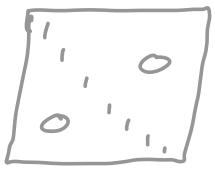
Last time: started unit on communication complexity (CC)

AB 13.1, 13.2'

- deterministic comm. cxity of functions: examples, protocols, rectangles, lower bounds:

n-bit strings

$EQ(x,y) = \begin{cases} 1 & x=y \\ 0 & o/w \end{cases}$

$D(EQ) \geq n+1$: 

$>2^n$ rectangles in any monochrom partition of comm. mtx of EQ

Today:
- application of ? : time/space tradeoffs for TMs
- randomized CC

AB 13.1, 13.2'

- application of ? LBs to 1-tape TM LBs
- (surprising) power of randomness...

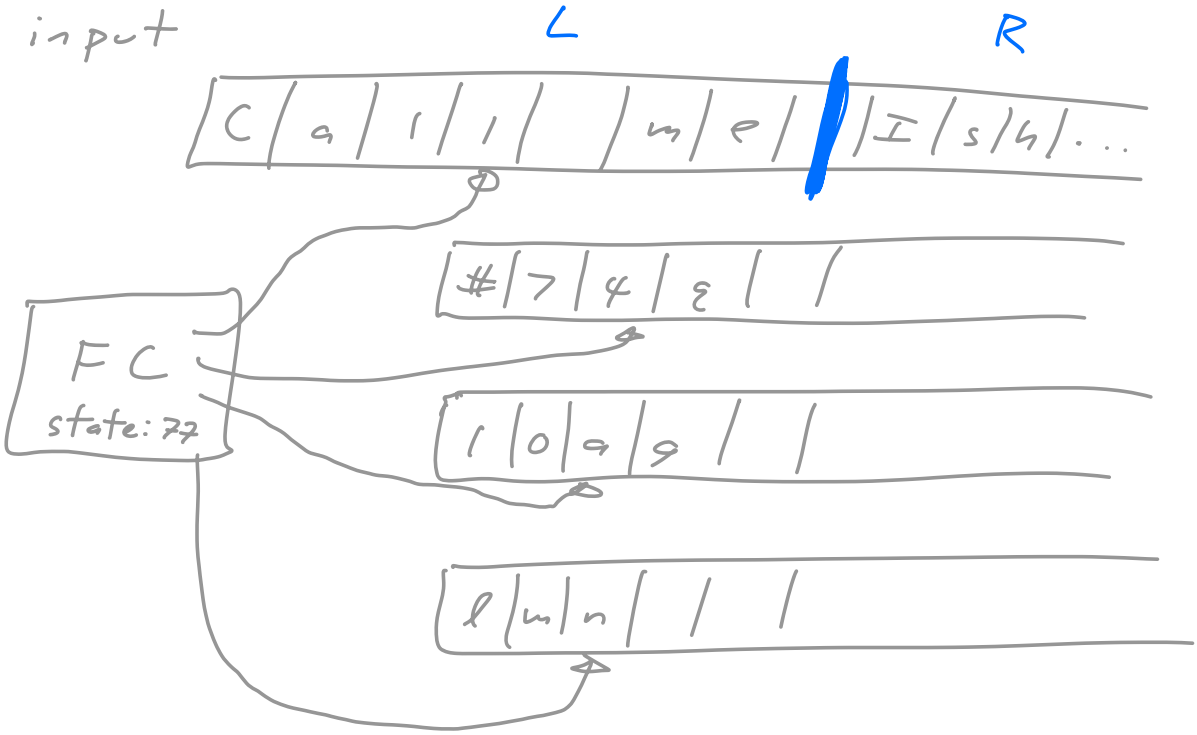
next up: circuit lower bounds

Questions?

Applic. of det. CC lower bounds to time-space tradeoffs for TMs

Recall multitape TM model ($k \geq 1$ work tapes):

- read-only input tape
- k R/W work tapes
- finite control w/ "head" on each tape



How does info "flow" between L + R portions of input?

