WORST POSSIBLE CONDITION NUMBER OF POLYNOMIAL SYSTEMS

GREGORIO MALAJOVICH

Abstract. A worst case bound for the condition number of a generic system of polynomial equations with integer coefficients is given. For fixed degree and number of equations, the condition number is (non-uniformly, generically) pseudo-polynomial in the input size.

1. Introduction

The Bézout problem may be stated as follows : given a *generic* system of n homogeneous polynomial equations of degree $d = (d_1, \ldots, d_n)$ in $n+1$ complex variables, *find* all the roots in complex projective space.

To *find* a root means to exhibit a (proven) *approximate zero*, i.e., a point whose iterates by a suitable Newton operator will converge quadratically. See Smale [13] , and Shub and Smale [8] .

The complexity of solving the Bézout problem was bounded in terms of the Shub and Smale condition number μ (See Shub and Smale [8, 9, 10, 11, 12] . For the corresponding discrete theory, see Malajovich [5, 6]).

The condition number μ may be defined by :

$$\mu(f) = \max_{\zeta \neq 0, f(\zeta)=0} \mu(f,\zeta)$$

where :

$$\mu(f,\zeta) = \|f\|_{\mathrm{k}} \left\| Df(\zeta)^{-1}_{|\zeta^\perp} \operatorname{diag}\left(\|\zeta\|^{d_i - 1} \sqrt{d_i} \right) \right\|_2$$

Here, $\|.\|_{\mathrm{k}}$ is Kostlan's invariant norm $\|f\|_{\mathrm{k}}{}^2 = \sum \|f_i\|_{\mathrm{k}}{}^2$ where :

$$\|f_i\|_{\mathrm{k}}{}^2 = \sum_{|J|=d_i} |f_{iJ}|^2 \frac{J_0! \ldots J_n!}{d_i!}$$

Date: August 27, 1995.
1991 *Mathematics Subject Classification.* 65H10, 65H20, 68Q25.
Sponsored by CNPq (Brasil).
Typeset using $\mathcal{AMS}$- LaTeX.

This norm is known to be $U(n+1)$-invariant. The set of all f such that $\mu(f) = \infty$ is an algebraic variety Σ , called the *discriminant variety* .

As we deal with such kind of continuous problems, it makes no sense to speak of a worst case complexity (i.e. a worst case bound for μ). Instances of the problem may be arbitrarily ill-conditioned.

However, one may be concerned with the restriction of a continuous problem to a discrete input set. For instance, one may study the Bézout problem restricted to systems of integer or Gaussian integer coefficients.

Then one may speak on the classical (Turing, BSS over $\mathbb{Z}$) complexity of solving the restricted (discrete) problem. That complexity analysis may use techniques and results from the original (continuous) problem.

Once we fix $d = (d_1, \ldots, d_n)$, the number of coefficients of f is bounded by $\sum_i \begin{pmatrix} d_i + n - 1 \\ d_i \end{pmatrix}$; therefore, *input size* may be measured by the *height* of the coefficients of f .

Heights may be defined in many ways. For convenience, we will set :

$$\mathbf{H}(\mathbf{a} + \mathbf{bi}) = |a| + |b| \ , a, b \in \mathbb{Z}$$

although this is a not the number-theoretical definition.

Let $\mathcal{H}_d$ be the space of all the systems of homogeneous polynomials of degree $d = (d_1, \ldots d_n)$ in n variables, with complex coefficients. We shall prove :

Main Theorem . *Let d be fixed. There is a Zariski closed set $\Sigma \subseteq \mathcal{H}_d$, $\Sigma \neq \mathcal{H}_d$, and there are numbers $d(\Sigma')$ and $\mu(\Sigma')$ such that, for any $f \in \mathcal{H}_d$, $f \notin \Sigma'$, f with Gaussian integer coefficients,*

$$\mu(f) \leq \mu(\Sigma)\ \mathbf{H}(\mathbf{f})^{d(\Sigma)}$$

Furthermore,

$$d(\Sigma') \leq n \prod d_i \sum d_i$$

$$\mu(\Sigma') \leq \frac{\pi}{2} d(\Sigma') \left(3 \prod d_i \left(\frac{e}{\sqrt{2\pi}} \right)^{n-1} n^{\sum d_i - n + 2} \right)^{1 + d(\Sigma')}$$

In other words : once we fix d, the condition number $\mu(f)$ is pseudo-polynomial (See Garey-Johnson [3]) in the input size (for f not in Σ, of course).

Another restatement: for non-degenerate f, $\mu(f)$ is non-uniform pseudo-polynomial in the input size.

One can take the discriminant variety Σ instead of Σ' in the statement of the Main Theorem. This will decrease $d(\Sigma)$, but may possibly increase $\mu(\Sigma)$.

The main Theorem provides us with an *a priori* bound on the condition number (for μ not in Σ). This bound may be used to bound the number of steps and the machine precision necessary for a homotopy algorithm to succeed generically.

Also, it can be used to guarantee that certain $z \in \mathbb{C}^{n+1}$ is indeed an approximate zero of a non-degenerate f. One would use the bound on $\mu(f)$ to bound the Wilkinson condition number κ of $Df(z)_{|z^\perp}$. Standard linear system solvers are known to provide a result within error bounded by $O(\kappa\epsilon_m)$, where ϵ_m is the *machine epsilon*. (Recall d and n are fixed). Therefore, one may compute :

$$\beta(f,z) = \|Df(z)_{|z^\perp}{}^{-1} f(z)\|$$

within error $O(\kappa\epsilon_m)$. Therefore, computing β to within error δ costs $O(\log \mathbf{H}(\mathbf{f}) - \log\delta)$.

The invariant γ may be bounded as in [8] by $\mu\frac{\max d_i{}^{\frac{3}{2}}}{2}$, hence we may obtain a reasonably cheap bound for α.

