Last time: • FPRAS for #DNF: alg + proof
• hardness of approx. #CYCLES
• sketch of FPRAS for <u>any</u> fn in #P
(provided we have an NP-oracle)

(an example of "concrete complexity")

Today: start (short) unit on <u>communication complexity</u> CC

AB 13.1, 13.2

- deterministic comm. cxity of functions: examples, protocols, rectangles, lower bounds
- applications: time/space tradeoffs for TMs

Questions?

Basic setup of CC: 2 parties A + B.
<u>Cooperating</u> to compute a fn

$$f: X \times Y \to Z \qquad f(x,y) = z$$

very often for us: $X = Y = \{0,1\}^n$; $Z = \{0,1\}$

Both "know" f, but only A has $x \in X$, only B has $y \in Y$.

Central question: How many bits do they need to communicate s.t. each can output correct value $f(x,y)$?

Computation is "free"

Ex #1: $X = Y = \{0,1\}^n$, $Z = \{0,1\}$.

Can always do any $f: X \times Y \to Z$ with $n+1$ bits:

A sends x to B

B has $x + y$: computes $f(x,y)$, sends it to A.

For general Z, this X, Y: $n + \lceil \log |Z| \rceil$ bits.

Ex #2: $X = Y = \{0,1\}^n$,

$$f(x,y) = PAR(x \circ y) = \sum_{i=1}^{n} x_i + y_i \mod 2.$$

2 bit prot: A computes $\sum_{i=1}^{n} x_i \mod 2$, sends to B; he computes $\sum_{i=1}^{n} y_i \mod 2$, returns $\cdot + \cdot \mod 2$

Ex #3 $X = Y = \{0,1\}^n$ (view $x \in \{0,1\}^n$ as subset of $[n]$, y likewise.

multiset union

$Z = [n]$, $f(x,y) =$ median of multiset $x \cup y$

$x = \{2, 3, 4, 7, 8, 11\}$

$y = \{3, 4, 5, 7, 9, 10, 12, 14\}$

multiset union $2, 3, 3, 4, 4, 5, \boxed{7}, 7, 8, 9, 10, 11, 12, 14$

$f(x,y) = 7$

Bin. search based prot. : let $[i,j]$ be curr. interval we know $f(x,y)$ is in. $[1,n]$

let $k =$ midpoint $= \frac{i+j}{2}$.

Current stage:

A sends (# of elts of x that are $\leq k$, # " " " " " " $> k$)

B uses this + his complete knowledge of y to determine whether median is $\leq k$ or not; sends A "above" or "below."

$O(\log n)$ bits total comm./stage;

$O(\log n)$ stages $\Rightarrow O(\log^2 n)$ comm. total.

Ex #4: $X = Y = \{0,1\}^n$; $f(x,y) = EQ(x,y)$

$$= \begin{cases} 1 & \text{if } x = y \\ 0 & \text{o/w}. \end{cases}$$

? c.c. of EQ ?

We'll see: Best poss. prot. requires $n+1$ bits.

We'll consider only <u>det</u> (for now) protocols.

