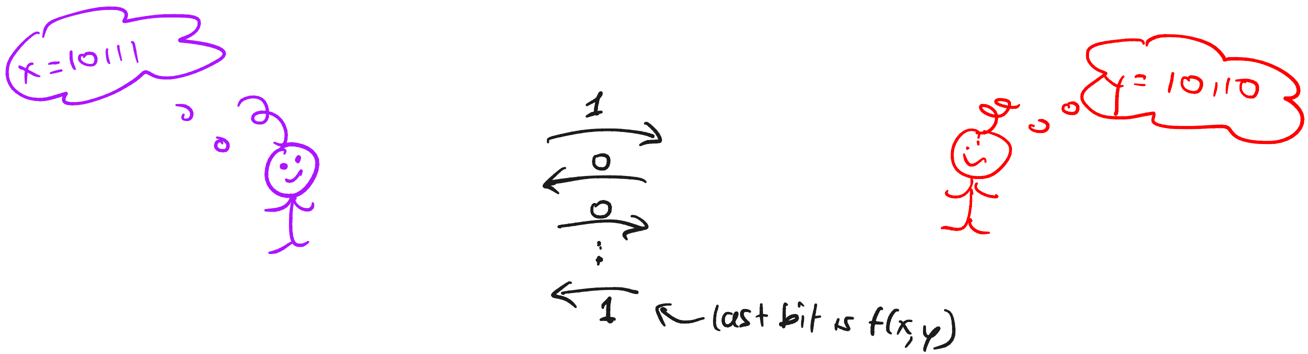
CS 6998:

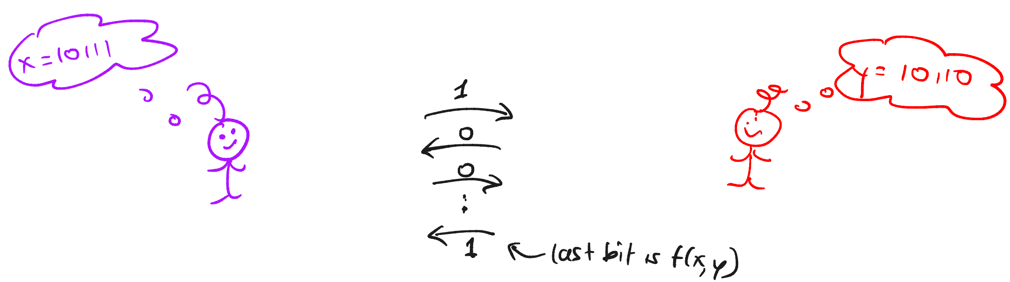
COMMUNICATION COMPLEXITY & APPLICATIONS



CS 6998:

COMMUNICATION COMPLEXITY & APPLICATIONS

Toniann Pitassi   tonipitassi@gmail.com



Course Webpage:

www.cs.toronto.edu/~toni/courses/commComplexity2022/
cc2022.html

(or go to www.cs.toronto.edu/~toni
and follow teaching link)

Lectures: Wed 2:10 - 4

Office hrs: TBA or by appointment

All course materials provided on webpage

Optional Textbooks:

Nisan-Kushilevitz	Communication Complexity
Rao-Yehudayoff	Comm Comp + Applications
Lee-Shraibman	Lower Bounds in Comm Complexity

Course Outline/Evaluation: see Webpage

- 2-3 assigments
- Short Presentations

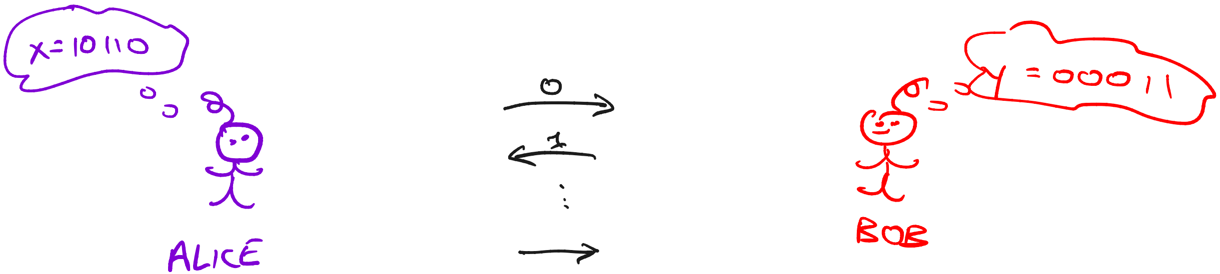
Lecture Notes (see webpage)

Please email me (tonipitassi@gmail.com)
using heading "cc2022"

* I would like your opinions on what applications you are most interested in!
(see Lecture 1 + papers on website for list of possibilities)

Please email!

