Michael Forbes
MForbes@illinois.edu
2019-03-07.4 ⇄ 2019-03-12.1
2019-03-12.2
CS579

cs 579 Computational Complexity : Lecture 17

~~ps4 q4 typo~~

over 5

admin: ps 3 back Thurs
ps4 due Thurs
project topics released - find partner, or ask to be assigned [piazza announce] ⇒ submit by Mar 20
- rank top 3 papers
[pref to those who submit early]
[advanced students pick harder paper]

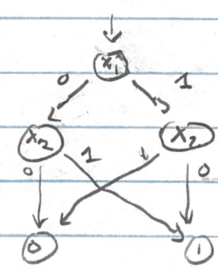
last time: $BPP \subseteq PSPACE, P/poly, \Sigma^2 P$

today: - randomized algo for $EQ_{\text{read once BP}}$
- algebraic techniques

def. a **branching program** (BP) is a labelled directed acyclic [no loops!] graph with
- a node labelled as "start" node
- two nodes labelled as "output" nodes, labelled "0" and "1", w/ no outgoing edges
- non-output nodes
  - two outgoing edges labelled "0" and "1"
  - node labelled w/ variable x_i

a BP w/ variables $x_1, \ldots, x_n$ computes a function $f: \{0,1\}^n \to \{0,1\}$ by walking on the DAG
- start at start node
- if at output node, output its value
- if at non-output node labelled w/ x_i: $x_i = 1$: follow "1" out-edge
  $= 0$: " "0" "

ex. B:



$B(x_1, x_2) = x_1 \oplus x_2$

fact: $EQ_{BP} = \{\langle B_1, B_2 \rangle : B_1, B_2 \text{ compute same function } f: \{0,1\}^n \to \{0,1\}\}$ is coNP-complete
[in coNP]
[unlikely to be in BPP unless PH collapses]

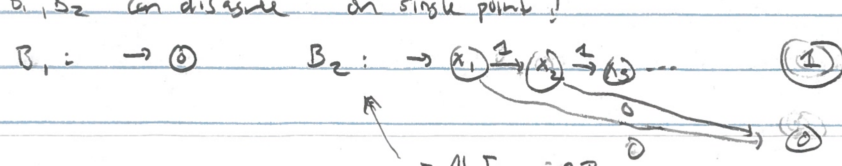
def: a BP is **read-once** if every start-output path queries each variable at most once [eg parity]

thm: $EQ_{\text{read once BP}} \in BPP$

motivation: - not known in P ~~deterministic~~
- uses algebraic techniques [very useful in later lectures]

idea: evaluate B_1, B_2 on randomly sampled inputs $x \in \{0,1\}^n$
but B_1, B_2 can disagree on single point!

eg



$= \mathbb{1}[x = 1^n]$

Michael Forbes
miforbes@illinois.edu
2019-03-12.2
CS579

← 2019-03-12.1
→ 2019-03-12.3

idea: evaluate B_1, B_2 on random inputs $x \in \mathbb{F}^n$ ← finite field

def. a field $\mathbb{F}$ is a set with

addition: commutativity: $a+b = b+a$

associativity: $a+(b+c) = (a+b)+c$

identity: $\exists 0$: $a = a+0 = 0+a$

inverses: any a $\exists -a$, $a+(-a) = (-a)+a = 0$

multiplication: → for non-zero elements

distributivity: $a(b+c) = ab+ac$

eg: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$

eg not: $\mathbb{Z}$ no multiplicative inverses $\mathbb{N}$, $\mathbb{Z}_4$ ← finite: no α s.t. $2\cdot\alpha \equiv 0 \pmod 4$

lem: $\mathbb{Z}_p$ is a field $\mathbb{F}$ and is finite $\mathbb{F}$ for p prime

Pf: addition: clear

multiplication: commute, assoc, ident: clear $\mathbb{F}$ didn't use primality $\mathbb{F}$

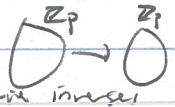
inverses: ?

