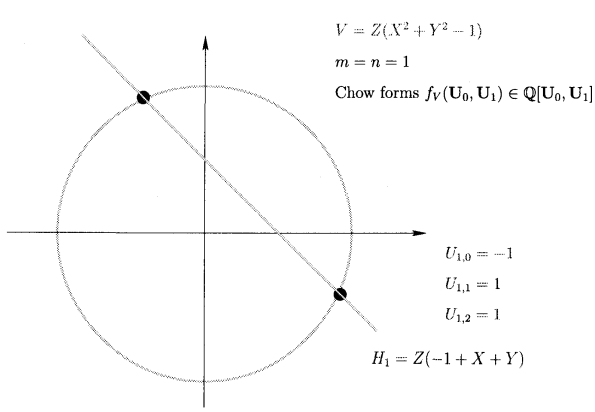
$$Ch_V(U_{0,0}, \mathbf{u}_0', \mathbf{u}_1, \ldots, \mathbf{u}_{m+n}) = c \prod_{\substack{\alpha \in V_0 \subset \mathbb{C}^{m+n} \\ \alpha \notin H_0}} (U_{0,0} + L_0(\alpha)), \tag{12}$$

otherly said, the univariate polynomial $Ch_V(U_{0,0}, \mathbf{u}_0', \ldots, \mathbf{u}_{m+n})$ is a primitive element for V_0 w.r.t the hyperplane H_0.

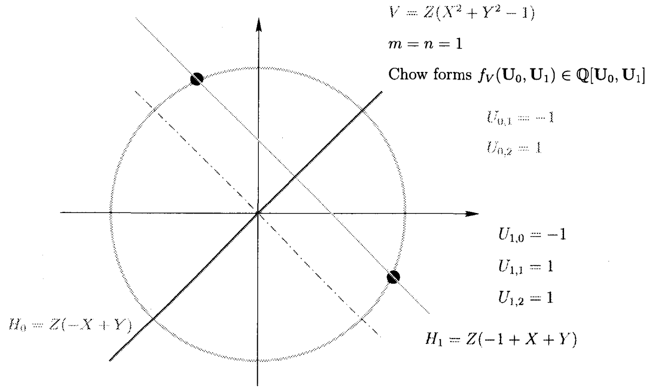
A toy example in the plane The circle has no point at infinity, so the projective hyperplanes (that are just lines here) will be represented w.l.o.g by affine ones.



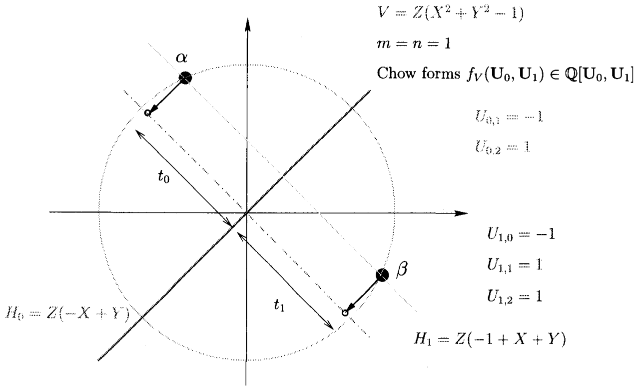
Next we choose an intersection line H_1. The circle being of degree 2, there are 2 intersection points.



By definition, the first set of variables parametrize a homogeneous linear form, whose line H_0 is going through the origin.



This gives the primitive element representation of the intersection of V with the H_1.



$$f_V(U_{0,0}, -1, 1; -1, 1, 1) = c(U_{0,0} + t_0)(U_{0,0} + t_1)$$
$$t_0 = u_{0,1}\alpha_1 + u_{0,2}\alpha_2 = -\alpha_1 + \alpha_2$$
$$t_1 = u_{0,1}\beta_1 + u_{0,2}\beta_2 = -\beta_1 + \beta_2$$

2.3 Mahler measures and height of varieties

The definitions are a bit more complicated, but we need only to manipulate the results.

Following some works of Nesterenko, Philippon in 1986 [9], defines a height of varieties using the *Mahler measure* of one of its Chow form:

$$f \in \mathbb{C}[X_1, \dots, X_n], \quad \mathsf{m}(f) := \int_0^1 \cdots \int_0^1 \log |f(e^{2i\pi t_1}, \dots, e^{2i\pi t_n})| dt_1 \dots dt_n.$$

