Algebrization: A New Barrier in Complexity Theory

Scott Aaronson* MIT

Avi Wigderson† Institute for Advanced Study

Abstract

Any proof of $\mathsf{P} \neq \mathsf{NP}$ will have to overcome two barriers: *relativization* and *natural proofs*. Yet over the last decade, we have seen circuit lower bounds (for example, that PP does not have linear-size circuits) that overcome both barriers simultaneously. So the question arises of whether there is a third barrier to progress on the central questions in complexity theory.

In this paper we present such a barrier, which we call *algebraic relativization* or *algebrization*. The idea is that, when we relativize some complexity class inclusion, we should give the simulating machine access not only to an oracle A, but also to a low-degree extension of A over a finite field or ring.

We systematically go through basic results and open problems in complexity theory to delineate the power of the new algebrization barrier. First, we show that all known non-relativizing results based on arithmetization—both inclusions such as $\mathsf{IP} = \mathsf{PSPACE}$ and $\mathsf{MIP} = \mathsf{NEXP}$, and separations such as $\mathsf{MA_{EXP}} \not\subset \mathsf{P/poly}$ —do indeed algebrize. Second, we show that almost all of the major open problems—including P versus NP, P versus RP, and NEXP versus $\mathsf{P/poly}$—will require *non-algebrizing techniques*. In some cases algebrization seems to explain exactly why progress stopped where it did: for example, why we have superlinear circuit lower bounds for $\mathsf{PromiseMA}$ but not for NP.

Our second set of results follows from lower bounds in a new model of *algebraic query complexity*, which we introduce in this paper and which is interesting in its own right. Some of our lower bounds use direct combinatorial and algebraic arguments, while others stem from a surprising connection between our model and communication complexity. Using this connection, we are also able to give an MA-protocol for the Inner Product function with $O(\sqrt{n}\log n)$ communication (essentially matching a lower bound of Klauck), as well as a communication complexity conjecture whose truth would imply $\mathsf{NL} \neq \mathsf{NP}$.

1 Introduction

In the history of the P versus NP problem, there were two occasions when researchers stepped back, identified some property of almost all the techniques that had been tried up to that point, and then proved that *no technique with that property could possibly work.* These "meta-discoveries" constitute an important part of what we understand about the P versus NP problem beyond what was understood in 1971.

The first meta-discovery was *relativization*. In 1975, Baker, Gill, and Solovay [5] showed that techniques borrowed from logic and computability theory, such as diagonalization, cannot be powerful enough to resolve P versus NP. For these techniques would work equally well in a

*Email: aaronson@csail.mit.edu.

†Email: avi@ias.edu.