Claim: $\alpha \in \mathbb{Z}_p$ $\alpha \neq 0$. $\mu_\alpha : \mathbb{Z}_p \to \mathbb{Z}_p$, $x \mapsto \alpha \cdot x$ is bijection

Pf. $\mu_\alpha(x) = \mu_\alpha(y)$

$\Rightarrow$ $\alpha \cdot x = \alpha \cdot y$ $\Rightarrow$ $\alpha(x-y) = 0 \equiv q \mid \alpha\cdot(x-y)$ $\Rightarrow q \mid x-y$

$\alpha \neq 0 \equiv p \mid \alpha$ $\Rightarrow x \equiv y \pmod p$

$\Rightarrow \mu_\alpha$ injective  $\Rightarrow \mu_\alpha$ bijective ∎

cor: $\mathbb{Z}_p$ has multiplicative inverses

Pf: $\alpha \neq 0 \Rightarrow \mu_\alpha$ bijection $\Rightarrow 1 \in \text{im}\,\mu_\alpha \Rightarrow \exists \beta$ ($\mu_\alpha(\beta) = \alpha\cdot\beta = 1$) ∎ ∎

Rmk. existential argument $\Rightarrow$ poly(p) runtime

efficient arguments exist $\Rightarrow$ poly(log p)

Thm: EQ reduces BP GBPP

Pf: arithmetization: ← defined over any $\mathbb{F}$

$\alpha \wedge \beta \mapsto \alpha\beta$

$\bar{\alpha} \mapsto 1-\alpha$

$\alpha \vee \beta \mapsto \alpha+\beta-\alpha\beta$

given $\alpha, \beta \in \{0,1\}$

$\mathbb{F}$ arithmetize BP $\mathbb{F}$

def: ~~for~~ BP B. node $v \in B$ define $f_v : \{0,1\}^n \to \{0,1\}$ by

$f_v(x) = \begin{cases} 1 & \text{if } \underbrace{\text{start} \to \text{output path}}_{\text{unique}} \text{ goes through } v \text{ when input } x \\ 0 & \text{else} \end{cases}$

edge $e \in B$ define f_e similarly

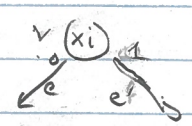
Michael Forbes
mforbes@illinois.edu

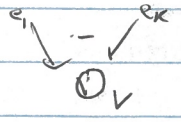
2019-03-12.2 → 2019-03-12.4 ← 2019-03-12.5

CS571

new big bound

ker.





$f_e = \neg x_i \wedge f_v$ $\quad f_v = f_{e_1} \vee \cdots \vee f_{e_k}$

$f_{e'} = x_i \wedge f_v$

def. edges $e, e' \in B$ define $p_e, p_{e'} \in \mathbb{F}[x_1, \dots, x_n]$, node $v \in B$ $p_v \in \mathbb{F}[x_1, \dots, x_n]$

$p_{start} := 1$ $\quad p_e := (1 - x_i) p_v$ $\quad p_v := p_{e_1} + \cdots + p_{e_k}$

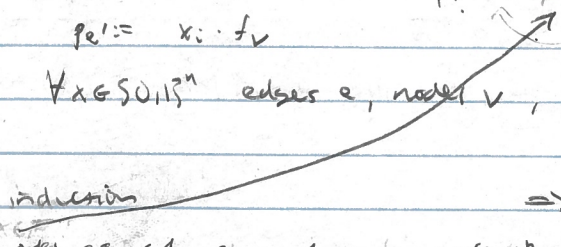
$p_{e'} := x_i \cdot p_v$

lem: $\forall x \in \{0,1\}^n$ edges e, node v, $f_v(x) = p_v(x)$

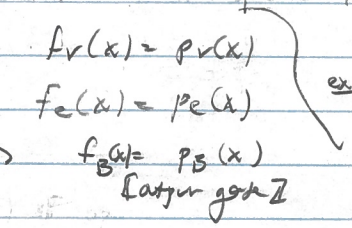
$f_e(x) = p_e(x)$

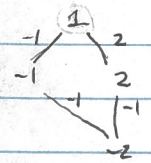
$\Rightarrow f_B(x) = p_B(x)$ [output gate]

Pf: induction



marks as $\in 1$ p_e is 1 on any $x \in \{0,1\}^n$





algo: "on input $\langle B_1, B_2 \rangle$ ← on $x_1, \dots, x_n$:

1) pick prime q s.t. $3n \le q \le 6n$

↳ exists by Bertrand's postulate [out of scope]

can find in poly(n) steps deterministically [primality testing not needed]

2) pick $\alpha \in \mathbb{F}_q^n (= \mathbb{Z}_q^n)$ at random

3) evaluate $p_{B_1}(\alpha)$, $p_{B_2}(\alpha)$

4) if $\neq$ equal, accept, else reject."

complexity: prop: $p_e(\alpha), p_v(\alpha)$ can be computed in poly$(|B|, \underbrace{\lg q}_{O(\lg n)})$ steps

