Announcements

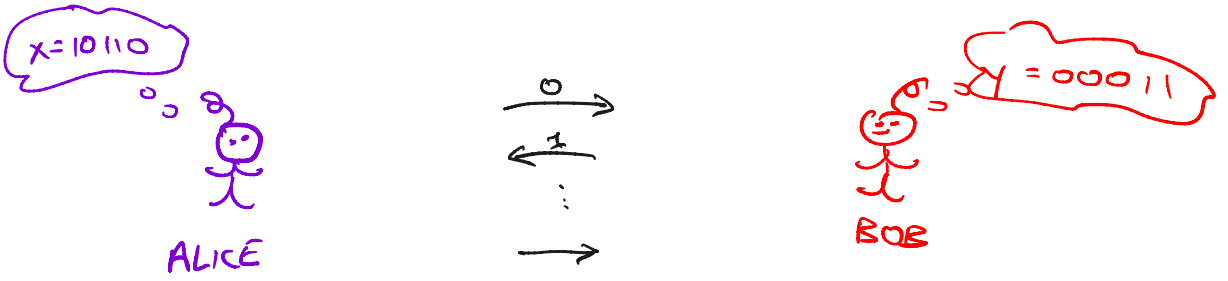
No class next week -- Happy Thanksgiving!

HW4 (last homework) will be posted Nov 30

Due 12/10

Today: comm complexity

COMMUNICATION COMPLEXITY



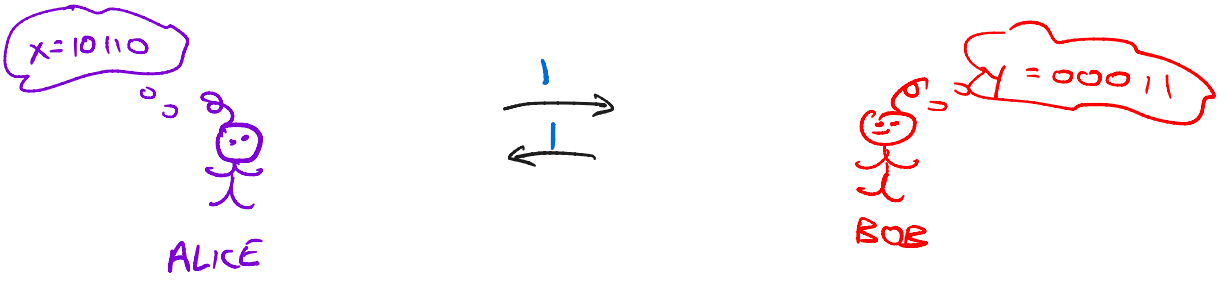
Alice & Bob have private inputs x and y respectively

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

They want to compute some joint function (or search problem) $F(x, y)$ by sending bits back & forth (bits can be arbitrary Not nec bits of x or y)

