SHAFRIRA GOLDWASSER, MIT and Weizmann

Pseudo Deterministic Algorithms and Proofs

Probabilistic algorithms for both decision and search problems can offer significant complexity improvements over deterministic algorithms. One major difference, however, is that they may output different solutions for different choices of randomness. This makes correctness amplification impossible for search algorithms and is less than desirable in setting where uniqueness of output is important such as generation of system wide cryptographic parameters or distributed setting where different sources of randomness are used. Pseudo-deterministic algorithms are a class of randomized search algorithms, which output a unique answer with high probability. Intuitively, they are indistinguishable from deterministic algorithms by an polynomial time observer of their input/output behavior. In this talk I will describe what is known about pseudo-deterministic algorithms in the sequential, sub-linear and parallel setting. We will also describe n extension of pseudo-deterministic algorithms to interactive proofs for search problems where the verifier is guaranteed with high probability to output the same output on different executions, regardless of the prover strategies.