Today

Toda's Theorem: $PH \subseteq P^{\#P}$

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

Part 2: $BP\cdot\oplus P \subseteq P^{\#P}$

Lecture 18: Computational Complexity (2 Apr, 2020)

Instructor: Prahladh Harsha

Toda's Theorem: $PH \subseteq P^{\#P}$

Part 1: $PH \subseteq BP\cdot\oplus P$ [Valiant-Vazirani & extensions]

Part 2: $BP\cdot\oplus P \subseteq P^{\#P}$ [Modular Arithmetic Magic]

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.

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

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

Recall

$\oplus SAT = \{\varphi \mid \varphi$ has an odd # of sat assignments$\}$

Notation: $BP\cdot\mathcal{C}$, $\oplus\cdot\mathcal{C}$.

$\mathcal{C}$ - complexity class (eg: P)

① $\exists\cdot\mathcal{C} = \{L \,/\, \exists L' \in \mathcal{C},$
$x \in L \iff \underset{|y| = \mathrm{poly}(|x|)}{\underline{\exists y}},\ (x,y) \in L'\}$

Obs:
$\exists P = NP$

② $\oplus\cdot\mathcal{C} = \{L \,/\, \exists L' \in \mathcal{C}$
$x \in L \iff \#\{y \,/\, (x,y) \in L'\} = \text{odd}\}$

③ $BP\cdot\mathcal{C} = \{L \,/\, \exists L' \in \mathcal{C}.$
$x \in L \Rightarrow \#\{y \,/\, (x,y) \in L'\} \geq \frac{2}{3}\cdot\#y$
$x \notin L \Rightarrow \#\{y \,/\, (x,y) \in L'\} \leq \frac{1}{3}\cdot\#y\}$

Obs:
$BP\cdot P = BPP$

Classes of form:
$BP\ \oplus\cdot BP\cdot\oplus\cdot P$

Concise of writing Thm I

Theorem I: $\forall k,\ \Sigma_k^P \subseteq BP\cdot\oplus P$ [Operator Algebra]

Thm 1 in the flavour of Valiant-Vazirani

Thm [Valiant-Vazirani]

There exists a polynomial time randomized reduction A s.t $\forall$ n-var Boolean formulae f

$$\varphi \in SAT \Rightarrow \Pr[f(\varphi) \in USAT_Y] \geq \frac{1}{8n}$$

$$\varphi \notin SAT \Rightarrow \Pr[f(\varphi) \in USAT_N] = 1$$

Open: If $1/8n$ can be increased further in stmt above
([CH] - unlikely)

1 is an odd # & 0 is an even #.

Thm [Valiant-Vazirani]

There exists a polynomial time randomized reduction A s.t $\forall$ n-var Boolean formulae f

$$\varphi \in SAT \Rightarrow \Pr[f(\varphi) \in \oplus SAT] \geq \frac{1}{8n}$$

$$\varphi \notin SAT \Rightarrow \Pr[f(\varphi) \notin \oplus SAT] = 1$$

Now, we can increase $\frac{1}{8n} \rightarrow 1 - \frac{1}{2^m}$ for m of our choice.

Arithmetic with $\oplus$SAT formulae:

$$\bigoplus_x \varphi(x) \qquad \bigoplus_y \psi(y)$$

$$\left(\bigoplus_x \varphi(x)\right) \wedge \left(\bigoplus_y \psi(y)\right) = \bigoplus_{x,y} \left(\varphi(x) \wedge \psi(y)\right)$$

($\oplus P$ is closed under $\wedge$)

$$\neg\left(\bigoplus_x \varphi(x)\right) = \bigoplus_x \left((\varphi+1)(x)\right)$$

($\oplus P$ is closed under complementation)

$$(\varphi+1)(x) = \begin{cases} \varphi(x) & \text{if } x \neq 0^n \\ 1-\varphi(x) & \text{if } x = 0^n \end{cases}$$

Hence, it is also closed under $\vee$

$$\left(\bigoplus_x \varphi(x)\right) \vee \left(\bigoplus_y \psi(y)\right) = \bigoplus_{x,y} \left((\varphi+1)(x) \cdot (\psi+1)(y) + 1\right)$$

