Comparison of Complexity over the Real vs. Complex Numbers

Peter Scheiblechner

Department of Mathematics
Purdue University
West Lafayette, IN 47907-2067, USA,
pscheibl@math.purdue.edu

Abstract. We compare complexity questions over the reals with their corresponding versions over the complex numbers. We argue in particular that the problem of deciding membership to a subspace arrangement is strictly harder over $\mathbb{C}$ than over $\mathbb{R}$. There exist decision trees of polynomial depth over $\mathbb{R}$ deciding this problem, whereas certain complex arrangements have no polynomial depth decision trees. This follows from a new lower bound for the decision complexity of a complex algebraic set X in terms of the sum of its (compactly supported) Betti numbers $b_c(X)$, which is for the first time better than logarithmic in $b_c(X)$. On the other hand, the existential theory over $\mathbb{R}$ is strictly harder than that over $\mathbb{C}$. This follows from the observation that the former cannot be solved by a complex BSS-machine.

1 Introduction

1.1 Membership to Subspace Arrangements

This paper consists of two settings, in which we compare the complexity of certain algorithmic problems over the real numbers with that over the complex numbers. In the first setting we study the problem of testing membership of a point to an arrangement of affine linear subspaces of k^n, where k is either $\mathbb{R}$ or $\mathbb{C}$. A famous example of such a problem is the knapsack problem, which is an arrangement of 2^n hyperplanes in k^n. Meyer auf der Heide [MadH84] proved that one can solve the knapsack problem over $\mathbb{R}$ by linear decision trees of polynomial depth. This result is generalized in [Cla87,Mei93] to arbitrary subspace arrangements. More precisely, it is proved that one can decide membership to an arrangement of m subspaces of $\mathbb{R}^n$ by a linear decision tree of depth polynomial in $n \log m$ (see also [BCS97, §3.4]).

It is easy to see by a generic path argument that such a result over $\mathbb{C}$ is impossible [BCSS98,Koi94]. We provide a second proof for this fact by proving a general lower bound for the decision tree complexity of a complex algebraic set X in terms of its (compactly supported) Betti numbers. There is a tradition of lower bounds for the decision complexity in terms of topological invariants [BO83,BLY92,Yao92,BO94,Yao94,LR96], see also the survey [Bür01]. All known lower bounds are *logarithmic*. For instance, the result of [Yao94] bounds the complexity of X by $\Omega(\log b_c(X))$, where $b_c(X)$ denotes the sum of the (compactly supported) Betti numbers of X. Our bound is the first non-logarithmic one. In particular, we prove that the decision tree complexity of an algebraic set X in $\mathbb{C}^n$ is bounded below by $(b_c(X)/m)^{\Omega(\frac{1}{n})}$, where m denotes the number of irreducible components of X. Although this looks like a big improvement, it yields better lower bounds only for quite large Betti numbers. Note that we need $b_c(X)$ to be at least of order $2^{n \log^{1+\varepsilon} n}$ for some $\varepsilon > 0$ to have $b_c(X)^{\frac{1}{n}}$ larger than $\log b_c(X)$. So for instance, our result yields worse lower bounds than Yao's for the element distinctness and k-equality problems. Examples of varieties on which our lower bound performs better are generic hyperplane arrangements or cartesian products of those. We are currently looking for more natural computational problems, where this is the case.

1.2 Existential Theory

The second part of the paper is motivated by the following question. Consider a system

$$f_1 = 0, \ldots, f_r = 0, \quad f_i \in \mathbb{R}[X_1, \ldots, X_n], \tag{1}$$

of *real* polynomial equations. We compare the following two problems:

$\textsc{Feas}_{\mathbb{R}}$: Given $f_1, \ldots, f_r$, decide whether (1) has a *real* solution $x \in \mathbb{R}^n$.

$\mathrm{HN}_{\mathbb{C}}$: Given $f_1, \ldots, f_r$, decide whether (1) has a *complex* solution $x \in \mathbb{C}^n$.

