Bounds for the Condition Number of Polynomials Systems with Integer Coefficients

Aaron Herman, Elias Tsigaridas

Bounds for the Condition Number of Polynomials Systems with Integer Coefficients

Aaron Herman[1] and Elias Tsigaridas[2,3]

[1] Department of Mathematics, North Carolina State University, aherman@ncsu.edu
[2] INRIA, Paris-Rocquencourt Center, PolSys Project
[3] UPMC, Univ Paris 06, LIP6, CNRS, UMR 7606, LIP6, Paris, France
elias.tsigaridas@inria.fr

Abstract. Polynomial systems of equations are a central object of study in computer algebra. Among the many existing algorithms for solving polynomial systems, perhaps the most successful numerical ones are the homotopy algorithms. The number of operations that these algorithms perform depends on the condition number of the roots of the polynomial system. Roughly speaking the condition number expresses the sensitivity of the roots with respect to small perturbation of the input coefficients. A natural question to ask is how can we bound, in the worst case, the condition number when the input polynomials have integer coefficients? We address this problem and we provide effective bounds that depend on the number of variables, the degree and the maximum coefficient bitsize of the input polynomials. Such bounds allows to estimate the bit complexity of the algorithms that depend on the separation bound, like the homotopy algorithms, for solving polynomial systems.

1 Introduction

The study of algorithms for solving polynomial systems are in the center of study of computational algebra and computational mathematics in general. In this context, it is of great importance to define measures of hardness to express the difficulty to compute the solutions of a polynomial system. By "compute" we mean to approximate, up to any desired precision, one or all the roots of a polynomial system.

The condition number of the roots of a polynomial system could be considered, among other things, as such a measure of hardness. It expresses the sensitivity of the roots of a polynomial system, when we allow perturbations in the coefficients of the input polynomials. We refer to the fundamental work of Shub and Smale [11], see also [4], or to the recent book of Bürgisser and Cucker [5] for a detailed exposition. The complexity of numerical algorithms for polynomial system solving depends on the condition number. Among these numerical algorithms, the most successful, in theory and in practice, are the homotopy methods, e.g. [5, 2].

When the coefficients of the input polynomials are rational numbers, then besides the number of variables and degree of the polynomials, we have one more input parameter; the bitsize of the coefficients. We consider the maximum bitsize

of the coefficients of a polynomial as the bitsize of the polynomial. Then, we should be able to express or to bound the measure of hardness for solving a polynomial system, or especially the condition number of the roots, with respect to these three parameters. That is to provide effective bounds as a function of the number of variables, the degree, and the bitsize of the input polynomials [9].

From a, first glance completely, different point of view, when the input coefficients are rational numbers, then a fundamental question of great importance is the following: What is the number of bits up to which we need to approximate the roots of a polynomial system, to distinguish them from each other? Can we provide such a bound as a function in the number of variables, the degree, and bitsize of the polynomials? Separation bounds, that is lower bounds on the minimum distance between the isolated roots of a polynomial system provide an answer to this question, in the worst case. We refer the reader to the `DMM` bound [6], that is the best known such bound. It is a natural question to ask if the bounds on the condition number and the separation bounds are connected. We will provide a positive answer to this question.

1.1 Our results

We consider the problem of bounding the condition number of the roots of square-free univariate polynomials and 0-dimensional polynomial systems with a smooth zero set, when the input polynomials have integer coefficients. We also introduce an aggregate version of the condition number and we prove bounds of the same order of magnitude as in the case of the condition number of a single root.

In the univariate case we improve the currently known bounds [9, Theorem 2.4] by a factor of d (Proposition 1), where d is the degree of the polynomial. For the multivariate case the previous bounds [9, Theorem 2.5], which like ours are single exponential with respect to the number of variables, do not specify the constant in the exponent. We provide precise bounds (Theorem 1) and our approach leads to better bounds than the ones we can obtain by performing the calculations using the previously known approach [9]. The exact constants in the exponents can be useful in many applications e.g. [1, 7, 8]. Such bounds are also needed to establish a connection between Turing machines and the Blum-Cucker-Shub-Smale model and to certify and analyze the Boolean complexity of algorithms based on homotopy techniques [3].

