Today

- Proof of Toda's Theorem ($PH \subseteq P^{\#P}$)
  - Review Part 1: $PH \subseteq BP\cdot\oplus P$
  - Part 2: $BP\cdot\oplus P \subseteq P^{\#P}$
- Approximate Counting

Lecture 19

Computational Complexity (11 April, '20)

Instructor: Prahladh Harsha

Recall last time:

Part 1: $PH \subseteq BP\cdot\oplus P$

Theorem I: $\forall k, \forall m$, there is a probabilistic polynomial time reduction A that when given as input an instance ψ of $\exists_k$-SAT (an alternating quantified Boolean formula starting w/ $\exists$ & at most k alternations of quantifiers) outputs an instance $A(\psi)$ of $\oplus$SAT s.t.

ψ is true $\Rightarrow \Pr_A[A(\psi) \in \oplus SAT] \geq 1 - \frac{1}{2^m}$

ψ is false $\Rightarrow \Pr_A[A(\psi) \in \oplus SAT] \leq 1/2^m$.

ie, $\forall k, m$ $\exists$ redn A_k (randomized)

$$\exists_k\text{-SAT} \xrightarrow[\text{(rand)}]{A_k} \oplus SAT$$

BP

$\oplus$

error of redn $\leq \frac{1}{2^m}$

$\forall k$, Σ_k-SAT $\in BP\cdot\oplus P$

Part II : $\underbrace{BP\cdot\oplus P}_{\text{What is this class?}} \subseteq P^{\#P}$

$L \in \mathcal{C}$, $\quad \oplus L = \{ x \mid \#\{y \mid (x,y) \in L\} = \text{odd}\}$

$L \in \mathcal{C}$ $\quad BP\cdot L$: $\quad YES = \{x \mid \#\{y \mid (x,y) \in L\} \geq \frac{2}{3}\cdot \#y\text{'s}\}$

$NO = \{x \mid \#\{y \mid (x,y) \in L\} \leq \frac{1}{3}\#y\text{'s}\}$

$L \in BP\cdot\oplus P$

$\exists\, L' \in P$ s.t

Instances

$x \in L \Rightarrow \#\{y \mid \#\{z \mid (x,y,z) \in L'\} \text{ is odd}\} \geq \frac{2}{3}\#y\text{'s}$

$x \notin L \Rightarrow \#\{y \mid \#\{z \mid (x,y,z) \in L'\} \text{ is odd}\} \leq \frac{1}{3}\#y$

Obs: $BP\cdot\oplus P \subseteq P^{\#(P^{\#P})}$ (2 levels of counting)

Want: - reduce it to 1 level of counting

Idea:

$x \in L \Rightarrow \#\{z \mid \{(x,y,z) \in L'\}\} = 1 \pmod{2}$ for most y's

$x \notin L \Rightarrow \#\{z \mid (x,y,z) \in L'\} = 0 \pmod{2}$ for most y's

Instead of mod 2 this stmt was true for 2^k

$x \in L$

$\Rightarrow \#\{(y,z) \mid (x,y,z) \in L'\} \in \left[\frac{2}{3} \cdot 2^m, 2^m\right] \pmod{2^k}$

$\#y' = 2^m$

$x \notin L \Rightarrow \#\{(y,z) \mid (x,y,z) \in L'\} \in \left[0, \frac{1}{3} \cdot 2^m\right] \pmod{2^k}$

Qn: Can we distinguish these 2 cases

Yes, if $k \geq m$

Goal: Boost the modulus from $2 \rightarrow 2^k$.

Polynomial/Counting magic for #P:

① $f \in \#P, \quad g \in \#P \quad \Rightarrow \quad f+g \in \#P$

$\underbrace{\#\{y \mid M_f(x,y)=1\}}_{= f(x)}$ $\quad \underbrace{\#\{y \mid M_g(x,y)\}}_{= g(x)}$

$M_+(x, yb) = \begin{cases} 1 & \text{if } M_b(x,y)=1 \\ 0 & \text{otherwise} \end{cases}$

② $f \in \#P \ \& \ g \in \#P \quad \Rightarrow \quad f \cdot g \in \#P$

$f(x) = \#\{y \mid M_1(x,y)=1\}$ $\quad g(x) = \#\{z \mid M_2(x,z)=1\}$

$M_*(x,y,z) = \begin{cases} 1 & \text{if } M(x,y)=1 \ \& \ \tilde{M}(x,z)=1 \\ 0 & \text{o.w.} \end{cases}$

Claim: p be a poly w/ positive integer coeffs (eg: $p(x) = 2x^2+3x+1$)

$f \in \#P \quad \Rightarrow \quad p(f) \in \#P$

(as long as the coeffs are not too large)

Goal : Find a poly h s.t

$$a \equiv 1 \pmod 2 \Rightarrow h(a) \equiv 1 \pmod{2^k}$$
$$a \equiv 0 \pmod 2 \Rightarrow h(a) \equiv 0 \pmod{2^k}$$

Unfortunately, there is no such poly w/ positive coeffs & small coeffs. However following trick works (1 to -1).

