PROBABILISTICALLY CHECKABLE PROOFS: A SURVEY

SANJEEV ARORA

Abstract

The study of Probabilistically Checkable Proofs (PCPs) is an active area in theoretical computer science. At its heart is a new definition of the class NP. Classically, NP is defined as the class of decision problems such that a "Yes" answer has a short, efficiently verifiable certificate. An example is the CLIQUE problem: Given a graph G and an integer k, determine if G has a complete subgraph ("clique") on at least k nodes. Note that a "Yes" answer can be certified by exhibiting the subgraph in question.

Work during the past decade gives a new definition of NP: it is the class of decision problems for which a "Yes" answer has a certificate that is probabilistically checkable by examining a constant number of bits in it. (In fact, the strongest such result shows that the certificate can be checked by examining only 3 bits in it!) Proving that this definition is equivalent to the classical definition is fairly difficult.

This new definition of NP has many ramifications, one of which is that for many NP-hard problems, computing approximate solutions (solutions whose cost is within a factor 2 of the optimum, say) is no easier than computing optimum solutions. This result holds great interest for those who encounter NP-hard problems in their work.

The talk will be a survey of this area, and will be self-contained.

References

[1] L. Babai: Transparent proofs and limits to approximation. In: Proc. First European Congress of Mathematics (1992), Vol. I, Birkhuser Verlag, 1994, pp. 31-91.

[2] The Approximability of NP-hard problems, Survey based upon a plenary lecture at ACM STOC'98. In Proc. ACM Symposium on Theory of Computing, 1998. Also available from http://www.cs.princeton.edu/ arora/publist.html.

E-mail address: arora@cs.princeton.edu

Department of Computer Science, Princeton University, Princeton, NJ 08544, USA