For a more algorithmic explanation of the consequences this Theorem, see [5], chapter 5.

2. Outline of the proof

It was proven by Shub and Smale ([8]) that :

$$\mu(f,\zeta) = \frac{1}{d_k(f, \Sigma \cap V_\zeta)}$$

where V_ζ is the subspace of all $f \in \mathcal{H}_d$ such that $f(\zeta) = 0$, and Σ is the discriminant variety. The distance d_k is taken in Projective Space, i.e. :

$$d_k(f,g) = \min_{\lambda\in\mathbb{C}} \frac{\|f - \lambda g\|_{\mathrm{k}}}{\|f\|_{\mathrm{k}}} \tag{1}$$

Equation (1) implies :

$$\mu(f) \leq \frac{1}{d_k(f,\Sigma)}$$

where we removed the restriction of the distance to subspace V_ζ . If Σ' is a Zariski closed set containing Σ, then :

$$\mu(f) \leq \frac{1}{d_k(f,\Sigma')}$$

Assuming that $f \notin \Sigma$, we want to obtain a bound for $d(f, \Sigma)$. As $\mathbf{H}(\mathbf{f})$ is bounded, such a bound $\min_{f \notin \Sigma, \mathbf{H}(\mathbf{f}) \leq H} d(f, \Sigma)$ should certainly exist.

The discriminant variety Σ is the set of all f such that there is $\zeta \neq 0$ with $f(\zeta) = 0$ and $Df(\zeta)$ not surjective. (recall that $Df(\zeta)$ is a $(n+1) \times n$ matrix). The root ζ can be taken to have norm 1, or to belong to $\mathbb{P}^n$.

An easy way to produce a proper Σ' containing Σ is to consider a chart A_i of $\mathbb{P}^n$ given by :

$$A_i : (x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \mapsto (x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$$

Then Σ' contains Σ where Σ' is the zero-set of $p = \operatorname{discr}(f \circ A_i) = R(f_1 \circ A_i, \ldots, f_n \circ A_i, \det D(f \circ A_i)$, where R is the resultant (See Salmon [7], Macaulay [4] or Van der Waerden [14]) . In section 3, we will show that :

Proposition 1. *The polynomial p defined above is a multi-homogeneous polynomial of degree $r_1, \ldots, r_n$ in sets of m_1 variables f_1, ..., m_n variables f_n, with integer coefficients, where $m_i = \begin{pmatrix} d_i + n - 1 \\ d_i \end{pmatrix}$ and $r_i = (\prod d_j)(1 + \frac{\sum d_j - n}{d_i})$. The sum of the absolute values of the coefficients of p is bounded above by :*

$$\mathbf{B}(\mathbf{p}) \leq \left(3 \prod d_i \left(\frac{e}{\sqrt{2\pi}} \right)^{n-1} n^{\sum d_i - n + \frac{3}{2}} \, e^{\frac{1}{12}} \right)^{\sum r_i}$$

We may lower each of the numbers r_i by choosing the discriminant variety instead of Σ'. The author does not know how to provide a reasonable bound for $\mu(\Sigma)$.

In section 4, we will prove the :

Theorem 1. *Let p be a multi-homogeneous polynomial of degree $r_1, \ldots, r_n$ in sets of variables $f_1 \in \mathbb{C}^{m_1}$, ..., $f_n \in \mathbb{C}^{m_n}$, with integer coefficients. Assume also that groups of variables f_i range over Gaussian integers. Then either $p(f) = 0$, or :*

$$d_2(f, Z(p)) \geq \frac{1}{\frac{\pi}{2} \max \sqrt{m_i} \sum r_i \mathbf{B}(\mathbf{p})} \left(\frac{1}{\mathbf{H}(\mathbf{f})} \right)^{\sum r_i}$$

where $Z(p)$ is the zero-set of p and d_2 is the projective 2-distance.

Proof of the Main Theorem : We set $d(\Sigma) = \sum r_i$. In section 5, we shall prove the Lemma :

Lemma 1.

$$\sum r_i \leq n \prod d_i \sum d_i$$

We apply Theorem 1 to the polynomial $p = \mathrm{discr}(f)$ defined above. We conclude that if f has Gaussian integer coefficients then either $\mathrm{discr} f = 0$, or :

$$d_2(d, \Sigma_i) \geq \frac{1}{\frac{\pi}{2} \max \sqrt{m_i} d(\Sigma) \left(3 \prod d_i (\frac{e}{\sqrt{2\pi}})^{n-1} n^{\sum d_i - n + \frac{3}{2}} e^{\frac{1}{12}}\right)^{d(\Sigma)}} \left(\frac{1}{\mathbf{H}(\mathbf{f})}\right)^{d(\Sigma)}$$

Furthermore, we will need from section 5 the :

Lemma 2.

$$d_k(f, g) \leq \sqrt{n^{\max d_i} (\frac{e}{\sqrt{2\pi}})^{n-1} e^{1/12} \sqrt{n}}\ d_2(f, g)$$

Therefore, under the conditions of the Main Theorem, either $f \in \Sigma_i$ (some i), or for all i :

$$d_k(d, \Sigma_i) \geq \frac{1}{\frac{\pi}{2} \max \sqrt{m_i} d(\Sigma) \left(3 \prod d_i (\frac{e}{\sqrt{2\pi}})^{n-1} n^{\sum d_i - n + \frac{3}{2}} e^{\frac{1}{12}}\right)^{1+d(\Sigma)}} \left(\frac{1}{\mathbf{H}(\mathbf{f})}\right)^{d(\Sigma)}$$

We may also bound :

$$\sqrt{m_i} = \sqrt{\begin{pmatrix} d_i + n - 1 \\ d_i \end{pmatrix}} \leq \sqrt{(n-1)^{d_i + n - 1}} \leq \sqrt{n}^{d(\Sigma)}$$

