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

Ali Çivril*

May 10, 2023

Abstract

We show that the problem of determining the feasibility of quadratic systems over $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Z}$ requires exponential time. This separates $P$ and $NP$ over these fields/rings in the BCSS model of computation.

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 $P_{\mathbb{C}} \neq NP_{\mathbb{C}}$, $P_{\mathbb{R}} \neq NP_{\mathbb{R}}$, and $P_{\mathbb{Z}} \neq NP_{\mathbb{Z}}$. 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 $P$ and $NP/poly$, as proved in [3], already implies $P_{\mathbb{C}} \neq NP_{\mathbb{C}}$ (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. There exist infinitely many $n \in \mathbb{Z}^+$ such that for any constant $\epsilon > 0$, 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 $2^{\left(\frac{1}{3} - \epsilon\right)n}$ deterministic 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 do not repeat the definitions related to the Hilbert functor and the amplifying functor, which can be found in Section 2 of [3]. The only difference in the current paper is the underlying field, which is $\mathbb{C}$ instead of $\mathbb{F}_2$.

* Atlas University, Computer Engineering Department, Kagithane, Istanbul Turkey, e-mail: ali.civril@atlas.edu.tr, website: www.alicivril.com
All the following definitions are with regard to QUAD. A computational problem defined via a non-empty subset of the instances of QUAD is called a sub-problem. A sub-problem \( \Lambda \) is called a simple sub-problem if the instances of \( \Lambda \) have the same Hilbert polynomial. Two instances with distinct solution sets are said to be distinct. Two distinct instances are said to be disparate if one is not a subset of another. In this case we also say that one instance is disparate from the other.

Given two instances \( I_1 \) and \( I_2 \), a computational procedure transforming \( I_1 \) to \( I_2 \) is called a unit instance operation. If \( I_1 \) and \( I_2 \) are defined via the variable set \( S = \{x_1, \ldots, x_n\} \), \( I_2 \) is said to be a variant of \( I_1 \) if there is a unit instance operation from \( I_1 \) to \( I_2 \) performing the following: It replaces all \( x_i \) in a subset of \( S \) with \( 1 - x_i \) followed by a permutation of \( S \). In this case we also say that \( I_1 \) and \( I_2 \) are variants of each other. Two unit instance operations are said to be distinct if they result in distinct instances when applied on the same instance. They are said to be disparate if they are distinct and one is not a subset of another.

A sub-problem \( \Lambda \) whose instances are defined via the variable set \( S = \{x_1, \ldots, x_n\} \), is said to be homogeneous if the following three conditions hold: (1) All the variables in \( S \) appear in each instance of \( \Lambda \). (2) The instances of \( \Lambda \) are pair-wise disparate. (3) None of the instances of \( \Lambda \) is a variant of another. A sub-problem \( \Lambda \) is said to be prime if the unit instance operations between all pairs of its instances are pair-wise disparate.

We define \( \tau(\text{QUAD}) \) to be the minimum number of deterministic operations required to solve QUAD. Given a prime homogeneous simple sub-problem \( \Lambda \), we denote the number of instances of \( \Lambda \) by \( b(\Lambda) \). Over all such sub-problems \( \Lambda \), we denote by \( \kappa(\text{QUAD}) \) the maximum value of \( b(\Lambda) \).

The proof of the following result is omitted, as the only change from the Fundamental Lemma of [3] is the underlying field. The proof is oblivious to the method of comparison used by the machine (equality or inequality). It essentially uses the fact that the complexity of a non-trivial reduction is non-zero, which obviously holds for any type of machine.

**Lemma 2** (Fundamental Lemma). \( \tau(\text{QUAD}) \geq \kappa(\text{QUAD}) \).

### 3 Proof of Theorem [1]

The following theorem implies Theorem [1] by Lemma [2]

**Theorem 3.** There exist infinitely many \( n \in \mathbb{Z}^+ \) such that for any constant \( \epsilon > 0 \), we have

\[
\kappa(\text{QUAD}) \geq 2^{\left(\frac{4}{3} - \epsilon\right)n},
\]

where \( n \) is the number of variables in the QUAD instance.

**Proof.** We construct a prime homogeneous simple sub-problem \( \Lambda \) with \( \binom{r}{2} \) instances, each having \( 3r \) variables and \( 4r \) equations, for \( r \geq 1 \). The result follows by Lemma [2] and the definition of \( \kappa \).

For \( r = 1 \), consider first the instance with the following equations:

\[
\begin{align*}
(x_1 - 1)(x_2 - 1) &= 0, \\
x_1x_3 &= 0, \\
x_2x_3 &= 0, \\
x_1^2 - x_3^2 &= 0.
\end{align*}
\]

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
Table 1: Modification to form a prime sub-problem on block sequence I-I

| Equation | Instance 1 | Instance 1 |
|----------|------------|------------|
| 1        | \((x_1 - 1)(x_2 - 1) = 0\) | \((x_4 - 1)(x_5 - 1) = 0\) |
| 2        | \((x_4 + x_5 - 1)x_3 = 0\) | \((x_1 + x_2 - 1)x_6 = 0\) |
| 3        | \(x_2x_3 = 0\) | \(x_5x_6 = 0\) |
| 4        | \(x_1^2 - x_3^2 = 0\) | \(x_5^2 - x_6 = 0\) |

Table 2: Modification to form a prime sub-problem on block sequence I-II

| Equation | Instance 2 | Instance 2 |
|----------|------------|------------|
| 1        | \((x_1 - 1)(x_2 - 1) = 0\) | \((x_4 - 1)(x_5 - 1) = 0\) |
| 2        | \(x_1x_3 = 0\) | \(x_4x_6 = 0\) |
| 3        | \((x_4 + x_6 - 1)x_3 = 0\) | \((x_1 + x_3 - 1)x_6 = 0\) |
| 4        | \(x_1^2 - x_3^2 = 0\) | \(x_5^2 - x_6 = 0\) |

