Michael Forbes
mforbes@illinois.edu

2019-04-09.4 → 2019-04-11.1
2019-04-11.2 ← cs 579

- ⇒ ✓ ≤ ✓
- by picture ✓
- schedule ✓

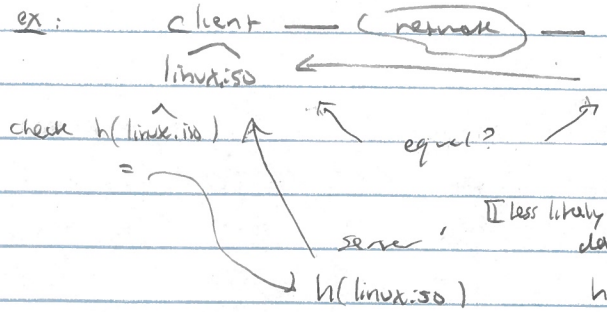
cs 579 Computational Complexity: Lecture 24

admins: ps 5 back [[end of class]]

last time: query complexity - computing $f(x)$, charged each access of some x_i
- $P \overset{dec}{\subseteq} NP^{dec} \neq coNP^{dec}$ [[expected]]
- $P \overset{dec}{=} NP^{dec} \cap coNP^{dec}$ [[unexpected]]

today: communication complexity - model: computing $f(x,y)$ [[two players]]
- separations

ex: client — (network) — server



ex:

Q: book a meeting? how much communication?

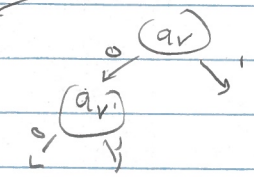
A: worst case must give entire calendar

[[formal model?]]

Alice $x \in \{0,1\}^n$ — Bob $y \in \{0,1\}^n$ [[like interactive proofs, but not charging for computation]]

$m_1 = f_1(x)$ →
← $m_2 = g_2(m_1, y)$
$m_3 = f_3(m_1, m_2, x)$ →
...
$f(x,y)$ →

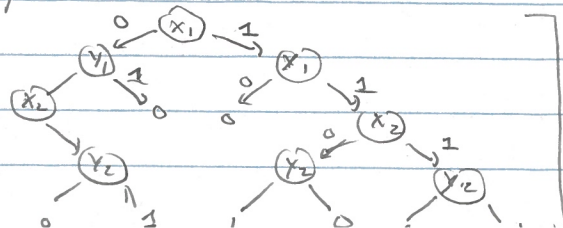
def: a protocol P is a rooted binary tree
- internal nodes v labelled by $a_v : \{0,1\}^n \to \{0,1\}$ [[alice's turn]]
  $b_v : \{0,1\}^n \to \{0,1\}$ [[bob's turn]]
- leaves labelled by $\{0,1\}$



the value of P on input $(x,y) \in \{0,1\}^n \times \{0,1\}^n$ is the label of the leaf when
- start at root
- at internal node v
  - labelled by a_v: follow left child if $a_v(x)=0$, right " 1
  - " b_v " $b_v(y)=0$, $b_v(y)=1$

depth is max length of root-leaf path

ex: $EQ_2 : \{0,1\}^2 \times \{0,1\}^2 \to \{0,1\}$



Michael Forbes
MForbes@illinois.edu
2019-04-11.2 ← 2019-04-11.1 → 2019-04-11.3
CS 579

def: $D^{cc}(f)$ = min depth of protocol P computing f

lem: $D^{cc}(f) \le n+1$, any f

pf. Alice $\xrightarrow{x}$ Bob $\xleftarrow{f(x,y)}$

def. $P^{cc} = \{ f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\} \text{ s.t. } D^{cc}(f) \le \text{poly}(\lg n) \}$

Q. P^{cc} vs NP^{cc}?

A. $\neq$

= Questions?