In 1 variable, let us write $f = a_d \prod_{i=1}^d (X - \alpha_i)$, then:

$$\mathsf{m}(f) = \log |a_d| + \sum_{i=1}^{d} \max\{0, \log |\alpha_i|\} \qquad \text{(Jensen's formula)}$$

showing a clear link with the traditional height of a polynomial $h_\infty(f)$ defined in § 2.1. We note the additivity of $\mathsf{m}(\,.\,)$:

$$\mathsf{m}(fg) = \mathsf{m}(f) + \mathsf{m}(g).$$

This Mahler measure appeared to be not completely satisfactory, and later Philippon [10] modified it with the "S_n^r-Mahler measure". We assume that f is a polynomial in $(m+1)$ groups of $(m+n+1)$ variables. homogeneous for each groups. Let $k = m+n$ be the dimension of the ambient space. Let $S_{k+1}^{m+1} = S_{k+1} \times \cdots \times S_{k+1}$, where S_{k+1} is the unit sphere in $\mathbb{C}^{k+1}$. The S_{k+1}^{m+1}-Mahler measure is defined by:

$$\mathsf{m}(f, S_{k+1}^{m+1}) = \int_{S_{k+1}^{m+1}} \log |f| \mu_{k+1}^{\wedge(m+1)}.$$

Now if V is an m-dimensional variety in $\mathbb{C}^k$, with $k = m+n$, then a Chow form of V is a polynomial in $m+1$ groups of $n+m+1$ variables, denoted $Ch_V(\mathbf{U}_0, \dots, \mathbf{U}_m)$. It is possible to take its S_{k+1}^{m+1}-Mahler measure.

Remark: The following inequalities permit to link the above two definitions of Mahler measures with the height of a polynomial. Let $d = \deg(f)$.

$$0 \leq \mathsf{m}(f) - \mathsf{m}(f, S_{k+1}^{m+1}) \leq (m+1)d \sum_{j=1}^{k} \frac{1}{2j} \tag{13}$$

$$|\mathsf{m}(f) - h_\infty(f)| \leq d \log(k+1) \tag{14}$$

Here is how Philippon defined the height of a variety: ($V \subset \mathbb{C}^k$, $k = m+n$, equidimensional of dimension m as usual):

$$h_V := \sum_{p \text{ primes}} h_p(Ch_V) + \mathsf{m}(Ch_V, S_{k+1}^{m+1}) + (m+1)d_V \sum_{j=1}^{k} \frac{1}{2j}. \tag{15}$$

The last term $\sum_{j=1}^{k} \frac{1}{2j}$ permits to ensure that $h_V \geq 0$. Also,

$$h_{V \cup W} = h_V + h_W, \qquad \text{if} \qquad V \cap W = \emptyset, \qquad \text{and} \qquad \dim(V) = m = \dim(W).$$

Finally, we mention the arithmetic counterpart of the Bézout inequality, in a slighlty different formulation than in Equation (10).

Arithmetic Bézout theorem (ABT): Let $V = Z(f_1, \dots, f_s) \subset \mathbb{C}^n$, defined over $\mathbb{Q}$, with $h(f_j) \leq h$ and $\operatorname{tdeg}(f_j) = d_j$, and $n_0 = \min\{n, s\}$:

$$h_V \leq \Big(\prod_{j=1}^{n_0} d_j\Big)\Big(\Big(\sum_{j=1}^{n_0} \frac{1}{d_j}\Big)h + (n+n_0)\log(n+1)\Big). \tag{16}$$

3 The case of dimension 0

We assume here that $V \subset \mathbb{C}^n$ is the finite set of solutions of a polynomial system $f_1, \ldots, f_n \in \mathbb{Q}[X_1, \ldots, X_n]$.

3.1 Bounds for the RUR

Let $\Delta(X_1, \ldots, X_n) = u_1X_1 + \cdots + u_nX_n$ be a separating linear form for V and let $(q(T), q'(T)X_1 - w_1(T), \ldots, q'(T)X_n - w_n(T))$ be the associated Rational Univariate Representation of V. Let Ch_V be *the monic* Chow form of V. Since V is 0-dimensional, there is only 1 group of $n+1$ variables $\mathbf{U}_0 = U_{0,0}, \ldots, U_{0,n}$. By Equation (12), we have:

$$Ch_V(U_{0,0}, -u_1, \ldots, -u_n) = \prod_{\alpha \in V} U_{0,0} - u_1\alpha_1 - \cdots - u_n\alpha_n, = \prod_{\alpha \in V} U_{0,0} - \Delta(\alpha), \tag{17}$$

hence $Ch_V(T, -u_1, \ldots, -u_n) = q(T)$ since they both vanishes on $\Delta(V)$ and have same degree, by Equation (5). This implies,

$$\frac{\partial}{\partial U_{0,0}} Ch_V(U_{0,0}, -u_1, \ldots, -u_n) = q'(U_{0,0}). \tag{18}$$

