CS 221 LECTURE 11

Today
- APPROXIMATE COUNTING
- PARITY & $\mathbf{AC}^0$ [ + implications to $\mathbf{PH}$]

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

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

\( \dagger \)-approx = \text{exact computation}
\( \alpha > 1 \) - approximation

Later in course will 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

\[ 2^k \leq \#\text{Clique}(G) \leq n^k \]

(1) if $G$ has clique of size $k$ then $G \times K_N$ has clique of size $k \cdot N$

\[ n^k \leq \#\text{clique}(G \times K_N) \leq \left( \frac{n}{\log n} \right)^k \]
\[ w(G) \geq k \Rightarrow \#\text{cliques}(G \times K_n) \geq 2^{kn} \]

\[ w(G) \leq k-1 \Rightarrow \binom{n}{k} \leq 2^{(k-1)n} \binom{n}{k} \]

If \( n^2 \leq 2^{kn} \), then
\[
2^{kn} \geq 2^{(k-1)n} \binom{n}{k} \left( \frac{2^{N}}{n^k} \right) \geq 2^{n^2-n} \cdot 2^{(k-1)n} \binom{n}{k}
\]

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

Aside: Approx Counting \( \approx \) Almost-uniform-sampling.

**Defn:** A is an \( \beta \)-almost-uniform-sampler for \( S \subseteq \Sigma^* \) if \( A() \) outputs elements \( S \in \Sigma \) s.t.
\[
\frac{1}{|S| \cdot \alpha(n)} \leq \Pr[A() = s] \leq \frac{\alpha(n)}{|S|}
\]

**FRAS:** if \( \alpha(n) = 1 + \frac{1}{\text{poly}(n)} \) \( \exists \) poly time \( \alpha(n) \)-approx. alg.

**Thm:** for self-reducible problems, fully polynomial approx. alg. exist if and only if almost uniform samplers exist.

\[ \Rightarrow \text{Sample } X_i = 1 \text{ w.p. } \#S \leq 1 \times \epsilon_0 \times 10^{10^{10^3} n^{-1}} \]

Continue j \( \beta \)-approx \( \frac{1}{2} \) almost counter \( \beta \)-approx \( \frac{1}{2} \) almost counter.
to count |S|

use estimate of count of $|S| \sim \sum_i x_i = 1^2$

divide by $Pr[x_i = 1]$

Estimate $Pr[x_i = 1]$ by randomly sampling elements of S and finding fraction that has $x_i = 1$.

How hard is #P? Answer in PH.

Stockmeyer $\Rightarrow$ Goldwasser-Sipser

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

\[
\begin{array}{c}
\text{a} \\
\text{b} \\
\text{c} \\
\text{V}(\ldots)
\end{array}
\]

If $|S| > 2^k$, $\exists (a,b,c)$ accepts

If $|S| < \frac{2^k}{2}$, $\exists (a,b,c)$ rejects.
Idea (Details omitted) (work with $\mathcal{E}$ to prove $1^{\mathcal{E}} \geq 2^{k\ell}$)

or $1^{\mathcal{E}} \leq 2^{k\ell - 1}$

\[ h_i : \mathcal{E} \rightarrow \{0, 1\} \quad \text{for all } i \]

\[ \land_i h_i \quad \forall x \in \mathcal{E} \text{ s.t. } h_i(x) = 1. \]

$x \leftarrow x$

\[ y, i \rightarrow \]

\[ V(h_i, h_i, x_i, y, i) = 1 \text{ if } y \in \mathcal{E} \land h_i(y) = x. \]

Rest of this lecture & next:

- Parity $\equiv \mathcal{AC}^0$

  - Definition: $\mathcal{AC}^0 = \text{constant depth poly-size } \land, \lor, \neg$ circuits.

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

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

Why?

1. "Randomized approximation technique"
2. Only circuit lower bound in course
3. "Relativized separation of PH from \#P".
Thm: \exists \text{ Oracle } A \text{ s.t. } \mathsf{PH}^A = \mathsf{PSPACE}^A

Proof: Assume otherwise consider the language

\[ \oplus^A = \{ x \mid \exists y : A(y) = 1 \text{ if } |y| = |x| \} \]

Clearly in \( \mathsf{P} \neq \mathsf{P}^A \).

