Toda's Theorem`

15 April, 2021 15:05

UNIQUE-SAT = { φ : φ is satisfiable Boolean formula with exactly one satisfying assignment }

Q: Is UNIQUE-SAT NP-complete?

... Almost. Via probabilistic reduction.

We will build a probabilistic alg f which takes as its input a Bool. fle φ & outputs another Bool. fle

$$\varphi' = F(\varphi) \quad \text{s.t.}$$

$$\varphi \in SAT \implies \text{prob. } \varphi' \in SAT \geq \frac{1}{50n}$$

$$\varphi \notin SAT \implies \varphi' \text{ is never satisfiable}$$

$\to$ $F(\varphi(x)) = \varphi(x)$ & $h(x)$ where $h(x)$ restricts the possible satisfying ass. of φ.

technique (Isolation lemma):

Let $S \subseteq \{0,1\}^n$. E.g. $S = \{x ; \varphi(x) \text{ is true}\}$

Set k so that $2^{k-2} \leq |S| \leq 2^{k-1}$

Consider a random linear fcn over $GF(2)$

$$h_{A,b} : \{0,1\}^n \longrightarrow \{0,1\}^k$$

... 2-universal hash system

$h_{A,b}(x) = Ax + b$ $A \in \{0,1\}^{k \times n}$ $b \in \{0,1\}^k$

$_{A,b}$ hash algorithm

$$h_{A,b}(x) = Ax + b \qquad A \in \{0,1\}^{k \times n} \quad b \in \{0,1\}^k$$

- $\forall\, x \neq y \in \{0,1\}^n \qquad \Pr_{h_{A,b}}\left[h_{A,b}(x) = h_{A,b}(y) \right] = 2^{-k}$ (Exc)

$h_{A,b}$ ← random matrix A & vector b

for a fcn $h: \{0,1\}^n \to \{0,1\}^k$ define $C_h = \{\{x,y\} \in S^2 ;\ h(x) = h(y), x \neq y\}$

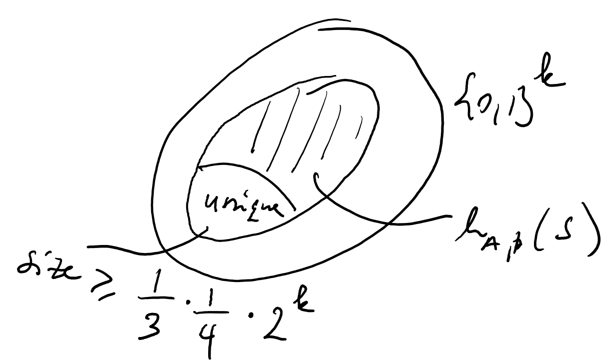
- $\mathbb{E}_{h_{A,b}}\left[|C_{h_{A,b}}| \right] = 2^{-k} \cdot \binom{|S|}{2} \le \frac{|S|}{4}$

$\Rightarrow \Pr_{h_{A,b}}\left[|C_h| \ge \frac{1}{3}|S| \right] \le \frac{3}{4}$ by Markov Ineq.

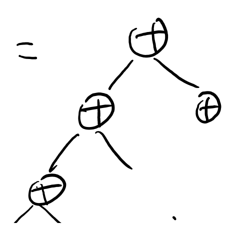
$\Rightarrow$ with probability at least $1/4$, at least $1/3$ fraction of elt's in S are mapped uniquely.

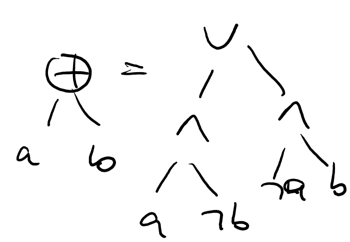
Since $b \in \{0,1\}^k$ is a random shift for $h_{A,b}$:

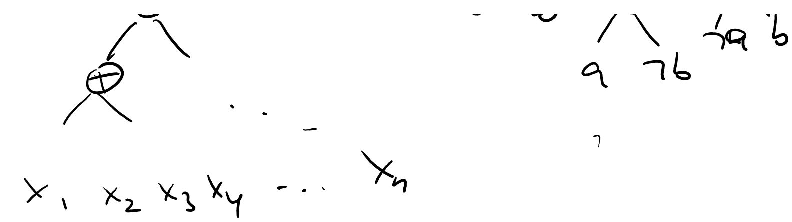
$$P_{h_{A,b}}\left[\exists!\, x \in S ;\ h_{A,b}(x) = 0^n \right] \ge \frac{1}{3 \cdot 16} = \frac{1}{48}$$



- formula for PARITY$(x_1, x_2, \ldots x_n)$ =







→ n^2 size formula for PARITY$(x_1, \dots x_n)$ using $\wedge, \vee, \neg$.