So we set, as in Main Theorem :

$$\mu(\Sigma) = \frac{\pi}{2} d(\Sigma) \left(3 \prod d_i \left(\frac{e}{\sqrt{2\pi}}\right)^{n-1} n^{\sum d_i - n + 2}\right)^{1+d(\Sigma)}$$

With this notation, either $f \in \Sigma_i$ for some i, or :

$$d(f, \Sigma) \geq \min d(f, \Sigma_i) \geq \mu(\Sigma)^{-1} \left(\frac{1}{\mathbf{H}(\mathbf{f})}\right)^{d(\Sigma)}$$

Therefore,

$$\mu(f) \leq \frac{1}{d_k(f, \Sigma)} \leq \mu(\Sigma)\ \mathbf{H}(\mathbf{f})^{d(\Sigma)}$$

concluding the proof of the Main Theorem.

The following Lemma is proved in Section 5 , and used two times in this paper. Therefore we state it here :

Lemma 3. *Let $d \geq 1$ be fixed, and let $J = J_1 \dots J_n$.*

$$\max_{|J|=d} \binom{d}{J} \leq n^d \left(\frac{e}{\sqrt{2\pi}}\right)^{n-1} \sqrt{n} e^{\frac{1}{12}}$$

3. Proof of Proposition 1

The purpose of this section is to prove Proposition 1 . The first part of the proposition is easy, and will be proved now. The second part will require some intermediate results, and therefore it will be postponed to the end of this section.

The number m_i of f_{iJ} is clearly $\binom{d_i + n - 1}{d_i}$, that is, the number of possible monomials of degree d_i in n variables.

3.1. **Degree of the discriminant.** Let $p = \operatorname{discr}(f) = R(f_1, \dots, f_n, \det Df)$, where the f_i are non-homogeneous polynomials of degree d_i in variables $x_1, \dots, x_n$. The notation $R(.)$ stands for the resultant of a system of polynomials.

As it is well-known, the resultant $R(f_1, \dots, f_n, g)$ is a multi-homogeneous polynomial in each set of variables f_i or g , with integer coefficients.

It's degree in each set of variables is given by :

$$\begin{aligned}
\deg_g R(f_1, \dots, f_n, g) &= \prod d_i \\
\deg_{f_i} R(f_1, \dots, f_n, g) &= (\deg g) \prod_{j \neq i} d_j
\end{aligned}$$

Now, if we set $g = \det Df$, then $\deg_x g = \sum d_j - n$. Each coefficient of g is a multi-homogeneous monomial of degree 1 in each set of variables f_i or g . Therefore,

$$\begin{aligned}
\deg_{f_i} p &= \deg_{f_i} R(f_1, \dots, f_n, g) + \deg_g R(f_1, \dots, f_n, g) \deg_{f_i} g \\
&= \prod d_j + \left(\prod_{j \neq i} d_j\right) \left(\sum d_j - n\right) \\
&= \prod d_j \left(1 + \frac{\sum d_j - n}{d_i}\right) \\
&= r_i
\end{aligned}$$

So the degree of p in the set of variables f_i is precisely r_i.

3.2. **Alternative definitions of height.** The second part of proposition 1 requires some alternative definitions of Height. Also, some properties of those new heights will be discussed.

We shall work in a more general framework. In this paper, we shall assume that some *height* $\mathbf{H}(.)$ is defined in a ring R. The main examples are the integers and the Gaussian integers. We require the following axioms to be true :

$$\mathbf{H}(\mathbf{1}) = \mathbf{H}(-\mathbf{1}) = \mathbf{H}(\mathbf{i}) = \mathbf{H}(-\mathbf{i}) = 1$$
$$\mathbf{H}(\mathbf{a}+\mathbf{b}) \leq \mathbf{H}(\mathbf{a}) + \mathbf{H}(\mathbf{b})$$
$$\mathbf{H}(\mathbf{ab}) \leq \mathbf{H}(\mathbf{a})\mathbf{H}(\mathbf{b})$$

Those are verified by our previous definition of $\mathbf{H}(.)$ as $\mathbf{H}(\mathbf{a}+\mathbf{bi}) = |a| + |b|$.

Let K be the field of fractions of R, and let $L = K[f_1, \ldots, f_N]$ where the f_i are indeterminates (transcendental) over K. If a is an integer in L, a can be written in the form $a = \sum a_I f^I$, where $a_I \in R$ and I are indices. We define a height $\mathbf{B}(.)$ on the ring of integers of L :

$$\mathbf{B}\left(\sum \mathbf{a_I f^I}\right) = \sum \mathbf{H}(\mathbf{a_I})$$

The following properties of $\mathbf{B}(.)$ are obvious :

$$\mathbf{B}(\mathbf{1}) = \mathbf{B}(-\mathbf{1}) = \mathbf{B}(\mathbf{i}) = \mathbf{B}(-\mathbf{i}) = 1$$
$$\mathbf{B}(\mathbf{g}+\mathbf{h}) \leq \mathbf{B}(\mathbf{g}) + \mathbf{B}(\mathbf{h})$$
$$\mathbf{B}(\mathbf{gh}) \leq \mathbf{B}(\mathbf{g})\mathbf{B}(\mathbf{h})$$

We also want to extend this definition to monic integral polynomials in $L[t]$ ($t \in R$), but in a different way. We define :

$$\mathbf{C}\left(\mathbf{t^d} + \mathbf{p_{d-1}t^{d-1}} + \cdots + \mathbf{p_0}\right) = \max\left(\mathbf{B}(\mathbf{p_i})^{\frac{1}{d-i}}\right)$$

This is not properly a height (since it make no sense to add monic polynomials).

