Modelling Errors and Recovery for Communication

Madhu Sudan

MIT, Cambridge, USA

The theory of error-correction has had two divergent schools of thought, going back to the works of Shannon and Hamming. In the Shannon school, error is presumed to have been effected probabilistically. In the Hamming school, the error is modeled as effected by an all-powerful adversary. The two schools lead to drastically different limits. In the Shannon model, a binary channel with error-rate close to, but less than, 50% is useable for effective communication. In the Hamming model, a binary channel with an error-rate of more than 25% prohibits unique recovery of the message.

In this talk, we describe the notion of list-decoding, as a bridge between the Hamming and Shannon models. This model relaxes the notion of recovery to allow for a "list of candidates". We describe results in this model, and then show how these results can be applied to get unique recovery under "computational restrictions" on the channel's ability, a model initiated by R. Lipton in 1994.

Based on joint works with Venkatesan Guruswami (U. Washington), and with Silvio Micali (MIT), Chris Peikert (MIT) and David Wilson (MIT).

J.R. Correa, A. Hevia, and M. Kiwi (Eds.): LATIN 2006, LNCS 3887, p. 25, 2006.