Michael Forbes
miforbes@illinois.edu

2019-03-26.4 → 2019-03-28.1
2019-03-25.2 ← CS579

CS579: Computational Complexity: Lecture 20 15

admin: ps4 back avg = 35/40

today: interactive

Q: what is computation?
- deterministic
- non uniform
- nondeterministic
- alternation
- randomness

Q: what is a proof? [NP, PH, ...]
randomness?
interaction? [eg: teaching]

mark: true statements have "proof" $x \in L$: completeness
false " no " $\notin$: soundness

eg: green vs blue [colorblindness]

def: $f, g : \{0,1\}^* \to \{0,1\}^*$ $k \in \mathbb{N}$. a k-round interaction of f, g on x denoted $(f \leftrightarrow g)_k(x)$ is a transcript $a_1, \dots, a_k \in \{0,1\}^*$

$a_1 = f(x)$
$a_2 = g(\langle x, a_1 \rangle)$
$a_3 = f(\langle x, a_1, a_2 \rangle)$
$a_4 = g(\ \ -\ \ )$

$a_k = \ \ -\ \ $ ← all messages

the output is $f(\langle x, a_1, \dots, a_k \rangle)$

rounds = k [Mars delay is 4-24 minutes]

f speaks first

def: language L has a deterministic k-round interactive proof if exists $V : \{0,1\}^* \to \{0,1\}^k$ s.t. V computable by deterministic TM s.t.
- $V(\langle x, a_1, \dots, a_\ell \rangle)$ takes time $\le \text{poly}(|x|)$ [$\Rightarrow \ell \le \text{poly}|x|$]
- completeness: $x \in L \Rightarrow \exists P : \{0,1\}^* \to \{0,1\}^*$ s.t. output $(V \leftrightarrow P)(x) = 1$ [prover speaks first]
- soundness: $x \notin L \Rightarrow \forall P$ " $= 0$

[IP = {L : L has poly(|x|) round interactive proof}]

Rmk: P is computationally unbounded

Michael Forbes
mikefobes@illinois.edu
2019-03-28.2 ← 2019-03-28.1
→ 2019-03-28.3
CS574

Prop: $dIP = NP$ ← $\in \{0,1\}^{poly(|x|)}$

pf: $\supseteq$: "$L = \{x : \exists y : M(x,y)=1\}$"

P —y→ V

output $M(x,y)$

$\subseteq$: dIP:

P ⇄ V (messages a_1, a_2, a_3)

P' —$a_1,\dots,a_k$→ V'

- check $a_1 = V(\langle x, \rangle)$
- $a_3 = V(\langle x, a_1, a_2, \rangle)$
- $a_{2k+1} = V(\langle x, a_1, \dots, a_{2k} \rangle)$
- output $V(\langle x, a_1, \dots, a_k \rangle)$

output y

NP: $x \in L \Rightarrow \exists\, a_1,\dots,a_k$ exists. w/ — output 1

$\notin \Rightarrow \forall$ any $a_1,\dots,a_k$ either fails check → V' outputs 0 — output 0

Thus no interesting, how do we make it interesting??

def: language L has k-round interactive proof, denoted $L \in IP[k]$,

if $V: (\{0,1\}^*)^2 \to \{0,1\}^*$ computable by deterministic TM s.t.

- $x \in L \Rightarrow \exists P: \{0,1\}^* \to \{0,1\}^*$ s.t. $\Pr_{r \in \{0,1\}^{poly|x|}}[\text{output}(V(\cdot,r) \leftrightarrow P))(x) = 1] \geq 2/3$
- $x \notin L \Rightarrow \forall P$ " $\leq 1/3$
- $V(\cdot,\cdot)$ on $(\langle x, a_1, \dots, a_k \rangle, r)$ runs in $poly(|x|)$ time

$IP = \{L : poly(n)$ round interactive proof for $L\}$

Rmk: - prover cannot see r ← "private coins"

- equiv: V is probabilistic TM, can flip additional coins each round

= Questions?

Q: What is part of IP?