- finite control: $O(1)$ bits
- $k = O(1)$ worktape: if TM uses space s, sk characters; $|\Sigma|$ (alphabet size) is $O(1)$, so $O(s)$ bits (even incl. worktape head locations).

Suggestive... Space-time tradeoff:

Lemma: Fix a fn $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.
Let M be a k-tape TM that runs in time $T(n)$, space $S(n)$ on $3n$-bit inputs.
Suppose that

- M accepts all inputs of the form $w = x0^n y$, $|x|=|y|=n$, s.t. $f(x,y)=1$;
- M rejects all inputs of the form $w = x0^n y$, $|x|=|y|=n$, s.t. $f(x,y)=0$.

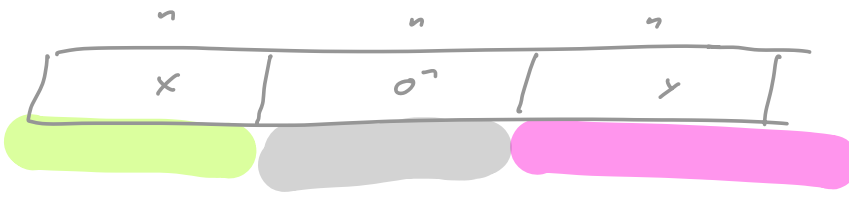
Then $D(f) \leq \frac{O(T(n)\cdot S(n))}{n}$. $\left(O(T)\cdot S = O(TS) = O(S)T\right)$

Pf: Need to get a det comm. prot. for f from the TM M. Here's how:

- on input A B
  x, y,

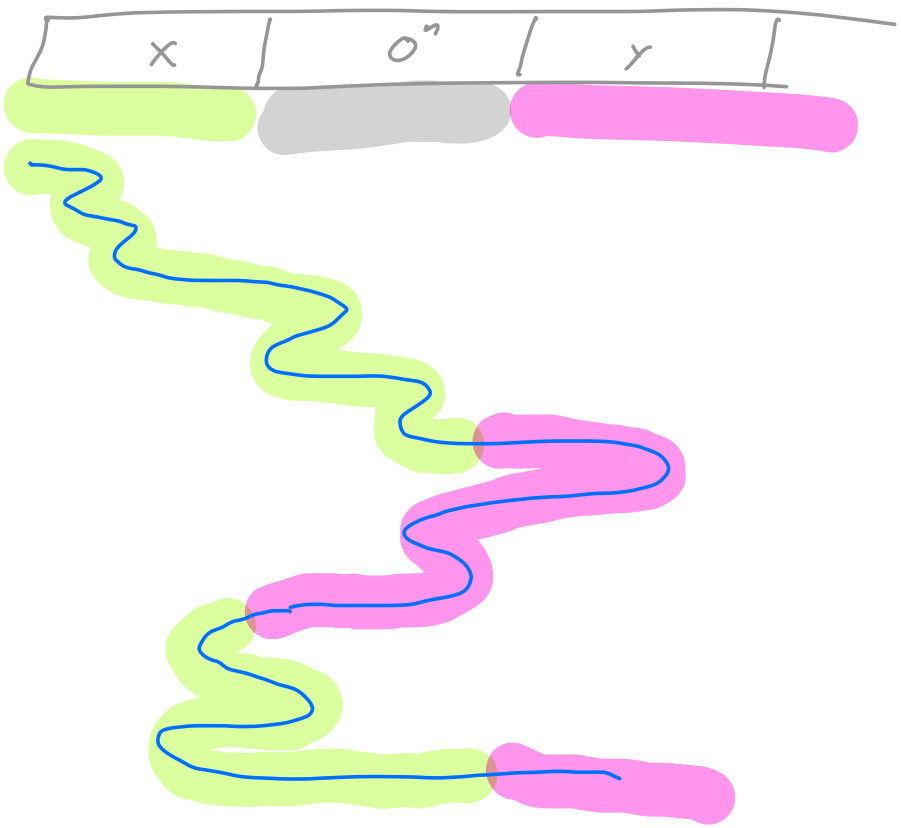
- A + B simulate M's exec. on $w = x0^n y$.

input tape



M's input head is always either in (A) x-region (A simulates M)
(B) y-region (B simulates M); or
(C) 0-region (whoever was most recently doing sim., continues to simulate it).