The aggregate versions of the condition numbers we introduce (Proposition 2 and Theorem 2) encapsulate the condition number of all the roots. Contrary to what is expected as a bound in this case, that is the number of roots times the worst case bound for the condition number at a single root, our aggregate version saves a factor equal to the number of roots. As a consequence, in the multivariate case, we gain a factor of d^n, where d is the degree of the polynomials and n the number of variables.

1.2 Notation

In what follows $\mathcal{O}_B$, resp. $\mathcal{O}$, means bit, resp. arithmetic, complexity and $\widetilde{\mathcal{O}}_B$, resp. $\widetilde{\mathcal{O}}$, means that we are ignoring logarithmic factors. For a polynomial $A = \sum_{i=0}^{d} a_i\, x^i \in \mathbb{Z}[x]$, $\mathsf{deg}(A) = d$ denotes its degree. We consider the height function $\mathsf{H}(\cdot)$ which is defined as follows. If $a \in \mathbb{Z}$ then $H(a) = |a|$. For $a, b \in \mathbb{Z}$, $\mathsf{H}(\frac{a}{b}) = \max\{\mathsf{H}(a), \mathsf{H}(b)\}$. For a polynomial A, we have $\mathsf{H}(A) = \max_k |a_k|$. Finally, for a matrix $M \in \mathbb{Z}^{n\times n}$, $\mathsf{H}(M) = \max_{i,j}|M_{i,j}|$. The logarithmic height is defined as $\mathsf{h}(\cdot) = \lg \mathsf{H}(\cdot)$, where $\lg(\cdot)$ is the logarithm of base 2. The Mahler bound (or measure) of A is $\mathcal{M}(A) = a_d \prod_{|\alpha|\geq 1} |\alpha|$, where α runs through the complex roots of A, e.g. [10, 12]. If $A \in \mathbb{Z}[x]$ and $\mathsf{H}(A) = 2^\tau$, then $\mathcal{M}(A) \leq \|A\|_2 \leq \sqrt{d+1}\mathsf{H}(A) = 2^\tau\sqrt{d+1}$.

2 Condition number for univariate polynomials

Let $A = \sum_{k=0}^{d} a_k X^k \in \mathbb{C}[X]$ and α be one of its roots. The condition number of A at α is defined as follows

$$\mu(A, \alpha) = \frac{\left(\sum_{i=0}^{d} |\alpha|^{2i}\right)^{\frac{1}{2}}}{|A'(\alpha)|} \tag{1}$$

where A' is the derivative of A. We define the condition number of A as

$$\mu(A) = \max_{\substack{\alpha\in\mathbb{C}\\ A(\alpha)=0}} \mu(A, \alpha) \tag{2}$$

If A is a square-free integer polynomial such that $\mathsf{H}(A) = 2^\tau$, Malajovich [9] provided the following bounds for the condition number at a root α,

$$\mu(A, \alpha) \leq 2^{2d^2-2} d^{2d} 2^{2\tau d^2}$$

which in turn leads to the following estimation for the condition number of A

$$\mu(A) = 2^{\mathcal{O}(\tau d^2)},$$

or

$$\lg(\ \mu(A)\ ) \in \mathcal{O}(\tau d^2).$$

The following proposition improves this bound by a factor of d.

Proposition 1. *Consider the square-free polynomial $A = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ with $\mathsf{H}(A) \leq 2^\tau$ and $a_0 \neq 0$. Let $\alpha \neq 0$ be a root of A. Then*

$$\mu(A, \alpha) \leq \sqrt{d+1}^{15d+1} 2^{15d\tau+\tau+18d\lg(d)}.$$

Hence $\lg(\mu(A)) \in \mathcal{O}(d\tau + d\lg(d))$.