Goal : Find a poly h s.t

$$a \equiv -1 \pmod 2 \Rightarrow h(a) \equiv -1 \pmod{2^k}$$
$$a \equiv 0 \pmod 2 \Rightarrow h(a) \equiv 0 \pmod{2^k}$$

Goal: Find a poly p s.t $\forall k$

$$a \equiv -1 \pmod{2^k} \Rightarrow p(a) \equiv -1 \pmod{2^{2k}}$$
$$a \equiv 0 \pmod{2^k} \Rightarrow p(a) \equiv 0 \pmod{2^{2k}}$$

$$h = \underbrace{p(p(p \ldots}_{\log k \text{ times}}(a)) \qquad 2 \rightarrow 2^k = 2^{2^{\log k}}$$

Claim: polynomial $p(x) = 3x^4 + 4x^3$ works.

Pf: $x \equiv 0 \pmod{2^k} \Rightarrow p(x) \equiv 0 \pmod{2^{2k}}$

$x \equiv -1 \pmod{2^k} \Rightarrow p(x) \equiv -1 \pmod{2^{2k}}$

Completes the proof that $BP \cdot \oplus P \subseteq P^{\#P}$.

Why this polynomial p

(1) $a \equiv 0 \pmod{2^k} \Rightarrow p(a) \equiv 0 \pmod{2^{2k}}$

(2) $a \equiv - \pmod{2^k} \Rightarrow p(a) \equiv -1 \pmod{2^{2k}}$

(3) p – positive integer coeffts

(1) is satisfied $a^2 / p(a)$ (No const & linear terms)

(2) is satisfied by $(a+1)^2 / (p(a)+1)$

One choice $p'(a)+1 = (a+1)^2(a-1)^2$

$$= (a^2-1)^2$$
$$= a^4 - 2a^2 + 1$$

But p' does not have +ve coeffts.

$p(a) = p'(a) + Ma^2(a+1)^2$ for every M also satisfies (1) & (2)

$$= (a^2-1)^2 + 2a^2(a+1)^2$$
$$= (a^4 - 2a^2 + 1) + (2a^4 + 4a^3 + 2a^2)$$
$$= 3a^4 + 4a^3 \checkmark$$

Completes the proof of Toda's Theorem $\boxtimes$

Approximate Counting:

$f \in \#P$ = Qn: $\forall \varepsilon$, Does $\exists$ alg A

$$(1-\varepsilon) f(x) \leq A(x) \leq (1+\varepsilon) f(x), \quad \forall x$$

This is also not an easy problem since for #SAT & any $\varepsilon \in (0,1)$ any such A will solve SAT.

Exact Counting is at least as hard as PH
Approximate Counting is at least as hard as NP.

Thm [Stockmeyer]
For every $f \in \#P$ & $\varepsilon \in (0,1)$, $\delta \in (0,1)$, there exists an randomized alg A_ε s.t

$$\Pr_A \left[(1-\varepsilon) f(x) \leq A_\varepsilon(x) \leq (1+\varepsilon) f(x) \right] \geq 1-\delta \quad \forall x$$

- using an SAT oracle
- and running in time $\mathrm{poly}(|x|, \frac{1}{\varepsilon}, \log \frac{1}{\delta})$.

Observations.

(1.) Suffices to solve the problem for #SAT.
(since there is a parsimonious redn from NP to SAT that preserves #witnesses.

(2) Sufficient to give an alg A that solves

$$\frac{1}{2} \cdot \#SAT(\varphi) \leq A(\varphi) \leq 2 \cdot \#SAT(\varphi)$$

Pf: A_ε: On input φ

1. $\psi = \varphi_1 \wedge \varphi_2 \ldots \wedge \varphi_k$ $\left(k = O\left(\frac{1}{\varepsilon}\right)\right)$
   disjoint vars
2. Solve $A(\psi)$.
3. Output.

φ has t sat assgns $\Rightarrow$ ψ has t^k sat assgns

$$\frac{1}{2} \cdot t^k \leq A(\psi) \leq 2 \cdot t^k$$

$$\left(\frac{1}{2}\right)^{1/k} \cdot t \leq \left(A(\psi)\right)^{1/k} \leq 2^{1/k} \cdot t$$

Choose k large enough st $2^{1/k} \leq (1+\varepsilon)$

& $\frac{1}{2^{1/k}} \geq 1-\varepsilon$

$k = O\left(\frac{1}{\varepsilon}\right)$ suffices.

(3) If a formula has φ has $O(1)$ assignments then $\#SAT(\varphi)$ can be obtained in P^{NP}

(Rand alg next lecture).