Michael Forbes
mforbes@illinois.edu

2019-03-28.4 → 2019-04-02.1
2019-04-02.2 ← CS 579

CS 579 Computational Complexity: Lecture 21 — 4/4 23

admin: project topic assignments released — presentation [see syllabus] — report
PS 5 due Thursday

last time: interactive proofs — IP ⊇ NP, BPP
— in PSPACE

today: $P^{\#P} \subseteq IP$

Thm [Lund Fortnow Karloff Nisan]: #3-SAT ∈ IP ← boolean formula

$\{\langle \varphi, k\rangle : \#\{x : \varphi(x)=1\} = k\}$

Cor: $coNP \subseteq PH \subseteq P^{\#P} \subseteq IP$ ↳ coNP-hard if $k=0$

↑ today

$P \xrightarrow{\varphi_n} V$ + #SAT is #P complete

$\langle \varphi, k\rangle \in \#SAT$

[not main, but is helpful]

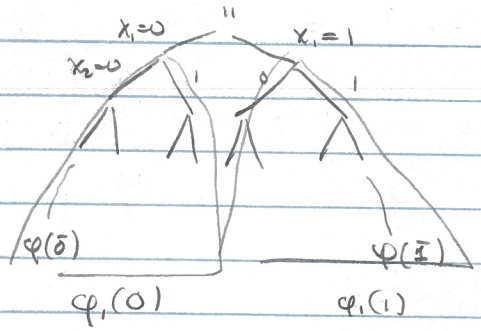
proof attempt: $\varphi(x_1, \dots, x_n)$ boolean formula

$\varphi_0 := \sum_{\alpha_1,\dots,\alpha_n \in \{0,1\}} \varphi(\alpha_1, \dots, \alpha_n)$ ← main

$\varphi_1(x_1) = \sum_{\alpha_2,\dots,\alpha_n \in \{0,1\}} \varphi(x_1, \alpha_2, \dots, \alpha_n)$

$\varphi_i(x_{\le i}) = \sum_{\alpha_{i+1},\dots,\alpha_n \in \{0,1\}} \varphi(x_{\le i}, \alpha_{>i})$

$\varphi_n(x_{\le n}) = \varphi(x)$



lem: $\varphi_i(x_{\le i}) = \varphi_{i+1}(x_{\le i}, 0) + \varphi_{i+1}(x_{\le i}, 1)$

pf: $\sum_{\alpha_{i+1},\alpha_{i+2},\dots,\alpha_n \in \{0,1\}} \varphi(x_{\le i}, \alpha_{i+1}, \alpha_{>i+1})$

$= \sum_{\alpha_{i+1} \in \{0,1\}} \underbrace{\sum_{\alpha_{i+2},\dots,\alpha_n \in \{0,1\}} \varphi(x_{\le i}, \alpha_{i+1}, \alpha_{>i+1})}_{= \varphi_{i+1}(x_{\le i}, \alpha_{i+1})}$

∎

protocol:

P		V
	φ	
	φ_0 →	check $\varphi_0 = k$ (received later / received now)
	$\varphi_1(0), \varphi_1(1)$ →	check $\varphi_0 = \varphi_1(0) + \varphi_1(1)$
	$\varphi_2(00), \varphi_2(01), \varphi_2(10), \varphi_2(11)$ →	check $\varphi_1(0) = \varphi_2(00) + \varphi_2(01)$, $\varphi_1(1) = \varphi_2(10) + \varphi_2(11)$
	⋯	
	$\{(\varphi_{i+1}(x_{\le i}, 0), \varphi_{i+1}(x_{\le i}, 1))\}_{x_{\le i} \in \{0,1\}^i}$ →	check $\varphi_i(x_{\le i}) = \varphi_{i+1}(x_{\le i}, 0) + \varphi_{i+1}(x_{\le i}, 1)$ $\forall x_{\le i} \in \{0,1\}^i$
	$\{\varphi_n(x_{\le n})\}_{x_{\le n} \in \{0,1\}^n}$ →	$\varphi(x_{\le n}) = \varphi_{\le n}(x_{\le n})$ $\forall x \in \{0,1\}^n$

