Transparent Proofs and Limits to Approximation

László Babai*

A good proof is one which makes us wiser.
Yu. I. Manin

Abstract

We survey a major collective accomplishment of the theoretical computer science community on efficiently verifiable proofs.

Informally, a formal proof is transparent (or holographic) if it can be verified with large confidence by a small number of spot-checks.

Recent work by a large group of researchers has shown that this seemingly paradoxical concept can be formalized and is feasible in a remarkably strong sense; every formal proof in ZF, say, can be rewritten in transparent format (proving the same theorem in a different proof system) without increasing the length of the proof by too much.

This result in turn has surprising implications for the intractability of approximate solutions of a wide range of discrete optimization problems, extending the pessimistic predictions of the P-NP theory to approximate solvability.

We discuss the main results on transparent proofs and their implications to discrete optimization. We give an account of several links between the two subjects as well as a table of known limits to approximating the solution to over two dozen optimization problems. We review the conceptual foundations, including the elements of complexity theory and interactive proofs, the immediate precursors of transparent proofs.

Table of Contents

1 Introduction ...................................................... 33
1.1 Cost of reliability reduced......................................................... 34
1.2 Prehistory in a nutshell......................................................... 35
1.3 Brief history, credits ......................................................... 37

* Partially supported by NSF Grant CCR-9014562

A. Joseph et al. (eds.), First European Congress of Mathematics © Birkhäuser Verlag 1994