Lower bounds for some decision problems over $\mathbb{C}$

Gregorio Malajovich*†‡

Second revision, Jan. 30, 2001

Abstract

Lower bounds for some explicit decision problems over the complex numbers are given. The decision problems considered are certain zero-dimensional subsets of $\mathbb{N}\times\mathbb{C}$, and can be assimilated to a countable family of polynomials g_i. More precisely, one should decide for input (i,x) if $g_i(x)=0$.

A lower bound for deciding if a polynomial g_i vanishes at some x can be derived from an uniform lower bound for the evaluation of all $f\in(g_i)$. That bound is obtained by means of an arithmetic invariant of the roots of g_i, the Newton diagram of f and other known techniques.

1 Introduction

A model of computation over the ring $\mathbb{C}$ of complex numbers was introduced in [**?**]. A *Machine over* $\mathbb{C}$ operates on a bi-infinite sequence of complex numbers $(\cdots,s_{-1},s_0,s_1,s_2,\cdots)$. The machine itself may be associated to a flowchart.

Nodes in the flowchart may be of five different types. A *Computation Node* is associated to a fixed polynomial in variables s_i, and operates by replacing the value of s_0 by the value of its associated polynomial. A *Decision Node* is also associated to a polynomial g in the s_i's, and allows the machine to branch on equality $g(s)=0$. A *Fifth Node* operates by shifting the variables s_i to the right ($s_{i+1}\leftarrow s_i$ for all i) or to the left ($s_{i-1}\leftarrow s_i$ for all i). An *Input Node* and an *Output node* provide an embedding (resp. projection) of the input space into the state space (resp. of the state space into the output space). The reader is referred to [**?**] for a formal definition.

The model of complexity over $\mathbb{C}$ presents striking similarities with the classical (Turing) model of complexity (See [**?**, **?**, **?**] for a discussion). Decision

*Departamento de Matemática Aplicada, Universidade Federal do Rio de Janeiro. Caixa Postal 68530, CEP 21945, Rio de Janeiro, RJ, Brasil. e-mail: gregorio@labma.ufrj.br.

†Part of this work was done while the author was visiting the Mathematical Sciences Research Institute at Berkeley. Research in MSRI was partially funded by the National Science Foundation through grant no. DMS-9701755.

‡On leave at City University of Hong Kong. He was partially supported by the CERG grant no. 9040393.

problems, complexity classes and the $\mathcal{P} \neq \mathcal{NP}$ conjecture are defined exactly as in the classical theory.

This paper is about lower bounds for certain decision problems over $\mathbb{C}$. As in the classical complexity theory, a decision problem is a subset X of the input space (here, the space of all finite sequences of complex numbers). A machine *decides* the problem X if it outputs 0 if and only if the input x belongs to X. and it outputs 1 otherwise.

Below, we will provide lower bounds for the complexity of deciding, given x, if $p^d(x) = 0$ for some explicit polynomials p^d.

A related problem is to give lower bounds for the evaluation of explicit polynomials. This has been an active subject of research since [**?**]. See [**?**] for modern developments and for bibliographical remarks. More recent results appeared in [**?**] and [**?**].

Most of those bounds use the Ostrowsky model of computation ([**?**] page 6): sum and multiplication by an algebraic constant are free, and the complexity of a computation for a polynomial $f(x)$ is the number of non-scalar multiplications, i.e., of multiplications of two polynomials in the variable x. For instance, Horner's rule for a degree d polynomial requires d non-scalar multiplications.

All those bounds apply trivially to the complexity of evaluating polynomials by a 'machine over $\mathbb{C}$' as defined in [**?**], or to the (multiplicative-branching) complexity of a computation tree for evaluating the same polynomial.

Little is known, however, about the application of those bounds to decision problems (Over $\mathbb{C}$, in the sense of [**?**], or by a decision tree as in [**?**], Definition (4.19) page 115. In this definition, each node of a computation tree can perform one algebraic operation or comparison, and therefore a natural measure of complexity is the depth of the tree).

