CS 221 LECTURE 11 2/27/2018

TODAY

- APPROXIMATE COUNTING
- PARITY & AC^0 [+ implications to PH]

- Given function $f: \{0,1\}^* \to \mathbb{R}^{\geq 0}$, A is an α-approx algorithm if $\forall n,\ \forall x \in \{0,1\}^n$

$$f(x) \leq A(x) \leq \alpha(n) \cdot f(x).$$

- 1-approx = ~~ep~~ exact computation
- $\alpha > 1$ - approximation
- Later in course with talk about approx algorithms for NP optimization problems. Today approximating #P functions
- Approximating #P functions can be NP-hard:

Proof: ⊙ if G has a clique of size k, then $2^k \leq \#\text{Clique}(G) \leq n^k$

⊙ if G has clique of size k then $G \times K_N$ has clique of size $k \cdot N$

$$\Rightarrow 2^{kN} \leq \#\text{clique}(G \times K_N) \leq 2^{kN} \cdot \binom{n}{k}$$

$\omega(G) \geq k \Rightarrow \#\text{cliques}(G \times K_N) \geq 2^{kN}$

$\omega(G) \leq k-1 \Rightarrow$ " " $\leq 2^{(k-1)N} \cdot \binom{n}{k}$

if $N \geq n^2$ then $2^{kN} \geq 2^{(k-1)N} \cdot \binom{n}{k} \cdot \left[\frac{2^N}{\binom{n}{k}} \right]$

$$\geq 2^{n^2-n} \cdot 2^{(k-1)N} \binom{n}{k}$$

so a 2^{n^2-n} approx. algorithm for #clique would solve NP-hard problems.

- Aside: Approx Counting $\approxeq$ Almost-uniform-sampling.

- Defn: A is an α-almost-uniform-sampler for $S \subseteq \{0,1\}^n$ if $A(\cdot)$ outputs elements of S & $\forall s \in S$

$$\frac{1}{|S| \cdot \alpha(n)} \leq \Pr[A() = s] \leq \frac{\alpha(n)}{|S|}$$

- FRAS: if $\forall \alpha(n) = 1 + \frac{1}{poly(n)}$ $\exists$ poly time $\alpha(n)$-approx. alg.
- Thm: for self-reducible problems, fully polynomial approx. alg. exist $\Longleftrightarrow$ Almost uniform samplers exist.

$\Rightarrow$ Sample $X_1 = 1$ w.p. $\frac{|S \cap 1 \times \{0,1\}^{n-1}|}{|S|}$

Continue; α-approx ~~unif sampler~~ counter $\Rightarrow \beta = \alpha^n$ almost ~~approx~~ unif sampler.

$\Leftarrow$ • to count $|S|$

use estimate of count of $|S \cap \{X_1 = 1\}|$

& divide by $\Pr[X_1 = 1]$

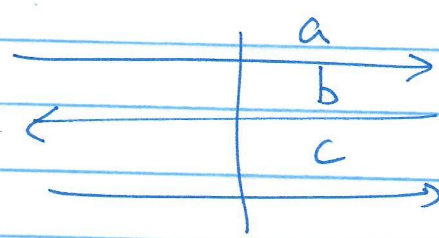
• Estimate $\Pr[X_1=1]$ by randomly sampling elements of S & finding fraction that has $X_1 = 1$.

$\boxtimes$

How hard is approx #P ? Answer in PH.

<u>Stockmeyer ⇒ Goldwasser-Sipser</u>

will "prove $|S| \geq \frac{2^k}{2}$" (unless $|S| \leq 2^k$).



$V(\ldots)$

if $|S| \geq 2^k$ $\exists a \forall b \exists c\, V(a,b,c)$ accepts

if $|S| < \frac{2^k}{2}$ $\forall a \exists b \forall c\, V(a,b,c)$ rejects.

<u>Idea</u> (Details omitted) (work with S^t & prove $|S^t| \geq 2^{kt}$ or $|S^t| \leq 2^{(k-1)t}$

$$h_1 \ldots h_\ell \xrightarrow{\text{"}\forall x\ \exists y \in S \text{ s.t. } h_i(y) = x\text{."}}$$

$$\xleftarrow{\quad x \quad}$$

$$\xrightarrow{\quad y, i \quad}$$

$V(h_1 \ldots h_\ell, x, y, i) = 1$ if $y \in S$ & $h_i(y) = x$.

<u>Rest of this lecture & next:</u>

Parity $\notin AC^0$

- <u>Definition</u>: AC^0 = constant depth poly size ∞-AND, ∞-OR, NOT circuits.

- $\text{Parity}(x_1 \ldots x_n) = \sum x_i \pmod 2$.

- <u>Thm</u>: $O(1)$-depth circuits for Parity require exp. size

Why? (1) "Randomized approx technique"

(2) Only circuit lower bound in course

(3) "Relativized separation of PH from #P".