The following facts were proved by Canny [2] for the particular case $L = K = \mathbb{Q}$.

Lemma 4. *Let p, q integral polynomials in L and let M be a $n \times n$ matrix with integral entries in L.*

$$\mathbf{C}(\mathbf{pq}) \leq \mathbf{C}(\mathbf{p}) + \mathbf{C}(\mathbf{q})$$
$$\mathbf{C}(\mathbf{p/q}) \leq \mathbf{C}(\mathbf{p}) + 2\mathbf{C}(\mathbf{q})$$
$$\mathbf{C}(\mathbf{detM} - \mathbf{tI}) \leq n \max \mathbf{B}(\mathbf{M_{ij}})$$

Proof of lemma 4 :

Part 1 : We write :

$$p(t) = t^m + p_{m-1}t^{m-1} + \cdots + p_0$$
$$q(t) = t^n + q_{n-1}t^{n-1} + \cdots + q_0$$
$$r(t) = p(t)q(t) = t^{m+n} + r_{m+n-1}t^{m+n-1} + \cdots + r_0$$

where :

$$r_i = \sum_{\substack{0\leq j\leq m\\ 0\leq i-j\leq n}} p_j q_{i-j}$$

By definition,

$$\mathbf{C}(\mathbf{pq}) = \max \mathbf{B}\left(\sum_{\substack{0\leq j\leq m\\ 0\leq i-j\leq n}} \mathbf{p_j q_{i-j}^{\frac{1}{n+m-i}}} \right)$$

$$\mathbf{C}(\mathbf{pq}) \leq \max \left(\sum_{\substack{0\leq j\leq m\\ 0\leq i-j\leq n}} \mathbf{B}(\mathbf{p_j})\mathbf{B}(\mathbf{q_{i-j}}) \right)^{\frac{1}{n+m-i}}$$

So there is i such that :

$$\mathbf{C}(\mathbf{pq})^{n+m-i} \leq \sum_{\substack{0\leq j\leq m\\ 0\leq i-j\leq n}} \mathbf{C}(\mathbf{p})^{m-j}\mathbf{C}(\mathbf{q})^{n-i+j}$$

On the other hand,

$$(\mathbf{C}(\mathbf{p}) + \mathbf{C}(\mathbf{q}))^{n+m-i} = \sum_{i-n\leq j\leq m} \binom{n+m-i}{m-j} \mathbf{C}(\mathbf{p})^{m-j}\mathbf{C}(\mathbf{q})^{n-i+j}$$

Comparing term by term,

$$\mathbf{C}(\mathbf{pq})^{n+m-i} \leq (\mathbf{C}(\mathbf{p}) + \mathbf{C}(\mathbf{q}))^{n+m-i}$$

Hence

$$\mathbf{C}(\mathbf{pq}) \leq \mathbf{C}(\mathbf{p}) + \mathbf{C}(\mathbf{q})$$

Part 2 :

$$p(t) = t^m + p_{m-1}t^{m-1} + \cdots + p_0$$
$$q(t) = t^n + q_{n-1}t^{n-1} + \cdots + q_0$$
$$r(t) = p(t)/q(t) = t^{m-n} + r_{m-n-1}t^{m-n-1} + \cdots + r_0$$

Since p and q are monic, the quotient $r(t)$ can be computed by the following recurrence :

$$\begin{aligned} r_{m-n} &= 1 \\ r_{m-n-j-1} &= p_{m-j-1} - \sum_{0\leq i\leq j} r_{m-n-i} q_{n+i-j-1} \end{aligned}$$

We have :

$$\begin{aligned} \mathbf{B}\left(\mathbf{r_{m-n-j-1}}\right) &\leq \mathbf{B}\left(\mathbf{p_{m-j-1}}\right) + \sum_{0\leq i\leq j} \mathbf{B}\left(\mathbf{r_{m-n-i}}\right)\mathbf{B}\left(\mathbf{q_{n+i-j-1}}\right) \\ \mathbf{B}\left(\mathbf{r_{m-n-j-1}}\right) &\leq \mathbf{C}\left(\mathbf{p}\right)^{j+1} + \sum_{0\leq i\leq j} \mathbf{B}\left(\mathbf{r_{m-n-i}}\right)\mathbf{C}\left(\mathbf{q}\right)^{j+1-i} \end{aligned}$$

We proceed by induction on i. Assume that $\mathbf{B}\left(\mathbf{r_{m-n-j}}\right) \leq (\mathbf{C}\left(\mathbf{p}\right) + 2\mathbf{C}\left(\mathbf{q}\right))^j$ for all $j \leq i$. This is trivially true for $i = 0$. By induction,

$$\begin{aligned} \mathbf{B}\left(\mathbf{r_{m-n-j-1}}\right) &\leq \mathbf{C}\left(\mathbf{p}\right)^{j+1} + \sum_{0\leq i\leq j} \left(\mathbf{C}\left(\mathbf{p}\right) + 2\mathbf{C}\left(\mathbf{q}\right)\right)^i \mathbf{C}\left(\mathbf{q}\right)^{j+1-i} \\ &\leq \mathbf{C}\left(\mathbf{p}\right)^{j+1} + \mathbf{C}\left(\mathbf{q}\right) \sum_{0\leq i\leq j} \left(\mathbf{C}\left(\mathbf{p}\right) + 2\mathbf{C}\left(\mathbf{q}\right)\right)^i \mathbf{C}\left(\mathbf{q}\right)^{j-i} \\ &\leq \mathbf{C}\left(\mathbf{p}\right)^{j+1} + \mathbf{C}\left(\mathbf{q}\right) \sum_{0\leq i\leq j} 2^{i-j} \left(\mathbf{C}\left(\mathbf{p}\right) + 2\mathbf{C}\left(\mathbf{q}\right)\right)^j \\ &\leq \mathbf{C}\left(\mathbf{p}\right)^{j+1} + 2\mathbf{C}\left(\mathbf{q}\right)\left(\mathbf{C}\left(\mathbf{p}\right) + 2\mathbf{C}\left(\mathbf{q}\right)\right)^j \\ &\leq \mathbf{C}\left(\mathbf{p}\right)\left(\mathbf{C}\left(\mathbf{p}\right) + 2\mathbf{C}\left(\mathbf{q}\right)\right)^j + 2\mathbf{C}\left(\mathbf{q}\right)\left(\mathbf{C}\left(\mathbf{p}\right) + 2\mathbf{C}\left(\mathbf{q}\right)\right)^j \\ &\leq \left(\mathbf{C}\left(\mathbf{p}\right) + 2\mathbf{C}\left(\mathbf{q}\right)\right)^{j+1} \end{aligned}$$

