Interactive Coding with Optimal Round and Communication Blowup

Yael Kalai, Microsoft

We construct an interactive coding scheme, a notion introduced by Schulman (FOCS 1992, STOC 1993). Loosely speaking, we show how to convert any two-party interactive protocol into one that is resilient to constant-fraction of *insertion* and *deletion* errors, while preserving computational efficiency, and blowing up the communication complexity and the *round* complexity by a constant factor that approaches 0 as the error-rate approaches 0.

Previous works were not concerned with the round complexity, and typically assumed that one bit is sent per round. Moreover, most previous works (with the exception of the recent work of Braverman et. al.) considered only substitution errors or erasures errors.

We consider the model where in each round each party may send a message of *arbitrary*, where the length of the messages and the length of the protocol may be adaptive, and may depend on the private inputs of the parties and on previous communication. This model is known as the (synchronous) message passing model, and is commonly used in distributed computing, and is the most common model used in cryptography.

We also construct an error-resilient scheme with communication blowup of 1+\tilde{O}(eps^{1/4}), where eps is a bound on the error-rate, and round blowup O(1). We give evidence that this communication blowup is optimal in our model.

This is joint work with Klim Efremenko and Elad Haramaty.