

Scheme-theoretic Approach to Computational Complexity II. The Separation of \mathbf{P} and \mathbf{NP} over \mathbb{C} , \mathbb{R} , and \mathbb{Z}

Ali Cıvril*

September 20, 2021

1 Introduction

The BCSS model of computation [1] extends the classical computational complexity theory to arbitrary fields/rings, in particular to \mathbb{C} , \mathbb{R} , and \mathbb{Z} , posing the conjectures $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$, $\mathbf{P}_{\mathbb{R}} \neq \mathbf{NP}_{\mathbb{R}}$, and $\mathbf{P}_{\mathbb{Z}} \neq \mathbf{NP}_{\mathbb{Z}}$. Here the machine is assumed to work with equality comparisons over \mathbb{C} , and inequality comparisons over \mathbb{R} and \mathbb{Z} . In the case of \mathbb{Z} , the bit cost model is assumed. The purpose of this paper is to show that the theory presented in the first paper of the series [3] naturally extends to these cases, answering the open questions raised in [1]. We first note that the separation of \mathbf{P} and $\mathbf{NP/poly}$, as proved in [3], already implies $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$ (see the introduction of [2] for relevant references). In this paper we make the separation over \mathbb{C} explicit, and also settle the case for \mathbb{R} and \mathbb{Z} :

Theorem 1. *The problem of determining the feasibility of a set of quadratic equations (over \mathbb{C} , \mathbb{R} , and \mathbb{Z}) with n variables requires at least $2^{n/3}$ operations in the BCSS model of computation.*

2 Preliminaries

We denote the underlying field/ring by $k = \mathbb{C}$, \mathbb{R} , or \mathbb{Z} . For \mathbb{R} and \mathbb{Z} , the scheme representing the computational problem of interest will be defined over the algebraic closure of \mathbb{R} , which is \mathbb{C} . We consider the problem QUAD whose instances are polynomial systems over k consisting of quadratic equations. The equations of a given instance are assumed to have a common solution in k^n , where n is the number of variables. QUAD is NP-complete over \mathbb{C} and \mathbb{R} as proved in [1], which also shows NP-completeness over \mathbb{Z} with the extra requirement that the norm of any point in the solution set is bounded.

We will define the *amplifying functor* from QUAD to the category of schemes over \mathbb{C} . It is a subfunctor of the Hilbert functor, which is representable by a projective scheme over \mathbb{C} by the following result.

Theorem 2 ([4]). *Let X be a projective scheme over \mathbb{C} . Then for every polynomial $P \in \mathbb{Q}[x]$, there exists a projective scheme $\text{Hilb}^P(X)$ over \mathbb{C} , which represents the functor $\mathcal{H}^P(X)$. Furthermore, the Hilbert functor $\mathcal{H}(X)$ is represented by the Hilbert scheme*

$$\text{Hilb}(X) := \coprod_{P \in \mathbb{Q}[x]} \text{Hilb}^P(X).$$

*Istinye University, Computer Engineering Department, Zeytinburnu, Istanbul 34010 Turkey, e-mail: ali.civril@enr.istinye.edu.tr

We consider $X = \mathbb{P}_{\mathbb{C}}^n$. In this case, the connectedness of the Hilbert scheme for a fixed Hilbert polynomial P was established by Hartshorne [5]. Note first that given a homogenized polynomial ϕ , one might consider the closed subscheme

$$\text{Proj } \mathbb{C}[x_0, x_1, \dots, x_n]/(\phi(x_0, x_1, \dots, x_n)),$$

so that each polynomial equation and hence a polynomial system identifies a closed subscheme of $\mathbb{P}_{\mathbb{C}}^n$ via the corresponding ideal. In particular, we refer to the Hilbert polynomial of an instance.

Given an instance of QUAD, a non-empty subset of the equations of the corresponding polynomial system is said to form a *sub-instance* of QUAD. As in an instance, a sub-instance also has a corresponding polynomial system induced by the polynomial equations it contains. Two sub-instances are called *disjoint* if both do not belong to a single instance of QUAD. A *sub-problem* of QUAD is a computational problem induced by a subset of the disjoint sub-instances of QUAD. A sub-problem Λ of QUAD is called a *simple sub-problem* if the polynomial systems of Λ have the same solution set and the same Hilbert polynomial. Given two sub-instances I_1 and I_2 of Π defined via the same variable set $\{x_i\}_{i \in I}$, I_2 is said to be a *variant* of I_1 if it can be obtained from I_1 by replacing each x_i in a subset of I by $c_i - x_i$ in its equations for some $c_i \in k \setminus \{0\}$, followed by a permutation of the variables. Two sub-instances of QUAD are said to be *distinct* if they are not variants of each other, so that distinct sub-instances of Π correspond to distinct points in moduli. A simple sub-problem Λ of Π is said to be *homogeneous* if the following two conditions hold.

- The instances of Λ are pair-wise distinct.
- None of the instances of Λ can be expressed as the Cartesian product of r sets of sub-instances of Λ defined via disjoint sets of variables, for some $r \geq 2$.