Thus,

$$\mathbf{C}\left(\mathbf{r}\right) \leq \mathbf{C}\left(\mathbf{p}\right) + 2\mathbf{C}\left(\mathbf{q}\right)$$

Part 3 :

$$\det(M - tI) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$$

Coefficient a_i is the sum of n^{n-i} products of at most $n - i$ entries of height $\mathbf{B}\left(.\right)$ less than $\mathbf{B}\left(\mathbf{M}\right)$, so we have : $|a_i| \leq (n\mathbf{B}\left(\mathbf{M}\right))^{n-i}$.

$$\mathbf{C}\left(\det(\mathbf{M} - \mathbf{tI})\right) \leq n\mathbf{B}\left(\mathbf{M}\right)$$

Lemma 4 is now proved.

3.3. **Height of the determinant.** If $g = \sum g_J x^J \in L[x]$, we write $\mathbf{B}(\mathbf{g}) = \max_J \mathbf{B}(\mathbf{g_J})$.

Lemma 5. *Let $g = \det Df(x) \in L[x]$. Then :*

$$\mathbf{B}(\mathbf{g}) \leq \prod d_i \left(\frac{e}{\sqrt{2\pi}}\right)^{n-1} n^{\sum d_i - n + \frac{1}{2}} e^{\frac{1}{12}}$$

Proof : If we consider g as an element of $R[f,x]$, then we may bound : $\mathbf{H}(\mathbf{m_I}) \leq \prod d_i$, where m_I is the coefficient of a monomial of g .

Indeed, each monomial : $m_I f_{1,I_1} f_{2,I_2} \dots f_{n,I_n} x^{\sum I_j - \sum e_j}$ can be written as :

$$\det \begin{pmatrix} f_{1,I_1}\frac{\partial x^{I_1}}{\partial x_1} & \dots & f_{1,I_1}\frac{\partial x^{I_1}}{\partial x_n} \\ \vdots & & \vdots \\ f_{n,I_n}\frac{\partial x^{I_n}}{\partial x_1} & \dots & f_{n,I_n}\frac{\partial x^{I_n}}{\partial x_n} \end{pmatrix} = \det \begin{pmatrix} I_{1,1} & \dots & I_{1,n} \\ \vdots & & \vdots \\ I_{n,1} & \dots & I_{n,n} \end{pmatrix} f_{1,I_1} f_{2,I_2} \dots f_{n,I_n} x^{\sum I_j - \sum e_j}$$

Therefore, we may write :

$$m_I = \det \begin{pmatrix} I_{1,1} & \dots & I_{1,n} \\ \vdots & & \vdots \\ I_{n,1} & \dots & I_{n,n} \end{pmatrix}$$

Each line of this matrix has 2-norm bounded above by d_i. Therefore, $m_I \leq \prod d_i$. Set :

$$\rho = \max_{|J| = \sum d_i - n} \#\{I, |I_j| = d_j, \sum I_j - \sum e_j = J\}$$

Now we have : $\mathbf{B}(\mathbf{g}) \leq \rho \prod d_i$. It remains to bound ρ. Clearly,

$$\rho \leq \begin{pmatrix} \sum d_j - n \\ d_1 - 1 \dots d_n - 1 \end{pmatrix} = \frac{\sum d_i - n!}{d_1 - 1! \dots d_n - 1!}$$

Indeed, this is the number of arrangements of $\sum d_i - n$ different variables into n sets of size $d_i - 1$. This seems to the author a rather pessimistic bound, and may be improved.

We may now apply Lemma 3 :

$$\rho \leq n^{\sum d_i - n} \left(\frac{e}{\sqrt{2\pi}}\right)^{n-1} \sqrt{n} e^{\frac{1}{12}}$$

Proving Lemma 5 .

3.4. **Macaulay's formula for the resultant.** Let $\mathcal{M}$ be the vector space generated by all monomials of degree $\mathcal{D} = \sum \tilde{d}_i - n$ in variables $x_1, \ldots, x_n$.

To each system of $n+1$ homogeneous polynomials of degree $\tilde{d}_1, \ldots, \tilde{d}_{n+1}$, we associate a matrix $A(f)$, that corresponds to the operator :

$$g \mapsto \sum g_i f_i$$

where g_i is a polynomial of degree $\mathcal{D} - \tilde{d}_i$. This matrix is defined as follows :

Let x^m be a monomial of degree $\mathcal{D}$. Monomial x^m is said to be unreduced in x_i if and only if $m_i \geq \tilde{d}_i$. Obviously, x^m is unreduced in at least one of the variables $x_1, \ldots, x_n$. Let x_l be the first variable x^m is unreduced in :

Matrix $A(f)$ maps x^m into $\frac{x^m}{{x_l}^{d_l}} f_l$.

