COS522: Computational Complexity Fall 2011

Princeton University

Instructor: Sanjeev Arora

Lecture 10 notes Oct 13. Crypto wrapup.

1. One-way function formal defn. Weak/strong. Fact: can turn weak into strong (k-wise direct product). Hardness amplification.
2. Recall: PRG from a oneway permutation. Yao’s hybrid argument means that we can focus on
3. Yao’s hybrid argument: fn is a PRG iff it passes the next bit test. Only if is clear: a next-bit test can be used to distinguish from random. So better pass it! If is harder.
4. Hybrid argument. Suppose distinguisher A has prob ½ + \delta of saying “1” on the pseudorandom string vs ½ on random string. Let P\_i = Pr[distinguisher says 1 when first i bits are from PRG and last n^c –i are random].
5. \delta = P\_{n^c} – P\_0. E\_i[P\_i –P\_{i-1}] is at least \delta/n^c.
6. Predictor: Given first i bits, add the I’th and then fill the remaining bits randomly. Run A. If it says 1, go with your guess otherwise with the other guess.
7. Analysis of correctness. Four possibilities: We guessed the right/wrong bit; A said 1/0. See which contribute to correct guess. Advantage is exactly p\_{i+1} – p\_i.
8. How to extend by 1 bit. Goldreich-Levin hardcore bit.
9. Clearly, predictor cannot have any success predicting any of the first n bits. So it only has a chance of predicting the n+1 th bit. Suppose this success probability is ½ +\eps. Then for \epsilon/2 of the x’s this prob. Is at least ½ +\eps/2. Show that this suffices to recover x.
10. Warmup: Pr of prediction is 0.9. Query on r and r+ e^i. Both correct with prob. 0.8. So repeat poly(n) times, and get x\_i. Chebyshev’s inequality.
11. Actual analysis: Use pairwise indep r’s; about poly(n)/\eps^2 of them.
12. Pseudorandom functions briefly.