It is proved in [BSS89] that $\textsc{Feas}_{\mathbb{R}}$ is complete for the class $\mathrm{NP}_{\mathbb{R}}$ of languages decidable *nondeterministically* in polynomial time in the BSS-model over $\mathbb{R}$. The second problem $\mathrm{HN}_{\mathbb{C}}$ is the restriction to the reals of the $\mathrm{NP}_{\mathbb{C}}$-complete problem called *Hilbert Nullstellensatz*. The reductions used in these completeness-statements are polynomial time reductions in the BSS-model over $\mathbb{R}$ resp. $\mathbb{C}$.

A simple observation is that $\mathrm{HN}_{\mathbb{C}}$ reduces (over the reals) to $\textsc{Feas}_{\mathbb{R}}$ by replacing the n complex variables by $2n$ real ones and separating the real and complex parts of the equations. Conversely, one might ask whether one can reduce $\textsc{Feas}_{\mathbb{R}}$ to $\mathrm{HN}_{\mathbb{C}}$. We will answer this question negatively. More precisely, there is no (in fact not only polynomial time) reduction from $\textsc{Feas}_{\mathbb{R}}$ to $\mathrm{HN}_{\mathbb{C}}$ in the BSS-model over $\mathbb{R}$ *without order*. The question remains open whether there is one using the order.

2 A Lower Bound over $\mathbb{C}$

An *algebraic decision tree* of degree d over $\mathbb{C}$ is a rooted binary tree, whose inner nodes (*branching nodes*) are labeled with polynomials in $\mathbb{C}[X_1, \ldots, X_n]$ of degree at most d, and whose leaves are labeled with either "yes" or "no". The tree encodes a program that on input $(x_1, \ldots, x_n) \in \mathbb{C}^n$ parses the tree from the root to some leaf by testing at each branching node labeled with f, whether $f(x) = 0$, and continuing to the left or right according to the outcome of the test. The program answers the label of the leaf it reaches. Algebraic decision trees over $\mathbb{R}$ are defined analogously by testing $f \le 0$.

For lower complexity bounds one needs invariants which are subadditive. We use the compactly supported Betti numbers (or equivalently, Borel-Moore Betti numbers). These are defined for a locally closed semialgebraic set X via the cohomology with compact support [Bür01]. We denote by $b_c(X)$ the sum of all compactly supported Betti numbers of X. Our result is based on the fundamental Oleinik-Petrovski/Milnor/Thom-Bound. The following is a version for the compactly supported Betti-numbers which is proved in [Bür01].

Theorem 1. *Let $X = \{f_1 = 0, \ldots, f_r = 0\} \subseteq \mathbb{R}^n$ be an algebraic set defined by the real polynomials f_i of degree at most d. Then $b_c(X) \le d(2d-1)^n$.*

We need it for locally closed sets over the complex numbers.

Corollary 1. *Let X be the locally closed subset of $\mathbb{C}^n$ defined by $f_1 = 0, \ldots, f_r = 0, g_1 \ne 0, \ldots, g_s \ne 0$, where $s \ge 1$ and $f_i, g_j \in \mathbb{C}[X_1, \ldots, X_n]$ have degree at most d. Then $b_c(X) \le (sd+1)(2sd+1)^{2n+2}$.*

For a constructible set $X \subseteq \mathbb{C}^n$ the *degree d decision complexity* $C_d(X)$ is the minimal depth of a degree d algebraic decision tree deciding X. Denote by $\#\mathrm{ic}(X)$ the number of irreducible components of X.

Theorem 2. *Let $X \subseteq \mathbb{C}^n$ be a closed algebraic set. Then*

$$C_d(X) \ge \frac{1}{4d^2} \left(\frac{b_c(X)}{\#\mathrm{ic}(X)} \right)^{\frac{1}{3n+1}}.$$

In the following we sketch the proof of this theorem. Its beginning is analogous to the proof of Yao's lower bound. Let T be a degreee d decision tree of depth k deciding X. For a leave ν denote by D_ν its *leaf set* consisting of those $x \in \mathbb{C}^n$ following the path of T to the leaf ν. We clearly have the decomposition $X = \bigsqcup_{\nu \in \Upsilon} D_\nu$, where $\Upsilon = \{\text{yes-leaves of } T\}$. Furthermore, each leaf set can be written as

$$D_\nu = \{f_1 = 0, \ldots, f_r = 0, g_1 \ne 0, \ldots, g_s \ne 0\}, \quad \text{where} \quad \deg f_i,\ \deg g_i \le d. \tag{2}$$

Note that $s \le k-1$ if $X \ne \mathbb{C}^n$. Using the subadditivity and Corollary 1 we conclude

$$b_c(X) \le \sum_{\nu \in \Upsilon} b_c(D_\nu) \le |\Upsilon| kd(2kd)^{2n+2}. \tag{3}$$

Yao now bounds $|\Upsilon|$ by the number of *all* leaves, which is in our case at most 2^k. The new idea is to improve this to a polynomial bound in k.