Matrix $A(f)$ is square. It is easy to see that if the f_i have a non-zero common root, then $\det A(f) = 0$. Indeed, let $\tilde{x}$ be that common root, and let $\tilde{X} \in \mathcal{M}$ be the vector of all $\tilde{x}^m$. For any system g,

$$gA(f)\tilde{X} = \sum g_i(\tilde{x}) f_i(\tilde{x}) = 0$$

Therefore, $A(f)\tilde{X} = 0$, hence $A(f)$ is not surjective.

The converse is not true. The polynomial $\det A(f)$ may assume different values, depending on the ordering of variables x_i . It was proven by Macaulay [4] that :

$$R(f_1, \ldots, f_{n+1}) = \gcd \det A(f)$$

where the gcd is taken over all possible orderings of the x_i's. Furthermore, let $B(f)$ be the submatrix of $A(x)$ corresponding to the subspace of monomials unreduced in more than one variable.

Theorem 2 (Macaulay)**.**

$$R(f_1, \ldots, f_{n+1}) = \frac{\det A(f)}{\det B(f)}$$

For a proof, see Macaulay [4] .

3.5. **End of the proof of Proposition 1.** We proved (Lemma 5) that the height $\mathbf{B}(\det \mathbf{Df}) \in L[x]$ is bounded by :

$$\mathbf{B}(\det \mathbf{Df}) \leq \prod d_i \left(\frac{e}{\sqrt{2\pi}}\right)^{n-1} n^{\sum d_i - n + \frac{1}{2}} e^{\frac{1}{12}}$$

Hence, the height of matrices $A(f)$ and $B(f)$ defined above verifies :

$$\mathbf{B}\left(\mathbf{A}(\mathbf{f})\right) \leq \prod d_i \left(\frac{e}{\sqrt{2\pi}}\right)^{n-1} n^{\sum d_i - n + \frac{1}{2}} e^{\frac{1}{12}}$$

$$\mathbf{B}\left(\mathbf{B}(\mathbf{f})\right) \leq \prod d_i \left(\frac{e}{\sqrt{2\pi}}\right)^{n-1} n^{\sum d_i - n + \frac{1}{2}} e^{\frac{1}{12}}$$

Let I denote the identity. According to Lemma 4 :

$$\begin{aligned}
\mathbf{B}\left(\mathrm{discr}(\mathbf{f})\right) &\leq \left(\mathbf{C}\left(\det \mathbf{A} - \mathbf{t}\mathbf{I}\right) + 2\mathbf{C}\left(\det \mathbf{B} - \mathbf{t}\mathbf{I}\right)\right)^{\sum r_i} \\
&\leq \left(n\mathbf{B}\left(\mathbf{A}(\mathbf{f})\right) + 2n\mathbf{B}\left(\mathbf{B}(\mathbf{f})\right)\right)^{\sum r_i} \\
&\leq \left(3n\mathbf{B}\left(\det \mathbf{Df}\right)\right)^{\sum r_i} \\
&\leq \left(3n \prod d_i \left(\frac{e}{\sqrt{2\pi}}\right)^{n-1} n^{\sum d_i - n + \frac{1}{2}} e^{\frac{1}{12}}\right)^{\sum r_i}
\end{aligned}$$

4. Proof of Theorem 1

We shall construct an embedding of $\mathcal{H}_d$ into $\mathbb{C}^N$, N large enough, so that the image of Σ be the intersection of a hyperplane with the image of $\mathcal{H}_d$.

4.1. Embedding of $\mathcal{H}_d$ into $\mathbb{C}^N$.

More precisely : Let

$$V_{r_i} : \mathbb{C}^{m_i} \to \mathbb{C}^{M_i}$$

where $M_i = \begin{pmatrix} m_i + r_i - 1 \\ r_i \end{pmatrix}$, be the r_i-uple embedding. Let

$$S_n : \mathbb{C}^{M_1} \times \cdots \times \mathbb{C}^{M_n} \to \mathbb{C}^N \ , \ N = \prod M_i$$

be the Segre embedding. Define :

$$\begin{array}{rccl} E: & \mathcal{H}_d & \to & \mathbb{C}^N \\ & f & \mapsto & S_n(V_{r_1}(f_1), \ldots, V_{r_n}(f_n)) \end{array}$$

Embedding E maps $\mathcal{H}_d$ into the space of all monomials that may appear in multivariate homogeneous polynomial $p(f_1, \ldots, f_n)$.

Therefore, if we define the push-forward E_*p of p as the linear form whose coordinates are the monomials of p, we have the relation :

$$p(f) = (E_*p)(E(f))$$

Hence $\Sigma = p^\perp \cap E(\mathcal{H}_d)$. (We associated $\mathbb{C}^n$ to its dual, and p to a vector. Recall that p has integer – hence real – coefficients).

4.2. **Linear case.**

Lemma 6. *Let $\Pi = p^{\perp}$ be a hyperplane in $\mathbb{C}^N$, where p has integer coordinates. Let $y \in \mathbb{C}^N$ have Gaussian integer coordinates. Then either $y \in \Pi$, or :*

$$d_2(y, \Pi) \geq \frac{1}{\mathbf{B}(\mathbf{p})\mathbf{H}(\mathbf{y})}$$

Proof : The orthogonal projection of y in Π is given by :

$$y - \frac{pp^{\mathrm{t}}}{\|p\|_2{}^2} y$$

so the projective distance to Π is :

$$d_2(y, \Pi) = \frac{\|p\|_2}{\|p\|_2{}^2 \|y\|_2} |p^{\mathrm{t}} y|$$

If $p \notin \Pi$, then $p^{\mathrm{t}} y \neq 0$, so $|p^{\mathrm{t}} y| \geq 1$ and :

$$d_2(y, \Pi) \geq \frac{1}{\|p\|_2 \|y\|_2} \geq \frac{1}{\mathbf{B}(\mathbf{p})\mathbf{H}(\mathbf{y})}$$

Lemma 6 implies, for $f \notin \Sigma$, that :

$$d_2(E(f), E(\Sigma)) \geq \frac{1}{\mathbf{B}(\mathbf{p})\mathbf{H}(\mathbf{E}(\mathbf{f}))} \geq \frac{1}{\mathbf{B}(\mathbf{p})\mathbf{H}(\mathbf{f})^{\sum r_i}}$$

The distance $d_2(f, \Sigma)$ can be bounded once we know a bound for the Lipschitz constant of E :

Lemma 7.

$$d_2(E(f), E(g)) \leq \lambda d_2(f, g)$$

where one can take $\lambda = \frac{\pi}{2} \sum r_i \max \sqrt{m_i}$

Lemma 7 will be proved in the next three subsections.