I.e. control shifts only when input head enters other player's region:



Whenever they do handoff, the player who was doing the sim. of M tells the TM's entire k worktape contents + tape head locations + state of finite control to other player (not his/her x or y input). O(S(n)) bits

This suffices for new simulating player to handle the sim. until next transfer.

How many transfers?

At least n steps between each transfer $\Rightarrow$ $\leq T(n)/n$ transfers.

So total comm. is $\leq O(S(n)) \cdot \frac{T(n)}{n}$. ∎

Applic: Palindromes:

$L = \{ww^R : w \in \{0,1\}^*\}$ ↩

Let M be K-tape TM for running in $T(n)$ time, $S(n)$ space on $3n$-bit inputs.

Let $f(x,y) = \begin{cases} 1 & x = y^R \\ 0 & x \neq y^R \end{cases}$

M acc all $x0^n y$ w/ $f(x,y)=1$, $|x|=|y|=n$
rej " " " $=0$ " .

$f \equiv_{to} EQ$; so know $D(f) \geq n$, hence by lemma,

$$n \leq D(f) \leq \frac{c \cdot T(n) \cdot S(n)}{n}, \text{ so}$$

$$\boxed{cn^2 \leq T(n) \cdot S(n)}$$

[$T(n) = S(n) = O(n)$ achievable : copy + check.
$T(n) = n^2$, $S(n) = O(\log n)$ " : check char by char.]

Rand. Comm. Cxity : A, B can use rand.

2 settings:

"Private-coin": A, B each have own coins.

Equiv: A has own ∞ rand string r_A

B " " " " " r_B

A's functions (in prot tree) can dep. on x, r_A

B's " " " " y, r_B .

"Public coin": A, B have access to single rand string r_{pub}.

A's functions (in prot tree) can dep. on x, r_{pub}

B's " " " " y, r_{pub} .

Equiv. to having a prob. dist. over det prot's.

Def: A zero-error pub. coin rand prot P_{rand} for f is a distrib. over det prot's $P_1, P_2, \ldots$; each P_i is a correct prot. for f.

The Average-case cost of P_{rand} on (x,y) is

$\mathbb{E}_{\text{rand. choice of } P_i}$[depth of leaf of P_i that (x,y) reaches]

$= \mathbb{E}$[# bits A, B communicate on (x,y)].

The Average-case cost of P_{rand} is max of) over all (x,y).

Finally, $R_0^{pub}(f)$ is min of) over all zero-error pub. coin rand prot. for f.

Can be shown:

$$R_0^{pub}(EQ) = \Omega(n).$$

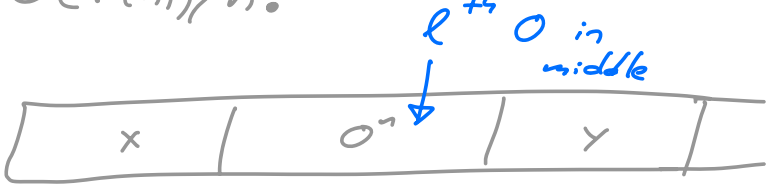
Applic. of rand CC to 1-tape TM lower bounds

Lemma: Fix a fn $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.
Let M be a 1-tape TM that runs in time $T(n)$ on $3n$-bit inputs.