This paper was motivated by the desire to gain new insights on the theory of NP-completeness over $\mathbb{C}$ (See [**?**]). A decision problem in NP is essentially a collection of algebraic sets presented in a certain way. We will show below that in certain particular cases, there is an arithmetic invariant for decision problems that implies a lower bound for their deterministic complexity.

In this paper, only decision problems of the form below will be considered: Let $X \subseteq \mathbb{N} \times \mathbb{C}$, and let $X_d = \{x \in \mathbb{C} : (d, x) \in X\}$. Typically, d is the problem size and $\#X_d \leq d$. One can think of X as the disjoint union of the zero-set of a family of polynomials of degree $\leq d$, where $d \in \mathbb{N}$. The two following forms of a decision problem are natural in this setting:

Problem 1. For any fixed d, decide wether $x \in X_d$.

Problem 2. Decide wether $(d, x) \in X$.

Problem 1 is non-uniform, in the sense that we allow a different machine over $\mathbb{C}$ or a different decision tree to be used for each value of d. However, we want a bound on the running time or on the multiplicative complexity of the tree, as a function of d.

Problem 2 is uniform. It is harder than Problem 1, in the sense that it cannot be solved by a decision tree, since $\#X_d$ can be arbitrarily large. It requires a machine over $\mathbb{C}$, that will eventually branch according to the value of d.

Lower bounds for Problem 1 are also lower bounds for Problem 2.

A trivial, topological lower bound for Problems 1 and 2 when $\#X_d = d$ is $\log_2 d$. Sharper known bounds come from the 'Canonical Path' argument, see [**?**] section 2.5: Let f be a univariate polynomial. The complexity of deciding $f(x) = 0$ is bounded below by the minimum of the complexity of evaluating $g(x)$, where g ranges over the non-zero multiples of f.

If one assumes some property of f that propagates to its multiple g, then one eventually obtains sharper, non-trivial lower bounds.

The main result in this paper is Lemma 1 below. We will give conditions on the roots of f that will provide lower bounds for the evaluation of g. Essentially, we will require a subset of the roots to be rapidly growing. This will imply a rapid growth property for the coefficients of g. Then, the results of [**?**, **?**] imply a lower bound for the complexity of evaluating g. Thus we will be able to construct specific polynomials that are hard to decide in the *non-uniform* sense, viz.

Lower bound 1. *The set* $X = \{(d, x) \in \mathbb{Z} \times \mathbb{C} : x = 2^{2^{di}}, 1 \leq i \leq d\}$*, cannot be decided in time polylog(d) in the setting of Problem 1.*

Lower bound 2. *The set* $Y = \{(d, x) \in \mathbb{Z} \times \mathbb{C} : p^d(x) = 0\}$*, where* $p^d(t) = \sum_{i=0}^{d} 2^{2^{d(d-i)}} t^i$*, cannot be decided in time polylog(d) in the setting of Problem 1.*

In a more classical computer-science language, we can define the input size of some (d, x) as $\log d$. This means that the integer d is represented in binary notation, while variable x can contain an arbitrary complex number. In that case, 'time polylog(d) in the setting of Problem 1' can be rephrased as $\mathcal{P}_{/\mathrm{poly}}$. The lower bounds above become now: $X \notin \mathcal{P}_{/\mathrm{poly}}$ and $Y \notin \mathcal{P}_{/\mathrm{poly}}$.

Non-uniform lower bounds 1 and 2 can be compared to the following easier, uniform lower bound:

Lower bound 3. *The set* $Z = \{(d, x) \in \mathbb{Z} \times \mathbb{C} : q^d(x) = 0\}$*, where* $q^d(t) = \sum_{i=0}^{d} 2^{2^i} t^i$*, cannot be decided in time polylog(d) in the setting of Problem 2.*

This means that the set Z, where d is represented in binary notation and x is a complex number, does not belong to $\mathcal{P}$ over $\mathbb{C}$.

Thanks to Pascal Koiran, José Luis Montaña, Luis Pardo, Steve Smale and three anonymous referees for their suggestions and comments.

Lower bound 1 was obtained independently by Walter Baur and Karin Halupczok in [**?**] using a different technique.

