Today (Pset 4 out)
- Approximate Counting
- Interactive Proofs
  * Graph Non-isomorphism

Lecture 20: Computational Complexity (14 Apr, 2020)
Instructor: Prahladh Harsha

Approximate Counting

Thm: $\forall f \in \#P$, there is an algorithm that on input x, ε & δ outputs $A(x)$ s.t.

$$\Pr_A\left[(1-\varepsilon)f(x) \le A(x) \le (1+\varepsilon)f(x)\right] \ge 1-\delta$$

in time $\mathrm{poly}\left(|x|, \frac{1}{\varepsilon}, \log\frac{1}{\delta}\right)$ using an NP oracle (ie SAT oracle)

Last time: Simplifying Observations

1. Suffices to prove for $f = \#SAT$

2. Sufft to give an alg that yields the following weaker approximation

$\frac{1}{c}\cdot \#SAT(\varphi) \le A(\varphi) \le c\cdot\#SAT(\varphi)$ for some constant $c \ge 1$.

3. If $\#SAT(\varphi) = O(1)$ & this is promised then can compute $\#SAT(\varphi)$ exactly in P^{NP}.

Consider the following gap problem

$$\text{a-comp}(\varphi, k) = \begin{cases} \text{YES} & \text{if } \#SAT(\varphi) \geq 2^{k+1} \\ \text{NO} & \text{if } \#SAT(\varphi) \leq 2^{k} \\ \text{Don't care} & \text{otherwise} \end{cases}$$

Use a-comp to obtain 2-approx.

A: On input φ
a-comp $(\varphi, 0)$
a-comp $(\varphi, 1)$
a-comp $(\varphi, 2)$
⋮
a-comp (φ, n) — NO

If ans is NO, then use NP oracle to figure out $\#SAT(\varphi)$ exactly
else, suppose ans is YES $\forall$ $~~t~~=0, \ldots i-1$
& NO i onwards
output 2^i. $\boxtimes$

Suppose a-comp o/p YES $(\varphi, i-1) \ldots (a)$
& NO on $(\varphi, i) \ldots (b)$

(a) $\Rightarrow$ $\#SAT(\varphi) > 2^{i-1}$
(b) $\Rightarrow$ $\#SAT(\varphi) < 2^{i+1}$
Hence the ans 2^i is a 2-approximation.

Hence, suff to design an alg for a-comp.

Constructing a-comp:

Ingredient: Pairwise Independent family of hash fns

(similar to Valiant-Vazirani redn)

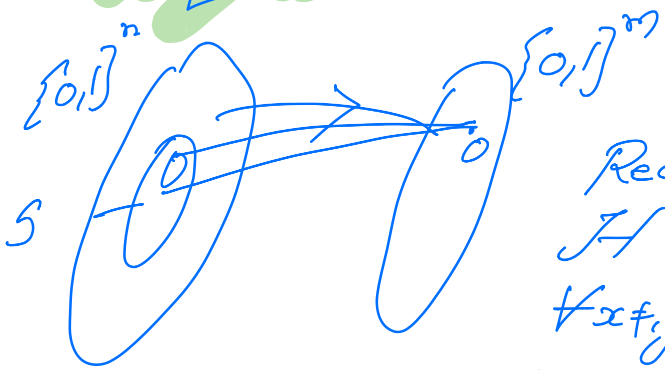
Lemma [Left-over hash Lemma] Impagliazzo-Levin-Luby.

$\mathcal{H}$ - be a family of p.w ind hash fns.

$h : \{0,1\}^n \to \{0,1\}^m$; $S \subseteq \{0,1\}^n$, $|S| \geq \frac{4 \cdot 2^m}{\varepsilon^2}$

Then

$$\Pr_{h \in \mathcal{H}}\left[\,\left|\{a \in S \mid h(a) = \bar{0}\} - \frac{|S|}{2^m}\right| > \frac{\varepsilon |S|}{2^m}\right] \leq \frac{1}{4}$$



Recall:

$\mathcal{H}$ is p.w ind family

$\forall x \neq y \in \{0,1\}^n$ & $a, b \in \{0,1\}^m$

$$\Pr_{h \in \mathcal{H}}[h(x) = a \wedge h(y) = b] = \frac{1}{2^{2m}}$$

(eg: $h(x) = Ax + b$; $A \in \{0,1\}^{m \times n}$; $b \in \{0,1\}^m$)
works

a-comp : (uses a SAT-oracle).

On input (φ, k)

(1). If $k \leq 5$, then use SAT-oracle to check if φ has at least 2^k sat assig if so, output YES else o/p NO.

(2) If $k \geq 6$

Pick $h : \{0,1\}^n \to \{0,1\}^m$ where $m = k-5$ from a pw. ind family $\mathcal{H}$.

& o/p YES if there are at least 48 satisfying assign to φ & $h(a)=0$.

Proof of correctness:

· Case 1: $\#SAT(\varphi) \geq 2^{k+1}$

$S = \{a \mid \varphi(a) = 1\}$. $|S| \geq 2^{k+1}$

$$|S| > 2^{k+1} = 2^{m+6} = \frac{4 \cdot 2^m}{(1/4)^2}$$

Now setting $\varepsilon = 1/4$.

