A Tutorial on the Likely Worst-Case Complexities of NP-Complete Problems

Russell Impagliazzo

Abstract

The P vs. NP problem has sometimes been unofficially paraphrased as asking whether it is possible to improve on exhaustive search for such problems as Satisfiability, Clique, Graph Coloring, etc. However, known algorithms for each of these problems indeed are substantially better than exhaustive search, if still exponential. Furthermore, although a polynomial-time algorithm for any one of these problems implies one for all of them, these improved exponential algorithms are highly specific, and it is unclear what the limit of improvement should be.

In the past 15 years or so, a complexity theory for exponential complexities has emerged. Fundamental to this theory are two related hypotheses: the Exponential Time Hypothesis, that each \( k \)-SAT problem requires time \( 2^{c_k n} \) for \( 0 < c_k < 1 \), and the Strong Exponential Time Hypothesis, that these constants tend towards 1 as \( k \) grows. Like the Unique Games Conjecture for approximation algorithms, there is no consensus on whether these hypotheses are true or false. However, also like UGC, there are many consequences both of their truth and of their falsity. Either way gives a unified picture of the complexities of many NP-complete problems. Furthermore, recent work has shown that ETH and SETH have implications beyond exponential time algorithms, to parameterized complexity, cryptography, data structures, and to the question of whether fundamental polynomial-time algorithms can be further improved.

In this talk, I will discuss these hypotheses and their implications for complexity. We’ll see how they can be used to get results about which problems in NP might require exponential time, give evidence that some NP-complete problems are strictly harder than others, and characterize the hard instances of NP-complete problems. We’ll touch on recent work by Williams giving relationships between improved algorithms and circuit lower bounds. We’ll show how to translate results from the exponential realm to reason that certain polynomial time algorithms are unlikely to be improveable.

This is a survey of many results, only a fraction of which I am involved with, so I won’t give a complete list of references. However, my work on this subject is joint with Ramamohan Paturi and our students, Francis Zane, Chris Calabro and William Matthews.