Note: \( \text{Parity } \& \mathsf{AC}^0 \Rightarrow \oplus^A \subseteq \mathsf{PH}^A \)

Idea: Model \( \mathsf{PH}^A \) 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: - Fortnow-Saxe-Giaccarino, Aisai: Parity \& \mathsf{AC}^0

but did not get super
quasi poly lowerbounds

- Yao, Hastad [ Improved the FSS proof ]

- Razborov

- Razborov-Smolensky \( \Rightarrow \) Algebraic \( \Rightarrow \) Will cover this.
Method of Approximation

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

Needed: Definition of simple
Definition of approximation.

Simple = low-degree polynomial ( )
- Works nicely ⇒ composed.
- But not so nice ...

1. \( \text{AND}(x_1 \ldots x_n) = \prod x_i \cdot x_n \Rightarrow \deg \text{n poly.} \) as high as possible \((n \cdot \text{var, \#F(2)})\)

2. \( \text{Parity}(x_1 \ldots x_n) = \sum x_i \Rightarrow \deg 1 \text{ poly} \) as low as possible \(\)
Fixing Problem 2

Work over $GF(3)$

\[ \begin{align*}
    0 & \rightarrow +1 \\
    1 & \rightarrow -1 \text{ or } x \rightarrow 1 - 2x
\end{align*} \]

\[ \sum x_i \equiv 0 \pmod{2} \rightarrow \prod x_i \]

[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 with probability \( \prod x_i \) making the circuit will be correct with

Random approximation for OR:

\[ \text{OR}(z_1, \ldots, z_m) = \left( \sum x_i 2^i \right)^2 \]

\[ z_1, \ldots, z_m \in \{0, 1\} \]

\[ \Pr \left[ \left( \sum x_i z_i \right)^2 = \text{OR}(z_1, \ldots, z_m) \right] \geq \frac{2}{3} \]

(from Schwartz-Zippel).
Boosting prob.

\[ \text{approx-OR}(z_1, \ldots, z_m) = \text{exac-OR} (\text{approx-OR} (z_1, z_m), \ldots, \text{approx-OR} t) \]

\[ P [ \text{approx-OR} (\cdot) = \text{exact-OR} ] > 1 - 2^{-t} \]

\[ \deg \ \text{approx-OR}(\cdot) = O(t) \]

---

**Lemma:** \( \forall \text{and-or-not} \) linearly of size \( s \), there exists \( t \) and depth \( d \) such that

- \( s \) is a set \( s = \{0,1\}^n \)
- \( \mathcal{P}(\mathcal{A}) = \forall a \in s \ p(a) = c(a) \)
- \( |s| \geq 2^n(1 - s \cdot 2^{-t}) \)

[\( \mathcal{C} \) approximated by \( p \) on large set \( s \).]

---

But why is this a problem?

Is parity complex? to approximate?
Lemma: If \( p \) approximates parity on \( S \subseteq \{ -1, 1 \}^n \) and \( \deg(p) \leq D \), then \( |S| \leq \frac{2^n}{2 + \sqrt{n}} \cdot 2^n \).

Proof: If \( p(x_1, \ldots, x_n) = \prod x_{i_1} \cdot \ldots \cdot x_{i_m} \) for all \( x \in S \), then every monomial has degree \( \leq \frac{n}{2} + D \) on \( S \).

If \( \prod x_{i_1} \cdot \ldots \cdot x_{i_m} \) has \( \text{deg} \leq \frac{n}{2} + D \), leave it as is.

Else write as \( \prod_{i \in \mathcal{M}} x_{i_1} \cdot \ldots \cdot x_{i_m} = \prod_{i \in \mathcal{M}} x_{i} \cdot p(x_1, \ldots, x_n) \).

The dimension of the space of polynomials of degree \( \leq \frac{n}{2} + D \) is at most
\[
\binom{n}{\frac{n}{2} + D} \leq \frac{n!}{(\frac{n}{2} + D)! \cdot (\frac{n}{2})!} \leq \frac{2^n}{2 + \sqrt{n}} \cdot 2^n
\]

But \( \text{dim } = |S| \leq \frac{2^n}{2 + \sqrt{n}} \cdot 2^n \).

Putting things together: We have \( D \leq \frac{\sqrt{n}}{4} \) and \( |S| \leq \frac{3}{4} \cdot 2^n \).

\[
t \leq \frac{\sqrt{n}}{4} \quad \Rightarrow \quad t = \frac{1}{n^{2d}}
\]

\[
t = \frac{1}{n^{2d}} \quad \Rightarrow \quad 2^t \leq 2 \cdot \frac{1}{n^{2d}} \quad \Rightarrow \quad 2^t \leq 2 \quad \Rightarrow \quad 2 \cdot t \cdot s \geq \frac{1}{4} \quad \Rightarrow \quad s \geq 2.
\]