Pseudo-deterministic Algorithms*

Shafi Goldwasser[1]

1 MIT and Weizmann Institute of Science
Cambridge, MA, USA and Rehovot, Israel
shafi@csail.mit.edu

Abstract

In this talk we describe a new type of probabilistic algorithm which we call *Bellagio* Algorithms: a randomized algorithm which is guaranteed to run in expected polynomial time, and to produce a correct and unique solution with high probability. These algorithms are pseudo-deterministic: they can not be distinguished from deterministic algorithms in polynomial time by a probabilistic polynomial time observer with black box access to the algorithm.

We show a necessary and sufficient condition for the existence of a Bellagio Algorithm for an NP relation R: R has a Bellagio algorithm if and only if it is deterministically reducible to some decision problem in BPP. Several examples of Bellagio algorithms, for well known problems in algebra and graph theory which improve on deterministic solutions, follow.

The notion of pseudo-deterministic algorithms (or more generally computations) is interesting beyond just sequential algorithms. In particular, it has long been known that it is impossible to solve deterministically tasks such as *consensus* in a faulty distributed systems, whereas randomized protocols can achieve consensus in expected constant time. We thus explore the notion of pseudo-deterministic fault tolerant distributed protocols: randomized protocols which are polynomial time indistinguishable from deterministic protocols in presence of faults.

1998 ACM Subject Classification F.2. Analysis of Algorithms and Problem Complexity

Keywords and phrases randomized algorithms, distributed computing, Monte Carlo, Las Vegas

Digital Object Identifier 10.4230/LIPIcs.STACS.2012.29

* This work was partially supported by NSF Contract CCF-0729011 and ISF grant 700/08

29th Symposium on Theoretical Aspects of Computer Science (STACS'12).
Editors: Christoph Dürr, Thomas Wilke; pp. 29–29
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany
SYMPOSIUM ON THEORETICAL ASPECTS OF COMPUTER SCIENCE