Michael Forbes
miforbes@illinois.edu
2018-03-26.4 →
2018-03-28.2 ←
2018-03-28.1
CS579

CS 579 : Computational Complexity : Lecture 19

3 7

admin: signup for projects

today: communication complexity
- model
- $\Omega(n^2)$ time lb for one-tape TM

ex: client — {network} — server

linux.iso ← linux.iso

$x_i \neq x_j$?

equal? how much communication?

e.g. check sha1/md5 checksums

ex: Alice Bob

google calendar   outlook calendar

Q: book a meeting? how much communication?

A: have to give entire calendar [worst case]

[how to model communication?]

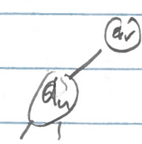
Alice $\xrightarrow{m_1 = f_1(x)}$ Bob

$x \in \{0,1\}^n$ $\xleftarrow{m_2 = g_2(m_1, y)}$ $y \in \{0,1\}^n$

$\xrightarrow{m_3 = f_3(m_1, m_2, x)}$

def: a protocol P is a rooted binary tree
- internal nodes v labelled by
  - $a_v : \{0,1\}^n \to \{0,1\}$
  - $b_v : \{0,1\}^n \to \{0,1\}$

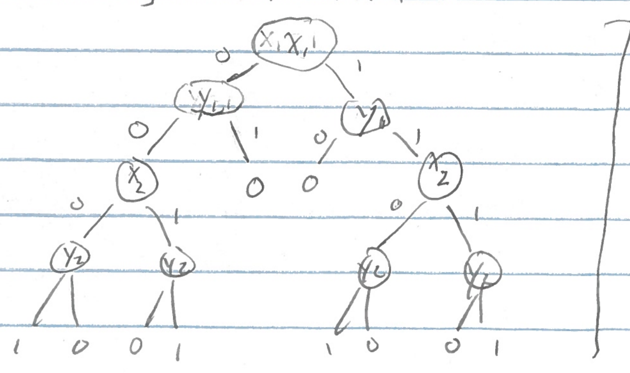
  one-bit messages
- leaves labelled w/ $\{0,1\}$



The value of P on input (x,y) is the label of leaf when
- starting at root
- at internal node v — if labelled by a_v — left if $a_v(x)=0$, right if $=1$; b_v "

depth = length root — leaf path

ex: $EQ_3 : \{0,1\}^2 \times \{0,1\}^2 \to \{0,1\}$



depth 4

Michael Forbes
mforbes@illinois.edu
2018-03-28.2 ← 2018-03-28.1
→ 2018-03-28.3
cs579

def: $D(f)$ = min depth of protocol P computing f reusing query notation

lem: $D(f) \leq n+1$, any f

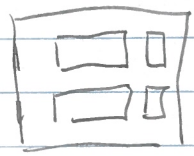
Pf: Alice $\xrightarrow{\bar{x}}$ Bob
$\xleftarrow{f(\bar{x},\bar{y})}$

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

Q: P vs NP? interesting functions in P?
↳ hw

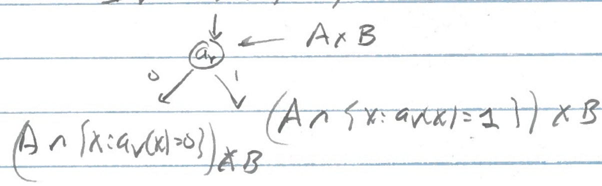
def: a combinatorial rectangle is a set $A \times B \subseteq \{0,1\}^n \times \{0,1\}^n$
$A \subseteq \{0,1\}^n \quad B \subseteq \{0,1\}^n$

eg:



lem: in protocol P, node v, define $I_v = \{(x,y) : \text{reach node } v\}$
then I_v is a combinatorial rectangle

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

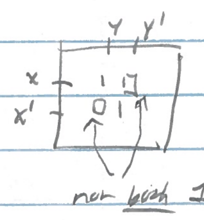


eg:

Cor: c-bit protocol for f ⇒ $\{0,1\}^n \times \{0,1\}^n$ partitioned into 2^c f-monochromatic comb rectangles

def: $S \subseteq \{0,1\}^n \times \{0,1\}^n$ is a 1-fooling set for f if
- $f(x,y) = 1$ $(x,y) \in S$
- $(x,y), (x',y') \in S \Rightarrow$ one of $f(x,y'), f(x',y) = 0$

ie



Clm: S 1-fooling set for f, $A \times B$ comb rect 1-monochromatic
$\Rightarrow |S \cap (A \times B)| \leq 1$

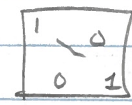
Cor: S 1 fooling set for $f \Rightarrow D(f) \geq \lg|S|$

