Feature Review for Mathematical Reviews

Oded Goldreich
Department of Computer Science and Applied Mathematics
Weizmann Institute of Science, Rehovot, ISRAEL.

Appeared in April 1999 issue of MR [99d:68077ab]

- S. Arora and S. Safra. Probabilistic Checkable Proofs: A New Characterization of NP. *J. ACM*, Vol. 45, no. 1, pages 70–122, 1998.
- S. Arora, C. Lund, R. Motwani, M. Sudan and M. Szegedy. Proof Verification and Intractability of Approximation Problems. *J. ACM*, Vol. 45, no. 3, pages 501–555, 1998.

These two papers make important contributions to two areas of complexity theory: the study of approximation algorithms and the study of probabilistic proof systems.

Complexity theory is concerned with the attempt to understand the nature of efficient algorithms, procedures and systems. This attempt is at the very heart of Theoretical Computer Science. Arguably, the most important type of algorithms are those designed to solve optimization problems. Fundamental works by Cook, Karp and Levin, done in the early 1970's, have provided a strong systematic evidence to the intractability of many important optimization problems (by showing the latter to be NP-Hard; cf. [Garey and Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W.H. Freeman and Company, New York, 1979]). Approximation algorithms are supposed to bypass the difficulty of finding the best solution to an optimization problem by finding a solution which is "nearly" the best one. The main question to be investigated in this context is what is the trade-off between the running-time of an algorithm and the quality of the approximation that it can achieve. However, very little progress in resolving this question has been achieved in the 1970's and 1980's. The connections established by Feige et al [*J. ACM*, Vol. 43 (1996), no. 2, 268-292; MR97h:68037] (and further developed in the second paper), between probabilistically-checkable proof (PCP) systems and the difficulty of approximating several central optimization problems, and the results concerning such proof systems, have provided a breakthrough in the investigation of approximation algorithms.

Probabilistically-checkable proof (PCP) systems are proof systems which allow super-fast verification by probing the proof at very few random locations. Thus, the alleged proof is in redundant form, and the verification procedure is efficient and probabilistic. For every valid statement there exists a valid proof which is always accepted by the verification procedure, whereas for a non-valid statement each false proof is rejected with probability at least 1/2 (taken over the coin tosses of the verification procedure). Furthermore, proofs relative to any automatic verification procedure (known as "NP-proofs"), can be efficiently transformed into proofs of the above form. Also, by going over all possible random choices, one may regain absolute certainty in the validity of a probabilistically-checkable proof. The most important parameters regarding a PCP system are the number of coins tossed by the verification procedure and the number of locations (in the alleged proof) probed by the procedure.

The main result of the first paper is that any NP-proof system can be transformed into a PCP proof system in which both the number of coin-tosses and probed-locations are logarithmic in the length of the original proof (and/or the claimed statement). In the second paper the number of probes is reduced to an absolute constant (independent of the statement to be proven). Subsequent works have reduced this constant to 5 (cf., the two papers as well as [Goldreich, *Modern Cryptography, Probabilistic Proofs, and Pseudorandomness*, Springer 1998] for survey of subsequent improvements and wider perspective).

Using the connection established by Feige et al, it is shown that, for some constant $c > 0$, the problem of approximating the size the maximum clique in an N-vertex graph up to a factor of N^c is NP-Hard (and thus probably infeasible). Subsequent work has shown that c may be any constant smaller than 1. The second paper also presents a new connection between PCP and approximation. Via this connection a large number of optimization problems (known as MaxSNP) were shown to be NP-Hard to approximate to within some (problem specific) constants. Again, subsequent work has improved on these constants, reaching tight results for some natural optimization problems (e.g., Max3SAT).

Thus the above works are milestones in the study of probabilistically-checkable proof systems and their relation to the difficulty of approximating several central optimization problem, which in turn constitutes the most important development in Complexity Theory in the current decade. Both papers are also very interesting from a technical point of view. The first paper introduces the paradigm of "proof composition" as a tool in the design of PCP systems. Indeed this paradigm has played a key role in all subsequent developments. Both papers present important improvements in the analysis of "low-degree tests" (i.e., algorithms which, by probing a given function at few random inputs, test whether it is a low degree polynomial or far from any such polynomial). Finally, the second paper presents two PCP systems which are especially amenable for "proof composition" aimed at achieving very probe-efficient PCP systems.