[develop more insight into model]

def: a **combinatorial rectangle** is a set $A \times B \subseteq \{0,1\}^n \times \{0,1\}^n$ s.t. $A \subseteq \{0,1\}^n$, $B \subseteq \{0,1\}^n$

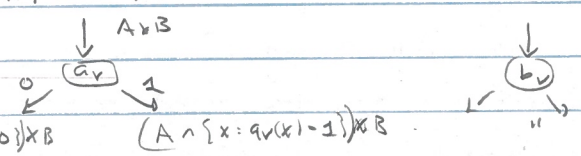
eg:

Key Lemma: in protocol P, node v, define $I_v = \{(x,y) : \text{input } (x,y) \text{ reaches } v \text{ on } P\}$

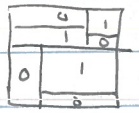
then I_v is combinatorial rectangle.

pf. by induction - root: $I_v = \{0,1\}^n \times \{0,1\}^n$

- internal node



eg: $\{0,1\}^n$



[partition, same f-value]

[same value of f]

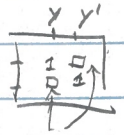
Cor. c-bit protocol for $f \Rightarrow \{0,1\}^n \times \{0,1\}^n$ partitioned into $\le 2^c$ f-monochromatic combinatorial rectangles

[how do we use this?]

def: $S \subseteq \{0,1\}^n \times \{0,1\}^n$ is a **1-fooling set** for f if

- $f(x,y) = 1$ for $(x,y) \in S$
- $(x,y) \ne (x',y') \in S \Rightarrow$ at least one of $f(x,y') = 0$ or $f(x',y) = 0$

Rmk: $\Rightarrow x' \ne x$, $y' \ne y$



Clm: S 1-fooling set for f, $A \times B$ comb. rect. w/ $f(A \times B) = 1$ not both 1

$\Rightarrow |S \cap (A \times B)| \le 1$ [pf by picture] i.e. $(x,y) \ne (x',y') \in A \times B$

$\Rightarrow x, x' \in A$, $y, y' \in B$

$\Rightarrow (x,y'), (x',y) \in A \times B$

$\Rightarrow f(x,y') = f(x',y) = 1$

Cor. S 1-fooling set for $f \Rightarrow D^{cc}(f) \ge \lg |S|$

pf: c-bit protocol P for $f \Rightarrow \le 2^c$ leaves $\Rightarrow$ partition into $\le 2^c$ f-monochromatic comb rect

$(x,y) \in S \Rightarrow f(x,y) = 1 \Rightarrow$ some 1-monochromatic comb rect $A \times B$ ($x \in A$, $y \in B$)

and $(x',y') \notin A \times B$ ($(x',y') \overset{\ne}{\in} S$, $(x,y) \in A \times B$)

$\Rightarrow 2^c \ge |S| \Rightarrow c \ge \lg |S|$

i.e.: injective map $S \hookrightarrow \{1\text{-monochromatic rect}\}$

Michael Faber
Mfaber@illinois.edu

2019-04-11.2 ⟶
2019-04-4.4 ⟵ 2019-04-4.3
CS 579

[now let's use this]

Prop: $D^{cc}(EQ_n) \geq n$

Pf: $S := \{(x,x) : x \in \{0,1\}^n\}$ is 1-fooling set

i.e. $EQ(x,x) = 1$

$x' \neq x$ $EQ(x',x) = EQ(x,x') = 0$

1	0
0	1

$|S| = 2^n \Rightarrow D^{cc}(EQ) \geq \lg |S| = n.$ ∎

Rmk: $D^{cc}(EQ_n) = n+1$.