Let $G(U_{0,1}, \ldots, U_{0,n}) := Ch_V(U_{0,1}X_1 + \cdots + U_{0,n}X_n, -U_{0,1}, \ldots, -U_{0,n})$. From Equation (17), it arrives:

$$G(u_1, \ldots, u_n) = Ch_V(\Delta, -u_1, \ldots, -u_n) \text{ vanishes on } V. \tag{19}$$

This implies:

$$\frac{\partial}{\partial U_{0,i}} G = \left(X_i \frac{\partial}{\partial U_{0,0}} Ch_V - \frac{\partial}{\partial U_{0,i}} Ch_V \right) (U_{0,1}X_1 + \cdots + U_{0,n}X_n, -U_{0,1}, \ldots, -U_{0,n}).$$

If we perform the evaluation $U_{0,i} = u_i$ in the above, it comes with Equation (18), that:

$$X_i q'(u_1X_1 + \cdots + u_nX_n) = \frac{\partial}{\partial U_{0,i}} Ch_V(u_1X_1 + \cdots + u_nX_n, -u_1, \ldots, -u_n),$$

vanishes on V, that is are equal modulo $I(V)$. We use $v_i(\Delta) \equiv X_i \bmod I(V)$ (Cf. Equation (4)), multiply it by q' and perform the substitution $T \leftrightarrow \Delta(X_1, \ldots, X_n)$:

$$v_i(T)q'(T) - \frac{\partial}{\partial U_{0,i}} Ch_V(T, -u_1, \ldots, -u_n) \equiv 0 \bmod q(T)$$

By Equation (7) what folloes it, $w_i(T) = v_i(T)q'(T) \bmod q(T)$. This gives:

$$w_i(T) = \frac{\partial}{\partial U_{0,i}} Ch_V(T, -u_1, \ldots, -u_n), \tag{20}$$

since both terms have same degree.

End of first step: This is the link between the Chow form and the polynomials occuring in the RUR.

Next step: Use height estimates. We start by two easy inequalities (21) and (22): if f is a univariate polynomial of degree d, x a number such that $|x| > 1$. then:

$$|f'(x)| \leq d^2 \ |x|^{d-1} \max\{| \text{ coeff of } f|\}. \tag{21}$$

If F is an $(n+1)$-variate polynomial of total degree d, and $x_2, \ldots, x_{n+1}$ are complex numbers such that $|x_i| > 1$, then:

$$\max\{|\text{ coeff of } \frac{\partial F}{\partial X_1}(X_1, x_2, \ldots, x_{n+1})|\} \leq d^{n+1} \max_i\{|x_i|\}^d \max\{|\text{ coeff of } F|\} \tag{22}$$

We apply it to Equation (20) and to Equation (18) to get:

$$\max\{|\text{ coeff of } q'|\} \text{ and } \max\{|\text{ coeff of } w_i|\} \leq d_V^{n+1} \max_i\{|u_i|\}^{d_V} \max\{|\text{ coeff of } Ch_V|\}.$$

By definition of the height:

$$h_\infty(w_i) \text{ and } h_\infty(q') \leq (n+1)\log d_V + d_V h_\infty(\Delta) + h_\infty(Ch_v). \tag{23}$$

Remark: When $v = p$, p a prime, the estimates for $h_p(w_i)$ are easy to obtain, and the details are not given in this survey: $h_p(w_i) \leq h_p(Ch_V) + d_V h_p(\Delta)$.

3rd step: From height of Chow forms to height of varieties.

By property of Mahler measures (13) and (14), $h_\infty(Ch_V) \leq \mathrm{m}(Ch_V, S_{n+1}) + d_V \log(n+2) + d_V \sum_{j=1}^{n+1} \frac{1}{2j}$, that implies:

$$h_\infty(w_i) \leq \mathrm{m}(Ch_V, S_{n+1}) + (n+1)\log(d_V) + d_V h_\infty(\Delta) + d_V \log(n+2) + d_V \sum_{j=1}^{n+1} \frac{1}{2j}.$$

By definition of the height of a polynomial, it remains to sum over the absolute values v:

$$\begin{aligned} h(w_i) &\leq \Big(\sum_{p \text{ prime}} h_p(Ch_V) + d_V h_p(\Delta)\Big) + \mathrm{m}(Ch_V, S_{n+1}) \\ &+ (n+1)\log(d_V) + d_V h_\infty(\Delta) + d_V \log(n+2) + d_V \sum_{j=1}^{n+1} \frac{1}{2j} \\ &\leq h_V + d_V h(\Delta) + d_V \log(n+2) + (n+1)\log d_V \end{aligned}$$

This is the intrinsic quantities that depends on the degree and the height of the variety V and the separating linear form Δ.