4.3. **The r-uple embedding.** Let :

$$\begin{array}{rccll} V_r : & \mathbb{C}^m & \to & \mathbb{C}^M & , \ M = \left(\begin{array}{c} m+r-1 \\ r \end{array} \right) \\ & x & \mapsto & (\ldots, x^J, \ldots)^{\mathrm{t}} & , |J| = r \end{array}$$

be the r-uple embedding; then :

Lemma 8.

$$\frac{\|DV_r(x)\|_\infty}{\|V_r(x)\|_2} \leq r \frac{1}{\|x\|_2}$$

and therefore :

$$\frac{\|DV_r(x)\|_2}{\|V_r(x)\|_2} \leq r\sqrt{m}\frac{1}{\|x\|_2}$$

Indeed, assume without loss of generality that $x_1 \geq x_2 \geq \cdots \geq x_m$. Then :

$$V_r(x) = \left({x_1}^r, {x_1}^{r-1}x_2, \ldots {x_1}^{r-1}x_m, {x_1}^{r-2}{x_2}^2, \ldots, {x_m}^r\right)^{\mathrm{t}}$$

Therefore,

$$\|V_r(x)\|_2 \geq |x_1|^{r-1}\|x\|_2 \tag{2}$$

On the other hand, for all monomials x^J,

$$\left|\frac{\partial x^J}{\partial x_i}\right| \leq J_i|x_1|^{r-1}$$

Hence,

$$\|DV_r(x)\|_\infty = \max\sum_i \left|\frac{\partial x^J}{\partial x_i}\right| \leq r|x_1|^{r-1} \tag{3}$$

Dividing inequality (3) by inequality (2) we prove Lemma 8.

4.4. **The Segre embedding.** Let $N = \prod M_i$ and let :

$$\begin{array}{rccl} S_n: & \mathbb{C}^{M_1} \times \mathbb{C}^{M_2} \times \cdots \times \mathbb{C}^{M_n} & \to & \mathbb{C}^N \\ & (y_1, \ldots, y_n) & \mapsto & (\ldots, y_{1,k_1}y_{2,k_2}\ldots y_{n,k_n}, \ldots)^{\mathrm{t}} \end{array}$$

be the Segre embedding. Then :

Lemma 9.

$$\frac{\left\|\frac{\partial S_n(y)}{\partial y_j}\right\|_2}{\|S(y)\|_2} \leq \frac{1}{\|y_j\|_2}$$

Indeed,

$$S_n(y) = \left(S^{\mathrm{t}}_{n-1}(y_1, \ldots, y_{n-1})y_{n,1}, \ldots, S^{\mathrm{t}}_{n-1}(y_1, \ldots, y_{n-1})y_{n,M_n}\right)^{\mathrm{t}}$$

Hence, $\|S_n(y)\|_2{}^2 = \|S_{n-1}(y_1, y_{n-1})\|_2{}^2\|y_n\|_2{}^2$. Therefore, by induction,

$$\|S_n(y)\|_2 = \|y_1\|_2\|y_2\|_2 \ldots \|y_n\|_2 \tag{4}$$

The norm of the derivative may be bounded as follows :

$$\frac{\partial S_n}{\partial y_n} = \begin{pmatrix} S_{n-1}(y_1,\dots,y_{n-1}) & & & \\ & S_{n-1}(y_1,\dots,y_{n-1}) & & \\ & & \ddots & \\ & & & S_{n-1}(y_1,\dots,y_{n-1}) \end{pmatrix}$$

Thus,

$$\left\| \frac{\partial S_n}{\partial y_n} \right\|_2 \leq \|S_{n-1}(y_1,\dots,y_{n-1})\|_2 = \|y_1\|_2 \|y_2\|_2 \dots \|y_{n-1}\|_2 \qquad (5)$$

Dividing equation (5) by equation (4), one proves Lemma 9 for the case $j = n$. Reordering variables, the Lemma is true for any j.

4.5. **End of the proof of Theorem 1.** Let d_{arc} be the arc-length 2-distance in Projective Space (or in the unit 2-sphere). Lemmas 8 and 9 imply that :

$$d_{\text{arc}}(E(f), E(g)) \leq \sum r_i \sqrt{m_i} d_{\text{arc}}(f,g) \leq \max \sqrt{m_i} \sum_{r_i} d_{\text{arc}}(f,g)$$

Using inequality $d_2(f,g) \leq d_{\text{arc}}(f,g) \leq \frac{\pi}{2} d_2(f,g)$, we get :

$$d_2(E(f), E(g)) \leq \frac{\pi}{2} \max m_i \sum_{r_i} d_2(f,g)$$

Proving Lemma 7 . Theorem 1 now follows directly from Lemma 6.

5. Proof of Lemmas

5.1. **Proof of Lemma 1.** Recall that $r_i = \prod d_j \left(1 + \frac{\sum d_j - n}{d_i}\right)$. Therefore :

$$\sum r_i \leq \prod d_j \left(n + \sum d_j \sum \frac{1}{d_j} - n \sum \frac{1}{d_j} \right)$$

If $\sum \frac{1}{d_j} \geq 1$, then $\sum r_i \leq \prod d_j \sum d_j \sum \frac{1}{d_j} \leq n \prod d_j \sum d_j$

On the other hand, if $\sum \frac{1}{d_j} < 1$, then $\sum r_i \leq \prod d_j (n + \sum d_j) < n \prod d_j \sum d_j$.