↑ verifier has φ ↑ received

M. Cheval Forbes
Mforbes@illinois.edu
2019-04-02.2 ← 2019-04-02.1 → 2019-04-02.3
CS 579

complexity - $n+1$ rounds

i-th round : sends 2^{i-1} numbers, each $\leq 2^{n-(i-1)}$

$\Rightarrow \geq 2^n$ communication

$\Rightarrow V$ never polytime $\mathbb{L} \neq \mathbb{L}$

rmk : - V is deterministic

- not interactive : $P \rightarrow V$

completeness : $\mathbb{L}$ lemma $\Rightarrow$ correct answers pass all checks

$\rightarrow \Pr[(V \leftrightarrow P)(\varphi, x) = 1] = 1$

soundness : $\langle \varphi, \tilde{k} \rangle \notin \#SAT$

$\langle \varphi, k \rangle \in \#SAT$

malicious prover $\tilde{P}$ sends $\tilde{\varphi}_0 = \tilde{k} \neq k = \varphi_0$

$\mathbb{L}$ it passes yes $\mathbb{L}$ sends $\tilde{\varphi}_1(0) + \tilde{\varphi}_1(1)$ $\quad \varphi_1(0) + \varphi_1(1)$

$\Leftarrow \exists b_1 \in \{0,1\}$ $\tilde{\varphi}_1(b_1) \neq \varphi_1(b_1)$

$\tilde{\varphi}_2(b_1,0) + \tilde{\varphi}_2(b_1,1)$ $\quad \varphi_2(b_1,0) + \varphi_2(b_1,1)$

$\Rightarrow \exists b_2 \in \{0,1\}$ s.t. $\tilde{\varphi}_2(b_1,b_2) \neq \varphi_2(b_1,b_2)$

$\Rightarrow \exists b_3$ ...

$\Rightarrow \exists b_1, \dots, b_n \in \{0,1\}$ s.t. $\tilde{\varphi}_n(b_1, \dots, b_n) \neq \varphi_n(b_1, \dots, b_n)$

$\uparrow \varphi(b_1, \dots, b_n)$

verifier has φ, can compute $\varphi(b_1, \dots, b_n)$ on its own, catches

$\Rightarrow$ verifier says $\Pr[(V \leftrightarrow P)(\varphi, \tilde{k}) = 1] = 0$.

problem $\varphi_{\leq i}(x_{\leq i}) = \varphi_{\leq i}(x_{\leq i}, 0) + \varphi_{\leq i+1}(x_{\leq i}, 1)$

1 claim $\mapsto$ 2 claims $\rightarrow 4 \rightarrow 8 \rightarrow \cdots$

idea : randomly reduce 1 claim on $\varphi_i(x_{\leq i})$ to 1 claim on $\varphi_{i+1}(x_{\leq i+1})$

↳ using arithmetization

eg. : reduce 1 claim on $\varphi_i(x_{\leq i})$ to many claims on $\varphi_{i+1}(x_{\leq i+1})$

correct $\mapsto$ all correct

incorrect $\mapsto$ most incorrect

idea : arithmetization : $\varphi(x) : \{0,1\}^n \rightarrow \{0,1\}$ boolean function

want : $\hat{\varphi}(x) : \mathbb{F}^n \rightarrow \mathbb{F}$ low degree polynomial

