

2019-04-23.4 →
 2019-04-25.2

CS 579 Computational Complexity: Lecture 28

admin: project presentations - must attend 2 other talks

- SC 4405 2019-04-30 1:30-7pm

SS-01 10:00-3pm

- doodle sent out - sign up as a group
- list all available slots if not just preferences
- 30 mins Reserve time for questions - switching?
- slides prepared

submit report + presentation by Wednesday 4:30pm

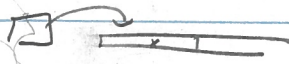
last time = natural proofs = strong crypto ⇒ existing methods cannot prove NP ≠ P/poly

today = applications of concrete complexity

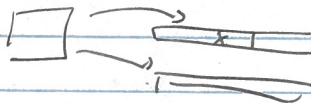
- communication vs 1-tape TMs

ICES form

recall - 1-tape TM

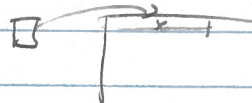


2-tape TM



3-tape TM

2-dimensional TM



Q: what is the "right" number of tapes?

want: - "realistic" model of physical storage

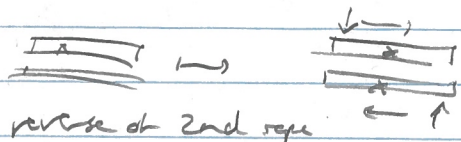
- 37-dimensional tape is "na" realistic if string theory is dimensional
- "efficient" model of computation

L) is efficiently simulates "realistic" physical storage

prop: $L = \{x \in \Sigma^* \mid x \in \text{SOIT}\}^*$ is solvable in $O(n)$ steps on a 2-tape TM

PF:

- 1) on input x , if $|x|$ not even, reject
- 2) copy x to 2nd tape
- 3) check if 1st tape = reverse of 2nd tape



prop:

is solvable in $O(n^2)$ steps on 1-tape TM

PF:

- 1) on input x :
- 1) if $|x|$ not even, reject
- 2) repeat until all symbols crossed off

e) pass over input and

- 1) find first active symbol of Σ and cross it off
- find last active symbol of Σ and cross it off
- if $a \neq b$, reject

2019-04-25.2 ← 2019-04-25.1
→ 2019-04-25.3
CS 539

~~is~~ $x_1 = f_1 \Rightarrow y = x x^R$ sorted
 $x_2 = f_2 \uparrow$ by even
complexity: $O(n)$ rounds, $O(n)$ work each round
 $\Rightarrow O(n^2)$

Q: des better?

↳ if we can't the 1-tape TMs are weaker than 2-tape

Q: 3 tape vs 2-tape?

If good, no great I

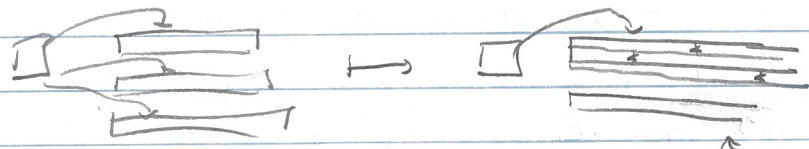
fact: $k = O(1)$, t steps on k -tape TM $\mapsto O(t^2)$ steps on 1-tape TM

sketch: similar to oblivious TM question on ps 1

fact: " $\mapsto O(t \lg t)$ steps on 2-tape TM

If very good I

sketch:



interleaved 3-tapes

used to copy data

key idea: keep the 3 tapes, so

their tape heads are always "close by"

↳ we move the tapes to ensure approximate alignment

allows for efficiency

Q: 1-tape TM?

thm: $L = \{x \in \{0,1\}^n : x \in \{0,1\}^n\}$ takes $\Omega(n^2)$ steps on 1-tape TM

fact: 1-tape TM is realistic but $O(n)$ on 2-tape TM [clear I

Rank: - 1-tape TM is realistic, but not as efficient as 2-tape

- 2-tape TM is realistic, essentially as efficient as k -tape TM any k

Prop: $L = \{x \in \{0,1\}^n\}$ the "right" model of TM

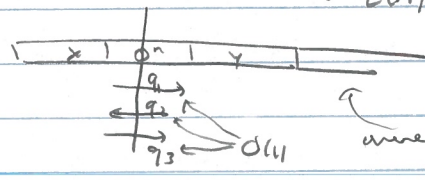
Prop: M 1-tape TM acc $\{x \in \{0,1\}^n : |x| = |y| = n \wedge f(x,y) = 1\}$
 $f(\{0,1\}^n \times \{0,1\}^n) \rightarrow \{0,1\}$ rej: $= 0$

$\Rightarrow N_c(f) \in O(\frac{t(n)}{n} + \lg n)$

pf: $f = EQ_n$ $n \in N_c(EQ_n) \in O(\frac{t(n)}{n} + \lg n)$
if falling set

$\Rightarrow t(n) \geq \Omega(n \cdot (n - O(\lg n))) = \Omega(n^2)$

pf:



idea: $x \mapsto$ Alice
 $y \mapsto$ Bob

make them work to communicate

even key

Let some $c \in [1, 2^n]$ such that $\leq \frac{t(n)}{n}$ transition

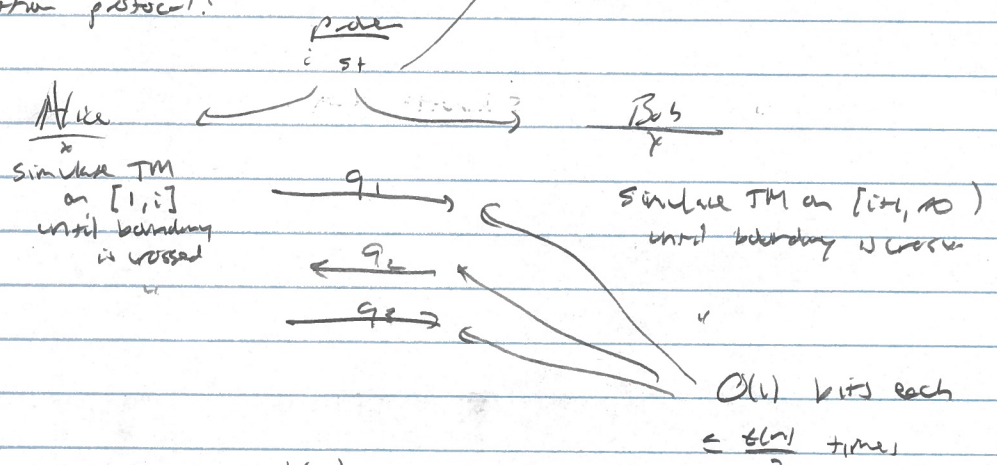
cross all $i \leftrightarrow i+1$

Pf: $t(n)$ steps: each cross ≤ 1 all boundary

n boundaries within O^n

averaging = desired boundary \square

communication protocol:



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

Rank: - many connections between online complexity and classical complexity

eg: proving $AC^0 \Rightarrow PH^{query} \not\subseteq PSPACE^{query}$

\Rightarrow exist oracle A s.t. $PH^A \not\subseteq PSPACE^A$

- many open questions.

eg: given 1^n output an n -bit prime

↑ easy w/ randomness

open deterministically

ICES: - what topic would you have liked to see more of? why?
 " " " " " " less " "