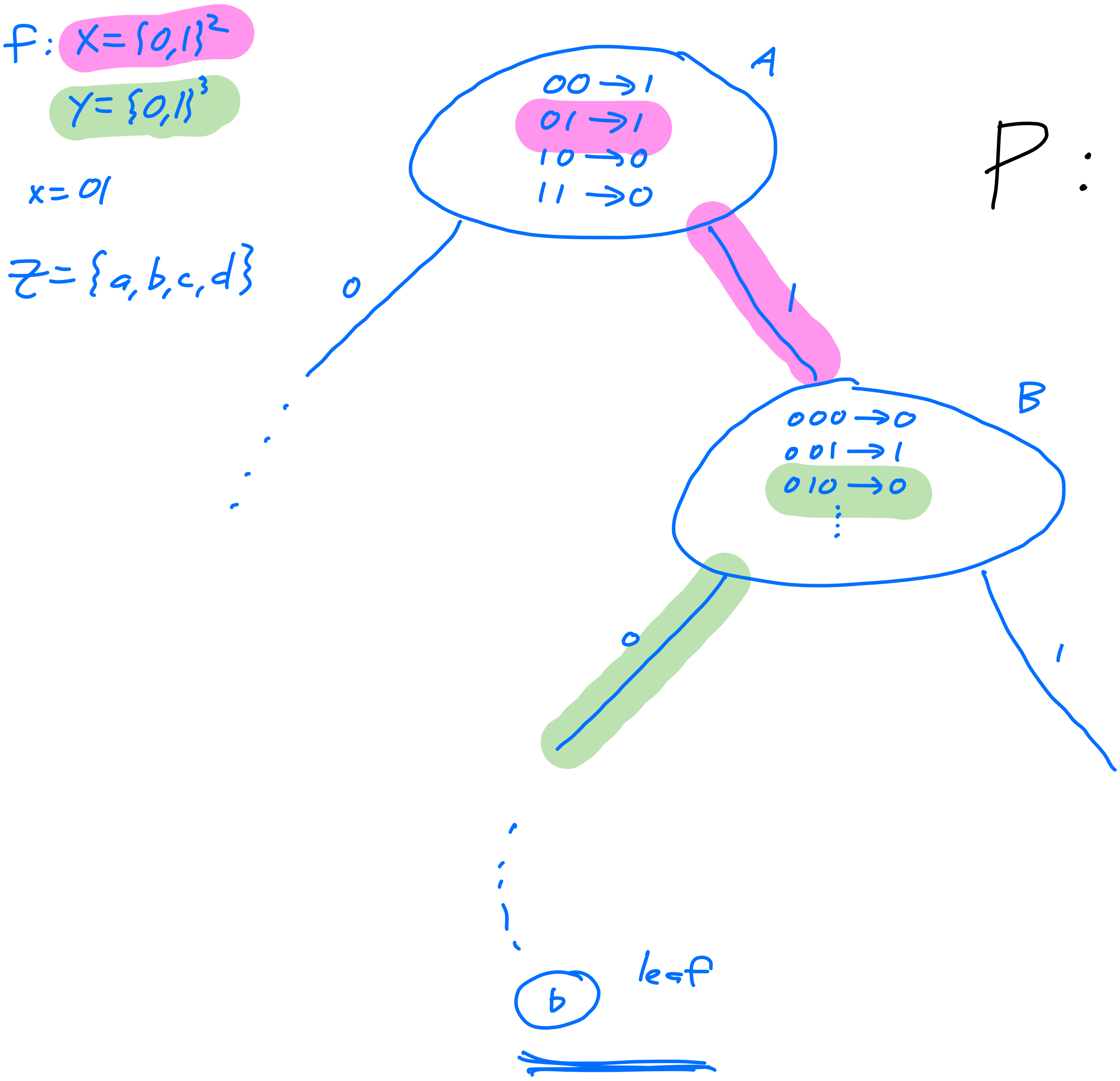
- Protocol for f: complete system of rules for who says what + when. (Both A + B "know" the protocol" + execute it.) → at end, both A + B "know" $f(x,y)$.

<u>Def</u>: A <u>(det. comm.) prot. P for $f: X \times Y \to Z$</u> is a rooted bin. tree where

- each internal node has a 0-child + a 1-child, + is labeled either with
  - a fn $X \to \{0,1\}$ (A-node) or
  - a fn $Y \to \{0,1\}$ (B-node)
- each leaf lab. with an elt $z \in Z$

$$z = f(x,y)$$

Prot. determines $f(x,y)$ by walking the tree.