s.t. : - $\forall x \in \{0,1\}^n$, $\hat{\varphi}(x) = \varphi(x) \in \{0,1\}$

- can evaluate $\hat{\varphi}(x)$ efficiently on $\mathbb{F}^n$

- degree $\hat{\varphi}(x) \in \text{poly}(n)$

Rmk : not asking for $\hat{\varphi}$ to be multilinear

Michael Forbes
mforbes@illinois.edu

2019-04-02.2 → 2019-04-02.3
2019-04-02.4 ← CS579

recall - $x_i \mapsto x_i$

$\varphi \wedge \psi \mapsto \hat{\varphi} \cdot \hat{\psi}$

$\neg \varphi \mapsto 1 - \hat{\varphi}$

$\varphi \vee \psi \mapsto 1 - (1-\hat{\varphi})(1-\hat{\psi})$

$\Rightarrow \varphi(x) = \hat{\varphi}(x)$ on $\{0,1\}^n$

$\Rightarrow$ arithmetic formula size $\text{poly}(|\varphi|)$ ← boolean formula

$\Rightarrow$ can evaluate efficiently

lem - $\deg \hat{\varphi} \le |\varphi|$ ← uses that φ is formula, not circuit

pf - induction:

- $|\varphi \wedge \psi| = |\varphi| + |\psi| + 1$

$\deg(\varphi \wedge \psi) \le \deg \hat{\varphi} + \deg \hat{\psi} \le |\varphi| + |\psi| \le |\varphi \wedge \psi|$

- etc

Sumcheck protocol:

input - $f(x)$ degree d poly over $\mathbb{F}_p[x_1, \dots, x_n]$, $k \in \mathbb{F}_p = \{0, \dots, p-1\}$

completeness - $\sum_{x_1, \dots, x_n \in \{0,1\}} f(x) = k \Rightarrow \Pr[(V \leftrightarrow P)(\langle f, k \rangle) = 1] = 1$

soundness - $\neq \Rightarrow \le 1 - \left(1 - \frac{d}{p}\right)^n$

parameters - for #SAT $d = O(|\varphi|)$

- $p \ge d(n+1) \Rightarrow \le 1 - 1/e \le .64$

Dummie naive protocol? $p = ?$ for #SAT $\varphi \le \varphi_0 \le 2^n \Rightarrow$ pick $2^n < p \le 2 \cdot 2^n$

↳ exists by Bertrand's postulate

- prover chooses, verifier checks

↳ uses primality testing, P

def: $f_0 = \sum_{x_1, \dots, x_n \in \{0,1\}} f(x)$

$f_1(x_1) = \sum_{x_2, \dots, x_n \in \{0,1\}} f(x_1, \bar{x}_{>1})$

$f_i(x_{\le i}) = \sum_{x_{i+1}, \dots, x_n \in \{0,1\}} f(\bar{x}_{\le i}, \bar{x}_{>i})$

$f_n(x) = f(x)$

$\Rightarrow f_i(x_{\le i}) = f_{i+1}(x_{\le i}, 0) + f_{i+1}(x_{\le i}, 1)$

f can eval over $\mathbb{F}$ and over $\{0,1\}$

protocol:

P → V: $\tilde{f}_0$ — V checks $\tilde{f}_0 = k$

P → V: $\tilde{f}_1(x_1)$ — V checks $\tilde{f}_0 = \tilde{f}_1(0) + \tilde{f}_1(1)$

↑ deg $\le d$ univariate over $\mathbb{F}_p \Rightarrow d \lg p$ bits

V → P: α_1 — V chooses $\alpha_1 \in \mathbb{F}_p$ randomly

P → V: $\tilde{f}_2(\alpha_1, x_2)$ — V checks $\tilde{f}_1(\alpha_1) = \tilde{f}_2(\alpha_1, 0) + \tilde{f}_2(\alpha_1, 1)$

V → P: $\alpha_2 \in \mathbb{F}_p$ — V chooses $\alpha_2 \in \mathbb{F}_p$ randomly

P → V: $\tilde{f}_3(\alpha_1, \alpha_2, x_3)$ — V checks $\tilde{f}_2(\alpha_1, \alpha_2) = \tilde{f}_3(\alpha_1, \alpha_2, 0) + \tilde{f}_3(\alpha_1, \alpha_2, 1)$

...