* Model is nonuniform: separate CC protocol for each n

COMMUNICATION COMPLEXITY

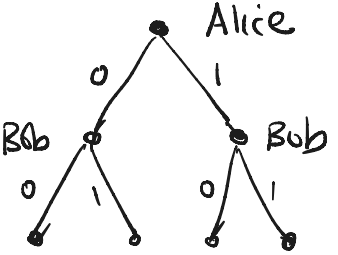


Example 1 Parity(x,y) = parity of number of 1's in combined string xy

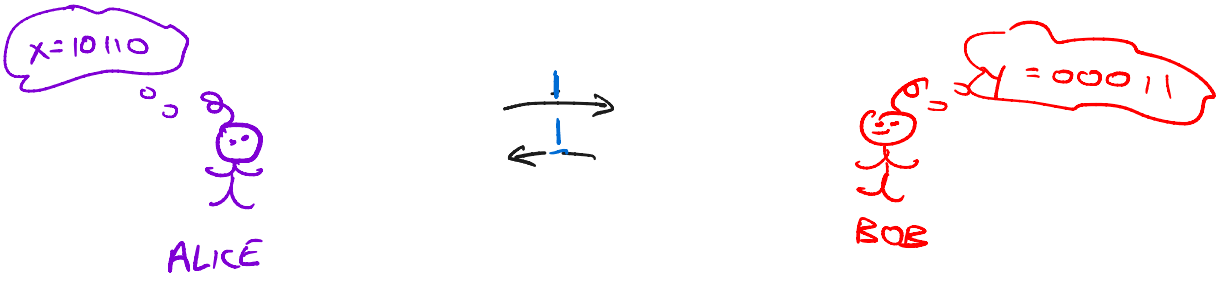
2 bit protocol:

Alice sends parity of # 1's of x

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



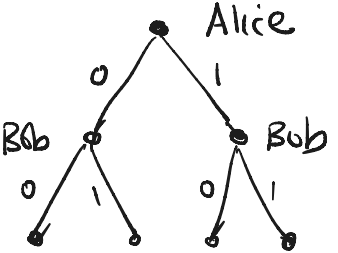
COMMUNICATION COMPLEXITY



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

$CC(\Pi_n) \triangleq$ max # bits sent over all x, y $|x| = |y| = n$

$CC(F) \triangleq \min_{\{\Pi_n\}} CC(\Pi_n)$



so $CC(\text{parity}) = 2 = O(1)$ ← independent of n!

So parity is very easy.

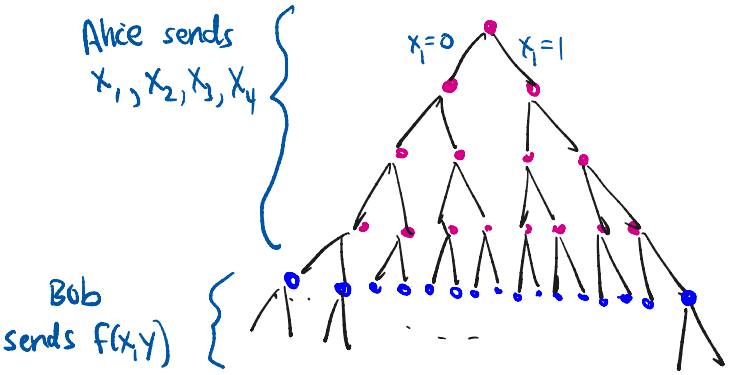
Observation: $\forall\ F: \underbrace{\{0,1\}^n}_{x} \times \underbrace{\{0,1\}^n}_{y} \to \{0,1\}$, $CC(f) \leq n+1$

Protocol:

Alice sends x to Bob in n rounds

Bob computes $F(x,y)$ and sends answer

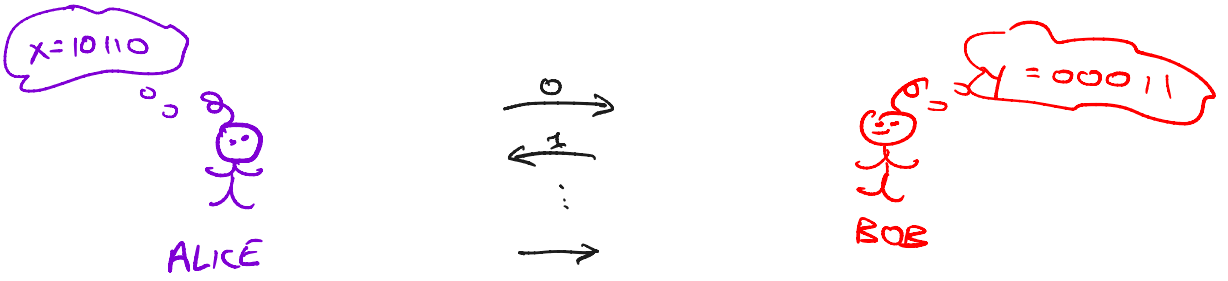
Example: $|x| = |y| = 4$



$\therefore$ We consider F "easy" for deterministic CC if $CC(F) = \text{polylog}(n)$

$$P^{cc} \triangleq \left\{ \{F_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}\}_n \mid \Pi(F_n) = O(\text{polylog } n) \right.$$