By LHL $\Pr_h\left[\left|\left|\{a \in S \mid h(a) = 0\}\right| - \frac{|S|}{2^m}\right| \leq \frac{1}{4} \cdot \frac{|S|}{2^m}\right] \geq \frac{3}{4}$.

Hence, $\Pr_h\left[\left|\{a \in S \mid h(a) = 0\}\right| \geq 48\right] \geq 3/4$

Case $\#SAT(\varphi) = |S| < 2^k$.

$S' \supseteq S, \quad |S'| = 2^k$

$$\Pr_h[\text{a-comp } YES] = \Pr[|\{a \in S \mid h(a) = 0\}| \geq 48]$$

$$\leq \Pr[|\{a \in S' \mid h(a) = 0\}| \geq 48]$$

$$\leq \Pr\left[\left| |\{a \in S' \mid h(a) = 0\}| - \frac{|S'|}{2^m} \right| > \frac{|S'|}{2 \cdot 2^m}\right]$$

$$\leq 1/4. \qquad \left(\varepsilon = \frac{1}{2}\right)$$

Proof of Left Over Hash Lemma:

$S = \{a_1 \ldots a_n\}$

$$X_i = \begin{cases} 1 & \text{if } h(a_i) = 0 \\ 0 & \text{o.w} \end{cases}$$

$X = \sum X_i \qquad \mathbb{E} X_i = \frac{1}{2^m} \; ; \; \mathbb{E}X = \frac{n}{2^m}$

$\Pr[|X - \mathbb{E}X| \geq \varepsilon \cdot \mathbb{E}X] \ldots$ qty to be computed.

$$\mathrm{Var}[X] = \sum_i \mathrm{Var}[X_i] \quad (\text{pairwise ind})$$

$$= n \cdot \left(\mathbb{E}[X_i^2] - (\mathbb{E}X_i)^2\right)$$

$$\leq n\left(\frac{1}{2^m} - \left(\frac{1}{2^m}\right)^2\right) \leq \frac{n}{2^m}$$

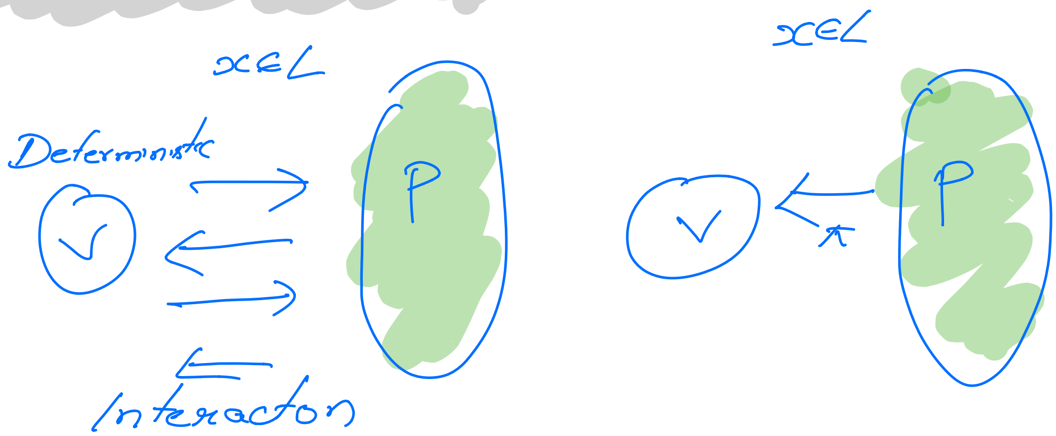
Prob: $\Pr[|X - \mathbb{E}X| \geq \varepsilon \mathbb{E}X] \leq \dfrac{\mathrm{Var}[X]}{\varepsilon^2 (\mathbb{E}[X])^2}$

$$\leq \frac{r/2^m}{\varepsilon^2 (r/2^m)^2} \leq \frac{2^m}{\varepsilon^2 \cdot r}$$

$$\leq \frac{1}{4} \quad \left(\text{since } r \geq \frac{4 \cdot 2^m}{\varepsilon^2}\right)$$

$\boxtimes$

Interactive Proofs:



Does interaction increase the power?

Not really, the prover can give the transcript

However, not true if verifier is randomized.

Example

Graph Non-Isomorphism

$GNI = \{(G_1, G_2) \mid G_1 \not\cong G_2\}$

$GI \in NP$, $GNI \in coNP$

V — (G_0, G_1) — P

1. $b \in_R \{0,1\}$

2. $\sigma \in_R S_n$; $n = |V(G_1)| = |V(G_0)|$

3. $H = \sigma(G_b)$

$$\xrightarrow{\quad H \quad}$$

$$\xleftarrow{\quad c \quad}$$

Accept if $b = c$

$G_1 \cong G_2$, $\forall$ provers

$Pr[\text{succeeds}] = \frac{1}{2}$

$G_1 \not\cong G_2$, $\exists$ prover

$Pr[\text{succeeds}] = 1$