Pf: c-bit protocol P for f, 2^c leaves
$\forall (x,y) \in S \Rightarrow f(x,y) = 1 \Rightarrow$ some 1-monochromatic rect $A \times B$ $(x,y) \in A \times B$
↳ $(x',y') \notin A \times B$
$\Rightarrow 2^c \geq |S|$

Michael Forbes
miforbes@illinois.edu
2018-03-28.2 →
2018-03-28.4 ←
2018-03-28.3
CS 579

Prop: $D(EQ_n) \geq n$

pf: $S = \{(x,x) : x \in \{0,1\}^n\}$ is a 1-fooling set
$EQ(x,x) = 1$
$|S| \geq 2^n$



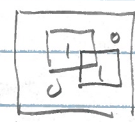
$D(EQ) \geq \lg |S| = n$ ☒

≥ Questions?

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

the 1-cover # $C_1(f) = \min$ # of 1 monochromatic rect $A_i \times B_i$
st $f(x,y) = \bigvee_i [(x,y) \in A_i \times B_i]$

eg



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

eg: Alice $\xrightarrow{\text{proof}}$ Bob   hence: $N_b(f) := \lg C_b(f)$

Fact: $D(f) \leq O(N_1(f) \cdot N_0(f)) \Rightarrow P^{cc} = NP^{cc} \cap coNP^{cc}$ // like in query complexity

lem: S is 1-fooling set $\Rightarrow C_1(f) \geq |S|$

Cor: $N_1(EQ_n) \geq n$

Prop: $N_0(EQ_n) \leq O(\lg n)$

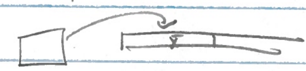
pf: prover provides i st $x_i \neq y_i$, alice & bob check

Fact: randomized communication of EQ is $\leq O(\lg n)$

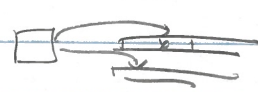
Sketch:
Alice x $\xrightarrow{h(x),\, h}$ Bob y $h \in \mathcal{H}$
$\xleftarrow{h(x) \overset{?}{=} h(y)}$

---

recall, 1-tape TM



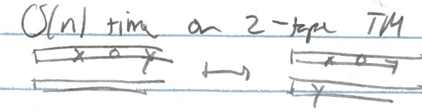
2-tape TM



fact: t steps on 2-tape TM $\Rightarrow O(t^2)$ steps on 1 tape TM

Q: tight?

eg: $L = \{x 0^n x : |x| = n\} \to O(n)$ time on 2-tape TM



↳ requires $\Omega(n^2)$ time on 1 tape TM

Prop: M 1 tape TM acc $\{x 0^n y : |x| = |y| = n,\ f(x,y) = 1\}$
rej $= 0$

in time $t(n)$

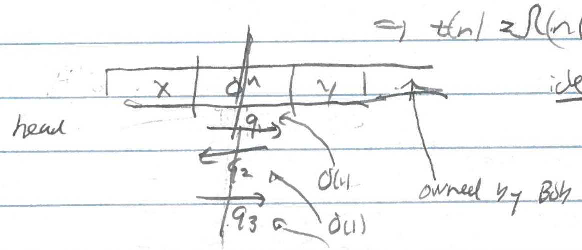
$\Rightarrow N_1(f) \leq O(\frac{t(n)}{n} + \lg n)$

Michael Forbes
miforbes@illinois.edu
2018-03-28.4 ← 2018-03-28-3
→ 2018-04-02.1

Pf: $f = EQ_n \Rightarrow n \le N_1(EQ) \le O\left(\frac{t(n)}{n} + \lg n\right)$

$\Rightarrow t(n) \ge \Omega(n(n - \lg n)) = \Omega(n^2)$

Pf:



idea: $x \to$ Alice
$y \to$ Bob
make them work to communicate

Lem: some $n \le i \le 2n$ st $\le \frac{t(n)}{n}$ transitions cross cell $i \leftrightarrow i+1$

Pf: $t(n)$ transitions: each cross ≤ 1 cell boundary

n boundarys within 0^n

by averaging $\Rightarrow$ desired boundary ☐

Protocol: prover: give i st $\le t(n)/n$ transitions $\leftarrow O(\lg n)$ communication

alice simulate TM on $[1, i]$

Bob $[i+1, \infty)$

$\Big]$ O(1) communication
do $\le t(n)/n$ times
↳ if TM doesn't halt, abort

$\Rightarrow O(1) \cdot \frac{t(n)}{n} + \lg n = O\left(\frac{t(n)}{n} + \lg n\right).$

next time: project topics due

circuit complexity