Proof: First we bound the numerator of formula (1) as follows

$$(\sum_{i=0}^{d} |\alpha|^{2i})^{\frac{1}{2}} = \|(1, \alpha, \ldots, \alpha^d)\|_2 = \sqrt{d+1}\,\|(1, \alpha, \ldots, \alpha^d)\|_\infty \leq \sqrt{d+1}\,2^d\,\mathsf{H}(A)^d \tag{3}$$

To bound the denominator we need the following result, e.g. [6]. For $A \in \mathbb{Z}[X]$, let Ω be a set of k pairs of indices of non-zero roots of A. Then

$$\prod_{(i,j)\in\Omega} |\alpha_i - \alpha_j| \geq d^{-18d}(d+1)^{-15d/2}\mathsf{H}(A)^{-15d} \geq 2^{-30d\lg d}\,\mathsf{H}(A)^{-15d}.$$

Using the previous bound we can bound $A'(\alpha)$. We notice that

$$|A'(\alpha)| = |a_d \prod_{\substack{\gamma\neq\alpha \\ f(\gamma)=0}} (\alpha - \gamma)| \geq \prod_{\substack{\gamma\neq\alpha \\ f(\gamma)=0}} |\alpha - \gamma| \geq 2^{-30d\lg d}\,\mathsf{H}(A)^{-15d}$$

as $|a_d| \geq 1$. Finally, by combining the equations

$$\begin{aligned}\mu(A,\alpha) = \frac{\left(\sum_{i=0}^{d} |\alpha|^{2i}\right)^{\frac{1}{2}}}{|A'(\alpha)|} &\leq 2^{2d}\,\mathsf{H}(A)^d\,2^{30d\lg d}\,\mathsf{H}(A)^{15d} \leq 2^{32d\lg d}\,\mathsf{H}(A)^{16d} \\ &\leq 2^{\mathcal{O}(d\tau + d\lg d)} = 2^{\widetilde{\mathcal{O}}(d\tau)}.\end{aligned}$$

□

The condition number of A, Eq. (2), expresses the maximum condition of all the roots. Hence, one might suggest that if we are interested in a notion of the condition number that accounts for all the roots, then we have to multiply the worst case bound by their number; in our case d. However, it turns out that this is not the case. We consider the following aggregate version of the condition number

$$\tilde{\mu}(A) = \prod_{i=1}^{d} \mu(A, \alpha_i)$$

where $\{\alpha_i\}_{1\leq i\leq d}$ is the set of roots of f. We prove that a bound similar to the one of Proposition 1 holds for $\tilde{\mu}$.

Proposition 2. *Consider the square-free polynomial* $A = \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X]$ *with* $\mathsf{H}(A) = 2^\tau$. *Then*

$$\tilde{\mu}(A) \leq \sqrt{d+1}^{2d} 2^{\tau d}.$$

Hence $\lg(\,\tilde{\mu}(A)\,) \in \mathcal{O}(d\tau + d\lg(d))$.

Proof: We obtain the bound using the properties of the Mahler measure and the discriminant, $\mathsf{disc}(A)$.

