Super-Efficient Rational Proofs

PABLO DANIEL AZAR, MIT CSAIL
SILVIO MICALI, MIT CSAIL

Information asymmetry is a central problem in both computer science and economics. In many fundamental problems, an uninformed principal wants to obtain some knowledge from an untrusted expert. This models several real-world situations, such as a manager's relation with her employees, or the delegation of computational tasks in mechanical turk.

Because the expert is untrusted, the principal needs some guarantee that the provided knowledge is correct. In computer science, this guarantee is usually provided via a *proof*, which the principal can verify. Thus, a dishonest expert will get caught and penalized (with very high probability). In many economic settings, the guarantee that the knowledge is correct is usually provided via *incentives*. That is, a game is played between expert and principal such that the expert maximizes her utility by being honest.

A rational proof is an interactive proof where the prover, Merlin, is neither honest nor malicious, but rational. That is, Merlin acts in order to maximize his own utility. Rational proofs have been previously studied when the verifier, Arthur, is a probabilistic polynomial-time machine [1].

In this paper, we study *super efficient rational proofs*, that is, rational proofs where Arthur runs in logarithmic time. Our new rational proofs are very practical. Not only are they much faster than their classical analogues, but they also provide very tangible incentives for the expert to be honest. Arthur only needs a *polynomial-size budget*, yet he can penalize Merlin by a large quantity if he deviates from the truth.

We give the following characterizations of which problems admit super-efficient rational proofs.

(1) Uniform TC^0 coincides with the set of languages L that admit a rational proof using $O(\log n)$ time, $O(\log n)$ communication, a constant number of rounds and a polynomial size budget.

(2) $P^{||NP}$ coincides with the set of languages having a rational proof using $O(\log n)$ time, $poly(n)$ communication, one round and a polynomial-size budget.

Furthermore, we show that when Arthur is restricted to have a polynomial-size budget, the set of languages which admit rational proofs with polynomial time verification, polynomial communication and one round is $P^{||MA}$

Categories and Subject Descriptors: F.1.3 [**Theory of Computation**]: Complexity Measures And Classes

General Terms: Theory,Economics,Verification

Additional Key Words and Phrases: Interactive Proofs, Crowdsourcing, Economics and Computation

REFERENCES

P. D. Azar and S. Micali. Rational Proofs. In *Proceedings of the 44th symposium on Theory of Computing*, STOC '12, pages 1017–1028, New York, NY, USA, 2012. ACM.

A full version of this paper is available at: http://people.csail.mit.edu/azar/wp-content/uploads/2013/04/EC-Full-Version.pdf

Author's addresses: Pablo D. Azar, MIT CSAIL, Cambridge, MA, 02139; Silvio Micali, MIT CSAIL, Cambridge, MA, 02139.

EC'13, June 16–20, 2013, Philadelphia, PA, USA.
ACM 978-1-4503-1962-1/13/06.