COMMUNICATION COMPLEXITY



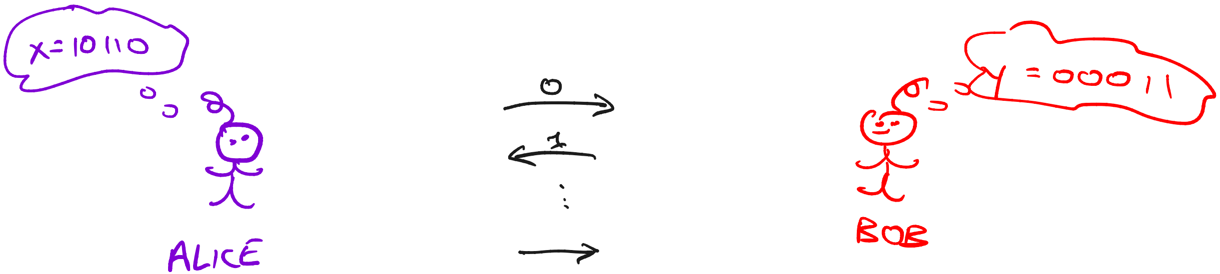
Alice & Bob have private information

Alice has boolean vector x, Bob y

Typically $|x| = |y| = n$

They want to compute some joint function (or search problem) $f(x,y)$

COMMUNICATION COMPLEXITY



<u>Example 1</u> Parity(x,y) = parity of number of 1's in combined string xy

2 bit protocol:

Alice sends parity of # 1's of x

then Bob sends parity of x, plus bit sent by Alice

so parity is <u>easy</u>

Note that if $|x| = |y| = n$

then any Boolean $f(x,y)$ can be computed

using $n+1$ bits

Alice (or Bob) can just send their whole

input to other player

+ then other player computes $f(x,y)$

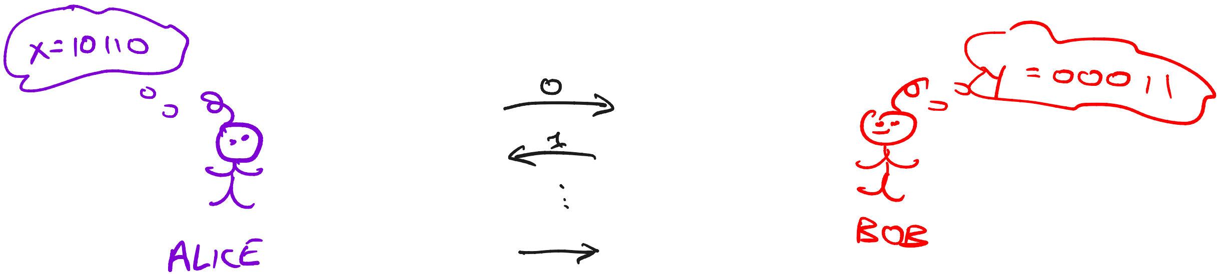
+ sends back answer

So all functions can be computed using $O(n)$ bits

So an efficient protocol will be one of

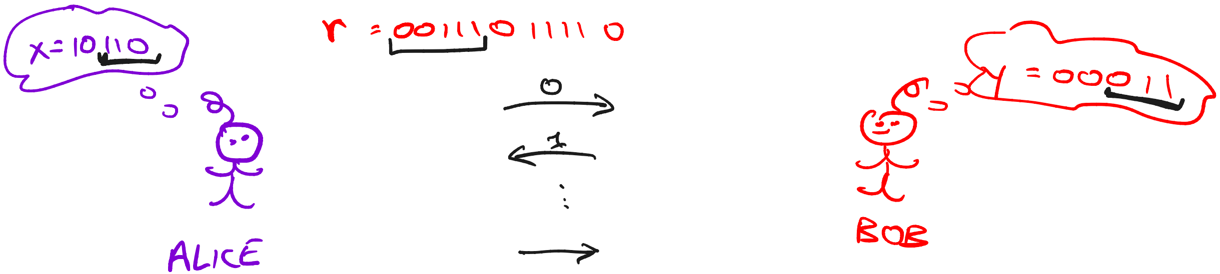
complexity $(\log n)^{O(1)}$

COMMUNICATION COMPLEXITY



Example 2 $EQ(x,y) = 1$ iff $x=y$

Randomized COMMUNICATION COMPLEXITY (public coin)



Example 2 $EQ(x,y) = 1$ iff $x = y$

We say Π computes $f(x,y)$ with success prob $1-\varepsilon$ if

$$\Pr_r\left[\Pi(x,y,r) = f(x,y)\right] \geq 1-\varepsilon$$

Randomized EQ protocol ($\varepsilon = \frac{1}{2}$)

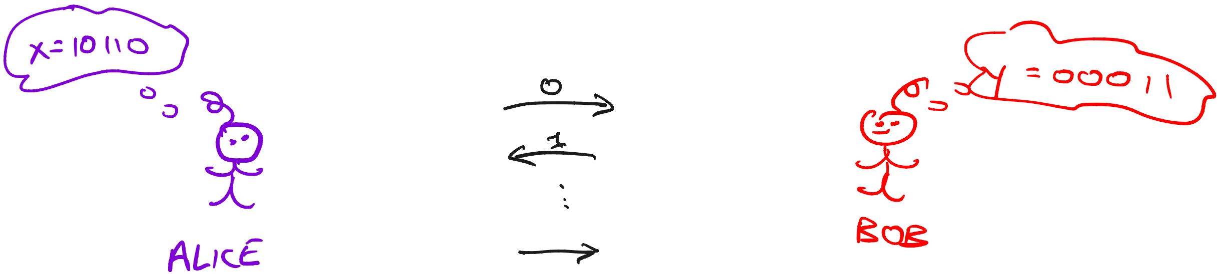
View 1st n bits of r as selecting a subset of $1 \ldots n$.

Alice sends parity of $x|_r$

Bob sends parity of $y|_r$

Accept (output 1) iff parities are the same

COMMUNICATION COMPLEXITY



Example 3 DISJ$(x,y) = 1$ iff $\exists i \;\; x_i = y_i = 1$

communication complexity analog of SATISFIABILITY problem

NP complete

DISJ requires $\Omega(n)$ cc, (det + randomized)

But easy nondeterministically

Nondeterministic CC

r

Alice $\quad \xrightarrow{b_1} \quad$ Bob

$x \quad \xleftarrow{b_2} \quad y$

$\vdots$

$|x| = |y| = n$

They share random string r, $|r| = O(\log n)$

Π computes f nondeterministically if

1. $f(x,y) = 0$ then $\forall r \ \Pi(x,y,r) = 0$
2. $f(x,y) = 1$ then $\exists r \ \Pi(x,y,r) = 1$

$$\text{complexity of } \Pi = \max_{\substack{x,y,r \\ |x|=|y|=n}} \left(\#\text{bits exchanged by } \Pi(x,y,r) + |r| \right)$$

Nondet protocol for DISJ:

