Prof. Madhu Sudan

Prof. Madhu Sudan is a Fujitsu Professor of EECS at Massachusetts Institute of Technology (MIT). Madhu Sudan's research interests include computational complexity theory, algorithms and coding theory. He is best known for his works on probabilistic checking of proofs, and on the design of list-decoding algorithms for error correcting. Madhu Sudan is a recipient of numerous awards including the ACM Doctoral Dissertation Award (1992), the IEEE Information Theory Society Paper Award (2000), the Gdel (2001) and the Nevanlinna Prize (2002). He visited IIT Kanpur from Jan 1-13, 2007.

1 Research Activities

Professor Sudan principally explored directions in algebraic computation with Professor Manindra Agrawal. These discussions spanned many diverse topics and were meant to be exploratory to find topics for future research. Some of the topics explored included:

1. *New approaches for factoring integers* : The topic of factoring integers is a long-standing open problem in mathematics. Professors Agrawal and Madhu Sudan considered the possibility of using information from the AKS algorithm for testing primality to factor non-prime numbers. They also explored the possibility of using lattice reduction algorithms and list-decoding algorithms for factorization.

2. *Algebraic approaches to the graph isomorphism problem* : This work was inspired by recent algorithms of Prof. Agrawal's group reducing graph isomorphism to several ring homomorphism problems. The graph isomorphism problem is a classical open problem in computational complexity, whose resolution would be considered a major breakthrough.

3. *Probabilistically checkable proofs (PCPs) and locally decodable codes (LDCs)* : Professors Madhu Sudan and Agrawal also discussed some of the recent results in PCPs and LDCs that are based on algebraic methods and discussed the possibility of improving some constructions.

On the non-algebraic side, Professors Madhu Sudan and Sumeet Ganguly discussed the possibility of using the concept of universal semantic communication to resolve some fundamental problems in heterogeneous databases. On the whole, while the discussions did not lead to any new results, they were very illuminating in suggesting many directions for joint work in future. During his visit to the Institute, Prof. Madhu Sudan gave three public lectures: The first was a guest lecture in a freshman seminar course. The second was a departmental colloquium addressed to computer scientists broadly (and attended by several members outside the department as well). The last was a technical talk on some new results in theoretical computer science. The specific details are as follows :

1. *Error-correcting codes* : 09-01-2007 (9am). Guest lecture in freshman seminar (D-0) run by Prof. Dheeraj Sanghi.

2. *Universal Semantic Communication* : (based on joint work with Brendan Juba). 09-01-2007 (5pm), hosted by Prof. Manindra Agrawal.

3. *Algebraic Property Testing* : (based on joint work with Tali Kaufman). 10-01-2007 (4pm), hosted by Prof. Manindra Agrawal.