$$\begin{aligned}
\tilde{\mu}(A) &= \prod_{i=1}^{d} \mu(A,\alpha_i) = \prod_{i=1}^{d} \frac{||(1,\alpha_i,\ldots,\alpha_i^d)||_2}{|A'(\alpha_i)|} = \prod_{i=1}^{d} \frac{||(1,\alpha_i,\ldots,\alpha_i^d)||_2}{a_d \prod_{j\neq i}|\alpha_i-\alpha_j|} \\
&= \frac{\prod_{i=1}^{d}||(1,\alpha_i,\ldots,\alpha_i^d)||_2}{a_d^d \prod_{i\neq j}|\alpha_i-\alpha_j|} = \frac{\prod_{i=1}^{d}||(1,\alpha_i,\ldots,\alpha_i^d)||_2}{a_d^d\left(\frac{|\mathsf{disc}(A)|}{a_d^{2d-2}}\right)} = a_d^{d-2}\frac{\prod_{i=1}^{d}||(1,\alpha_i,\ldots,\alpha_i^d)||_2}{|\mathsf{disc}(A)|} \\
&\leq a_d^{d-2}\frac{\prod_{i=1}^{d}\sqrt{d+1}||(1,\alpha_i,\ldots,\alpha_i^d)||_\infty}{|\mathsf{disc}(A)|} = a_d^{d-2}\sqrt{d+1}^d\frac{\prod_{i=1}^{d}||(1,\alpha_i,\ldots,\alpha_i^d)||_\infty}{|\mathsf{disc}(A)|} \\
&= a_d^{d-2}\sqrt{d+1}^d\frac{\prod_{i=1}^{d}\max\{1,|\alpha_i|^d\}}{|\mathsf{disc}(A)|} = a_d^{d-2}\sqrt{d+1}^d\frac{\left(\prod_{i=1}^{d}\max\{1,|\alpha_i|\}\right)^d}{|\mathsf{disc}(A)|} \\
&= \frac{\sqrt{d+1}^d}{a_d^2}\frac{\left(a_d\prod_{i=1}^{d}\max\{1,|\alpha_i|\}\right)^d}{|\mathsf{disc}(A)|} = \frac{\sqrt{d+1}^d}{a_d^2}\frac{(\mathcal{M}(A))^d}{|\mathsf{disc}(A)|} \\
&\leq \frac{\sqrt{d+1}^d}{a_d^2}\frac{(||A||_2)^d}{|\mathsf{disc}(A)|} \leq \frac{\sqrt{d+1}^d}{a_d^2}\frac{\left(\sqrt{d+1}\,\mathsf{H}(A)\right)^d}{|\mathsf{disc}(A)|} \\
&= \frac{\sqrt{d+1}^{2d}}{a_d^2}\frac{\mathsf{H}(A)^d}{|\mathsf{disc}(A)|} \leq \sqrt{d+1}^{2d}\mathsf{H}(A)^d.
\end{aligned}$$

□

3 Condition number for polynomial systems

In this section we generalize the bounds of Propositions 1 and 2 to the case of polynomial systems. The definition of the condition number of a root of a polynomial system is given in equation (4). We assume that the polynomial systems are 0-dimensional and their zero set is smooth, that is the Jacobian of the system is invertible.

First we need to introduce additional notation, which follows closely [3]. Let $\mathcal{H}_d^n$ be the vector space of homogeneous polynomials in $n+1$ variables, $X_0, X_1, \ldots, X_n$, of degree d. If $f \in \mathcal{H}_d^n$ then

$$f = \sum_{|\boldsymbol{\alpha}|=d} f_{\boldsymbol{\alpha}}\, \boldsymbol{X}^{\alpha} = \sum_{|\boldsymbol{\alpha}|=d} f_{\boldsymbol{\alpha}} X_0^{\alpha_0} X_1^{\alpha_1}\cdots X_n^{\alpha_n}.$$

For $f, g \in \mathcal{H}_d^n$ we consider the following inner product

$$\langle f, g\rangle = \sum_{|\boldsymbol{\alpha}|=d} f_{\boldsymbol{\alpha}}\, g_{\boldsymbol{\alpha}} \binom{d}{\boldsymbol{\alpha}}^{-1} = \sum_{|\boldsymbol{\alpha}|=d} f_{\boldsymbol{\alpha}}\, g_{\boldsymbol{\alpha}} \binom{d}{\alpha_0,\alpha_1,\ldots,\alpha_n}^{-1}$$

and the corresponding norm

$$\|f\|_b^2 = \langle f, f\rangle = \sum_{|\boldsymbol{\alpha}|=d} |f_{\boldsymbol{\alpha}}|^2 \binom{d}{\boldsymbol{\alpha}}^{-1}.$$

We consider $\boldsymbol{f} = (f_1, \ldots, f_n) \in \mathcal{H}_{d_1}^n \times \cdots \times \mathcal{H}_{d_n}^n = \mathcal{H}$ to be a 0-dimensional polynomial system of n homogeneous equations in $n+1$ variables, with a smooth zero set. For a system of equations, $\boldsymbol{f}$, we have the following definition of the norm

$$\|\boldsymbol{f}\|^2 = \sum_{i=1}^{n} \|f_i\|_b^2.$$

The condition number of a polynomial system $\boldsymbol{f}$ at a number $\boldsymbol{z} \in \mathbb{C}^n$ is defined in [4] as

$$\mu(\boldsymbol{f}, \boldsymbol{z}) = \|f\| \, \|(D\boldsymbol{f}(\boldsymbol{z})|_{\boldsymbol{z}^\perp})^{-1} \, \mathsf{Diag}(\|\boldsymbol{z}\|^{d_i - 1} d_i^{1/2})\|. \tag{4}$$