Pf: induction, add/mult mod q

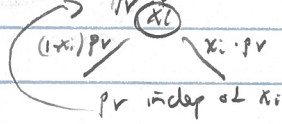
correctness:

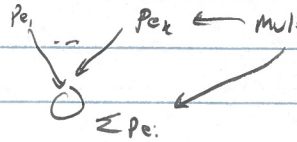
def: a polynomial $p \in \mathbb{F}[x_1, \dots, x_n]$ is multilinear if $\deg_{x_i} p \in 1$ all i

eg: $xy - x$, not $x^2 y - x$

Prop: all p_e, p_v are multilinear [use read-once]

Pf:





Prop [ps 6]: $f: \{0,1\}^n \to \{0,1\}$. exists unique multilinear polynomial $p \in \mathbb{F}[x_1, \dots, x_n]$

s.t. $f(x) = p(x)$ $\forall x \in \{0,1\}^n$

Cor: $\langle B_1, B_2 \rangle \in EQ_{roBP} \Rightarrow P_r[\text{acc}] = 1$

Pf. $\Rightarrow f_{B_1} = f_{B_2} \Rightarrow p_{B_1} = p_{B_2} \Rightarrow p_{B_1}(\alpha) = p_{B_2}(\alpha)$

↑ multilinear uniqueness

∎

Michael Forbes
MForbes@illinois.edu
2019-03-12.4 ← 2019-03-12.3
CS 574 → 2019-03-14.1

[Schwartz-Zippel lemma]

Prop: $p \in \mathbb{F}_q[x_1, \dots x_n]$ multilinear. if $p \neq 0$ then
$$\Pr_{\alpha \in \mathbb{F}_q^n}[p(\alpha) = 0] \leq \frac{n}{q}$$

Pf: $n=1$: $p(x_1) = \beta x_1 + \gamma$ ← unique root $\alpha = -\frac{\gamma}{\beta}$ (uses inverse of β!!!)
$$\Pr[\alpha = -\tfrac{\gamma}{\beta}] = \tfrac{1}{q}$$

$n > 1$: $p(x_1, \dots x_n) = p(y, z_1, \dots z_m)$
$$= p_1(\bar{z})\, y + p_0(\bar{z})$$ wlog $p_1 \neq 0$

$$\Pr_{\substack{\alpha \in \mathbb{F} \\ \bar{\beta} \in \mathbb{F}_q^m}}[p(\alpha, \bar{\beta}) = 0] \leq \underbrace{\Pr[p(\alpha,\bar{\beta}) = 0 \mid p_1(\bar{\beta}) = 0]}_{\leq 1} \cdot \underbrace{\Pr[p_1(\bar{\beta}) = 0]}_{\leq \frac{m}{q} = \frac{n-1}{q}}$$
$$+ \underbrace{\Pr[p(\alpha,\bar{\beta}) = 0 \mid p_1(\bar{\beta}) \neq 0]}_{\leq \frac{1}{q}} \cdot \underbrace{\Pr[p_1(\bar{\beta}) \neq 0]}_{\leq 1}$$
$$\leq \frac{n-1}{q} + \frac{1}{q} = \frac{n}{q}$$ ∎

Cor: $\langle B_1, B_2 \rangle \notin EQ_{ROBP} \Rightarrow \Pr[\text{acc}] \leq 1/3$

if: $\Rightarrow f_{B_1} \neq f_{B_2} \equiv p_{B_1} \neq p_{B_2} \equiv p_{B_1} - p_{B_2} \not\equiv 0$

$\Rightarrow \Pr_\alpha[(p_{B_1} - p_{B_2})(\alpha) = 0] \leq \frac{n}{q} \leq \frac{n}{3n} = 1/3$

$p_{B_1}(\alpha) = p_{B_2}(\alpha)$ ∎ accepting convert

Thm: EQ reduces BP ∈ coRP (polynomial identity testing)

recap:

	arithmetization	multilinear	random α	
f_{B_1}	⟼	$p_{B_1} \in \mathbb{F}_q[x_1, \dots x_n]$, $f_{B_1} = p_{B_1}\|_{\{0,1\}^n}$	⟼	$p_{B_1}(\alpha)$
f_{B_2}	⟼	p_{B_2}	⟼	$p_{B_2}(\alpha)$
$\in EQ_{ROBP}$	⟼	=	⟼	= w/p 1
$\notin$	⟼	≠	⟼	≠ w/p $\geq 2/3$

next time: counting complexity