Michael Forbes
miforbes@illinois.edu

2019-03-14.4
2019-03-26.2 ⇄ 2019-03-28.1
cs579

cs574 Computational Complexity: lecture 19 14 22

admin: project topics Friday

today: - unique SAT
- Valiant Vazirani theorem
- Toda's theorem [statement]

motivation: solutions are often unique - passwords [up to hashing]
- clustering [the "truth"]

unique solutions can be "easier" to find

eg: search ≤ decision for formula $\varphi(x_1, \dots x_n) \in SAT$

$$b_1 = \begin{cases} 1 & \varphi(1, x_2, \dots x_n) \in SAT \\ 0 & \text{else} \end{cases}$$

$$b_2 = \begin{cases} 1 & \varphi(b_1, 1, x_3, \dots x_n) \in SAT \\ 0 & \text{else} \end{cases}$$

sequential process

$$\Rightarrow \varphi(b_1, \dots, b_n) = 1$$

search ≤ decision for uniquely satisfiable φ

$$b_i = \begin{cases} 1 & \varphi(x_1, \dots x_{i-1}, 1, x_{i+1}, \dots x_n) \in SAT) \\ 0 & \text{else} \end{cases}$$

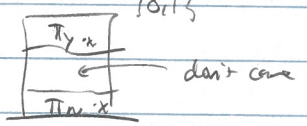
compute all b_i in parallel

$$\Rightarrow \varphi(b_1, \dots b_n) = 1$$

Q: are NP problems easier if they have unique solutions?

A [Valiant Vazirani] (disjoint): no [how to formalize?]

def - $\Pi_Y \sqcup \Pi_N \subseteq \{0,1\}^*$ is a promise problem



eg - $\Pi_Y = L$, $\Pi_N = \{0,1\}^* \setminus L$ [language problem]

eg - $\Pi_Y = \{\varphi \mid \exists! x \ \varphi(x) = 1\}$
$\Pi_N = \{\varphi \mid \nexists x \ \varphi(x) = 1\}$
(Π_Y, Π_N) = UNIQUE-SAT
= USAT

eg $\Pi_Y = \{\langle M, x\rangle \mid M$ randomized TM, $\Pr[M \text{ acc } x] \geq 2/3\}$
$\Pi_N = \{$ " $\leq 1/3\}$
↳ captures BPP

def - (Π_Y, Π_N) is in promise P = pr P, pr RP, pr BPP
if poly-time TM^M s.t.

$x \in \Pi_Y \Rightarrow$	M acc x	$\Pr[M \text{ acc } x] \geq 1/2$	$\geq 2/3$	
$x \in \Pi_N$	M rej x	" $= 0$	$\leq 1/3$	

def: $\Pi = (\Pi_Y, \Pi_N)$ poly-time reduces to $\Pi' = (\Pi_Y', \Pi_N')$ written $\Pi \leq_p \Pi'$ if poly-time f s.t. $x \in \Pi_Y \Rightarrow f(x) \in \Pi_Y'$
$x \in \Pi_N \Rightarrow f(x) \in \Pi_N'$

Michael Forbes
miforbes@illinois.edu
2019-03-26.2 ← 2019-03-26.1
→ 2019-03-26.3
CS579

eg: ↑ is prBPP complete wrt $\leq_p$ reductions

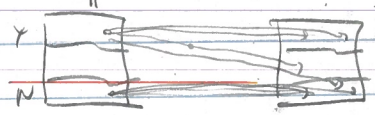
Cor: $\Pi \leq_p \Pi'$, $\Pi' \in_{p,r} P \Rightarrow \Pi \in_{p,r} P$

def: $\Pi \leq_{RP} \Pi'$ [randomized reduction] if poly time f s.t. (one-sided, randomized)

$x \in \Pi_Y \Rightarrow \Pr[f(x) \in \Pi'_Y] \geq 1/\text{poly}(|x|)$

$x \in \Pi_N \Rightarrow \Pr[f(x) \in \Pi_N] = 1$

Rmk: - f not a function, is randomized function $x \mapsto f(x,r)$



[can go outside problem]