2 Background and notations

We will need a few basic facts of valuation theory (See Chapters I and II of [**?**] for background):

If K is a number field, then for any $x \in K$, the fractional ideal (x) can be factorized uniquely as a product of prime ideals of K, say

$$(x) = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\cdots\mathfrak{p}_k^{r_k} \quad , \tag{1}$$

with $r_i \in \mathbb{Z}$. (See [**?**, I, §6]). For a fixed prime ideal $\mathfrak{p}_1$ of the ring of integers of K, we can define the function $\nu = \nu_{\mathfrak{p}_1} : K \to \mathbb{N}$ by setting $\nu(x) = r_1$ as in formula (1) when $\mathfrak{p}_1$ appears in the decomposition of (x), and 0 otherwise.

For instance, if $K = \mathbb{Q}$, we may define

$$\nu_2\left(2^n\frac{p}{q}\right) = n \quad , \tag{2}$$

where it is assumed that 2, p and q are pairwise relatively prime.

Two immediate properties of the function ν are that

$$\begin{aligned} \nu(xy) &= \nu(x) + \nu(y) \quad , \\ \nu(\sum_i x_i) &\geq \min_i(\nu(x_i)) \quad , \end{aligned}$$

with equality when the minimum is attained for only one value of i.

The function ν is also well-behaved with respect to field extensions. Let K and L be number fields, and let $\mathfrak{p}$ be a prime ideal in the ring of integers of K. The ideal $\mathfrak{p}$ can be decomposed as a product of prime ideals in the ring of integers of L:

$$\mathfrak{p} = \mathfrak{b}_1^{e_1}\mathfrak{b}_2^{e_2}\cdots\mathfrak{b}_n^{e_n} \quad .$$

Each e_i is called the ramification index of $\mathfrak{b}_i$ over $\mathfrak{p}$. It follows that for any $x \in K$, $e_1\nu_{\mathfrak{p}}(x) = \nu_{\mathfrak{b}_1}(x)$. In that sense, we will consider $\nu_{\mathfrak{b}_1}$ as an 'extension' of $\nu_{\mathfrak{p}}$ to L.

For instance, if If $K = \mathbb{Q}$ and $L = \mathbb{Q}[\sqrt{2}]$, then we may extend ν_2 to L by $\nu_{\sqrt{2}}(\sqrt{2}^k p/q) = k$. In this example, $e_1 = 2$, so $\nu_2(x) = 2\nu_{\sqrt{2}}(x)$ for all $x \in K$.

Definition 1. Let $g = \sum_{i=0}^{d} g_i x^i$ be a degree d polynomial with coefficients in some finite extension K of $\mathbb{Q}$. Let $\mathfrak{p}$ be a prime ideal in the ring of integers of K, and let $\mathfrak{p}$ be a prime ideal of K. The *Newton diagram* of g at $\mathfrak{p}$ is the (lower) convex hull of the set $\{(i, \nu_{\mathfrak{p}}(g_i)), i = 0\cdots d\}$.

We can take K to be the splitting field of g, so that the notation $\nu(\zeta)$ makes sense for ζ a root of g. (Up to rescaling, this is the same as the Newton diagram of g at $\nu_{\mathfrak{q}}$, where $\mathfrak{q}$ is a prime ideal in the ring of integers of $\mathbb{Q}[g_0, \cdots, g_d]$, and $\mathfrak{q}$ divides $\mathfrak{p}$.) The basic property of Newton diagrams used here is the following.

Proposition 1. *Suppose that $\zeta_1, \cdots, \zeta_d$ are the roots of a univariate polynomial $g \in K[x]$ and that $\nu = \nu_{\mathfrak{b}}$ where $\mathfrak{b}$ is a prime ideal of $K[\zeta_1, \cdots, \zeta_d]$. Let the roots of g be ordered so that*

$$\nu(\zeta_1) \geq \cdots \geq \nu(\zeta_d)$$

and let the increasing sequence i_j assume the values 0, d and all the values of i where:

$$\nu(\zeta_i) > \nu(\zeta_{i+1}) \quad .$$

Then the sharp corners of the Newton diagram of g at $\mathfrak{b}$ are precisely the points of the form $(i_j, \nu(g_{i_j}))$ for all j.