Alice/Bob view r, $|r| = \log n$ as some $i \in [n]$

Alice sends 1 iff ~~the~~ r^{th} bit of x $(x_r) = 1$

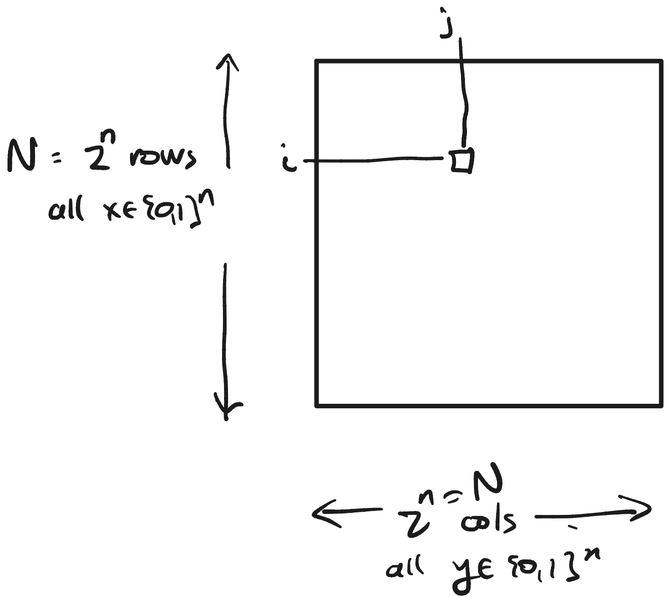
Bob sends 1 iff r^{th} " " y $= 1$

accept iff both send 1's

Formal Defn of a Deterministic Protocol

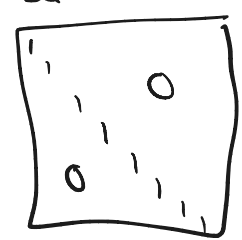
Let $f : \underbrace{\{0,1\}^n}_{x} \times \underbrace{\{0,1\}^n}_{y} \to \{0,1\}$

the comm. matrix M_f associated with f:



$M_{ij} = f(i,j)$

$M_{EQ} = I$



A protocol Π is a binary tree

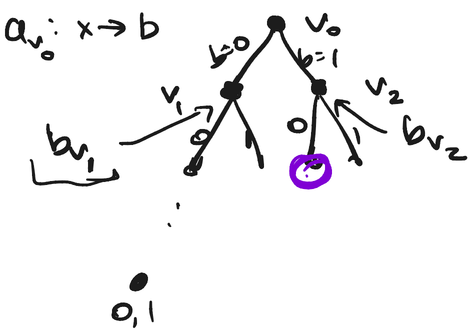
Every nonleaf vertex of tree is labelled by either a (Alice) or b (Bob)

also each nonleaf vertex v is labelled by a

function $a_v : \underbrace{\{0,1\}^n}_{x} \to \{0,1\}$

or $b_v : \underbrace{\{0,1\}^n}_{y} \to \{0,1\}$

~~to~~ each leaf vertex w is labelled by either 0 or 1

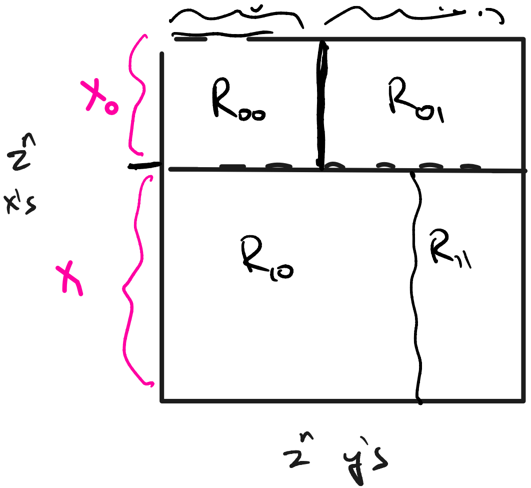


Alice x Bob y

max depth of tree corresponding to Π

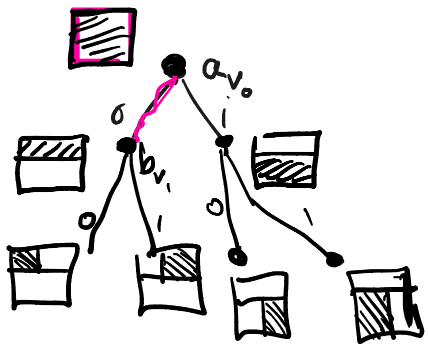
$= cc$ of Π

Matrix View of Protocol Π for $f(x,y)$



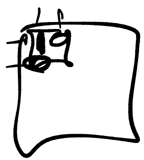
Say Alice sends 1st bit

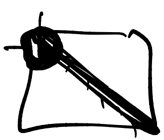
R_0 = inputs of Alice/Bob corresponding to transcript 0