Cor: $\Pi \leq_{RP} \Pi'$, $\Pi' \in_{p,r} RP \Rightarrow \Pi \in_{p,r} RP$

Pf: $x \in \Pi_Y \Rightarrow \Pr_{f}[f(x) \in \Pi'_Y] \geq 1/2 \Rightarrow \Pr[M' \text{ acc } f(x)] \geq \frac{1}{2}\cdot\frac{1}{\text{poly}} = \frac{1}{\text{poly}}$

$\Pi_N \Rightarrow \in \Pi'_N = 1$ $\quad = 0$

$\Rightarrow \Pi \in_{p,r} RP$ via completeness

Thm [Valiant Vazirani] USAT $\in_{RP}$ SAT

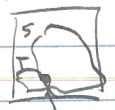
$\varphi \in SAT \Rightarrow \Pr[f(\varphi) \in USAT_Y] \geq 1/8n$

$\notin \quad USAT_N = 1$

Cor: $USAT \in_{p,r} RP \Rightarrow SAT \in_{p,r} RP \Rightarrow SAT \in RP \Rightarrow NP = RP$

Pf: idea: suffices to show SAT $\leq_{RP}$ UNIQUE-CKT-SAT $\leq_p$ UNIQUE 3SAT ↑ preserves # solns

idea: $\varphi(x)$ $x \in \{0,1\}^n$ $S = \{x : \varphi(x) = 1\}$



Choose $\psi(x)$ w/ $T = \{x : \psi(x) = 1\}$ [like]

consider $\varphi \wedge \psi$ want uniquely satisfiable

idea: choose ψ so $\forall x$ $\psi(x) = \begin{cases} 1 & \text{w/p } 1/|S| \\ 0 & \end{cases}$

$\Rightarrow \mathbb{E}[\#\text{solns to } \varphi \wedge \psi] = \mathbb{E} \sum_x \varphi(x) \wedge \psi(x)$

$= \sum_{x \in S} \Pr[\psi(x) = 1] = |S| \cdot \frac{1}{|S|} = 1$ [good so far]

$\Rightarrow \Pr[|S \cap T| = 1] = \sum_{x \in S} \Pr[S \cap T = \{x\}] = \sum_{x \in S} \frac{1}{|S|}\left(1 - \frac{1}{|S|}\right)^{|S|-1}$

$= \left(1 - \frac{1}{|S|}\right)^{|S|-1} \geq 1/e$

$\Rightarrow \Pr[\varphi \wedge \psi \in USAT_Y] \geq 1/e$ if $\varphi \in SAT$

$USAT_N = 1$ $\notin$ [done?]

problems - don't know $|S|$ [#P-hard] idea: - approximate $|S| \approx 2^k$ $k = \lceil \lg |S| \rceil$

- guess k

- $\psi(x)$ may not have small ckt idea: replace random choices w/ pseudorandom choices

Michael Forbes
mforbes@illinois.edu

2019-03-26.2 ⟵ 2019-03-26.3
2019-03-26.4 CS577

$\mathbb{F}_2 = \{0,1\}$ finite field

def: $h : \mathbb{F}_2^n \times \mathbb{F}_2^\ell \to \mathbb{F}_2^k$ is pairwise independent if

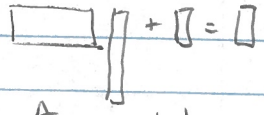
$\forall x \neq y \in \mathbb{F}_2^n$, $c, d \in \mathbb{F}_2^k$: $\Pr_{s \in \mathbb{F}_2^\ell}[h(x,s) = c \wedge h(y,s) = d] = \frac{1}{(2^k)^2}$ ‖ mimic random function ‖

seed length $= \ell$

Rmk: truly random function has $\ell = k \cdot 2^n$

Lem: $h : \mathbb{F}_2^n \times (\mathbb{F}_2^{k \times n} \times \mathbb{F}^k) \to \mathbb{F}^k$ defined by $h(x) = Ax + b$

is pairwise independent, seed length $= k \cdot (n+1)$



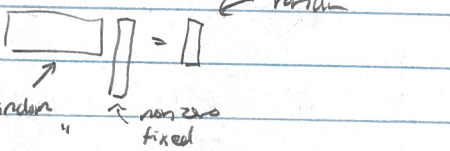
Pf: $\Pr_{A,b}[Ax + b = c \wedge Ay + b = d]$