This proves lemma 1

5.2. **Proof of Lemma 2.** By construction,

$$\frac{\|h\|_2}{\sqrt{\max_{i,|J|=d_i} \begin{pmatrix} d_i \\ J \end{pmatrix}}} \leq \|h\|_{\text{k}} \leq \|h\|_2$$

Therefore, as we switch to projective space,

$$d_k(f,g) \leq \sqrt{\max_{i,|J|=d_i} \begin{pmatrix} d_i \\ J \end{pmatrix}} d_2(f,g)$$

Inserting Lemma 3, we get :

$$d_k(f,g) \leq \sqrt{n^{\max d_i} \left(\frac{e}{\sqrt{2\pi}}\right)^{n-1} e^{\frac{1}{12}} \sqrt{n} \begin{pmatrix} d_i \\ J \end{pmatrix}} d_2(f,g)$$

As in Lemma 2

5.3. **Proof of Lemma 3.**

$$\max_{|J|=d} \begin{pmatrix} d \\ J \end{pmatrix} = \max_{|J|=d} \frac{\Gamma(d+1)}{\prod \Gamma(J_i+1)} \leq \frac{\Gamma(d+1)}{\Gamma(\frac{d}{n}+1)^n}$$

The following bound is a consequence of Stirling's formula (Ahlfors, [1], chapter 5, section 2.5, exercise 2, page 206) :

$$\sqrt{2\pi} z^{z-\frac{1}{2}} e^{-z} \leq \Gamma(z) \leq \sqrt{2\pi} z^{z-\frac{1}{2}} e^{-z} e^{\frac{1}{12z}}$$

Using this bound, we obtain :

$$\begin{aligned}
\max_{|J|=d} \begin{pmatrix} d \\ J \end{pmatrix} &\leq \sqrt{2\pi}^{1-n} \frac{(d+1)^{d+\frac{1}{2}}}{\left((\frac{d}{n}+1)^{\frac{d}{n}}+\frac{1}{2}\right)^n} \frac{e^{-d+\frac{1}{2}}}{\left(e^{-\frac{d}{n}-1}\right)^n} e^{\frac{1}{12(d+1)}} \\
&\leq \sqrt{2\pi}^{1-n} \left(\frac{d+1}{\frac{d}{n}+1}\right)^n \left(\frac{d}{n}+1\right)^{-\frac{n-1}{2}} e^{n-1} e^{\frac{1}{12(d+1)}} \\
&\leq n^d \left(\frac{e}{\sqrt{2\pi}\sqrt{\frac{d}{n}+1}}\right)^{n-1} \sqrt{n} e^{\frac{1}{12}} \\
&\leq n^d \left(\frac{e}{\sqrt{2\pi}}\right)^{n-1} \sqrt{n} e^{\frac{1}{12}}
\end{aligned}$$

As in Lemma 3

References

[1] Lars V. Ahlfors *Complex Analysis*, Third edition. McGraw-Hill, Auckland, 1979.

[2] John Canny, *The complexity of robot motion planning*, MIT Press, Cambridge, Mass., 1988.

[3] M. R. Garey and D. Johnson *Computers and Intractability, a guide to the theory of NP-completeness*, Freeman, San Francisco, 1979.

[4] F. S. Macaulay, Some formulæ in elimination, *Proceedings of the London Mathematical Society*, Vol XXXV, 1903.

[5] Gregorio Malajovich *On the complexity of path-following Newton algorithms for solving systems of polynomial equations with integer coefficients.* PhD Thesis, Berkeley, 1993. United Microfilms Inc, 300 North Zeeb Road, Ann Arbor, MI, 48106-1346 USA, Phone 800-521-0600.

[6] Gregorio Malajovich On generalized Newton algorithms : quadratic convergence, path-following and error analysis. *Theoretical Computer Science* **133** (1994) 65-84.

[7] George Salmon. *Lessons introductory to the modern higher algebra* 2^{nd} edition : Dublin, 1885. 5^{th} edition : reprint by Chelsea Pub. Co., Bronx, unknown date.

[8] Michael Shub and Steve Smale, On the Complexity of Bezout's Theorem I - Geometric aspects. *Journal of the AMS*, **6**, 2, Apr 1993.

[9] Michael Shub and Steve Smale, On the complexity of Bezout's Theorem II - Volumes and Probabilities. in: F. Eysette and A. Galligo, eds : *Computational Algebraic geometry*. Progress in Mathematics **109**, Birkhauser, 267-285, 1993.

[10] Michael Shub and Steve Smale, Complexity of Bezout's Theorem III ; Condition number and packing. *Journal of Complexity* **9**, 4-14, 1993.

[11] Michael Shub and Steve Smale, Complexity of Bezout's Theorem IV ; Probability of success ; Extensions Preprint, Berkeley, 1993.

[12] Michael Shub and Steve Smale, Complexity of Bezout's Theorem V : Polynomial time ; Preprint, Barcelona, 1993.

[13] Steve Smale, Newton method estimates from data at one point, in R. Erwing, K. Gross and C. Martin (editors). *The merging of disciplines : New directions in Pure, Applied and Computational Mathematics*. Springer, New York, 1986

[14] B. L. Van der Waerden, *Modern Algebra, Vol 2.* F. Ungar publishing Co, New York, 1950

Departamento de Matematica Aplicada da UFRJ, Caixa Postal 68530, CEP 21945, Rio, RJ, Brasil

E-mail address: gregorio@lyric.labma.ufrj.br