Last time:  
- det. comm. c.xit y f: X x Y -> Z  
- protocols, rectangles, leaves, lower bds: 
  if any partition of matrix f(x, y) into monochrom. rect.  
  requires \geq \log t rect., then \( D(f) \geq \log t \).  
  so \( D(\mathbb{EQ}) \geq n+1 \) (= n+1)  

Today:  
- application to time-space tradeoffs for TMs  
- randomized comm. c.xit, appl. to 1-tape TM lower bounds  
  (maybe) start last unit: circuit complexity

Questions?

---

Appl. of our det. c.c. lower bd: 
Time/Space tradeoff for TMs

K-tape TMs: 
read-only input tape, k worktape

How does info "flow" between A & B?  
- state of FC: O(c1) bits  
- contents of k worktapes: if space s TM,  
  \( O(k \cdot s) = O(s) \) bits.
Lemma: Let $f: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$

Let $M$ be a $k$-tape TM that runs in $T(n)$ time, $S(n)$ space on $3n$-bit inputs, s.t.:
1. $M$ acc. all $w = x O^\gamma$, $x, y \in \{0,1\}^n$ and $f(x, y) = 1$
2. $M$ rej " " " " " " " " $f(x, y) = 0$

Then $D(f) \leq O\left(\frac{T(n) \cdot S(n)}{n^2}\right)$.
(i.e. $n \cdot D(f) \leq O(T(n) \cdot S(n))$).

Here's a prot. for $f$:

**Pf:** On input $x y$, they sim $M$'s exec. on $w = x O^\gamma$ as follows:

1. $M$'s input head:
   - $M$'s input head:
   - always either in 1) $x$-region (A sim.)
   - 2) $y$-region (B sim.)
   - 3) $O$-region (whoever was most recently doing sim.)

i.e. they transfer control only when head enters other player's region.
When they switch control, the info transferred is 

At least \( n \) time steps between sucs, switches, so 

tot # switches \( \leq T(n)^{1/n} \).

So tot. comm. is \( \leq O(S(n)) \cdot T(n)^{1/n} \) bits.

So that's a prot. using \( O(S(n) \cdot T(n))^{1/n} \) bits of comm.

---

Application: Palindromes.

\[ L = \{ w w^R : w \in \{0,1\}^* \} \]

Let \( M \) be \( k \)-tape TM for \( L \),

\( M \) runs in \( T(n) \) time, \( S(n) \) space on \( 3n \)-bit inputs.

\( f(x,y) = 1 \) iff \( x = y^R \)

This \( M \) acc. \( w = x^O y \), \( x, y \in \{0,1\}^n \), \( f(x,y) = 1 \) 

"rej" "" "

\( f(x,y) = 0 \).

This \( f \) is equiv to \( EQ \), so \( O(f) \geq n + 1 \).

So

\[ n + 1 \leq O(f) \leq O\left( \frac{T(n) \cdot S(n)}{n} \right) \]

hence

\[ \Omega(n^2) \leq T(n) \cdot S(n). \]

Easy: TM using \( O(n) \) time, \( O(n) \) space

\( \bigvee \)

" " " \( O(n^2) \) time, \( O(\log n) \) space

No TM using \( n^{0.99} \) space, \( O(n) \) time can exist.
Randomized C.C. A, B use randomness.

- "private-coin protocol": $A$ has $\$A$, $B$ $\$B$.

We discuss

- public coin protocols: $A$, $B$ shared access to common $\$\text{pub}$ random string.
  
  In prot., each $A$ node is $f$ of $x \& \$\text{pub}$ $B$ $``$ $``$ $``$ $y \& \$\text{pub}$. 

  Equiv. to: prob. dist. over det. protocols.
  
  $f: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}$ $f(x,y)$

  Def: *A zero-error pub coin rand prot. for $f$* is a dist. over det prots $P$, each is a correct prot. for $f$.
  
  The avg-case cost of $P_{\text{rand}}$ on $(x,y)$ is
  
  $E[\# \text{bits comm. on } (x,y)] = E[\text{depth of leaf } (x,y) \text{ reaches}]$.

  The avg-case cost of $P_{\text{rand}}$ is $\max_{(x,y)}$.

  Finally,
  
  $R^{\text{pub}}_0(f) = \min_{P_{\text{rand}}} \max_{(x,y)}$ over all $P_{\text{rand}}$.