Run the V.V redn on i/p φ - k times to get $\psi_1 \ldots \psi_k$

$\varphi \in SAT \Rightarrow \Pr[\exists i : i \in [k], \psi_i \in \oplus SAT] \geq 1-\left(1-\frac{1}{8n}\right)^k$

$\varphi \notin SAT \Rightarrow \Pr[\exists i \in [k], \psi_i \in \oplus SAT] = 0$

$\exists i, \psi_i \in \oplus SAT \longrightarrow \bigoplus_x \psi \in \oplus SAT$

Choose $k = O(mn)$

$\varphi \in SAT \Rightarrow \Pr[\psi \in \oplus SAT] \geq 1 - \frac{1}{2^m}$

$\varphi \notin SAT \Rightarrow \Pr[\psi \in \oplus SAT] = 0$

When written in terms of $\oplus SAT$ (instead of USAT), the conclusion of VV can be strengthened (i.e., the error probability can be reduced arbitrarily).

This proves Thm 1 for the case of NP ⊆ coNP

How do we extend it to all $\exists_k$-SAT.

Idea: (1) By induction on k.

(2) Valiant-Vazirani is "oblivious"

What do want for $k=2$.

$k=1$ $\quad \exists x\, \varphi(x) \xrightarrow{A_1} \psi$

$$\left.\begin{array}{l} \exists x\, \varphi(x) \Rightarrow \Pr[\psi \in \oplus SAT] \geq 1-\frac{1}{2^m} \\ \nexists x\, \varphi(x) \Rightarrow \Pr[\qquad\qquad] = 0 \end{array}\right]$$

$k=2$ $\quad \exists x \forall y\, \varphi(x,y) \xrightarrow{A_2} \psi$

$$\exists x \forall y\, \varphi(x,y) \Rightarrow \Pr[\psi \in \oplus SAT] \geq 1-\frac{1}{2^m}$$

$$\forall x \exists y\, \overline{\varphi}(x,y) \Rightarrow \Pr[\psi \in \oplus SAT] \leq 1/2^m$$

Obliviousness of V.V

$\varphi \xrightarrow{f} \psi$

$\psi(x) = \varphi(x) \wedge (h(x)=1)$

Thm [Valiant-Vazirani] Oblivious version

There exists a polynomial time randomized reduction A s.t on 1^n, outputs a Boolean formula $\tau(x,y)$ where x is n-vars & y is a new set of vars. s.t $\forall$ Boolean fn $\beta : \{0,1\}^n \to \{0,1\}$

$$\exists x\, \beta(x) \Rightarrow \Pr\left[\bigoplus_{x,y}\left(\beta(x) \wedge \tau(x,y)\right)\right] \geq \frac{1}{8n}$$

$$\nexists\, \beta(x) \Rightarrow \Pr\left[\bigoplus_{x,y}\left(\beta(x) \wedge \tau(x,y)\right)\right] = 0.$$

Proof of Theorem I:

$\exists x\, \psi(x)$ $\qquad\qquad$ $\psi(x)$ – $(k-1)$ quantifiers.

By induction hypothesis.

there is a randomized redn that maps for each x

$$\psi(x) \rightsquigarrow \beta(x) = \bigoplus_{z} \rho(x,z)$$

is equivalent to $\psi(x)$ w/ prob $\geq 1 - \frac{1}{2^{m+1}}$

Oblivious VV will tell you that

$\beta(x) \wedge \tau(x,y) \in \oplus SAT$ w/p $\frac{1}{8n}$ if $\beta(x)$ is true.

Run Oblivious VV $R = O(mn)$ times

$$\alpha = \bigvee_{j=1}^{R} \left(\beta(x) \wedge \zeta(x, y_j)\right)$$

$$\exists x\ \psi(x) \Rightarrow \Pr[\alpha \in \oplus SAT] \geq \left[1 - \left(1 - \frac{1}{8n}\right)^R + \frac{1}{2^{m+1}}\right]$$

(α is an $\vee$ but can be converted to $\oplus$)

$$\nexists x\ \psi(x) \Rightarrow \Pr[\alpha \in \oplus SAT] \leq 0 + \frac{1}{2^{m+1}}$$

$R = O(m, n)$ — $\left(1 - \frac{1}{8n}\right)^R = \frac{1}{2^{m+1}}$

Hence $\frac{1}{2^{m+1}} + \frac{1}{2^{m+1}} = \frac{1}{2^m}$ — reqd error. $\boxtimes$