→ randomized reduction f : pick $k \in \{1, \dots, n\}$
pick $A \in \{0,1\}^{k \times n}$
$b \in \{0,1\}^k$
at random

output $\varphi'(x) = \varphi(x)$ & "$\underbrace{h_{A,b}(x) = 0^n}$"
k parities of subsets of $x_1, \dots x_n$ given by A & b.

$\varphi(x) \in SAT \Rightarrow \frac{1}{50 \cdot n}$ prob. $\varphi'(x) \in$ UNIQUE-SAT

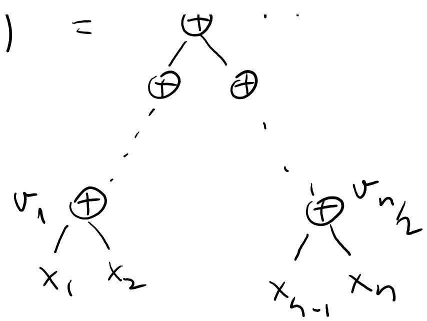
$\varphi(x) \notin SAT \Rightarrow \varphi'(x) \notin$ UNIQUE-SAT

→ repeat k-times and if any of the formulas is from UNIQUE-SAT $\Rightarrow \varphi$ is satisfiable

$k \simeq 500n$ prob of error $\leq \left(1 - \frac{1}{50n}\right)^{500n}$

$\leq e^{-\frac{1}{50n} \cdot 500n} \leq \frac{1}{1000}$

• PARITY$(x_1, \dots x_n)$ = $\oplus^{n-1}$ can be expressed as a uniquely

• PARITY$(x_1, \ldots, x_n)$ =  [illegible]

as a uniquely satisfiable 3SAT formula by introducing new variable v_i for each gate which should represent the gate value. Replacing the parity tree by a conjunction of 3SAT f-les, each representing the constraints on neighboring variables gives uniquely satisfiable 3SAT. (Unique sat. assignment to $v_1, \ldots v_{n-1}$)

<u>Toda's theorem</u>: 1) $PH \subseteq BPP^{\oplus P}$

2) $PH \subseteq P^{\#SAT}$

• We will show the first claim only

• <u>Define</u> $\oplus$ quantifier: $\oplus \bar{x}\, \varphi(\bar{x})$ ... true if $\varphi(\bar{x})$ has odd number of satisfying assignments for $\bar{x}$.

e.g. $\varphi(\bar{x}) \in$ UNIQUE-SAT $\Rightarrow \oplus \bar{x}\, \varphi(\bar{x})$ is true.

- <u>op's with $\oplus$</u> :

- $\neg \oplus \bar{x}\, \psi(\bar{x}) \equiv \oplus \bar{x}, y\ (y=0 \,\&\, \bar{x}=\bar{0}) \vee (y=1 \,\&\, \psi(\bar{x}))$

- $\oplus \bar{x} \oplus y\ \psi(\bar{x},\bar{y}) \equiv \oplus \bar{x}\bar{y}\, \psi(\bar{x},\bar{y})$

- $\oplus \bar{x}\, \psi(x) \,\&\, \oplus \bar{y}\, \varphi(y) = \oplus \bar{x}\bar{y}\, (\psi(x) \,\&\, \varphi(y))$

- $$\bigvee_{i=1}^{\ell} \oplus \bar{x}_i\, \varphi_i(\bar{x}_i) = \underbrace{\neg \underbrace{\bigwedge_{i=1}^{\ell} \underbrace{\neg \oplus \bar{x}_i\, \varphi_i(\bar{x}_i)}_{n+1 \text{ var's}}}_{\ell \times (n+1) \text{ var's}}}_{1+\ell(n+1) \text{ var's}}$$