Sam: $NP = dIP = IP$

$coNP \stackrel{?}{\subseteq} IP \subseteq ?$

Prop: $IP \subseteq PSPACE$

pf: rules = compute strategy of best prover

$x \in L \Rightarrow \exists P \Pr_r[(P \leftrightarrow V(\cdot,r))(x) = 1] \geq 2/3 \Rightarrow$ best $\geq 2/3$

$\notin \quad \forall P \quad < 1/3 \Rightarrow$ best $\leq 1/3$

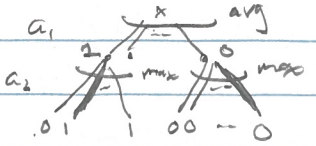
Last: compute

Michael Forbes
mforbes@illinois.edu

2019-03-28.2 → 2019-03-28.3
2019-03-28.4 ← CS579

[similar to games in PSPACE, but now with randomized players]

eg. $k=2$: interactive proof $V(\cdot,r)$ $\leftrightarrow$ P



idea - prover should pick best answer at each stage

$$\mathrm{val}(\langle x, a_1, -, a_\ell\rangle) := \max_r \Big[(V(\cdot,r) \leftrightarrow P)(x) = 1 \;\Big|\; a_1, -a_\ell \text{ sent} \Big]$$

↑ condition over r

[k-round] $\mathrm{val}(\langle x, a_1, -, a_k\rangle) = \begin{cases} 1 & \text{output } 1 \\ 0 & \text{output } 0 \end{cases}$

prover's move: $\mathrm{val}(\langle x, a_1, -a_\ell\rangle) = \max_{a_{\ell+1}} \mathrm{val}\langle x, a_1, -a_\ell\rangle$ [best response]

verifier's move: $= \mathop{\mathbb{E}}_{a_{\ell+1}} [\mathrm{val}\langle x, a_1, -a_{\ell+1}\rangle \mid a_1, -a_\ell \text{ sent}]$

$$= \sum_{a_{\ell+1}} \mathrm{val}\langle x, a_1, -, a_{\ell+1}\rangle \cdot \Pr[a_{\ell+1} \text{ sent} \mid a_1, -a_\ell \text{ sent}]$$

induction: $x \in L \Rightarrow \mathrm{val}\langle x\rangle \geq 2/3$

$\notin$ $\in 1/3$

Claim: $\mathrm{val}(\cdot)$ computable in PSPACE [same as before]

Pf: tree is of depth $\leq \mathrm{poly}(|x|) \Rightarrow$ polynomial space to traverse

computing each move is in PSPACE - average sums
- maximum

$$\Pr[a_{\ell+1} \text{ sent} \mid a_1, -a_\ell \text{ sent}] = \frac{\#\{r \text{ consistent w/ } a_1, a_2, -a_\ell, a_{\ell+1}\}}{\#\{r \text{ consistent w/ } a_1, -a_\ell\}}$$

[cheap] [PS]

Cor: IP_δ: $x \in L \Rightarrow \Pr[(V \leftrightarrow P)(x) = 1] \geq 1/2 + \delta$

$\notin$ $\leq 1/2 - \delta$

then $\mathrm{IP}_{1/n} = \mathrm{IP}_{1/6} = \mathrm{IP}_{1/2 - 1/2^n}$ [error reduction, as in BPP]

Pf: protocol: run $V(\cdot, r_1) \leftrightarrow P$ in sequence, take majority vote of outputs

$V(\cdot, r_2) \leftrightarrow P$ independent!

$V(\cdot, r_2) \leftrightarrow P$

complexity: clear

analysis: Chernoff bound [as done before]

but: prover can change strategies each trial, which violates independence!

Michael Forbes
Mforbes@illinois.edu
2019-03-28.4 ← 2019-03-28.3
→ 2019-04-02.1
c5579

Claim: optimal strategy in sequentially repeated game is repeated optimal strategy

⇒ each trial is independent

→ Pf: once $V(\cdot, r_1) \leftrightarrow P$ is dealt, any strategy player can play is no better than optimal when played a fresh $V(\cdot, r_2) \leftrightarrow P$, same for $V(\cdot, r_i) \leftrightarrow P$. ∎

Rmk: complementary / subadditivity

	$\geq 2/3$		$\geq 1 - 1/2^n$
	$\in Y_3$	⇒	$\leq 1/2^n$
	$\geq 1/2$	⇒	1
	$=0$		0
	$=1$		
	$\leq 1/2$	⇐	$\geq 2/3$
			$\leq 1/3$

= NP ∎ exercise

∎ will see T

next time: part of Pf