First note that each irreducible component Z of X must be contained in a unique $\overline{D}_{\nu(Z)}$. We set $I_1 := \{\nu(Z) \mid Z \text{ component of } X\}$ and $X_1 := \bigcup_{\nu \in \Upsilon \setminus I_1} \overline{D}_\nu$. Then X_1 is a lowerdimensional subvariety of X, and each component Z of X_1 is contained in a unique $\overline{D}_{\nu(Z)}$. We set $I_2 := I_1 \sqcup \{\nu(Z) \mid Z \text{ component of } X_1\}$ and $X_2 := \bigcup_{\nu \in \Upsilon \setminus I_2} \overline{D}_\nu$. Continuing this way we get sequences of subvarieties $X = X_0 \supseteq X_1 \supseteq \cdots \supseteq X_m \supseteq X_{m+1} = \emptyset$ and subsets $\emptyset = I_0 \subseteq I_1 \subseteq \cdots \subseteq I_m \subseteq I_{m+1} = \Upsilon$, where $m = \dim X$. By construction we have $|I_i| \leq \sum_{j<i} \#\mathrm{ic}(X_j)$, hence we are left with the task to bound $\#\mathrm{ic}(X_i)$ or $\deg X_i$. Using (2) and Bézout's Theorem we prove $\deg X_i \leq \deg X (kd)^i$ and conclude $|\Upsilon| \leq \sum_i \#\mathrm{ic}(X_i) \leq \deg X \sum_i (kd)^i \leq 2 \deg X (kd)^m$. Bounding $\deg X \leq \#\mathrm{ic}(X) d^n$, plugging this into (3) and solving for k yields our Theorem.

In order to bound the Betti numbers of subspace arrangements, we collect some well-known facts. We write $b(X)$ for the sum of the singular Betti numbers of a space X. Let $X = \bigcup_i A_i \subseteq \mathbb{R}^n$ be a real subspace arrangement. Its *complexification* is defined to be $X^{\mathbb{C}} := \bigcup_i A_i^{\mathbb{C}}$, where $A_i^{\mathbb{C}} \subseteq \mathbb{C}^n$ is defined by the same equations as A_i. Since the sum of the Betti numbers of the complement of an arrangement depends only on its intersection semilattice, we have $b(\mathbb{R}^n \setminus X) = b(\mathbb{C}^n \setminus X^{\mathbb{C}})$ [Bjö92, §8.3]. Furthermore, Alexander duality in $\mathbb{R}^n$ resp. its Alexandrov compactification $S^n = \mathbb{R}^n \cup \{\infty\}$ implies that for any closed subset $X \subseteq \mathbb{R}^n$ we have $b_c(X) = b(\mathbb{R}^n \setminus X)$.

With these facts it follows from [BCS97, Lemma (11.10)] that $b_c(\mathrm{Dist}_n) \geq n!$, where $\mathrm{Dist}_n = \bigcup_{i<j} \{x_i = x_j\}$ is the element-distinctness problem. Yao's bound shows $C_d(\mathrm{Dist}_n) \geq \Omega(n \log n)$, whereas Theorem 2 only implies $C_d(\mathrm{Dist}_n) \geq \Omega(\sqrt[3]{n})$. For the knapsack problem $\mathrm{KN}_n = \bigcup_{I \subseteq [n]} \left\{\sum_{i \in I} = 1\right\}$, Theorem 2 together with [BCS97, Lemma (11.14)] yields $C_d(\mathrm{KN}_n) \geq 2^{\Omega(n)}$, now better than Yao's quadratic bound. However, a simple generic-path argument implies $C_d(X) \geq \frac{m}{d}$ for a hyperplane arrangement X with m hyperplanes, which also shows the single exponential lower bound for the knapsack problem.