We now give a partial definition of the amplifying functor, which we denote by \mathcal{A} . Let Λ be a homogeneous simple sub-problem of QUAD consisting of a set of polynomial systems $\{P_i\}_{i=1}^{\ell}$ defined via the variables $x_{\lambda_1}, \dots, x_{\lambda_m}$. Let ϕ_{ij} be the homogenized j -th polynomial in the polynomial system P_i . Define

$$X_i = \text{Proj } \mathbb{C}[x_0, x_{\lambda_1}, \dots, x_{\lambda_m}]/(\phi_{i1}, \dots, \phi_{i|P_i|}),$$

$$\mathcal{A}(\Lambda) = \{X_i | i = 1, \dots, \ell\}.$$

We define the product of computational problems in the usual sense, i.e. the set of instances of the product is the Cartesian product of the sets of instances of the problems. Given a sub-problem $\Gamma = \prod_{i=1}^r \Lambda_i$ of Π , for some $r \geq 1$, where Λ_i are homogeneous simple sub-problems of Π defined via disjoint sets of variables, we set

$$\mathcal{A}(\Gamma) = \prod_{i=1}^r \mathcal{A}(\Lambda_i),$$

and

$$\mathcal{A}(\Pi) := \coprod_{\Gamma} \mathcal{A}(\Gamma).$$

By the connectedness of the Hilbert scheme for a fixed Hilbert polynomial, we have that there is a functor \mathcal{B} , which is an extension of \mathcal{A} , such that a homogeneous simple sub-problem always maps to a connected scheme via \mathcal{B} . Thus, we extend \mathcal{A} to \mathcal{B} , overriding the definition of the amplifying functor.

We define $\tau(\text{QUAD})$ to be the minimum number of *deterministic* operations required to solve QUAD. Given a homogeneous simple sub-problem Λ of QUAD, we denote the number of instances of Λ by $b(\Lambda)$. A sub-problem Γ is called a *normal sub-problem* if $\Gamma = \prod_{i=1}^r \Lambda_i$, for some $r \geq 1$,

where Λ_i are homogeneous simple sub-problems defined via disjoint sets of variables. Over all such normal sub-problems Γ , let $\kappa(\text{QUAD})$ denote the maximum value of $\sum_{i=1}^r b(\Lambda_i)$. The proof of the following result is omitted, as the only change from the Fundamental Lemma of [3] is the underlying field/ring. The proof is oblivious to the method of comparison used by the machine (equality or inequality). It essentially uses the fact that a sub-problem with a single instance has non-zero complexity, which obviously holds for any type of machine.

Lemma 3. $\tau(\text{QUAD}) \geq \kappa(\text{QUAD})$.

3 Proof of Theorem 1

We inductively construct a homogeneous simple sub-problem Λ of QUAD with 2^r instances, each having $3r$ variables and $4r$ equations, for $r \geq 1$. The result follows by Lemma 3 and the definition of κ .

For $r = 1$, consider first the instance with the following equations:

$$\begin{aligned} (x_1 - 1)(x_2 - 1) &= 0, \\ x_1 x_3 &= 0, \\ x_2 x_3 &= 0, \\ x_1^2 - x_3^2 &= 0. \end{aligned}$$

The first equation implies that at least one of x_1 and x_2 is 1, so that $x_3 = 0$ by the second and the third equations. Given these and the fourth equation, we have the following solution set: $\{(0, 1, 0)\}$. Note that it has integer coordinates and bounded norm, a property that will be extended to the general case. The following are the equations of another instance.

$$\begin{aligned} (x_1 - 1)(x_2 - 1) &= 0, \\ x_1 x_3 &= 0, \\ x_2 x_3 &= 0, \\ x_2^2 - x_3 &= 0. \end{aligned}$$

By a similar argument, it has the solution set $\{(1, 0, 0)\}$. Thus, both of the instances have the same constant Hilbert polynomial 1, resulting in a homogeneous simple sub-problem with 2 instances. Assume now the induction hypothesis for some $r \geq 1$. In the inductive step, we introduce 3 new variables $x_{3r+1}, x_{3r+2}, x_{3r+3}$, and 2 new blocks of equations on these variables each consisting of 4 equations in the exact form of the two instances given above. Appending these equations to each of the 2^r instances of the induction hypothesis, we obtain 2^{r+1} instances, which form a simple sub-problem. We make Λ into a homogeneous simple sub-problem as follows. Given an instance, consider the graph whose nodes are the equations of the instance, and there is an edge between two nodes if they share a common variable. We impose that this graph be connected for all the instances, which is clearly satisfied in the base case $r = 1$. For the inductive step, replace the positive literal x_{3r} , where it appears in the fourth equation of its block, by the positive literal x_{3r+3} . This operation does not change the solution set and hence the Hilbert polynomial, as x_{3r} is already forced to be 0 for all r by the other equations. It also ensures connectivity of the graph across all the blocks including the newly introduced one, thus constructing a homogeneous simple sub-problem, completing the induction and the proof.

We have the following by Theorem 1 and the NP-completeness of QUAD over \mathbb{C} , \mathbb{R} , and \mathbb{Z} .

Corollary 4. $P_{\mathbb{C}} \neq \text{NP}_{\mathbb{C}}$.

Corollary 5. $P_{\mathbb{R}} \neq \text{NP}_{\mathbb{R}}$.

Corollary 6. $P_{\mathbb{Z}} \neq \text{NP}_{\mathbb{Z}}$.

References

- [1] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer-Verlag, 1997.
- [2] P. Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*, volume 7 of *Algorithms and Computation in Mathematics*. Springer, 2000.
- [3] A. Çivril. Scheme-theoretic approach to computational complexity I. The separation of P and NP. manuscript.
- [4] A. Grothendieck. *Fondements de la Géométrie Algébrique [Extraits du Séminaire Bourbaki 1957-1962]*, chapter Techniques de construction et théorèmes d'existence en géométrie algébrique. IV. Les schémas de Hilbert. *Secr. Math.*, 1962.
- [5] R. Hartshorne. Connectedness of the Hilbert scheme. *Publications Mathématiques de l'IHÉS*, 29:5–48, 1966.