COS 522: Complexity Theory : Boaz Barak
Handout 4: Interactive Proofs.

Reading: Chapter 8

Continued from last time randomness efficient error reduction using walks on expander graphs.

randomized reduction if UNIQUESAT has a polynomial-time algorithm than $\mathbf{NP} \subseteq \mathbf{BPP}$. Main tool: *pairwise independent hash functions*.

Interactive proofs Formal definition of deterministic interaction, show this is the same as **NP**.

The class IP Definition of **IP**.

Few observations (1) probabilistic provers don't matter. (2) $\mathbf{IP} \subseteq \mathbf{PSPACE}$ (3) soundness constant can be arbitrary but noticeably smaller than 1 (4) completness constant can be 1 (5) private coins.

$\mathsf{GNI} \in \mathbf{IP}$

public coin proofs $\mathsf{GNI} \in \mathbf{AM}[O(1)]$. Note: corollary is that GI is not **NP**-complete unless the hierarchy collapses. Also, under assumptions this means that $\mathsf{GI} \in \mathbf{NP} \cap \mathbf{coNP}$.

$\mathbf{coNP} \subseteq \mathbf{IP}$ (If you know/read about **PSPACE**, see Section 8.5.3 for the proof that $\mathbf{IP} = \mathbf{PSPACE}$). Note that this is a non-relativizing result.

multi-prover proofs and PCP

The story of the discovery of the power of interactive proofs is described in an entertaining survey by Bababi (see website).

Homework Assignments

§1 (40 points)

(a) Prove that if $\mathbf{p}$ is a probability vector then $\|\mathbf{p}\|_2^2$ is equal to the probability that if i and j are chosen from $\mathbf{p}$, then $i = j$.

(b) Prove that if $\mathbf{s}$ is the probability vector denoting the uniform distribution over some subset S of vertices of a graph G with normalized adjacency matrix A, then $\|A\mathbf{p}\|_2^2 \geq 1/|\Gamma(S)|$, where $\Gamma(S)$ denotes the set of S's neighbors.

(c) Prove that if G is an (n, d, λ)-graph, and S is a subset of ϵn vertices, then

$$|\Gamma(S)| \geq \frac{|S|}{2\lambda^2\,(1 - o(1))},$$

where by $o(1)$ we mean a function of λ and ϵ that tends to 0 as ϵ tends to 0.

A graph where $|\Gamma(S)| \leq c|S|$ for every not-too-big set S (say, $|S| \leq n/(10d)$) is said to have *vertex expansion* c. This exercise shows that graphs with the minimum possible second eigenvalue $\frac{2}{\sqrt{d}}(1 + o(1))$ have vertex expansion roughly $d/4$. It is known that such graphs have in fact vertex expansion roughly $d/2$ (Kahale95), and there are counterexamples showing this is tight. In contrast, random d-regular graphs have vertex expansion $(1 - o(1))d$.

§2 (25 points) Solve all items except (b) in Exercise 8.1 (if you know the class **PSPACE**, you can solve (b) for extra 10 points).

§3 (30 points) Exercise 8.3

§4 (30 points) Exercise 8.4

For next week: Think how you would mathematically *define* an unbreakable (or unbreakable in polynomial time) *encryption scheme*. (That is, a method that given a secret key k and a message m, outputs a "scrambled" message c such that m can be recovered from c using k, but c "hides" the contents of m.)