COS522: Computational Complexity Fall 2011

Princeton University

Instructor: Sanjeev Arora

Lecture 11 notes Oct 20. Interactive Proofs.

1. Recall NP: small certificate for yes answer. In real life, proofs can be interactive.
2. Adding interaction to NP defn. Doesn’t change the class!
3. Add randomness to verifier. Now get PSPACE! In particular, note that can have interactive proofs for coSAT!
4. Simplest interactive proof: GNI.
5. Private coins vs public coins. GS set lowerbound protocol. Do it in full generality for any 1-round private coins protocol. Suppose |S| is either K or K/16. Hash to a set of size K/4. For a random element of the range, Pr[exists a preimage] is either > 0.5 or < ¼. Repeat.
6. IP=PSPACE. Warmup: protocol for #SAT.
7. Arithmetization. (Encountered in QUADEQ reduction.)
8. Sum check protocol.