Thm: $\exists$ ~~Oracle~~ oracle A s.t. $PH^A \neq PSPACE^A$

Proof: Assume otherwise. Consider the language

$$\oplus^A = \{ x \mid \bigoplus_{|y|=|x|} A(y) = 1 \}$$

- Clearly in $P^{\#P^A}$.
- ~~Not in~~ Parity $\notin AC^0 \Rightarrow \oplus^A \notin PH^A$

  Idea: Model PH^A algorithm as $O(1)$-depth AND-OR-NOT circuit whose inputs are $A(y)$ $|y|=|x|$. Should not be able to compute $\oplus^A$.

History: – Furst-Saxe-Sipser, Ajtai : Parity $\notin AC^0$

[but did not get super quasi poly lowerbounds]

– Yao, Håstad [Improved the FSS proof]

– Razborov
– Razborov-Smolensky

} Algebraic ... Will cover this.

Method of Approximations

- AND, OR, NOT gates "approximately" simple
- Circuit " "
- Parity not simple.

Needed: Definition of simple
Definition of approximation.

Simple = low-degree polynomial (

- works nicely ⇒ composes.
- But not so nice ....

① $AND(x_1 .. x_n) = \prod x_1 .. x_n$ ⇒ degree n poly.
as high as possible
(n-var, $GF(2)$)

② $Parity(x_1 .. x_n) = \sum x_i$ ⇒ deg. 1 poly
as low as possible

Fixing Problem 2

$x \to \bar{x}$

Work over $GF(3)$ $\quad 0 \to +1 \quad$ $x \to (-1)^x$

$\quad 1 \to -1 \quad$ or $x \to 1-2x$

$\sum x_i \pmod 2 \rightsquigarrow \prod x_i$

[Now parity is a deg n polynomial!]

Fixing Problem 1 : Approximation!

- Don't compute function on every input; suffices to compute on most inputs.
- But what is most? What is "right" distribution?

Key idea: Will replace every gate by a "randomized gate". for every fixed input, every gate will ~~be~~ correct whp. $\Rightarrow$ Circuit will be correct whp.

Random approximation for OR:

$$OR(z_1 \dots z_m) = \underbrace{\left(\sum \alpha_i z_i\right)}_{\Downarrow}^2$$

$z_1 \dots z_m \in \{0,1\}$ $\quad 0/1 \quad ; \quad \Pr_{\alpha_1 \dots \alpha_m}\left[\left(\sum \alpha_i z_i\right)^2 = OR(z_1 \dots z_m)\right] \geq \frac{2}{3}.$

(from Schwartz-Zippel).

Boosting prob.

$\text{APPROX-OR}^t(z_1 \ldots z_m) = \text{EXACT-OR}(\text{APPROX-OR}^1(z_1..z_m), \ldots \text{APPROX-OR}^t(\ ))$

$\Pr[\text{APPROX-OR}(\ ) = \text{EXACT-OR}] \geq 1 - 2^{-t}$

$\deg \text{APPROX-OR}(\ ) = O(t)$.

<u>Lemma</u>: $\forall$ AND-OR-NOT circuit C of size s & depth d, there exists a ~~circuit~~ ~~of~~ ~~the~~ ~~poly~~ poly of deg $O(t)^d$ ~~s~~ & a set $S \subseteq \{0,1\}^n$ s.t.

~~Pr[p(a)~~ $= \forall a \in S \quad p(a) = C(a)$

$\quad$ & $|S| \geq 2^n \cdot (1 - s \cdot 2^{-t})$

[C approximated by p on large set S.]

But why is this a problem?

is parity complex? to approximate?

Lemma: if p approximates parity on $S \subseteq \{-1,1\}^n$ & $\deg(p) \leq D$

then $|S| \leq \frac{2^n}{2} + \frac{D}{\sqrt{n}} \cdot 2^n$.

Proof: • if $p(x_1 \dots x_n) = \prod x_1 \dots x_n$ on all $\bar{x} \in S$

then every monomial has deg $\leq \frac{n}{2} + D$ on S.

[if $\prod_{i \in M} x_i$ has $|M| \leq \frac{n}{2}$, leave it as is

else write as $\prod_{i \notin M} x_i \cdot \prod_{i=1}^{n} x_i = \prod_{i \notin M} x_i \cdot p(x_1 \dots x_n)$].

• But ~~#~~ ~~poly~~ dim of space of poly of deg $\leq \frac{n}{2} + D$

is at most $\cancel{\binom{n}{\frac{n}{2}+D}}$ $\sum_{i \leq \frac{n}{2}+D} \binom{n}{i} \leq \frac{2^n}{2} + \frac{D}{\sqrt{n}} \cdot 2^n$

But dim $\geq |S|$ $\Rightarrow$ $|S| \leq \frac{2^n}{2} + \frac{D}{\sqrt{n}} \cdot 2^n$

$\boxtimes$

Putting things together: want $D \leq \frac{\sqrt{n}}{4}$ so $|S| \leq \frac{3}{4} \cdot 2^n$

$\Rightarrow t^d \leq \frac{\sqrt{n}}{4}$ $\Rightarrow$ $t =$ ~~log~~ $n^{\frac{1}{2d}}$

$\Rightarrow 2^{-t} = 2^{-n^{1/2d}}$; $2^{-t} \cdot S \geq \frac{1}{4}$ $\Rightarrow$ $S \geq 2^{n^{1/2d}}$.

$\boxtimes$