Last step: Use the Arithmetic Bézout Theorem to get non-intrinsic bounds, that depend on the input polynomial system, from the intrinsic ones obtained just above. If V is the set of solutions of a polynomial system $(f_1, \ldots, f_n)$ with $d = \max_i\{\mathrm{tdeg}(f_i)\}$ and $h = \max_i\{h(f_i)\}$, then from the standard Bézout inequality $d_V \leq d^n$, and from the ABT (16), $h_V \leq nd^{n-1}(h + 2d\log(n+1))$. Plugging these into the estimates of $h(w_i)$ obtained in Step 3 gives:

$$h(w_i) \leq d^n(nh + h(\Delta) + 3n\log(n+2)) = O((nh + h(\Delta))d^n)$$

Conclusion: we used 4 steps.

1. link between polynomials and the Chow forms
2. use height estimates
3. from height of Chow forms to height of variety. (use properties of Mahler measures)
4. Use of Arithmetic Bézout Theorem.

3.2 Bounds for triangular systems

We will treat only the easier case of the polynomials $N_1, \ldots, N_n$, when $n = 2$ and on an example (Cf. Figure 1). For the triangular sets $T_1, \ldots, T_n$, some extra complications occur to treat the denominators in Formula (1), when compared to Formula (2). This precisely explains the overhead quadratic behavior of their estimates, when compared to the linear behavior of the ones for the $N_1, \ldots, N_n$.

Highlights of the proof on an example This is not the purpose of this text to give the full details that require quite a lot of notations. Rather, the following might motivate to read the full proof in [5].

The example is the one of Figure 1. We have $\deg_X(T_1) = d_1 = 3$ and $\deg_Y(T_2) = d_2 = 2$ there. The monic Chow form of V is: $Ch_V(U_{0,0}, U_{0,1}, U_{0,2}) = \prod_{\alpha \in V} U_{0,0} + \alpha_1 U_{0,1} + \alpha_2 U_{0,2}$. That implies:

$$Ch_V(X, -1, 0) = \prod_{\alpha \in V} X - \alpha_1 = N_1(X)^2 = T_1(X)^2 \qquad \text{(in general } T_1(X_1)^{d_2}\text{)}$$

Remains to treat $N_2(X, Y)$. For $\alpha_1 = 3, 7$ or 9, let $v_{\alpha_1} := \pi_1^{-1}(\alpha_1)$ the fiber over α_1 of the projection of V on the X-axis. By a classical property of varieties described by triangular sets ("equiprojectable"), $\#v_3 = \#v_7 = \#v_9 = \deg_Y(T_2) = 2$. By additivity of Chow forms[4] (§ 2.2, Fact 2):

$$v_3 \cup v_7 \cup v_9 = V, \Rightarrow Ch_{v_3} Ch_{v_7} Ch_{v_9} = Ch_V. \tag{24}$$

We introduce the following subsets of V:

$$W_3 = v_7 \cup v_9\ ,\ W_7 = v_3 \cup v_9\ ,\ \text{and } W_9 = v_3 \cup v_7. \tag{25}$$

Since $Ch_{W_3} = \prod_{\alpha \in W_3} U_{0,0} + \alpha_1 U_{0,1} + \alpha_2 U_{0,2} \Rightarrow Ch_{W_3}(X, -1, 0) = \prod_{\alpha \in W_3} X - \alpha_1 = (X - 7)^2 (X - 9)^2$. Similarly, we can show that $Ch_{v_3}(Y, 0, -1) = q_3(Y) = (Y - 2)(Y - 3)$, and $Ch_{v_7}(Y, 0, -1) = q_7(Y) = (Y - 4)(Y - 5)$, and $Ch_{v_9}(Y, 0, -1) = q_7(Y) = (Y - 1)(Y - 6)$.

Then a look at the formula for N_2 in Figure 1 and the above shows that:

$$\begin{aligned} N_2(X, Y) = Ch_{v_3}(Y, 0, -1) Ch_{W_3}(X, -1, 0)^{1/2} + Ch_{v_7}(Y, 0, -1) Ch_{W_7}(X, -1, 0)^{1/2} \\ + Ch_{v_9}(Y, 0, -1) Ch_{W_9}(X, -1, 0)^{1/2} \end{aligned} \tag{26}$$

This ends the first step, which was intended to link the polynomial N_i with the Chow form Ch_V.