COMMUNICATION COMPLEXITY



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

2-party deterministic protocols (More formal Defn)

2 sets of inputs X, Y (usually $X = \{0,1\}^n = Y$)

A protocol Π specified by a rooted tree, fanout-2

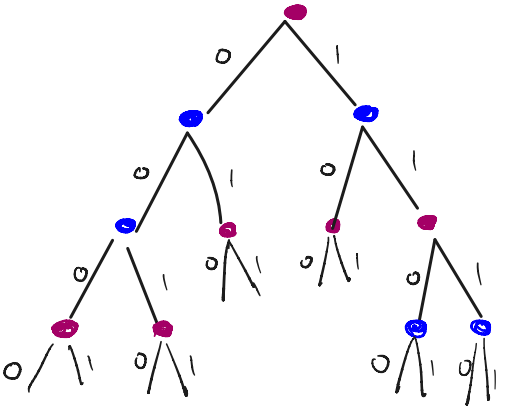
- each vertex associated with one player (Alice or Bob)
- If vertex v assoc. with Alice, then Alice computes a fxn $f_v : X \to \{0,1\}$ at v
- If v assoc. with Bob, then Bob computes $f_v : Y \to \{0,1\}$

default assumption: Players alternate and send one bit per round

2-party deterministic protocols

- Alice
- Bob

2 sets of inputs X, Y (usually $X = \{0,1\}^n = Y$)



A protocol Π specified by a rooted tree, fanout-2

- each vertex associated with <u>one</u> player (Alice or Bob)
- If vertex v assoc. with Alice, then Alice computes a fxn $f_v : X \to \{0,1\}$ at v
- If v assoc. with Bob, then Bob computes $f_v : Y \to \{0,1\}$

On input $(x,y) \in X \times Y$:

Players start at root of protocol tree

If at vertex v: player assoc. with v sends $f_v(x)$ to other player + both players move to child v' indicated by $f_v(x) \in \{0,1\}$.

Repeat until players reach a leaf vertex, v_ℓ, and output value of this leaf

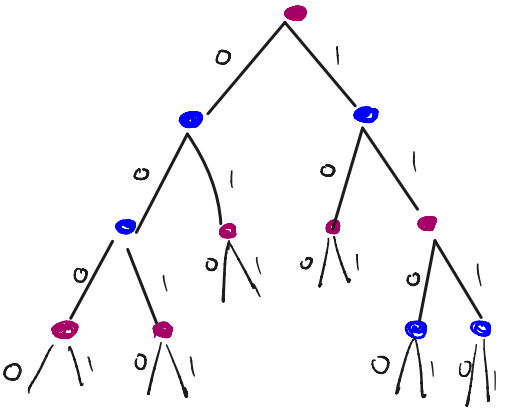
Π computes $g: X \times Y \to \{0,1\}$ if

$\forall (x,y) \in X \times Y \quad \Pi(x,y) = g(x,y)$

The comm. complexity of Π, $\|\Pi\|$, is the depth of protocol tree

The number of rounds of Π is max # of alternations (red/blue) over all paths of protocol tree.