Moreover, the slope of the segment $[(i_{j-1}, \nu(g_{i_{j-1}})), (i_j, \nu(g_{i_j}))]$ is precisely $-\nu(\zeta_{i_j})$.

If $\mathfrak{b}$ happens to divide a prime ideal $\mathfrak{p}$ of K with ramification factor e, then the Newton diagram of g at $\mathfrak{b}$ is a rescaling (by e) of the Newton diagram of g at $\mathfrak{p}$.

Proof of Proposition 1. Let $\sigma_i(x_1, \cdots, x_d)$ be the i-th elementary symmetric function, i.e. $\sigma_i(x) = \sum_S \prod_{j \in S} x_j$ where S ranges over all the subsets of $\{1, \cdots, n\}$ with exactly i elements. Let $i_{j-1} < k < i_j$. Writing

$$\begin{aligned} g_{i_{j-1}} &= \pm g_d \ \sigma_{d-i_{j-1}}(\zeta_1, \cdots, \zeta_d) \quad , \\ g_k &= \pm g_d \ \sigma_{d-k}(\zeta_1, \cdots, \zeta_d) \quad , \\ g_{i_j} &= \pm g_d \ \sigma_{d-i_j}(\zeta_1, \cdots, \zeta_d) \quad , \end{aligned}$$

one can pass to the ν by:

$$\begin{aligned} \nu(g_{i_{j-1}}) &= \nu(g_d) + \nu(\zeta_{i_{j-1}+1}) + \cdots + \nu(\zeta_d) \quad , \\ \nu(g_k) &\geq \nu(g_d) + \nu(\zeta_{k+1}) + \cdots + \nu(\zeta_d) \quad , \\ \nu(g_{i_j}) &= \nu(g_d) + \nu(\zeta_{i_j+1}) + \cdots + \nu(\zeta_d) \quad . \end{aligned}$$

Subtracting, one obtains:

$$\begin{aligned} \nu(g_{i_j}) - \nu(g_{i_{j-1}}) &= -\nu(\zeta_{i_{j-1}+1}) - \cdots - \nu(\zeta_{i_j}) \\ &= -(i_j - i_{j-1})\nu(\zeta_{i_j}) \quad , \\ \nu(g_{i_j}) - \nu(g_k) &\leq -\nu(\zeta_{k+1}) - \cdots - \nu(\zeta_{i_j}) \\ &\leq -(i_j - k)\nu(\zeta_{i_j}) \quad . \end{aligned}$$

This concludes the proof. □

3 Uniform lower bounds

We can now prove Lower Bound 3.

Proof of Lower bound 3. Let ν_2 be as in Equation (2). Let ν be an extension of ν_2 to the splitting field of q^d. We assume that ν is scaled such that $e_1\nu_2 = \nu$, for some ramification index $e_1 \in \mathbb{N}^*$. The Newton diagram of q^d at ν is $\{(i, e_1 2^i) : 0 \leq i \leq d\}$. (This last set is convex, since the points lie on the curve $y = 2^x$ and this curve is convex). Therefore, there is a unique root ζ of q^d that minimizes $\nu(\zeta)$.

Since $q^d_{d-1} = (-\sum \zeta_i) q^d_d$, where the sum ranges over all the roots, we have:

$$\nu(q^d_{d-1}) = \nu(q^d_d) + \min \nu(\zeta_i) = \nu(q^d_d) + \nu(\zeta) \quad .$$

Replacing by the actual values of the coefficients, one gets:

$$\nu(\zeta) = -e_1 2^{d-1} \quad . \tag{3}$$

Now, suppose that there is a machine M that decides $q^d(t) = 0$ in time polylog(d). One can assume without loss of generality that this machine has no constant but 0 and 1. Let its running time be bounded by $T = a(\log d)^b$.

Let us fix $d > 2 + T^2$. We will derive a contradiction.

