Will we one day be able to prove lower-bounds?

Bruno Loff

Faculty of Sciences of the University of Lisbon
E-mail: bruno.loff@gmail.com

Sobre o orador: Bruno Loff is a researcher in Computational Complexity. Broadly speaking, his research tackles the in the problem of proving lower-bounds, i.e., impossibility results of the form ”no algorithm A can solve problem X without spending more than R resources”.

He completed his PhD in 2014 at CWI, in Amsterdam, under Harry Buhrman. His PhD thesis was entitled ”A medley for Computational Complexity”. He was a postdoctoral researcher at Charles University, in Prague, in the group of Michal Koucký. He moved to Porto in 2017 where he would work for 6 years, first as a postdoc, and then as an assistant professor.

He is currently an associate professor at the Faculty of Sciences of the University of Lisbon, an integrated researcher of LASIGE, and the Principal Investigator of the ERC project HoFGA - The Hardness of Finding Good Algorithms.

In this project we are interested in answering the question, which has a deep connection with the problem of proving lower-bounds: in what settings, and to what extent, can we automate the task of finding an efficient algorithm for a given problem.

Sumário

Turing, or perhaps Church, first showed that there exists no algorithm for deciding whether a given mathematical statement is provable. But of course, one can decide if a given statement has a proof of length $\leq n$ by enumerating all proofs. This algorithm runs in time exponential in n. Gödel was the first to ask whether there exists an efficient ($n^{O(1)}$-time) algorithm for this problem. I.e., can mathematics be mechanized? This is question is currently known as the P vs. NP problem.

Let's suppose that there is no such algorithm. How can we prove this? Such a negative result is called a *lower-bound*, since we are in effect asking for a lower-bound on the computational complexity of some task.

It turns out that this question is somewhat self referential. Maybe if there exists no algorithm for finding proofs, this somehow implies that a proof of this statement is hard to find, maybe it is even independent? The natural proofs barrier of Razborov and Rudich, a classical result in computational complexity from the 1990s, is the best formal statement that approximates such an independence result, and it is not well

known outside of the field. So I will spend half of the talk, maybe a little more, trying to explain what it says.

Then I will discuss some ways how one might circumvent this barrier. I will discuss one particular approach, via convex geometry and duality. I will then report on two *failed* attempts using such an approach, one of which is technical, and will be glossed over, but the other has a fun, simple statement as a puzzle about the difference between classical and quantum physics.