Polynomial Circuits and Disjoint NP Pairs

Samik Sengupta
E-Mail: samik@cse.buffalo.edu
Dissertation Committee Chair: Dr. Alan Selman
Dissertation Committee Members: Dr. Kenneth Regan and Dr. Xin He

June 16, 2004

This proposal consists of two parts. The first part is about the existence of polynomial circuits for NP, and the second part is about disjoint NP Pairs.

It has been a longstanding open problem in complexity theory to determine whether languages in NP have polynomial-size families of circuits. A negative answer would separate P from NP, and therefore, is difficult to prove. However, several researchers have shown that if all languages in NP have polynomial-size circuits, then the polynomial hierarchy collapses to within the second level. This provides evidence in favor of the negative answer, because we believe that the hierarchy is infinite. We prove the best collapse known so far. We also prove a result showing that if the NP-complete language SAT does not have an n^k-size family of circuits, then there is a small set (size polynomial in n) of formulas with an interesting property: No circuit of size n^c, where c is a suitable constant smaller than k, can be correct on all of these formulas. Using this, we answer an open question raised by Buhrman and Fortnow in 1998.

The class of disjoint NP pairs (A,B), where A and B are nonempty, disjoint sets in NP, are interesting because of their relation to cryptography and their relation to propositional proof systems. Under reasonable complexity-theoretic hypotheses, we show that many-one reductions between NP pairs are not as powerful as Turing reductions. In other words, we obtain pairs (A,B) and (C,D) such that (A,B) Turing-reduces to (C,D) but (A,B) does not many-one-reduce to (C,D).

We also discuss future research directions.