Second step: We turn to the height estimation, starting by this simple result: If $f = \sum_{\mathrm{i} \in \mathbb{N}^n} f_{\mathrm{i}} X_1^{i_1} \ldots X_n^{i_n}$ is a polynomial, we denote by d_f its total degree, and by $|f|_\infty := \max_{\mathrm{i} \in \mathbb{N}^n} |f_{\mathrm{i}}|$ the maximal absolute of its coefficients. According to the definitions of § 2.1, we have $h_\infty(f) = \max\{1, \log |f|_\infty\}$. Let $g = \sum_{\mathrm{i} \in \mathbb{N}^n} g_{\mathrm{i}} X_1^{i_1} \ldots X_n^{i_n}$ be another polynomial, then:

$$h_\infty(f) + h_\infty(g) \leq h_\infty(fg) + 2(d_f + d_g) \log(n + 1). \tag{27}$$

Indeed, by Equation (14), $|h_\infty(fg) - \mathrm{m}(fg)| \leq (d_f + d_g) \log(n + 1)$, and by the additivity of $m(\,.\,)$, comes $\mathrm{m}(f) + \mathrm{m}(g) \leq |h_\infty(fg)| + (d_f + d_g) \log(n + 1)$. Again, using Equation (14) gives $h_\infty(f) \leq \mathrm{m}(f) + d_f \log(n + 1)$ and $h_\infty(g) \leq \mathrm{m}(g) + d_g \log(n + 1)$, yielding the inequality (27).

---

[4] these Chow forms are actually defined over a field extension of $\mathbb{Q}$, that would require a special definition of height. This is not treated here.

We can apply this result to $f = g = Ch_{W_3}(X,-1,0)^{1/2}$, that gives:

$$2h_\infty(Ch_{W_3}(X,-1,0)^{1/2}) \leq h_\infty(Ch_{W_3}(X,-1,0)) + 4(3-1)\log(2) \qquad \text{(in general, } (3-1) = d_1 - 1)$$

It is clear that the absolute value of the coefficients of $Ch_{W_3}(X,-1,0)$ are contained in those of Ch_{W_3}, hence $h_\infty(Ch_{W_3}(X,-1,0)) \leq h_\infty(Ch_{W_3})$ by definition of the height of a polynomial (Cf. § 2.1), this gives:

$$h_\infty(Ch_{W_3}(X,-1,0)^{1/2}) \leq \frac{1}{2}h_\infty(Ch_{W_3}) + 2(d_1-1)\log(2) \qquad \text{(in general, } \frac{1}{2} = \frac{1}{d_2}) \tag{28}$$

By Inequality (14), $h_\infty(Ch_{W_3}) \leq \mathsf{m}(Ch_{W_3}) + 2(3-1)\log(4)$, which is equal in general to $\mathsf{m}(Ch_{W_3}) + d_2(d_1-1)\log(n+2)$, since $n = 2$ and the Chow form is a polynomial in $n+1$ variables. Plugging this with $d_2 = 2$ in (28), we obtain:

$$h_\infty(Ch_{W_3}(X,-1,0)^{1/2}) \leq \frac{1}{2}\mathsf{m}(Ch_{W_3}) + (d_1-1)(2\log(2) + \log(n+2)). \tag{29}$$

A similar inequality holds for W_7 and W_9.

On the other hand, easier calculations than above, that we do not do, give:

$$h_\infty(Ch_{v_3}(Y,0,-1)) \leq \mathsf{m}(Ch_{v_3}) + d_2\log(n+2). \tag{30}$$

Next, for 2 polynomials f and g in n variables, the inequality $|fg|_\infty \leq (d_f + d_g)^n |f|_\infty |g|_\infty$ holds. This translates in terms of heights to $h_\infty(fg) \leq h_\infty(f) + h_\infty(g) + \log(n)(d_f + d_g)$. Follows the first inequality below, since $d_1 - 1 = 2 = \deg_X(Ch_{W_3}(X,-1,0)^{1/2})$ and $d_2 = 2 = \deg_Y(Ch_{v_3}(Y,0,-1))$:

$$\begin{aligned} h_\infty(Ch_{W_3}(X,-1,0)^{1/2}Ch_{v_3}(Y,0,-1)) \leq h_\infty(Ch_{W_3}(X,-1,0)^{1/2}) &+ h_\infty(Ch_{v_3}(Y,0,-1)) \\ &+ (d_1 - 1 + d_2)\log(n) \end{aligned} \tag{31}$$

With Equation (30) and (29), it becomes after a few simplifications:

$$h_\infty(Ch_{W_3}(X,-1,0)^{1/2}Ch_{v_3}(Y,0,-1)) \leq \frac{1}{2}\mathsf{m}(Ch_{W_3}) + \mathsf{m}(Ch_{v_3}) + (2d_2 + 3d_1)\log(n+2)$$