Fact: $R^{\text{pub}}_0(EQ) = \Theta(n)$.

Applic. of rand. CC to 1-tape TM lower bds.
Lemma: Let $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.

Let $M$ be $1$-tape TM running in $T(n)$ time on $3n$-bits.

$s.t.$ $\cdot$ $M$ acc. all $w = x \cdot 0^n$, $x, y \in \{0,1\}^n \Rightarrow f(x, y) = 1$ (as before)

$\cdot$ $M$ rej $\cdot \cdot \cdot \cdot \cdot \cdot f(x, y) = 0$.

Then $R_o(f) \leq O\left(\frac{T(n)}{n}\right)$.

Proof: Given $M$, here's a zero-error randomized protocol for $f$:

$A, B$ use log, $\log n$ (public) to pick a unit random index $i \in \{1, \ldots, n\}$. (log loc. in $0^n$ block)

$A, B$ simulate $M$:

Each switch costs $O(1)$ bits (finite control state)

Runtime $\leq T(n)$.

$l$ unit random from $\{1, \ldots, n\}$:

So $E\left[\#\text{times } M \text{ crosses } l \text{ (per switch)}\right] \leq \frac{T(n)}{n}$.

So $E\left[\text{cost of protocol}\right] \leq O\left(\frac{T(n)}{n}\right)$.
Since \( R^\text{pub}_o(EQ) = \Theta(n) \), again get PAC result:
\[
\Theta(n) \leq O\left( \frac{T(n)}{n} \right),
\]
\[ \text{i.e.} \]
any 1-tape TM for palindromes needs \( \Omega(n^2) \) time.

\text{Rand. prot. with error.}

Let’s relax, and consider \( \text{pub coin prot. for EQ} \)
s.t. for every \((x, y)\), prot. gives right answer
(1 if \( x = y \), 0 if \( x \neq y \))
w.p. \( \geq 99.9\% \). \( R^\text{pub}_\varepsilon(EQ) \)
\[ \Rightarrow \varepsilon = 0.001 \]

\text{Fact: For } \varepsilon = 0.001, \ R^\text{pub}_\varepsilon(EQ) = O(1). \quad O\left( \log \frac{1}{\varepsilon} \right).

\text{Here's how: Let } r = (r_1, \ldots, r_n) \in \{0,1\}^n \text{ be first } n \text{ bits of shared rand. string.}

x, r \in \{0,1\}^n

A computes \( x \cdot r \mod 2 \) \quad x, r, \ldots, x \cdot r_n \mod 2
t and send to B.

B computes \( y \cdot r \) and compare to what A sent.

• if \( x = y \) : of course the bits agree.
\[ \text{if } x \neq y: \quad \Pr[x \cdot r \mod 2 = y \cdot r \mod 2] = \frac{1}{2}. \]

So repeating \( \log \frac{1}{\varepsilon} \) times, if \( x = y \) \( \checkmark \)
if \( x \neq y \), they learn this w.p. \( 1 - \varepsilon \). \( \checkmark \)

**Last unit**

**Circuit complexity**

Recall **Boo's chrt**: natural way to compute
\[ f: \{0,1\}^n \rightarrow \{0,1\} \]

**Size of a chrt**: 
\# gates.

**Depth of chrt**: length of longest path to output.

**Def**: \( f \) : \( \{0,1\}^* \rightarrow \{0,1\} \) has circuit complexity \( s(n) \) if \( \forall n \), \( f \) on \( \{0,1\}^n \) is computed by
a size- \( s(n) \) chrt.

\[ L \leq \varepsilon^* \]

**Ex**: \( \text{Saw} \quad \text{PAR} : \{0,1\}^* \rightarrow \{0,1\} \)
\[ \text{PAR}(x_1, \ldots, x_n) = x_1 + \cdots + x_n \mod 2 \]
has \( O(n) \) size chrts.

Really, a \( f : \{0,1\}^* \rightarrow \{0,1\} \)
\[ \uparrow \]
\[ \downarrow \]
Recall: If $L \subseteq P$, then $L$ has a family of poly$(n)$-size cuts.

So... if could show $L$ doesn't have, would show $L \not\subseteq P$.

Hence, study circuit lower bound.

Next time: 
* nonexplicit very strong ckt LBs.
* start constant-depth circuit lower bounds.