$= \Pr[Ax + b = c \wedge A(x-y) = c - d]$

$= \Pr_{A,b}[Ax + b = c \mid A(x-y) = c-d] \cdot \Pr_A[A(x-y) = c-d]$ ← $\frac{1}{2^k}$

$A(x-y) = c-d$ independent of b; $x - y \neq 0$

↳ $b = c - Ax$, $\frac{1}{2^k}$



$= \frac{1}{2^k} \cdot \frac{1}{2^n} = \frac{1}{(2^k)^2}$

$\sum_{i : (x-y)_i \neq 0} A_{\cdot,i}$ ← random column vec

nonempty

Rmk: - seed length $\ell = k \cdot (n+1) \ll k \cdot 2^n$

- can get $\ell \leq O(k+n)$

Lem: $S \subseteq \mathbb{F}_2^n$, $2^{k-2} \leq |S| \leq 2^{k-1}$

$h : \mathbb{F}_2^n \times \mathbb{F}_2^\ell \to \mathbb{F}_2^k$ pairwise indep

$\Rightarrow \Pr_\Delta[|S \cap \underbrace{\{x : h(x, \Delta) = 0^k\}}_{T}| = 1] \geq 1/8$

Pf: $\mathbb{E}|S \cap T| = \sum_{x \in S} \frac{1}{2^k} \geq \frac{1}{4}$

union bound: $\Pr[|S \cap T| = 1] \leq \sum_{x \in S} \Pr[x \in T] \leq 1/2$

inclusion exclusion: $\geq \underbrace{\sum_{x \in S} \Pr[x \in T]}_{\geq 1/4} - \underbrace{\sum_{x \neq y \in T} \Pr[x, y \in T]}_{\leq \frac{1}{2^n} \cdot \frac{1}{2^k}}$

$\leq \frac{|S|^2}{2} \leq \frac{(2^{k-1})^2}{2}$

$\geq \frac{1}{4} - \frac{1}{8} \geq 1/8$. ∎ $\leq 1/8$

Pf [Valiant-Vazirani]

given φ

pick $k \in \{2, \ldots, n+1\}$ at random ← n choices

pick $h : \mathbb{F}_2^n \times \mathbb{F}_2^{k(n+1)} \to \mathbb{F}_2^k$ by random $\Delta \in \mathbb{F}_2^{k(n+1)}$

output $\varphi(x) \wedge \underbrace{[h(x, \Delta) = 0^k]}_{\psi(x)}$ ← polysize ckt

Michael Forbes
MForbes@illinois.edu
2019-03-26.4 ← 2019-03-26.3
2019-03-28.1
cs579

complexity :

correctness : $\varphi \notin SAT \Rightarrow \varphi \wedge \psi \notin SAT \Rightarrow \varphi \wedge \psi \in USAT_N$

$\varphi \in SAT \Rightarrow \Pr[2^{k-2} \le |S| \le 2^{k-1}] \ge 1/n$

$\Pr[|SAT| = 1] \ge 1/8$

$\Rightarrow \Pr[\varphi \wedge \psi \in USAT_\psi] \ge 1/8n$ ∎

what happened : guessed approx to $\#\{x : \varphi(x) = 1\}$
used pseudorandom filter to get unique SAT

Cor : RP reduction $\varphi \in SAT \Rightarrow \Pr[f(\varphi) \in \oplus SAT] \ge 1/8n$

$\varphi \notin SAT \Rightarrow \Pr[f(\varphi) \in \oplus SAT] = 0$

$\{\varphi : \#\{x : \varphi(x) = 1\} = 1 \bmod 2\}$

[counting]

ie : $NP \subseteq RP^{\oplus P} \subseteq BPP^{\oplus P}$

$\Rightarrow NP^{NP} \subseteq BPP^{\oplus P^{NP}} \subseteq BPP^{\oplus P^{BPP^{\oplus P}}} \subseteq BPP^{\oplus P}$ ← Chernoff + Union

...

$\Rightarrow PH \subseteq BPP^{\oplus P} \subseteq P^{\#P}$ ← modular arithmetic trick

Thm [Toda] : $PH \subseteq P^{\#P}$

Rmk : "just" - Valiant Vazirani
- error reduction
- modular trick

- $\oplus P, \#P$ are powerful

next time : interactive proofs