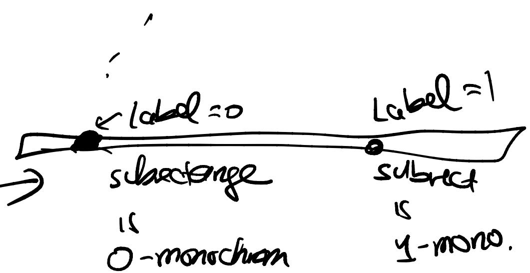
$R_0 = X_0 \times Y$

$R_1 = X_1 \times Y$





Partition of M_f into disjoint subrectangles

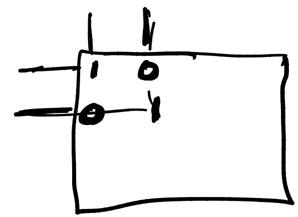


Observation any deterministic protocol Π for EQ must have at least 2^n leaves

(+ therefore has depth $\Omega(n)$)

$\therefore$ CC^{det} of EQ $= \Omega(n)$

all 1's in M_{EQ} have to end up at distinct leaves



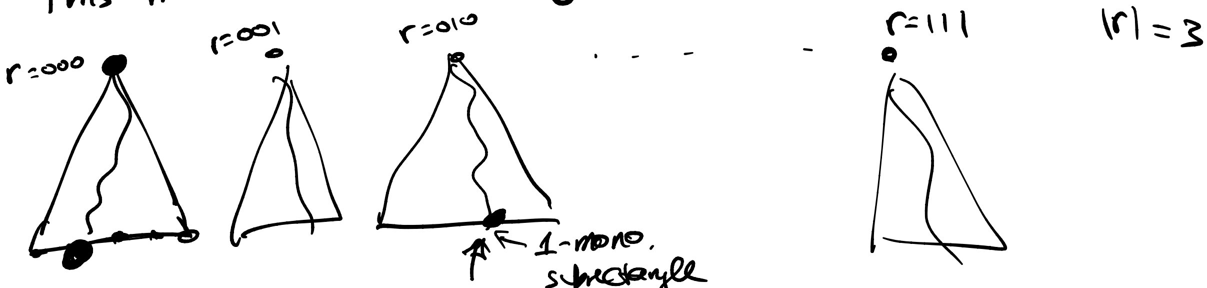
What happens to partition of matrix in a nondeterministic protocol?

Say $|r| = R$

For both rand. & nondet protocols, we have 2^R protocol trees one for each choice of r

Say Π is a nondet protocol where $|r| = \log n$ for $f(x,y)$

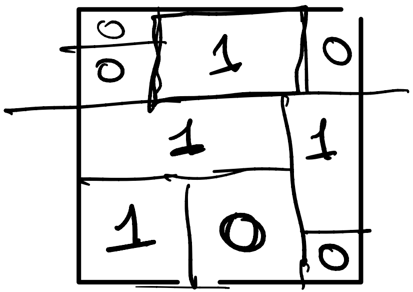
This means can describe Π by n protocol trees

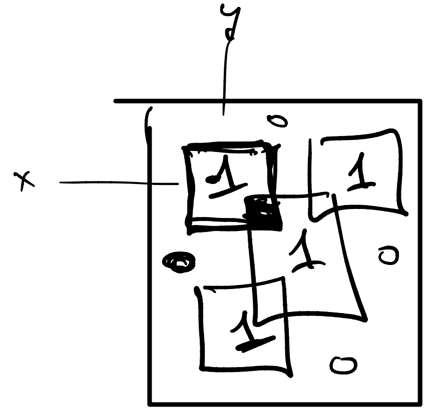


If $f(x,y)=0$ then x,y goes to a 0-mono rect. in all trees

If $f(x,y)=1$ then x,y goes to at least one 1-mono rect (in some tree)

So Π induces a <u>covering</u> of the 1's in M_f by 1-mono. rectangles





deterministic protocol.

$|\pi| = R$ cost b

$2^b \cdot 2^R$

nondet protocol

covering of 1's by at most $2^b \cdot 2^R$ 1-mono. subrectangle

Applications

→ VLSI / Bisection width of networks

→ Data structures

→ Boolean circuit complexity

→ Quantum complexity

→ Extended formulations of LPs

→ Streaming Algs

→ game theory

→ Privacy

→ learning theory

→ Proof complexity

→ graph theory, additive comb. + # theory

NOF

$f(x, y, z)$

Alice sees y, z

Bob sees x, z

Charlie sees x, y