However, to bound the various quantities that appear we use an equivalent definition, Eq. (5), from Malajovich [9]. Moreover, we follow the notation from [3] to bound condition number of a polynomial system of polynomials having integer coefficients. In this case we assume that $\mathsf{H}(f_i) \leq 2^\tau$ for all i.

Let $\boldsymbol{f} \in \mathcal{H}$ be a polynomial system and let $\boldsymbol{z} \in \mathbb{P}(\mathbb{C}^{n+1})$. Let $\chi_1 = \chi_1(\boldsymbol{f}, \boldsymbol{z})$ defined by

$$\chi_1 = \left\| \begin{pmatrix} D\boldsymbol{f}(\boldsymbol{z}) \\ \boldsymbol{z}^* \end{pmatrix}^{-1} \begin{pmatrix} \sqrt{d_1}\,\|\boldsymbol{f}\|\,\|\boldsymbol{z}\|^{d_1-1} & & \\ & \ddots & \\ & & \sqrt{d_n}\,\|\boldsymbol{f}\|\,\|\boldsymbol{z}\|^{d_n-1} \\ & & \|\boldsymbol{z}\| \end{pmatrix} \right\| = \|M_1^{-1} \cdot M_2\| \tag{5}$$

Note that these formulas do not depend on the representative of $\boldsymbol{z}$ and thus are well defined. Their value is also invariant under multiplication of $\boldsymbol{f}$ by a non–zero complex number $\lambda \in \mathbb{C}$. Our goal is to estimate a bound for $\chi_1(\boldsymbol{f}, \boldsymbol{\zeta})$, where $\boldsymbol{\zeta}$ is a root of $\boldsymbol{f}$.

Recall that for any matrix M it holds $\|M\| \leq \|M\|_F$. The second norm is the Frobenius norm, that is $\|M\|_F = \sqrt{\sum_{i,j} |M_{i,j}^2|}$.

First we consider bounds for the norm of M_2. To bound $\|\boldsymbol{f}\|$, assuming $\mathsf{H}(f_i) \leq 2^\tau$, we proceed as follows:

$$\|\boldsymbol{f}\| = \sqrt{\sum_{i=1}^{n} \|f_i\|_b^2} \leq \sqrt{\sum_{k=1}^{n} 2^{2\tau + d_k \lg(nd_k)}} \leq 2^{\tau + d \lg(nd)}. \tag{6}$$

To bound $\|\boldsymbol{\zeta}\|$ we use the `DMM` bounds [6]. The `DMM` is defined for sparse systems but we can also use it for the homogeneous case. To see this notice that we consider all the possible dehomogenizations of the system and we apply to each of them `DMM`. Then we take the worst bound.

For any root $\boldsymbol{\zeta} = (\zeta_0, \zeta_1, \ldots, \zeta_n)$ of the system it holds [6, Cor. 4]

$$\lg(\max_{0\le k\le n} |\zeta_k|) \le 1+\prod_{i=1}^{n} d_i+\sum_{i=1}^{n}\prod_{j\neq i} d_i\,(\tau+\lg(2\,d_i^n)) = \eta_1 = \mathcal{O}(d^n+nd^{n-1}\tau+n^2d^{n-1}\lg d). \tag{7}$$

Now we are ready to bound $\|M_2\|$ by combining equations (6) and (7). The bound is as follows:

$$\|M_2\|_F^2 \le \sum_{i=1}^{n}\left(\sqrt{d_i}\,\|\boldsymbol{f}\|\,\|\boldsymbol{\zeta}\|^{d_i-1}\right)^2 + \|\boldsymbol{\zeta}\|^2 \le 2^{2\tau+3d\lg(nd)+d\,\eta_1},$$

which simplifies to

$$\lg\|M_2\|_F \le \mathcal{O}(d^{n+1} + nd^n\tau + n^2d^n\lg d) = \widetilde{\mathcal{O}}(d^{n+1} + d^n\tau). \tag{8}$$