<u>Pf of $PH \subseteq BPP^{\oplus P}$</u> :

<u>idea</u>: convert all quantifiers to $\oplus$ quantifiers

<u>step</u>: $\exists \bar{x} \oplus \bar{y}\, \varphi(\bar{x},\bar{y},\bar{z})$ $\quad$ $\bar{z}$ ... m free var's, $\bar{x}$ ... n var's

$\overset{\text{want}}{\Longrightarrow}$ $\oplus \bar{x}\bar{y}\bar{w}\ \varphi'(\bar{x},\bar{y},\bar{z},\bar{w})$ ... equivalent to $\exists \bar{x} \oplus \bar{y}\, \varphi(\bar{x},\bar{y},\bar{z})$ for all settings of $\bar{z}$

$\rightarrow$ pick $k \in \{1,\dots,n\}$ at random
$h : \{0,1\}^n \rightarrow \{0,1\}^k$ at random among linear

hash fcn's over $GF[2]$

For fixed $\bar{z} \in \{0,1\}^m$

1) If $\exists \bar{x} \oplus \bar{y}\, \varphi(\bar{x},\bar{y},\bar{z})$ is true then

$$\Pr\left[\oplus \bar{x} \oplus \bar{y} \left(\varphi(\bar{x},\bar{y},\bar{z}) \,\&\, h(\bar{x}) = 0^k\right) \text{ is true}\right] \geq \frac{1}{50n}$$

2) If $\exists \bar{x} \oplus \bar{y}\, \varphi(\bar{x},\bar{y},\bar{z})$ is false then

$$\Pr\left[\oplus \bar{x} \oplus \bar{y} \left(\varphi(\bar{x},\bar{y},\bar{z}) \,\&\, h(\bar{x}) = 0^k\right) \text{ if true}\right] = 0$$

$\Rightarrow$ repeat the procedure ℓ-times for independently chosen k & h and take OR of the formulas:

$\ell = 100 \cdot m \cdot n$

In 1) $$\Pr\Big[\overbrace{\bigvee_{i=1}^{\ell} \oplus \bar{x} \oplus \bar{y} \left(\varphi(\bar{x},\bar{y},\bar{z}) \,\&\, h_i(\bar{x}) = 0^{k_i}\right)}^{(***)} \text{ is true}\Big] \geq 1 - 2^{-2m}$$

$$\left(1 - \frac{1}{50n}\right)^{\ell} \leq e^{-\frac{\ell}{50n}} = e^{-2m}$$

In 2) $\Pr\left[\bigvee \ \ldots \right] = 0$

We can transform $(***)$ into $\oplus \bar{x}' \varphi'''(\bar{x}', \bar{z})$ equivalent to the original formula for each z w.p. $\geq 1 - 2^{-2m}$.

$\Rightarrow$ w.p. $\geq 1 - 2^{-n}$, $\oplus \bar{x}' \varphi'''(\bar{x}', \bar{z})$

is equivalent to $\exists \bar{x} \oplus y\, \varphi(\bar{x}, \bar{y}, \bar{z})$
for all $\bar{z} \in \{0,1\}^m$.

$\varphi''()$ is polynomially larger than $\varphi()$.

- for $\forall \bar{x} \oplus \bar{y}\, \varphi(\bar{x}, \bar{y}, \bar{z})$ we use

$$\neg \exists \bar{x}\ \underbrace{\underbrace{\underbrace{\neg \oplus \bar{y}\, \varphi(\bar{x}, \bar{y}, \bar{z})}_{\oplus \bar{y}'\, \varphi(\bar{x}, \bar{y}', \bar{z})}}_{\oplus \bar{x}'\, \varphi'''(\bar{x}', \bar{z})}}_{\oplus \overline{x''}\, \varphi''''(\overline{x''}, \bar{z})}$$

→ we can convert quantifiers $\forall$ & $\exists$ one by one into $\oplus$ quantifiers. If the # of quantifiers is fixed, the resulting formula has size polynomially related to the original formula & it will be equivalent to it with prob. close to 1.

→ prob alg for deciding quantified Bool. formula with fixed # of alternations using a single

2 query to $\oplus P$.

$\Rightarrow$ $PH \subseteq BPP^{\oplus P}$.