On the Complexity of Circuit Satisfiability

Ramamohan Paturi
University of California, San Diego
Email:paturi@cs.ucsd.edu

December 1, 2009

Abstract

In this paper, we are concerned with the exponential complexity of the *Circuit Satisfiability* (**CircuitSat**) problem and more generally with the exponential complexity of **NP**-complete problems. Over the past 15 years or so, researchers have obtained a number of exponential-time algorithms with improved running times for exactly solving a variety of **NP**-complete problems. The improvements are typically in the form of better exponents compared to exhaustive search. Our goal is to develop techniques to prove specific lower bounds on the exponents under plausible complexity assumptions. We consider natural, though restricted, algorithmic paradigms and prove lower bounds on the exponent of the success probability. Our approach has the advantage of clarifying the relative power of various algorithmic paradigms.

Our main technique is a a success probability amplification technique, called *the Exponential Amplification Lemma*, which shows that for any $f(n, m)$-size bounded probabilistic circuit family $\mathcal{A}$ that decides **CircuitSat** with success probability at least $2^{-\alpha n}$ for $\alpha < 1$ on inputs which are circuits of size m with n variables, there is another probabilistic circuit family $\mathcal{B}$ that decides **CircuitSat** with size roughly $f(\alpha n, f(m, n))$ and success probability about $2^{-\alpha^2 n}$. In contrast, the standard method for boosting success probability by repeated trials will improve it to $(1-(1-2^{-\alpha n})^t)$ ($\approx t2^{-\alpha n}$ for $t = O(2^{\alpha n})$) using circuits of size about $tf(n, m)$.

Using this lemma, we derive tight bounds on the exponent of the success probability for deciding the **CircuitSat** problem in a variety of probabilistic computational models under complexity assumptions.

(jointly with Pavel Pudlák of the Mathematical Institute of the Czech Academy of Sciences)