Project Abstract: AF: Small: Disjoint NP-pairs and Structural Properties of Complete Sets

A (disjoint) NP-pair is a pair of disjoint, nonempty sets in the complexity class NP. The study of disjoint NP-pairs is motivated by their relations to public-key cryptosystems and to propositional proof systems. In particular, answers to questions about existence of NP-hard or P-inseparable NP-pairs informs us about the question of whether secure public-key cryptosystems exist; existence of complete NP-pairs is implied by existence of optimal propositional proof systems. This project will investigate P-inseparable and complete NP-pairs further, in particular whether they can be derived from a hypothesis that is weaker than any of the known ones, and whether existence of these NP-pairs have strong consequences that are unknown before. We will examine commonly (dis)believed hypotheses in complexity theory such as that NP≠coNP and that PH collapses, and research on their relations to the existence of P-inseparable and complete NP-pairs. It is also our goal to build on recent results regarding relations between NP-pairs and propositional proof systems and obtain deeper insight into both subjects.

It is important to study structural properties of complete sets because they gives us a better understanding of the computational power of various complexity classes, and also might lead to proofs of separation results in complexity theory. The proposed project will focus on the following structural properties of complete sets:

- Robustness: does a complete set remain complete if certain amount of elements are taken away from the set?
- Autoreducibility: does a complete set reduce to itself via a reduction that does not query on the input string?
- Mitoticity: can a complete set be split into two complete sets?

Most complete sets have been known to have one or more of these properties. The proposed project aims to address the remaining open questions regarding these properties especially those having major impact in complexity theory if settled. For example, are EXP-complete sets autoreducible for the truth-table reductions? Solving this problem would either separate EXP from PH, or PSPACE from P.

Broader Impact: The proposed project will be implemented at a Hispanic-serving institution and will promote interest among students, especially Hispanic minorities, for research and study in theoretical computer science and for computer science and engineering at large. The project will be part of the ongoing effort in the computer science community to understand the computation limits of computers. All results from the project will be disseminated broadly through conferences and journal publications.