To bound M_1^{-1} it suffices to bound $\|M_1\|$. It holds $\|M_1^{-1}\| \le n^n\,\mathsf{H}(M_1)$, e.g. [9, Lemma 4.5]. To obtain a bound for $\mathsf{H}(M_1)$, first we need an estimation on the evaluation of the derivatives $G_{i,j}(\boldsymbol{X}) = \frac{\partial}{\partial X_j} f_i(\boldsymbol{X})$ at the roots of the system, $\boldsymbol{\zeta}$.

Let $f_{n+1}^{(i,j)}(\boldsymbol{X}, Y) = Y - G_{i,j}(\boldsymbol{X}))$ and consider the polynomial system

$$(\Sigma_{i,j}) \quad \{f_1(\boldsymbol{X}) = \cdots f_n(\boldsymbol{X}) = f_{n+1}^{(i,j)}(\boldsymbol{X}, Y) = 0\}. \tag{9}$$

This is a system in $n+1$ equations in $n+1$ variables. It holds $\mathsf{deg}(f_{n+1}^{(i,j)}) = \mathsf{deg}(G_{i,j}) \le d_i - 1$ and $\mathsf{H}(f_{n+1}^{(i,j)}) = \mathsf{H}(G_{i,j}) \le d\,\mathsf{H}(f_i) \le \tau + \lg d_i$.

The resultant of $(\Sigma_{i,j})$ that eliminates the variables $X_1, \ldots, X_n$, is

$$R_{i,j} = \mathsf{Res}_{d_1,\ldots,d_n}(f_1(\boldsymbol{X}), \ldots, f_n(\boldsymbol{X}), y - G_{i,j}(\boldsymbol{X})) \in \mathbb{Z}[y]$$

where $R_{i,j} \in \mathbb{Z}[Y]$. The roots of $R_{i,j}$ correspond to the evaluations of $G_{i,j}$ at the roots of the system $\boldsymbol{f} = 0$. Therefore, an upper bound on the roots of $R_{i,j}$ provides an upper bound on the evaluation. We should notice that $R_{i,j}$ is not identically zero.

Hence, to obtain the required bounds we can consider the system $(\Sigma_{i,j})$. From this point of view we need to provide lower bounds on the coordinates of solutions of the system. For this we use `DMM` [6, Thm. 3 and Cor. 4] directly.

First, we need to define (bound) various quantities, see [6, Eq. (3)]. The mixed volume(s) $\mathsf{M}_0 = d_1\cdots d_n(d_i{-}1) \le d^n(d{-}1) \le d^{n+1}$, $\mathsf{M}_k = d_1\ldots d_{k-1}\,d_{k+1}\cdots d_n(d_i{-}1) \le d^{n-1}(d-1) \le d^n$ for $1 \le k \le n$, and $\mathsf{M}_{n+1} = d_1\cdots d_n \le d^n$; and the integer coefficients that appear in the resultant polynomial

$$\varrho = \prod_{k=1}^{n+1}(\#Q_k)^{\mathsf{M}_k} \le 2^{\sum_{k=1}^{n+1}\mathsf{M}_i}\prod_{i=1}^{n} d_k^{n\mathsf{M}_k}(d_i-1)^{nM_{n+1}} \le 2^{2nd^n}\,d^{2n^2d^n}.$$