The generic-path arguement does not apply to arrangements of higher codimension. To get such a subspace arrangement with sufficiently large Betti numbers, one can take $\mathrm{KN}_n^2 \subseteq \mathbb{C}^{2n}$, which has codimension 2. Using the Künneth-Theorem one can show $b_c(X \times Y) \geq b_c(X) + b_c(Y)$, hence Theorem 2 implies $C_d(\mathrm{KN}_n^2) \geq 2^{\Omega(2n)}$. However, this lower bound may also be derivable by reducing to the knapsack problem. An interesting problem for our bound would be the following: $\{(X, b) \in \mathbb{C}^{n \times n} \times \mathbb{C}^n \mid \exists e \in \{0,1\}^n \; Xe = b\}$. Unfortunatley, at present we don't know a bound for the Betti numbers of this arrangement.

3 Real Parts

For a complexity class $\mathcal{C}$ of languages in $\mathbb{C}^\infty$ define its *real part* as $\mathbb{R}\mathrm{P}(\mathcal{C}) := \{A \cap \mathbb{R}^\infty \mid A \in \mathcal{C}\}$.

Proposition 1. *We have* $\mathbb{R}\mathrm{P}(\mathrm{P}_{\mathbb{C}}) = \mathrm{P}_{\mathbb{R}}^{=}$ *and* $\mathbb{R}\mathrm{P}(\mathrm{NP}_{\mathbb{C}}) \subseteq \mathrm{NP}_{\mathbb{R}}^{=} = \mathrm{NP}_{\mathbb{R}}$.

This proposition is proved as follows. One sees $\mathbb{R}\mathrm{P}(\mathrm{P}_{\mathbb{C}}) \subseteq \mathrm{P}_{\mathbb{R}}^{=}$ by simulating a complex machine by a real =-machine. For the reverse inclusion, view a real =-machine as a complex machine and ensure by clocking a polynomial running time on all complex inputs. The second inclusion of Proposition 1 follows from the first. Finally, $\mathrm{NP}_{\mathbb{R}} = \mathrm{NP}_{\mathbb{R}}^{=}$ follows from the observation that $\mathrm{F{\scriptsize EAS}}_{\mathbb{R}}$ is $\mathrm{NP}_{\mathbb{R}}$-complete also for polynomial =-reductions, and $\mathrm{NP}_{\mathbb{R}}^{=}$ is closed under those.

We call a subset $S \subseteq \mathbb{R}^n$ *constructible*, iff S can be defined by a quantifier-free first-order formula whose atoms are of the form $f = 0$ or $f \neq 0$ with a polynomial f. We need the following result of [CR93].

Theorem 3. *If* $A \subseteq \mathbb{R}^\infty$ *is decidable by a =-machine, then* $A \cap \mathbb{R}^n$ *is constructible for all* $n \in \mathbb{N}$.

Observe that $\mathrm{F{\scriptsize EAS}}_{\mathbb{R}}$ is not decidable, since $\{(a,b,c) \in \mathbb{R}^3 \mid b^2 - 4ac \geq 0\}$ is not constructible. Theorem 3 implies

Theorem 4. *We have* $\mathbb{R}\mathrm{P}(\mathrm{P}_{\mathbb{C}}) \subseteq \mathbb{R}\mathrm{P}(\mathrm{NP}_{\mathbb{C}}) \subsetneq \mathrm{NP}_{\mathbb{R}}^{=}$.

Note that for this separation one can also use the language $\{x_1 > 0\}$. It also follows from [MMD83]. To answer the question of the introduction, we remark that there can be no polynomial time =-reduction of $\textsc{Feas}_{\mathbb{R}}$ to $\mathrm{HN}_{\mathbb{C}}$, since $\mathbb{R}\mathrm{P}(\mathrm{NP}_{\mathbb{C}})$ is closed under those reductions.

