Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity

Benny Chor, Tel Aviv University

A model for weak random physical sources is presented. This model strictly generalizes previous models (e.g., the Santha and Vazirani model, 1984).
The sources considered output strings according to probability distributions in which no single string is too probable.

The new model provides a fruitful viewpoint on problems studied previously, such as:

• Extracting almost-perfect bits from sources of weak randomness. The question of possibility as well as the question of efficiency of such extraction schemes are addressed.
• Probabilistic communication complexity. It is shown that most functions have linear communication complexity in a very strong probabilistic sense. This result extends to certain simple, explicit functions.
• Robustness of BPP with respect to sources of weak randomness (generalizing a result of Vazirani and Vazirani, 1985).

(Joint work with Otto Goldreich, 1988)