Mathematical Sciences 2014

"My vision for the work that I do is to eventually make computers communicate as effectively as humans are able to do... How to get there from here would involve finding a lot of solutions. New problems, new solutions. And we'd like to find solutions that can be put inside computers of today, tomorrow or maybe 50 years from now and then make them work better."

Madhu Sudan

Principal Researcher, Microsoft Research New England and Adjunct Professor, EECS Department and CSAIL, MIT, USA

- B. Tech. in Computer Science and Engineering from the Indian Institute of Technology, Delhi
- Ph.D. in Computer Science from the University of California, Berkley

Prof. Madhu Sudan has made seminal contributions in the domains of Probabilistically Checkable Proofs (PCP) and error-correcting codes. His algorithm for list-decoding of Reed-Solomon codes was a major breakthrough that found applications in diverse areas.

Correcting errors in data and logic

Whenever one stores data for a long time, or transmits it over long distances, errors inevitably creep in, flipping some of the bits of the data. Error-correcting codes are mathematical objects that are designed to protect data from such errors. They show how to add redundancy, by a process called encoding, to the data so that when errors happen, the redundancy helps determine what the original data was. The process of recovering the original data from the erroneous one is called decoding.

Prof. Madhu Sudan has made significant contributions to the design of efficient algorithms for decoding. In particular, he is best known for his algorithms, with Guruswami, for list-decoding Reed-Solomon codes. These are the codes that are used in all CDs and DVDs to protect their data. His work shows how to correct many more errors efficiently in these codes than was previously believed possible.

Sudan has also made contributions to new ways of writing proofs called Probabilistically Checkable Proofs or PCPs. Consider the task of reviewing a thousand-page proof of some mathematical theorem. The reviewer's task appears daunting as the proof could have a fatal error and the error could be hidden anywhere in the thousand pages. PCP proposes alternate formats in which proofs can be written so that the reviewer would be able to scan portions of the proof somewhat randomly, and be confident that if the proof is really wrong, then an error would be discovered with high probability. PCPs were proposed in the late 1980s, but it was unclear if formats satisfying the desires of the proposal actually existed.

In 1992, Sudan, with his collaborators, Arora, Lund, Motwani and Szegedy, proved "The PCP Theorem" that showed that PCPs, in which the reviewer looked at only a constant number of bits of the proof, do exist! For the PCP they give, the number of bits that the reviewer needs to look at depends only on the level of confidence that the reviewer desires and is not based on the length of the theorem or proof. In practice such PCPs can potentially be used to verify results of long computation. In theory it led to a revolution in the understanding of "approximability of optimization problems".

Optimization problems describe a large body of problems that one wishes to solve using computers. The task is to find a solution that satisfies given constraints while maximizing or minimizing some objective. An example is the Travelling Salesperson Problem (TSP). A salesperson wishes to visit some 'n' cities while minimizing the total distance travelled. The TSP is a classic example of an "NP-hard problem", where the brute force method of enumerating all possible orders in which the salesperson could visit the cities and taking the minimum is the best known method to optimize. Given the seeming hardness of finding the best solution, researchers were hoping that nearly optimal solutions could be found more efficiently. The PCP Theorem dashed this hope by showing that for the TSP, finding approximately optimal solutions was as hard as finding optimal ones.