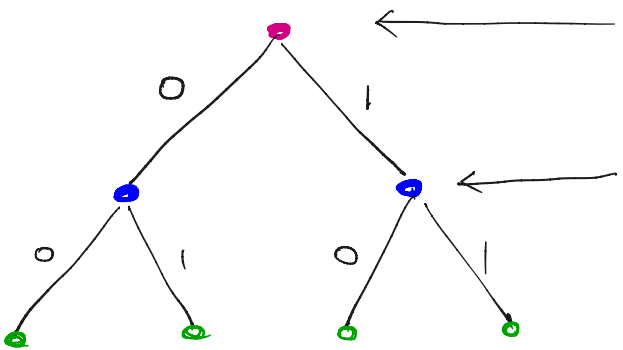
- Alice
- Bob





if $y^1_{x^1} = 1$ output a
else if $y^2_{x^2} = 1$ output b
else output 0

Example 1 Protocol for Parity (x, y)



Alice sends $m_1 = \text{Parity}(x)$

Bob sends $m_2 = \text{Parity}(y) + m_1 \mod 2$

ex: $x = 00110$: $m_1 = 0$

$y = 10110$: $m_2 = m_1 + \text{Parity}(y) \mod 2$

$= 0 + 1 \mod 2$

$= 1$

2 rounds

comm. complexity = 2 ← for any input lengths $|x|, |y|$

Another example: 2-Level Pointer jumping

Index function

Alice gets $x \in \{0,1\}^n$

Bob gets $y \in \{0,1\}^{2^n}$

output $y|_x$

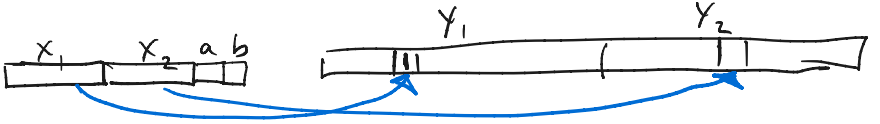


Pointer Jumping Function:

Alice gets $x^1, x^2 \in \{0,1\}^n$

$a, b \in \{0,1\}$

Bob gets $y^1, y^2 \in \{0,1\}^{2^n}$



If $Y_1|_{x_1} = 1$ output a

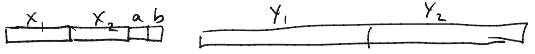
else if $Y_2|_{x_2} = 1$ output b

else output 0

Pointer Jumping Function:

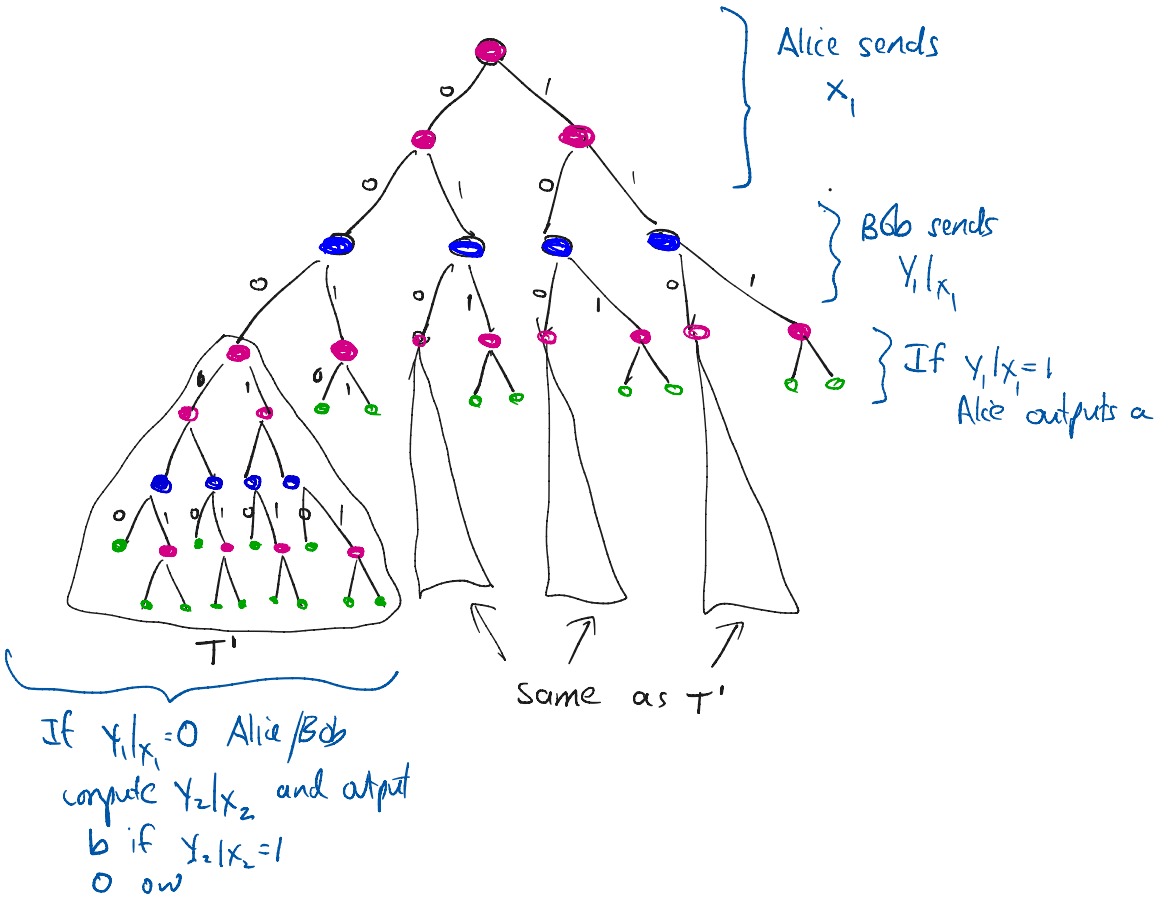
Alice gets $x^1, x^2 \in \{0,1\}^n$
$a, b \in \{0,1\}$