Suppose that

- M accepts all inputs of the form $w = x 0^n y$, $|x|=|y|=n$, s.t. $f(x,y)=1$;
- M rejects all inputs of the form $w = x 0^n y$, $|x|=|y|=n$, s.t. $f(x,y)=0$.

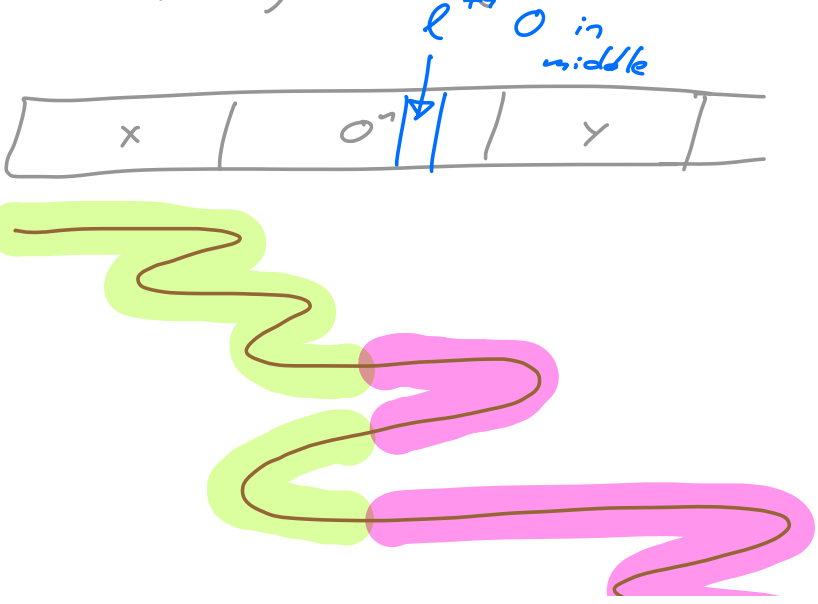
Then $R_0^{pub}(f) \leq O(T(n))/n$.



Pf:

A + B use shared rand (first $\log n$ bits) to choose rand $1 \leq \ell \leq n$: (loc in 0's)

They sim. M where A does the sim. when tape head is to left of ℓ, B " " " " "
" " at ℓ or to right of ℓ



At each handoff, only $O(1)$ bits exchanged (state of finite control).

Total runtime of M is $\leq T(n)$;
n =ly likely poss. for ℓ, each time crosses ℓ is a time step of computation, so

$$\mathbb{E}[\#\text{ times } M \text{ crosses loc. } \ell] \leq T(n)/n.$$

So

$$R_0^{pub}(f) \leq \mathbb{E}[\text{cost of this prot}] \leq O(1) \cdot T(n)/n.$$

Applic: Palindromes again.
$f(x,y)=1$ iff $x=y^R$; let M be any 1-tape TM for palindr. running in $T(n)$ time on $3n$-bit inputs.

M fits the above bill.

So

$$\Omega(n) = R_0^{pub}(EQ) \leq c \cdot T(n)/n, \text{ so}$$

$$\Omega(n^2) \leq T(n).$$

Rand. CC allowing error:
(pub. coin only for now)

Def An *ε-error pub. coin rand prot. P_{rand} for f* is a dist. over det prot's $P_1, P_2, \ldots$ s.t. for each (x,y), rand prot. computes f correctly on (x,y) w.p. $\geq 1-\varepsilon$.

The *(worst-case) cost of P_{rand} on (x,y)* is max # bits any prot P_i in dist. could communicate on (x,y).

The *(worst-case) cost of P_{rand}* is max of over all (x,y)

Finally, $R_\varepsilon^{pub}(f)$ = min of over all ε-error pub coin protocols for f.

Q: Fix $\varepsilon = 10^{-6}$.
What is $R_\varepsilon^{pub}(EQ)$?

A: $O(\log \frac{1}{\varepsilon})$ (const indep. of n!)

(Next time.)