V → P: α_n

P → V: $\tilde{f}_n(\alpha_1, \dots, \alpha_n)$ — V checks $\tilde{f}_n(\alpha_1, \dots, \alpha_n) = f(\alpha_1, \dots, \alpha_n)$ ← we have this, can eval

completeness - if prover picks $\tilde{f}_i := f_i$, everything passes $\Rightarrow \Pr[\text{acc}] = 1$

soundness - idea - if prover cheats, verifier forces why prover to convince cheating

↳ gets caught in last round if $\tilde{f}_n \ne f$

↳ lies before last round

Michael Forbes
m(forbes@cs.umd.edu)
2019-04-02.4 ← 2019-04-02.3
CS571 → 2019-04-04.1

Lem. $h \in \mathbb{F}[x]$ deg $\le d \Rightarrow \le d$ roots α w/ $h(\alpha) = 0$ [fundamental thm of alg-ish]

$\langle \varphi, \tilde{k} \rangle \notin \#SAT$ $\quad \langle \varphi, k \rangle \in \#SAT$

prover sends $\tilde{f}_0 \neq \tilde{k}$ verifier rejects

$= \tilde{k} \neq k = f_0 = f_1(0) + f_1(1)$

to prevent instant rejection → $\tilde{f}_1(0) + \tilde{f}_1(1)$

$\Rightarrow \exists b_1 \in \{0,1\}$ s.t. $\tilde{f}_1(b_1) \neq f_1(b_1)$

$\Rightarrow \tilde{f}_1(x_1) \neq f_1(x_1)$ in $\mathbb{F}[x_1]$

$\Rightarrow \tilde{f}_1(x_1) - f_1(x_1) \neq 0$

$\Rightarrow \Pr\left[\tilde{f}_1(\alpha_1) \neq f_1(\alpha_1)\right] \ge 1 - \frac{d}{p}$ [V reads to keep living]

if $\tilde{f}_1(\alpha_1) \neq f_1(\alpha_1) = f_2(\alpha_1,0) + f_2(\alpha_1,1)$ $\alpha_1 \in \mathbb{F}$

also instant reject → $\tilde{f}_2(\alpha_1,0) + \tilde{f}_2(\alpha_1,1)$

$\Rightarrow \exists b_2 \quad \tilde{f}_2(\alpha_1, b_2) \neq f_2(\alpha_1, b_2)$

$\Rightarrow \tilde{f}_2(\alpha_1, x_2) \neq f_2(\alpha_1, x_2)$ in $\mathbb{F}[x_2]$

$\Rightarrow \Pr_{\alpha_2 \in \mathbb{F}_p}\left[\tilde{f}_2(\alpha_1,\alpha_2) \neq f_2(\alpha_1,\alpha_2) \;\middle|\; \text{“}\right] \ge 1 - \frac{d}{p}$

...

$\Rightarrow \Pr\left[\tilde{f}_n(\alpha_1, \dots, \alpha_n) \neq f_n(\alpha_1, \dots, \alpha_n)\right] \ge \Pr[\text{“} \mid \tilde{f}_{n-1}(\cdot) \neq f_{n-1}(\cdot)] \cdot \Pr[f_{n-1}(\cdot) \neq f_{n-1}(\cdot)]$

verifier evaluates → $f(\alpha_1, \dots, \alpha_n)$

$\ge 1 - \frac{d}{p}$ $\qquad \ge \left(1 - \frac{d}{p}\right)^{n-1}$

$\ge \left(1 - \frac{d}{p}\right)^n$ ☐

Rmk:
- non-relativizing: given oracle for $L \subseteq \{0,1\}^*$ cannot evaluate it over $\mathbb{F}^*$
- crucially uses algebra: non-zero polynomials distinct distinct often
- $x \in L \Rightarrow \Pr[\text{acc}] = 1$ $\quad \ge 2/3$
  $\notin \quad \le 1 - 1/R$ (perfect completeness) $\quad \le 1/T$ (standard deviation)
- lies beget lies

$\Rightarrow P^{\#P} \subseteq IP \subseteq PSPACE$

next time:
- TQBF $\in IP$ [more algebra]
- graph non-isomorphism
- ps 5 due