Finally, we bound the weighted heights of the input polynomials $C = \prod_{k=1}^{n+1}\mathsf{H}(f_k)^{M_k} \le 2^{(n+\lg d)\,\tau\,d^n}$. An isolated root of the system with Y coordinate equal to y follows the bound $|y| \le 2^{\mathsf{M}_0}\,\varrho\,C$. Thus

$$|G_{i,j}(\boldsymbol{\zeta})| \le 2^{\mathsf{M}_0}\,\varrho\,C \le 2^{d^{n+1}+8n^2d^n\lg d+(n+\lg d)\tau d^n}$$

for any i, j and for any root $\boldsymbol{\zeta}$ of the system. For $\boldsymbol{\zeta}^*$ it holds that $\mathsf{H}(\boldsymbol{\zeta}^*) \leq \mathsf{H}(\boldsymbol{\zeta})$ and so we can use the bound from (7). Putting all these together we have the bound

$$\mathsf{H}(M_1) \leq 2^{\eta_2}$$

where

$$\eta_2 = \mathcal{O}(d^{n+1} + n^2 d^n \lg d + (n + \lg d)\tau d^n) = \widetilde{\mathcal{O}}(d^{n+1} + n^2 d^n + n\tau d^n)$$

and so $\|M_1^{-1}\| \leq n^n \, \mathsf{H}(M_1) \leq 2^{\eta_2} \leq 2^{\widetilde{\mathcal{O}}(d^{n+1} + n^2 d^n + n\tau d^n)}$.

Combining the bounds for $\|M_1^{-1}\|$ and $\|M_2\|$ we obtain the following bound for χ_1 which also a bound for the condition number of a complex root of the system.

$$\chi_1 \leq 2^{\eta_2} \leq 2^{\mathcal{O}(d^{n+1} + n^2 d^n \lg d + (n + \lg d)\tau d^n)}. \tag{10}$$

The previous discussion leads to the following theorem

Theorem 1. *Let $\boldsymbol{f} = (f_1, \ldots, f_n) \in \mathcal{H}$ be a 0-dimensional polynomial system such that its zero set consists of smooth points. Assume $f_i \in \mathbb{Z}[X_0, X_1, \ldots, X_n]$ such that they have degrees bounded by d and $\mathsf{H}(f_i) \leq 2^\tau$. Then, we have the following bound for the condition number of any root $\boldsymbol{\zeta}$ of the system*

$$\mu(\boldsymbol{f}, \boldsymbol{\zeta}) \leq 2^{\mathcal{O}(d^{n+1} + n^2 d^n \lg d + (n + \lg d)\tau d^n)}.$$

3.1 Multivariate aggregate condition number

In this section we sketch the proof of an aggregate version of Theorem 1. It provides bounds similar to the ones of Proposition 2 and to the aggregate nature of the `DMM` bounds [6, Theorem 3].

In the view of Theorem 1 if we wanted to consider a bound on the condition number for all the roots of the system, then we have to multiply $\mu(\boldsymbol{f}, \boldsymbol{\zeta})$ by their number. There are d^n roots in the worst case, by the Bézout bound. This leads to a bound of $\widetilde{\mathcal{O}}_B(d^{2n+1} + d^{2n}\tau)$.

In the sequel we will improve this bound to $\widetilde{\mathcal{O}}_B(d^{n+1} + d^n\tau)$ using aggregation.

Some elementary properties are in place.

$$\|M\| \leq \|M\|_F \leq \sqrt{n^2 \, \mathsf{H}(M)^2} \leq n \, \mathsf{H}(M).$$

If the entries of the matrix M depend on a root $\boldsymbol{\zeta}$ then we write $M(\boldsymbol{\zeta})$ to emphasize this. In this context it holds

$$\chi_1(\boldsymbol{\zeta}) \leq \|M_1^{-1}(\boldsymbol{\zeta}) \, M_2(\boldsymbol{\zeta})\| \leq (n+1)^2 \mathsf{H}(M_1(\boldsymbol{\zeta}))^{n+1} \mathsf{H}(M_2(\boldsymbol{\zeta}))$$

and

$$\tilde{\chi}_1(\boldsymbol{\zeta}) = \prod_{\boldsymbol{\zeta}} \chi_1(\boldsymbol{\zeta}) \leq (n+1)^{2d^n} \prod_{\boldsymbol{\zeta}} \mathsf{H}(M_1(\boldsymbol{\zeta}))^{n+1} \prod_{\boldsymbol{\zeta}} \mathsf{H}(M_2(\boldsymbol{\zeta})).$$

We have to bound each factor independently. We sketch the approach for the second one. For the first factor we work similarly.

