Direct Product Results and the GCD Problem, in Old and New Communication Models

Itzhak Parnafes
Ran Raz
Avi Wigderson

Abstract
This paper contains several results regarding the communication
complexity model and the 2-prover games model, which are based on interaction between the two models:

1. We show how to improve the rate of exponential decrease in the parallel repetition theorem of [Ra] in terms of the communication complexity of the verifier's predicate.

2. We apply the improved parallel repetition theorem of 2-prover games to derive, for the first time, a direct product theorem for communication complexity.

The second derivation uses a common generalization of the two models, which is independently interesting. We initiate a study of its power by considering the GCD problem, and some variations of it, which exhibit a power gap between the new model and the classical communication complexity model. This gap is partly based on the following upper bounds: Given n-bit inputs x and y to Alice and Bob respectively, they can achieve the tasks below with very high probability using only $O(n= log n)$ communication bits:

1. Decide if $GCD(x; y) = 1$ and b (by Bob), satisfying $a _ x + b _ y = 1$.

Observe that the outputs in the second task are in general of length (n). A complete analysis of the communication complexity of these two problems (in several models and modes) is given.