It is interesting that $\mathrm{NP}_{\mathbb{R}}^{=}$ contains undecidable languages, and also that in the presence of an existential quantifier the destinction between full and =-machines disappears. These remarks extend to the higher levels of the polynomial hierarchy. We pose the following questions:

1. We have the following transfer result: $\mathrm{P}_{\mathbb{C}} = \mathrm{NP}_{\mathbb{C}} \Rightarrow \mathrm{P}_{\mathbb{R}}^{=} = \mathbb{R}\mathrm{P}(\mathrm{NP}_{\mathbb{C}})$. Does the other direction hold?
2. We only have $\mathbb{R}\mathrm{P}(\mathrm{NP}_{\mathbb{C}}) \neq \mathrm{NP}_{\mathbb{R}}^{=}$ for a silly reason. Is there a natural class of problems $\mathcal{C}$ such that $\mathbb{R}\mathrm{P}(\mathrm{NP}_{\mathbb{C}}) = \mathrm{NP}_{\mathbb{R}}^{=} \cap \mathcal{C}$? Maybe the class of decidable languages?
3. Does the order help in deciding $\mathrm{HN}_{\mathbb{C}}$? In other words, is $\mathbb{R}\mathrm{P}(\mathrm{NP}_{\mathbb{C}}) \subseteq \mathrm{P}_{\mathbb{R}}$? Note that the reverse inclusion does not hold: $\{x_1 > 0\} \in \mathrm{P}_{\mathbb{R}} \setminus \mathbb{R}\mathrm{P}(\mathrm{NP}_{\mathbb{C}})$.

Acknowledgements

Peter Scheiblechner is supported by DFG grant SCHE 1639/1-1. The author would like to thank the anonymous referees for valuable comments.

References

[BCS97] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1997.

[BCSS98] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer, 1998.

[Bjö92] A. Björner. Subspace arrangements. In *Proc. of 1st European Congress of Mathematics*, pages 321–370, Paris, 1992, 1992. Birkhäuser.

[BLY92] A. Björner, L. Lovász, and A. Yao. Linear decision trees: volume estimates and topological bounds. In *STOC '92: Proceedings of the twenty-fourth annual ACM symposium on Theory of computing*, pages 170–177, New York, NY, USA, 1992. ACM.

[BO83] M. Ben-Or. Lower bounds for algebraic computation trees. In *STOC '83: Proceedings of the fifteenth annual ACM symposium on Theory of computing*, pages 80–86, New York, NY, USA, 1983. ACM.

[BO94] M. Ben-Or. Algebraic computation trees in characteristic $p > 0$. In *FOCS '94: Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 534–539, Washington, DC, USA, 1994. IEEE Computer Society.

[BSS89] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers. *Bull. Amer. Math. Soc.*, 21:1–46, 1989.

[Bür01] Peter Bürgisser. Lower bounds and real algebraic geometry. In *Algorithmic and Quantitative Aspects of Real Algebraic Geometry in Mathematics and Computer Science*, pages 35–54, 2001.

[Cla87] K. L. Clarkson. New applications of random sampling in computational geometry. *Discrete Comput. Geom.*, 2:195–222, 1987.

[CR93] Felipe Cucker and Francesc Rosselló. Recursiveness over the complex numbers is time-bounded. In *Proceedings of the 13th Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 260–267, London, UK, 1993. Springer-Verlag.

[Koi94] P. Koiran. Computing over the reals with addition and order. In *Selected papers of the workshop on Continuous algorithms and complexity*, pages 35–47, New York, NY, USA, 1994. Elsevier Science Inc.

[LR96] T. Lickteig and M.M. Roy. Semi-algebraic complexity of quotients and sign determination of remainders. *J. Compl.*, 12(4):545–571, 1996.

[MadH84] F. Meyer auf der Heide. A polynomial linear search algorithm for the n-dimensional knapsack problem. *J. ACM*, 31(3):668–676, 1984.

[Mei93] S. Meiser. Point location in arrangements of hyperplanes. *Inf. Comput.*, 106(2):286–303, 1993.

[MMD83] A. Macintyre, K. McKenna, and L. van den Dries. Elimination of quantifiers in algebraic structures. *Advances in Mathematics*, 47:74–87, 1983.

[Yao92] A. Yao. Algebraic decision trees and Euler characteristics. In *FOCS '92: Proceedings of the 33rd Annual Symposium on Foundations of Computer Science*, pages 268–277, Washington, DC, USA, 1992. IEEE Computer Society.

[Yao94] A. Yao. Decision tree complexity and Betti numbers. In *STOC '94: Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 615–624, New York, NY, USA, 1994. ACM.