To bound $\prod_{\boldsymbol{\zeta}} \mathsf{H}(M_2(\boldsymbol{\zeta}))$ we can apply directly Eq. (5) or (8). However, this approach gives an exponent of d^{2n+1}, which is a big overestimation; by a factor of d^n.

We rely on aggregation bounds of polynomial system, provided by the DMM bounds [6]. Consider the polynomial $f_{n+1}(\boldsymbol{X}, Y) = Y - X_1^2 - \cdots - X_n^2$ and the polynomial system

$$(\Sigma_{i,j}) \quad \{f_1(\boldsymbol{X}) = \cdots f_n(\boldsymbol{X}) = f_{n+1}(\boldsymbol{X}, Y) = 0\}. \tag{11}$$

The resultant of the system encapsulates (all) the evaluations of f_{n+1} over the roots of $\boldsymbol{f}$. Therefore, it suffices to bound the height of the resultant. The bounds that we get are similar to the ones of the previous section. The calculations lead to the following theorem

Theorem 2. *Let $\boldsymbol{f} = (f_1, \ldots, f_n) \in \mathcal{H}$ be a 0-dimensional polynomial system. Assume $f_i \in \mathbb{Z}[X_0, X_1, \ldots, X_n]$ such that they have degrees bounded by d and $\mathsf{H}(f_i) \leq 2^\tau$. Then, if $\boldsymbol{\zeta}$ runs over all the solutions of the system, it holds*

$$\tilde{\chi_1}(\boldsymbol{f}) = \prod_{\boldsymbol{\zeta}} \chi_1(\boldsymbol{\zeta}) \leq 2^{\widetilde{\mathcal{O}}(d^{n+1} + d^n \tau)}.$$

Acknowledgments

ET is partially supported by GeoLMI (ANR 2011 BS03 011 06), HPAC (ANR ANR-11-BS02-013), and an FP7 Marie Curie Career Integration Grant.

References

1. S. Basu and M. Roy. Bounding the radii of balls meeting every connected component of semi-algebraic sets. *J. Symb. Comp.*, 45:1270–1279, 2010.
2. D. J. Bates, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. *Numerically solving polynomial systems with Bertini*, volume 25. SIAM, 2013.
3. C. Beltrán and A. Leykin. Robust certified numerical homotopy tracking. *Foundations of Computational Mathematics*, 13(2):253–295, Apr. 2013.
4. L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer-Verlag, 1998.
5. P. Bürgisser and F. Cucker. *Condition: The geometry of numerical algorithms*, volume 349. Springer Science & Business Media, 2013.
6. I. Z. Emiris, B. Mourrain, and E. P. Tsigaridas. The DMM bound: Multivariate (aggregate) separation bounds. In S. Watt, editor, *Proc. 35th ACM Int'l Symp. on Symbolic & Algebraic Comp. (ISSAC)*, pages 243–250, Munich, Germany, July 2010. ACM.
7. K. A. Hansen, M. Koucky, N. Lauritzen, P. B. Miltersen, and E. P. Tsigaridas. Exact algorithms for solving stochastic games. In *Proc. 43rd Annual ACM Symp. Theory of Computing (STOC)*, 2011.
8. K. A. Hansen, M. Koucky, and P. B. Miltersen. Winning concurrent reachability games requires doubly-exponential patience. In *Proc. 24th Annual IEEE Symposium on Logic In Computer Science (LICS)*, pages 332–341, Washington, DC, USA, 2009. IEEE Computer Society.

9. G. Malajovich. Condition number bounds for problems with integer coefficients. *Journal of Complexity*, 16(3):529–551, Sept. 2000.
10. M. Mignotte. *Mathematics for Computer Algebra*. Springer-Verlag, New York, 1991.
11. M. Shub and S. Smale. Complexity of bezout's theorem: Iii. condition number and packing. *J. Complexity*, 9(1):4–14, 1993.
12. C. Yap. *Fundamental Problems of Algorithmic Algebra*. Oxford University Press, New York, 2000.