Recall that by Equalities (24) and (25), $V = W_3 \cup v_3$. Also the positivity and additivity of the Mahler measure implies: $\frac{1}{2}\mathsf{m}(Ch_{W_3}) + \mathsf{m}(Ch_{v_3})\ lem(Ch_V)$. Replaced in the equation above,

$$h_\infty(Ch_{W_3}(X,-1,0)^{1/2}Ch_{v_3}(Y,0,-1)) \leq \mathsf{m}(Ch_V) + (2d_2 + 3d_1)\log(n+2).$$

A similar inequality holds for W_7, v_7 and for W_9, v_9. It remains to add the height of these 3 terms in the interpolation formula (26) of $N_2(X,Y)$. It is easy to see that:

$$\begin{aligned} h_\infty(N_2) &\leq \max_{i=3,7,9}\left\{h_\infty(Ch_{W_i}(X,-1,0)^{1/2}Ch_{v_i}(Y,0,-1))\right\} + \log(3) \qquad \text{(in general, } 3 = d_1) \\ &\leq \mathsf{m}(Ch_V) + (2d_2 + 3d_1)\log(n+2) + \log(d_1). \qquad \text{(when } n = 2,\ d_1 = \prod_{j=1}^{n-1} d_i) \end{aligned} \tag{32}$$

3rd step: We use the definition of a height of a variety (15), relying on the Mahler measure. First the work done in 2nd step concerns exclusively the component $h_\infty(\,.\,)$ of the height (Cf. § 2.1 for definitions). The p-adic components $h_p(\,.\,)$ were not treated, but it is easier and we refer to the original paper for a proof:

$$h_p(N_2) \leq h_p(Ch_V).$$

Finally,

$$\begin{aligned} h(N_2) &= \sum_{p \text{ prime}} h_p(N_2) + h_\infty(N_2), \\ &\leq \sum_p h_p(Ch_V) + \mathrm{m}(Ch_v, S_{n+1}) + \deg(V)(\log(n+2) + \sum_{j=1}^{n} \frac{1}{2j}) \\ &+ (d_1 + d_2)\log(n+1) + \log(d_1) \end{aligned}$$

After simplifications, such as $d_1 + d_2 \leq d_1 d_2 = d_V$ (assuming $\max\{d_1, d_2\} > 1$) and using the definition of the height of a variety (15)

$$h(N_2) \leq h_V + 5 d_V \log(n+2), \qquad \text{(true in general)}$$

This is the upper-bound presented in the introduction.

4th step. Using intrinsic bounds to get extrinsic ones through the Arithmetic Bézout theorem. If $V = Z(\langle f_1, \ldots, f_n \rangle)$, with $\max_i\{\mathrm{tdeg}(f_i)\} = d$ and $\max_i\{h(f_i)\} = h$, then $d_V \leq d^n$ by the standard Bézout theorem, by the ABT (16) $h_V \leq n d^{n-1}(h + 2d\log(n+1))$. Using these inequalities in the upper-bound for $h(N_2)$ just obtained above gives:

$$h(N_2) \leq d^n(nh + 7\log(n+2)) = O(nhd^n).$$

4 Toward the positive dimension

We assume here that V is of positive dimension $m > 0$, equidimensional. For convenience we introduce the variables $\mathbf{Y} = Y_1, \ldots, Y_m$ along with the usual $\mathbf{X} = X_1, \ldots, X_n$ ones. We make the assumption:

Assumption 2 The projection of all irreducible components V on the $\mathbf{Y}$-space is dense (for the Zariski topology).

Let $K = \mathbb{Q}(\mathbf{Y})$. Under Assumption 2, the variety $V^* \subset \bar{K}^n$ defined by the same defining equations of V after scalar extension from $\mathbb{Q}[\mathbf{Y}, X_1, \ldots, X_n]$ to $\mathbb{Q}(\mathbf{Y})[X_1, \ldots, X_n]$ is of dimension 0. Similarly, we assume that V^* **verifies Assumption 1** that is can be defined by a triangular set $T_1, \ldots, T_n$ over the field K. We define as in Equation (8), the corresponding polynomials $N_1, \ldots, N_n$. How large the *integer* coefficients of the T_i's and N_i's can be in this case ?

For $1 \leq \ell \leq n$, let us write N_ℓ as

$$N_\ell = \sum_{\mathbf{i}} \frac{\gamma_{\mathbf{i},\ell}}{\varphi_{\mathbf{i},\ell}} X_1^{i_1} \cdots X_\ell^{i_\ell} + \frac{\gamma_\ell}{\varphi_\ell} X_\ell^{d_\ell}$$

and T_ℓ as

$$T_\ell = \sum_{\mathbf{i}} \frac{\beta_{\mathbf{i},\ell}}{\alpha_{\mathbf{i},\ell}} X_1^{i_1} \cdots X_\ell^{i_\ell} + X_\ell^{d_\ell},$$

where:

- all multi-indices $\mathbf{i} = (i_1, \ldots, i_\ell)$ satisfy $i_r < d_r$ for $r \leq \ell$;
- all polynomials $\gamma_{\mathbf{i},\ell}$, $\varphi_{\mathbf{i},\ell}$, γ_ℓ and φ_ℓ, and $\beta_{\mathbf{i},\ell}$, $\alpha_{\mathbf{i},\ell}$, are in $\mathbb{Z}[\mathbf{Y}]$;

- in $\mathbb{Z}[\mathbf{Y}]$, the equalities $\gcd(\gamma_{\mathrm{i},\ell}, \varphi_{\mathrm{i},\ell}) = \gcd(\gamma_\ell, \varphi_\ell) = \gcd(\beta_{\mathrm{i},\ell}, \alpha_{\mathrm{i},\ell}) = \pm 1$ hold.

Then, all polynomials $\gamma_{\mathrm{i},\ell}$ and γ_ℓ, $\varphi_{\mathrm{i},\ell}$ and φ_ℓ, as well as the LCM of all $\varphi_{\mathrm{i},\ell}$ and φ_ℓ, have degree bounded by d_V and height bounded by

$$\mathcal{H}_\ell \leq 2h_V + \big((4m+2)d_V + 4m\big)\log(d_V) + \big((10m+16)d_V + 5\ell + 2m\big)\log(m+\ell+3).$$

All polynomials $\beta_{\mathrm{i},\ell}$ and $\alpha_{\mathrm{i},\ell}$, as well as the LCM of all $\alpha_{\mathrm{i},\ell}$, have degree bounded by $2d_V^2$ and height bounded by

$$\begin{aligned}\mathcal{H}'_\ell \quad \leq \quad & 4d_V h_V + 3d_V^2 + 4\big((2m+1)d_V^2 + m(d_V+1)\big)\log(d_V+1) \\ & + \big((20m+22)d_V^2 + 5(d_V+\ell+m)\big)\log(m+\ell+3).\end{aligned}$$

Here again, the polynomials N_i's enjoy a better behavior in term of complexity bounds (linear, versus quadratic for the polynomials T_i's), also experimentally observed.

Strategy of proof Regarding Assumption 2 made above, the idea is naturally to reduce to dimension 0 by *specialization* of the variables $\mathbf{Y}$, use the upper-bounds that were just proven in § 2 and then lift back the variables $\mathbf{Y}$ while evaluating the growth of the coefficients of the overall process.

While the strategy is simple, several technical difficulties arise. We introduce some new notations in order to detail them more. Let $f_1, \dots, f_n \in \mathbb{Q}[\mathbf{Y}, \mathbf{X}]$ an input polynomial system defining V. Let $\mathbf{y} = (y_1, \dots, y_m)$ be a point in $\mathbb{Q}^m$. For convenience, the polynomials $f_{i,\mathbf{y}}$ will denote the evalution of the variables $\mathbf{Y}$ at the pint $\mathbf{y}$: $f_{i,\mathbf{y}} := f_i(y_1, \dots, Y_m, X_1, \dots, X_n)$. We say that $\mathbf{y} = (y_1, \dots, y_m)$ is a "good" specialization point if:

- the polynomials in K at the denominators of the polynomials in T do not vanish at $\mathbf{y}$; that is the polynomials $T_{i,\mathbf{y}}$ are well-defined.
- the triangular set $(Y_1 - y_1, \dots, Y_m - y_m, T_{1,\mathbf{y}}(X_1), T_{2,\mathbf{y}}(X_1, X_2), \dots, T_{n,\mathbf{y}}(X_1, \dots, X_n))$ is the reduced Gröbner basis of the variety $V_{\mathbf{y}} := V \cap Z(\langle Y_1 - y_1 \dots, Y_m - y_m\rangle)$

It is easy to show that there are reasonnably "small" enough good specialization points $\mathbf{y}$ (Cf. [3, Prop. 8]). Using the bounds in the case of dimension 0, upper-bounds on the heights of the $T_{i,\mathbf{y}}$ and $N_{i,\mathbf{y}}$ can be deduced, but in term of the *monic* Chow form $\widetilde{Ch_{\mathbf{y}}}$ of $V_{\mathbf{y}}$, that lies in $K[\mathbf{U}_0]$. However, interesting Chow forms of V lie in $\mathbb{Z}[\mathbf{U}_0, \dots, \mathbf{U}_m]$, and it is necessary to link both Chow forms (Cf. § 6 of [3]). A particularly nice case is when V verifies the following:

Assumption 3 The degree of the projection fiber is equal to the degree of the variety.

It is the case for the example of the figures of § 2.2. The circle is a degree 2 variety and in each fiber of its projection on the Y-axis, there are generically 2 points.