Let $g(x) = \sum g_p x^p$ be the polynomial defining the canonical path (recall that d is fixed now, so this is the path followed by generic $t \in \mathbb{C}$). It can be computed in time $\leq T^2$, so we have the following bounds:

$$\begin{aligned} \deg g &\leq 2^{T^2} \quad , \\ 0 \leq \nu(g_p) &\leq e_1 2^{T^2} \quad . \end{aligned}$$

Since ζ is also a root of g, there are coefficients g_i and g_j, $i \neq j$, such that:

$$(j - i)\nu(\zeta) = \nu(g_i) - \nu(g_j) \quad . \tag{4}$$

Thus, $|\nu(\zeta)| \leq |\nu(g_i)| + |\nu(g_i)|$. This implies:

$$|\nu(\zeta)| \leq e_1 2^{1+T^2} < e_1 2^{d-1} \quad .$$

Replacing by equation 3, one obtains $2^{d-1} < 2^{d-1}$, a contradiction. □

4 Non-uniform lower bounds

Lemma 1. *Let $g = g(t) = \sum_{i=0}^{D} g_i t^i$ be a degree D polynomial with algebraic coefficients. Let $\nu = \nu_{\mathfrak{p}}$ where $\mathfrak{p}$ is a prime ideal in the ring of integers of the splitting field of g. Suppose that there are roots ζ_j of g, $j = 1 \cdots d$, such that the following holds:*

1. $\nu(\zeta_d) \geq 1$,

2. $\nu(\zeta_j) \geq 2D\ \nu(\zeta_{j+1})$, *for* $1 \leq j \leq d-1$.

Then g cannot be evaluated in less than

$$L \geq \sqrt{\frac{d}{28\log_2(D+1)}} - 1$$

multiplications.

The hypotheses of Lemma 1 need only be checked for ν defined on $\mathbb{Q}[\zeta_1, \cdots, \zeta_d]$. This will imply items 1 and 2 for any extension ν' of ν, since $\nu' = e\nu$ in $\mathbb{Q}$ for some fixed ramification index $e \in \mathbb{N}, e \geq 1$.

Proof of Lemma 1. We will first assume that $\nu(g_l) = 0$ for a certain value of l specified below. Then we will derive a lower bound L' in this particular case. Since any polynomial can be brought to the particular case at the cost of one extra multiplication (by g_l^{-1}), we will obtain also a lower bound $L \geq L' - 1$ for the complexity of evaluation in the general case.

Let $\xi_1, \cdots \xi_D$ be the roots of g, and assume they are ordered in such way that:

$$\nu(\xi_1) \geq \cdots \geq \nu(\xi_D) \quad .$$

For $i \in \{1, \cdots, d\}$, le j_i be minimal such that

$$\nu(\zeta_i) > \nu(\xi_{j_i+1}) \qquad \text{or} \qquad j_i = D \quad .$$

Also, le k_i be maximal such that

$$\nu(\xi_{k_i}) > \nu(\zeta_i) \qquad \text{or} \qquad k_i = 0 \quad .$$

Under that notation, the roots of g satisfy, for $k_i \neq 0$ and $j_i \neq D$:

$$\nu(\xi_{k_i}) > \nu(\xi_{k_i+1}) (= \nu(\zeta_i)) = \cdots = \nu(\xi_{j_i}) > \nu(\xi_{j_i+1})$$

and the points $(k_i, \nu(\xi_{k_i}))$ and $(j_i, \nu(\xi_{j_i}))$ correspond to some of the "sharp corners" of the Newton diagram of g at $\mathfrak{p}$.

From Proposition 1, we have the following identity:

$$\nu(g_{k_i}) - \nu(g_{j_d}) = \sum_{l=k_i+1}^{j_d} \nu(\xi_l) \quad .$$

Since we ordered the ξ_l's so that $\nu(\xi_l)$ is non-increasing, and since we took $\nu(\xi_{j_d}) = \nu(\zeta_d) > 1$, all the terms in the right-hand-side satisfy: $\nu(\zeta_i) > \nu(\xi_l) \geq 1$, so we have the bound:

$$(j_i - k_i)\nu(\zeta_i) \leq \nu(g_{k_i}) - \nu(g_{j_d}) \leq (D - k_i)\nu(\zeta_i) \quad .$$