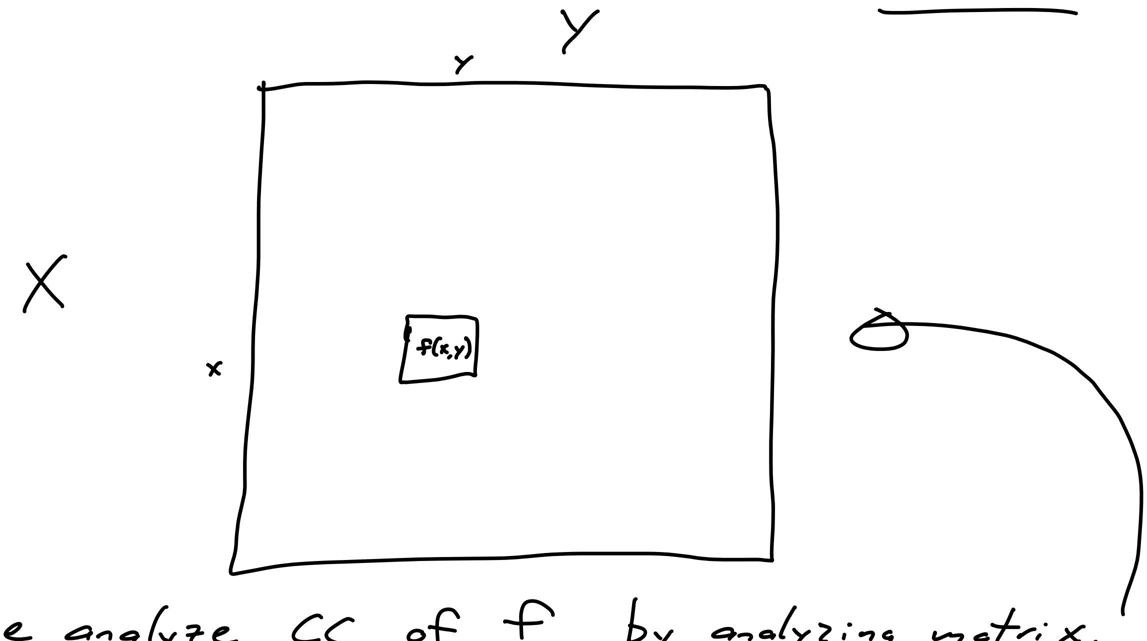


<u>Def</u>: The (worst-case) <u>cost</u> of prot. P is the (max) depth of the tree; = to the worst-case # bits A & B communicate on any pair $x \in X$, $y \in Y$.

The det. CC of f, $D(f)$, is the min cost of any prot. that computes f. (depth of shallowest tree)

Let's consider the fn $f: X \times Y \to Z$.

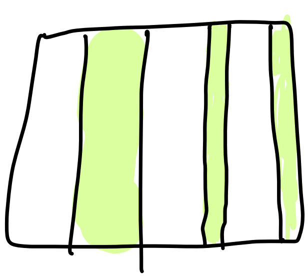
View such an f as an $X \times Y$ matrix:

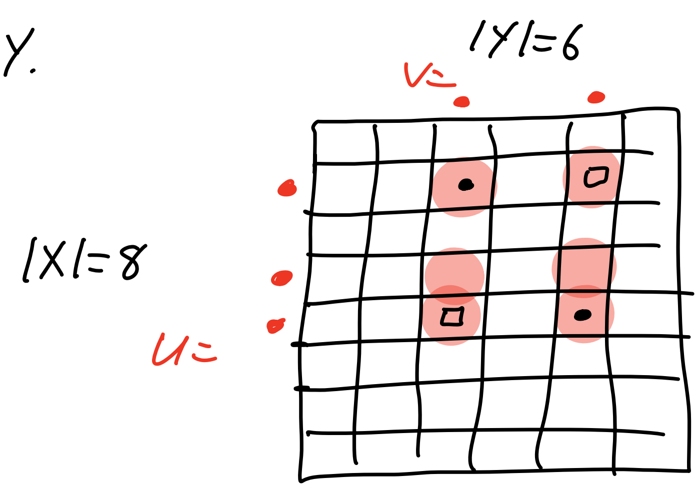


we analyze CC of f by analyzing matrix.

Key insight: any prot. for f partitions the mtx into disjoint "monochromatic (combinatorial) rectangles".

Def: A (combinatorial) rectangle in $X \times Y$ is a subset $R \subseteq X \times Y$ s.t. $R = U \times V$ for some $U \subseteq X$, $V \subseteq Y$.





Obs: $R \subseteq X \times Y$ is a rect. iff $\forall x_1, x_2 \in X$, $\forall y_1, y_2 \in Y$, have

$$(x_1, y_1) \in R + (x_2, y_2) \in R \implies (x_1, y_2) \in R.$$

Notation: Fix prot. P, node v of prot. tree. Write $R_v :=$ set of pairs (x,y) that would reach v.

- $\{R_\ell : \ell \text{ is a leaf of } P\}$ is a partition of $X \times Y$ into disjoint subsets.

- For any node v in P, R_v is a rectangle.

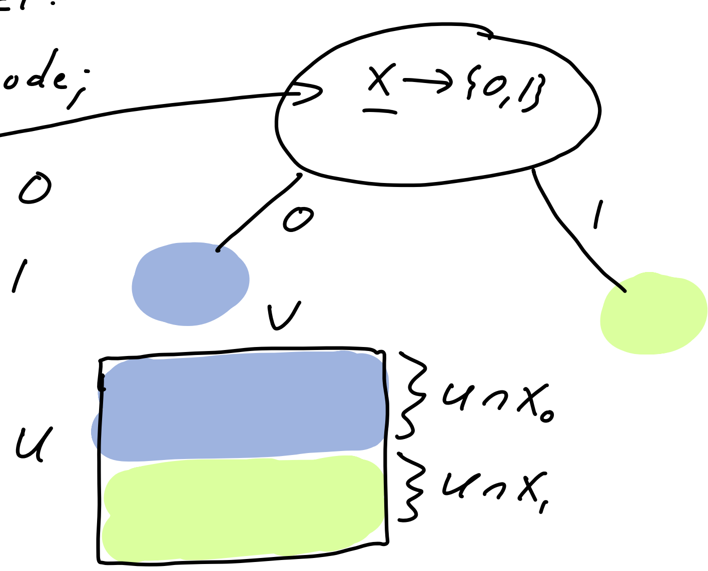
Pf by induc. on depth of v: depth 0: $R_{root} = X \times Y$

Sps R_w is a rect.