Then given a Chow form of V, $Ch_V \in \mathbb{Z}[\mathbf{U}_0, \dots, \mathbf{U}_m]$ if we perform the following specialization in Ch_V:

$$\begin{bmatrix} \mathbf{U}_0 \\ \mathbf{U}_1 \\ \vdots \\ \mathbf{U}_m \end{bmatrix} \leftarrow \left[\begin{array}{c|ccc|ccc} U_0 & 0 & \cdots & 0 & U_1 & \cdots & U_n \\ Y_1 & -1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ Y_m & 0 & \cdots & -1 & 0 & \cdots & 0 \end{array}\right],$$

the resulting polynomial that is in indeed in $\mathbb{Z}[\mathbf{Y}, \mathbf{U}]$, is a Chow form of V^*. Unfortunately, considering varieties verifying Assumption 2, that are the subject of this study, Assumption 3 is not automatically verified (Cf. Example following Prop. 2 in [3]). To circumvent this problem, a generic linear change of the coordinates $\mathbf{Y}$ is necessary (the full details can not be explained briefly, Cf § 5 in [3]).

This permits to deduce an estimates on $\widetilde{Ch_{\mathbf{y}}}$ in function of Ch_V, required to pursue the computations of the upper-bound on the height of $N_{i,\mathbf{y}}$ in function of the variety V.

5 One application and some remarks

Besides the understanding of the triangular representations of algebraic varieties, the bounds presented in this article find a natural application in the context of *modular methods.*

Probability estimates for modular computations Let us say that this consists here roughly in performing the computations modulo a prime p instead of over $\mathbb{Q}$, aiming at staying with reasonably small coefficients. For polynomial system solving with rational coefficients, large numbers is typically a strong bottleneck.

Of course, a prime p must guarantee *compatibility* between the reduction modulo p of the resulting polynomial system computed over $\mathbb{Q}$, and the resulting one computed modulo p. Such primes are called *compatible primes* in [8]. There are a lot of compatible primes, but the question is rather,

Are there a lot of *small* compatible primes ?

Without bounds like the ones written here, that give an idea of the size of the ouptut, no quantification of the choice of compatible primes is possible. It is convenient here to make a parallel with a classical problem in linear algebra: the inversion of a non-singular matrix. This operation typically increases the coefficients, and modular computations are routinely implemented. Then, the *Hadamard's inequality* give a quantification in the choice of compatible primes for the inversion operation. The bounds given here play the same role as does the Hadamard's inequality in linear algebra, but in polynomial systems.

Concluding remarks The bounds provided are the first one polynomial w.r.t. the degree and the height of the variety. The hypotheses required are quite strong, but they constitute a first step toward hopefully a whole generality. Nonetheless, using triangular decomposition permits to lever Assumption 1 up. Indeed, the *equiprojectable decomposition* [4] of V permits to reduce the general case of a 0-dimensional variety to the ones verifying Assumption 1. We mention that in 2 variables, similar results for the lexicographic Gröbner bases of 0-dimensional varieties that do not verify Asssumption 1 have been achieved [2].

How tight are the bounds ? We have no answer to this question. Still, we believe that the growth rate of the degree and the height in these bounds is tight.

All the results are based on the Lagrange interpolation allowed by the elimination property hold by lexicographic orders. Somehow, this property is hold also by the degree lexicographic monomial orders. It would be interesting, and quite challenging, to obtain upper-bounds on the coefficients of degre lexicographic Gröbner bases. They are indeed widely used in practice due to a better computational efficiency.

References

[1] M.-E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. In *Progress in Math.*, volume 143 of *Algorithms in Algebraic Geometry and Applications*, pages 1–15. Proceedings MEGA'94, Birkhäuser, 1996.

[2] X. Dahan. Size of coefficients of lexicographical Gröbner baes. In *ISSAC'09*, pages 117–126. ACM, 2009.

[3] X. Dahan, A. Kadri, and É. Schost. Bit-size estimates for triangular sets in positive dimension. `arXiv:1008.3459`.

[4] X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115. ACM, 2005.

[5] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, pages 103–110. ACM Press, 2004.

[6] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *J. of Complexity*, 17(2):154–211, 2001.

[7] T. Krick, L. M. Pardo, and M. Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke math. Journal*, 109:521–598, 2001.

[8] M. Noro and K. Yokoyama. A modular method to compute the rational univariate representation of zero-dimensional ideals. *J. Symb. Comput.*, 28(1-2):243–263, 1999.

[9] P. Philippon. Critères pour l'indépendance algébrique. *IHES Publ. math*, 64:5–52, 1986.

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

[11] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Appl. Algebra Eng. Commun. Comput.*, 9(5):433–461, 1999.