We assume that g was scaled so that $\nu(g_{j_d}) = 0$. Therefore, we can simply write:

$$\nu(\zeta_i) \leq \nu(g_{k_i}) \leq D\nu(\zeta_i) \quad .$$

Hence, for $i = 1, \cdots, d-1$:

$$\nu(g_{k_i}) \geq \frac{\nu(\zeta_i)}{D\nu(\zeta_{i+1})}\nu(g_{k_{i+1}}) \geq 2\nu(g_{k_{i+1}}) \quad .$$

Also, $\nu(g_{k_d}) = \nu(g_{k_d}) - \nu(g_{j_d}) \geq \nu(\zeta_d) \geq 1$. Thus for $i = 1, \cdots, d-1$, $\nu(g_{k_i}) > \sum_{l=i+1}^{d} \nu(g_{k_l})$. It follows that

$$\#\left\{\sum_{j=1}^{d} s_j \nu(g_{k_j}), s_j \in \{0;1\}\right\} = 2^d \quad ,$$

and thus:

$$\#\left\{\sum_{l=1}^{D} s_l \nu(g_l), s_l \in \{0;1\}\right\} \geq 2^d \quad .$$

Hence:

$$\#\left\{\nu(\prod_{s\in S} g_s), S \subset \{0, \cdots, D\}\right\} \geq 2^d \quad ,$$

and finally

$$\mu(g) = \#\left\{\sum_{S\subset\{0,\cdots,D\}} \theta_S \prod_{s\in S} g_s, \theta_S \in \{0;1\}\right\} \geq 2^{2^d} \quad .$$

By Lemma 1 in [**?**] or by Lemma 4 in [**?**],

$$\mu(g) \leq 2^{(D+1)^{28L'^2}}$$

and hence, taking logs:

$$(D+1)^{28L'^2} \geq 2^d \quad .$$

Taking logs again:

$$28L'^2 \geq \frac{d}{\log_2(D+1)} \quad ,$$

and hence:

$$L' \geq \sqrt{\frac{d}{28\log_2(D+1)}} \quad .$$

We remove now the assumption $\nu(g_{j_d}) = 0$, at the cost of one extra multiplication:

$$L \geq L' - 1 \geq \sqrt{\frac{d}{28\log_2(D+1)}} - 1 \quad .$$

□

Note: Lemma 1 in [**?**] is slightly more general than Lemma 4 in [**?**]. However, using Lemma 4 in [**?**] it is possible to replace all the appearances of the number 28 in the statement and proof of Lemma 1 above by the number 21.

Proof of Lower Bound 2. Let ν by an extension of ν_2 to the splitting field of p. Let e_1 be the corresponding ramification index, so that $\nu = e_1\nu_2$ on $\mathbb{Q}$. We see from its Netwon diagram that the polynomial p has distinct roots $\zeta_1, \cdots \zeta_d$ with:

$$\nu(\zeta_i) = e_1\left(2^{d(d-i+1)} - 2^{d(d-i)}\right) = e_1 2^{d(d-i)}(2^d - 1) \quad .$$

So we have $\nu(\zeta_d) = e_1(2^d - 1) > 1$, and

$$\nu(\zeta_i)/\nu(\zeta_{i+1}) = 2^d \quad . \tag{5}$$

Assume that there are a, b such that for each d, there is a machine M over $\mathbb{C}$ deciding $p(t) = 0$ in time $T = a(\log d)^b$. Its generic path is defined by a polynomial $g(t)$ of degree $\leq 2^T$.

Let us fix $d > 28(T+1)^3$. In particular $d \geq T+1$. We are in the conditions of Lemma 1, where $D = 2^T$. From that Lemma, it follows that

$$T \geq \sqrt{\frac{d}{28\log_2(2^T+1)}} - 1 \geq \sqrt{\frac{d}{28(T+1)}} - 1 \quad .$$

Hence

$$28(T+1)^3 \geq d \quad ,$$

contradicting our choice of d. □

Equation (5) holds trivially in the proof of Lower bound 1. The rest of the proof is verbatim the same.