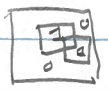
— Questions? [how to define NP]

def: $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

1-cover-number $C_1(f) :=$ min # of 1-monochromatic rect $A_i \times B_i$

[vs partition] s.t. $f(x,y) = \bigvee_i [(x,y) \in A_i \times B_i]$

eg:



fact: any "reasonable" model of nondeterministic communication to compute f uses $\Theta(\lg C_1(f))$ bits

eg: Alice ⟶ Bob hence: $N_b^{cc} := \lg C_b(f)$

[zero-cover #]

fact: $D^{cc}(f) \leq O(N_0^{cc}(f) \cdot N_1^{cc}(f))$

$N P^{cc} = \{ N_2^{cc}(L) \leq \text{poly}(\lg n) \}$

$\Rightarrow P^{cc} = NP^{cc} \cap coNP^{cc}$ [similar to query complexity proof]

Lem: S is 1-fooling set $\Rightarrow C_1(f) \geq |S|$ [same proof ≤1 rect per fooling element]

Cor: $N_1(EQ_n) \geq n$

Prop: $N_0(EQ_n) \leq \lg n + 1$

Pf: $x \neq y$ iff $\bigvee_i (x_i = 0 \wedge y_i = 1) \vee \bigvee_i (x_i = 1 \wedge y_i = 0)$

$\bigvee_i$ ($i \in n$): $A_i \times B_i$; $\bigvee_i$ ($i \in \lg n$): $A_i' \times B_i'$

$\Rightarrow C_0(EQ) \leq 2n$

Cor: $P^{cc} \subsetneq coNP^{cc} \neq NP^{cc}$

P^{cc} ↛ EQ; $coNP^{cc}$ ↓ EQ; NP^{cc} ↓ EQ

Prop: EQ_n solvable w/ $O(\lg n)$ randomized communication [won't formalize model here]

Pf: [using polynomials, finite fields]

$x \in \{0,1\}^n \longmapsto p_x(z) = \sum_{i=1}^{n} x_i z^i \in \mathbb{F}[z]$ deg $\leq n$

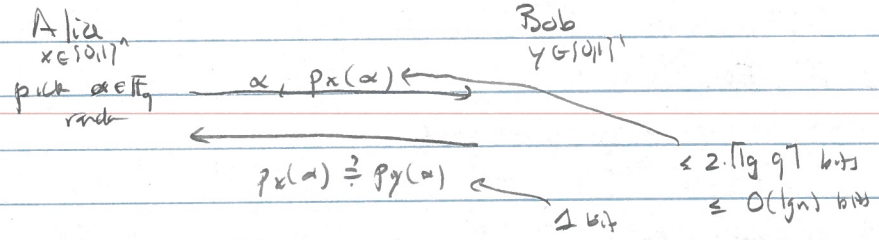
$y \longmapsto p_y(z) = \sum_i y_i z^i \in \mathbb{F}[z]$ deg $\leq n$

$x = y$ iff $p_x = p_y$ in $\mathbb{F}[z]$ iff $\underbrace{p_x - p_z}_{\text{deg} \leq n \text{ poly}} = 0$

Michael Forbes
miforbes@illinois.edu
2019-04-11.4 ← 2019-04-11.3
→ 2019-04-16.1
CS579

Recall: $q(z)$ nonzero poly, $\deg \le d$ $\Rightarrow$ $\Pr_{\alpha \in \mathbb{F}_q}[p(\alpha) \neq 0] \le \frac{d}{q}$

protocol: n fixed $\Rightarrow$ use fixed prime $q \in [4n, 8n]$ (exists by Bertrand's postulate)



$\forall \alpha$

$x = y \rightsquigarrow p_x = p_y \Rightarrow p_x(\alpha) = p_y(\alpha) \rightsquigarrow \Pr[\text{output} = 1] = 1$

$x \neq y \Rightarrow \Pr[p_x(\alpha) = p_y(\alpha)] \le \frac{n}{q} \le \frac{1}{4} \Rightarrow \Pr[\text{output} = 1] \le \frac{1}{4}$

[can amplify]

Cor: $P^{cc} \subsetneq coRP^{cc}$, $coRP^{cc} \not\subseteq NP^{cc}$ [not expressed in TM model]

(EQ, EQ, EQ)

Open: is PH^{cc} infinite?

next time: circuit complexity