COS522: Computational Complexity Fall 2011

Princeton University

Instructor: Sanjeev Arora

Lecture 8 notes Oct 11. Randomized computation. Moving on to crypto.

1. Randomized computation. Simulating arbitrary bias with fair coin and vice versa. Difference between expected running time and worst-case.
2. BPP is in P/poly. Sipser Gacs Theorem. (Recap from last time.)
3. Identity testing when polynomials are presented as circuits. Why doesn’t Schwartz-Zippel lemma suffice? Circuit of size m computes a poly of degree at most 2^m. However, answer can take 2^m bits to represent. Need fingerprinting trick.
4. Complete problems? Don’t know. Semantic vs Syntactic classes.
5. Randomized reductions.
6. Cryptography. Most basic task: encryption. How to define? Desired properties?
7. Simplest system using shared random string. XOR. Satisfies most stringent defn of security.
8. How to share a random string: Alice picks a, sends over g^a. Bob pics b, sends over g^b. They both compute g^{ab}, which they now share.
9. One way function. Example: g^a. Random self-reducibility. One-way permutation.
10. Another example: multiplication. Not known to be rsr.
11. One-way function formal defn. Weak/strong. Fact: can turn weak into strong (k-wise direct product). Hardness amplification.
12. Pseudorandom generator. Extend by one bit. Next time: prg from one-way permutation