Sps w is an $\underline{A}$-node;

$X_0 \subseteq X$ s.t. fn outputs 0

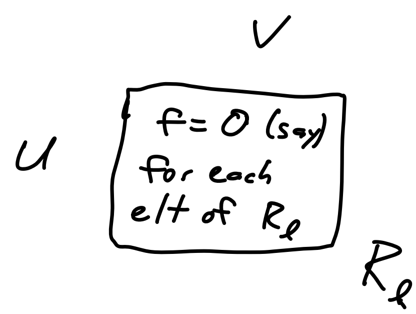
$X_1 \subseteq X$ s.t. " " 1



So... R_ℓ is a rect., for each leaf ℓ of P.

Fix ℓ. Every pair $(x,y) \in R_\ell$ must be labeled with same $z = f(x,y)$ for the prot. to correctly compute f:

such a rect. is "f-monochromatic."



Summarizing: Fix any P that correctly computes f.

- The leaves of P induce a partition of $X \times Y$ into f-monochr. rectangles.
- \# rect. in partition = \# leaves in P.

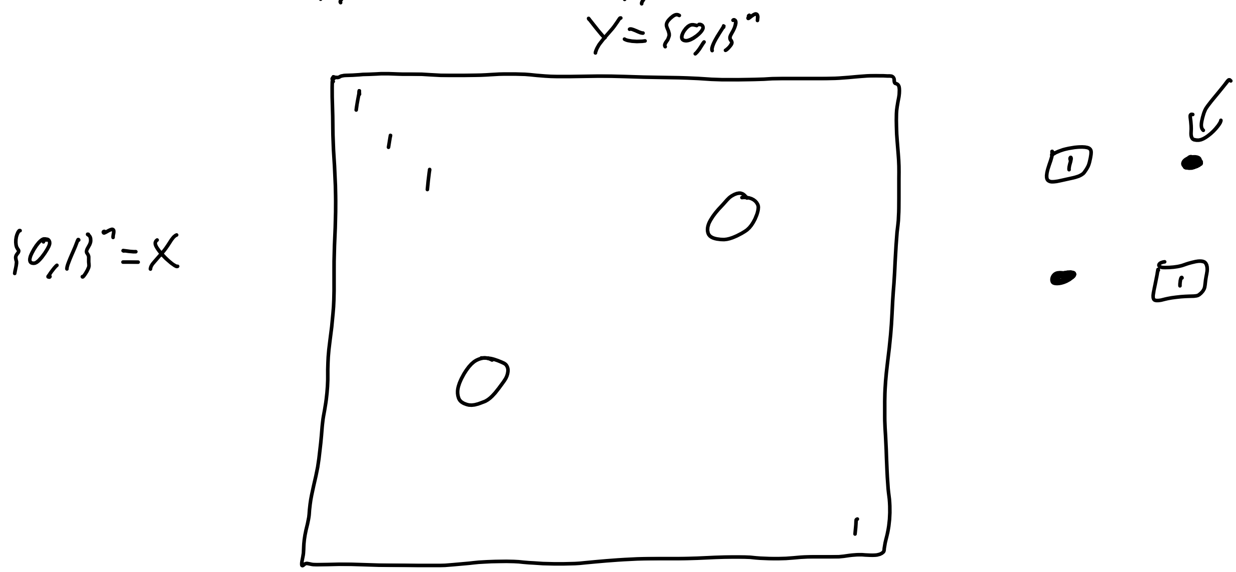
- Suppose we can argue that any part. of $X \times Y$ into f-monochr. rect. must use $\geq t$ rect.

  This'd mean any prot P for f must have $\geq t$ leaves.

So P must have depth $\geq \log_2 t$,

hence $D(f) \geq \lceil \log_2 t \rceil$

EQ: $f(x,y) = EQ(x,y)$ $\qquad X = Y = \{0,1\}^n$



Every 1 requires its own rect. (or else rects wouldn't be monochr.); 2^n rect.

Need ≥ 1 0-rect;

so $t > 2^n$

& $\lceil \log_2 t \rceil \geq n+1$.

So $D(EQ) = n+1$.

Next: applic. to time-space tradeoffs, & rand c.c.