Table 3: Modification to form a prime sub-problem on block sequence II-II

| Equation | Instance 2 | Instance 2 |
|----------|------------|------------|
| 1        | \((x_1 - 1)(x_2 - 1) = 0\) | \((x_4 - 1)(x_5 - 1) = 0\) |
| 2        | \(x_1x_3 = 0\) | \(x_4x_6 = 0\) |
| 3        | \((x_4 + x_6 - 1)x_3 = 0\) | \((x_1 + x_3 - 1)x_6 = 0\) |
| 4        | \(x_1^2 - x_3^2 = 0\) | \(x_5^2 - x_6 = 0\) |

The following are the equations of another instance.

\[
\begin{align*}
(x_1 - 1)(x_2 - 1) &= 0, \\
x_1x_3 &= 0, \\
x_2x_3 &= 0, \\
x_1^2 - x_3^2 &= 0.
\end{align*}
\]

By a similar argument, it has the solution set \{\((1, 0, 0)\)\}. Thus, both of the instances have the same constant Hilbert polynomial 1. Note also that they are disparate from and not variants of each other. This results in a homogeneous simple sub-problem with 2 instances. Assume now the induction hypothesis that there exists a homogeneous simple sub-problem of size 2\(r\), 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 homogeneous simple sub-problem. Next, we describe how to make \(\Lambda\) into a prime homogeneous simple sub-problem.

For simplicity, we describe the procedure for \(r = 2\). The construction is easily extended to the general case. Suppose that the first block is defined via Instance 1. We perform the following operation: If the second block is defined via Instance 1, replace Equation 2 of the first block with \((x_4 + x_5 - 1)x_3 = 0\). If the second block is defined via Instance 2, replace it with \((x_4 + x_6 - 1)x_3 = 0\). In extending this to the general case, the second block is generalized as the next block to the current one, and the variables used for replacement are the ones of the next block with increasing indices, respectively corresponding to \(x_4, x_5\) and \(x_6\). If the first block is defined via Instance 2, we perform
Table 4: Modification to form a prime sub-problem on block sequence II-I

| Equation | Instance 2 | Instance 1 |
|----------|------------|------------|
| 1        | \((x_1 - 1)(x_2 - 1) = 0\) | \((x_4 - 1)(x_5 - 1) = 0\) |
| 2        | \(x_1x_3 = 0\) | \((x_4 + x_3 - 1)x_6 = 0\) |
| 3        | \((x_4 + x_5 - 1)x_3 = 0\) | \(x_5x_6 = 0\) |
| 4        | \(x_1^2 - x_3^2 = 0\) | \(x_5^2 - x_6 = 0\) |

the same operations, but this time considering Equation 3 of the first block. As a final step in the general case, we perform this operation for the last block indexed \(r\) for which the next block is defined as the first block. Thus, the operations complete a cycle over the blocks. All the cases are illustrated in Table 1, Table 2, where the interchanged variables are shown in bold. Upon these operations, a specific equation of each block depending on its type contains variables belonging to the next block in a way distinguished by the type of the next block. Since the problem is homogeneous, a unit instance operation between instances can only be via the mixed clauses. This ensures that we have a prime sub-problem.

We next select a simple sub-problem of the constructed homogeneous prime sub-problem. Observe the following on the first block, which extends to all the other blocks by the construction. Suppose it is defined via Instance 1 and \(x_3 = \alpha\) for some \(\alpha \neq 0\). This implies \(x_2 = 0\), so that by the first equation \(x_1 = 1\) and \(\alpha \in \{-1, 1\}\). The solution set is then \{(1, 0, 1)\} \cup \{(1, 0, -1)\}. If it is defined via Instance 2 and \(x_3 = \alpha\) for some \(\alpha \neq 0\), we get \(x_1 = 0\), so that by the first equation \(x_2 = 1\) and \(\alpha = 1\). The solution set is then \{(0, 1, 1)\}. Observe next that the replaced equations are satisfiable. Assume \(x_3 \neq 0\). If the second block is defined via Instance 1, then \(x_4 + x_5 - 1 = 0\) by the solution set associated to this instance, which is \{(0, 1, 0)\} \cup \{(1, 0, 1)\} \cup \{(1, 0, -1)\}. Similarly, if the second block is defined via Instance 2, we have \(x_4 + x_6 - 1 = 0\) by the associated solution set, which is \{(1, 0, 0)\} \cup \{(0, 1, 1)\}.

Recall that for \(x_3 = 0\), Instance 1 and Instance 2 had solutions implying the same Hilbert polynomial. Note however that the solution sets associated to Instance 1 and Instance 2 for \(x_3 \neq 0\) have distinct Hilbert polynomials. In order to make the Hilbert polynomials of the constructed instances uniform, we impose that the number of blocks associated to Instance 1 is equal to that of Instance 2. There are \(\binom{r}{r/2}\) such blocks out of \(2^r\). Using the Stirling approximation, we have for all \(\epsilon > 0\),

\[
\binom{r}{r/2} > 2^{(1-\epsilon)r},
\]

as \(r\) tends to infinity. Since \(r = n/3\), the proof is completed.

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

**Corollary 4.** \(P_C \neq NP_C\).

**Corollary 5.** \(P_R \neq NP_R\).

**Corollary 6.** \(P_Z \neq NP_Z\).

**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. *arXiv e-prints*, page arXiv:2107.07386, 2021.