Bob gets $y^1, y^2 \in \{0,1\}^{2^n}$



If $y_1|_{x_1} = 1$ output a
else if $y_2|_{x_2} = 1$ output b
else output 0

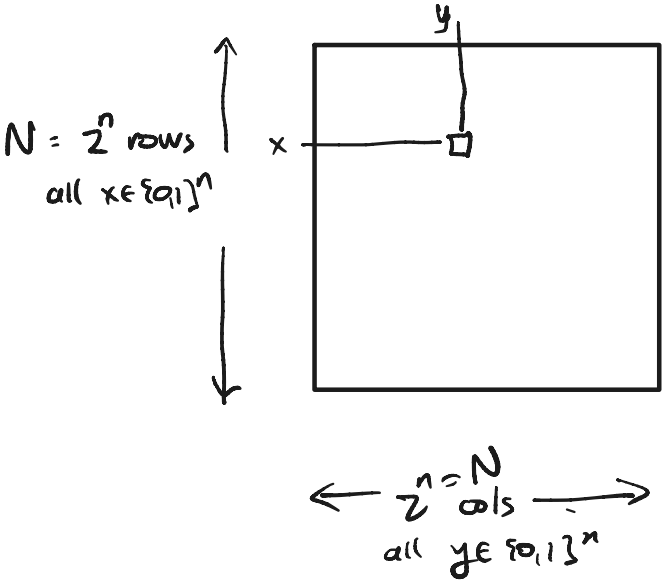
Protocol ($n = 2$)



Equivalent Matrix view of Deterministic CC protocol Π:

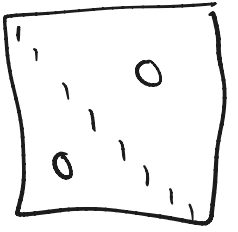
Let $f : \underbrace{\{0,1\}^n}_{x} \times \underbrace{\{0,1\}^n}_{y} \to \{0,1\}$

the comm. matrix M_f associated with f:



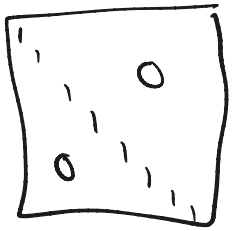
$M(x,y) = f(x,y)$

M_{EQ} = Identity matrix



Examples

1. Equality : $EQ(x,y) = 1$ iff $x = y$

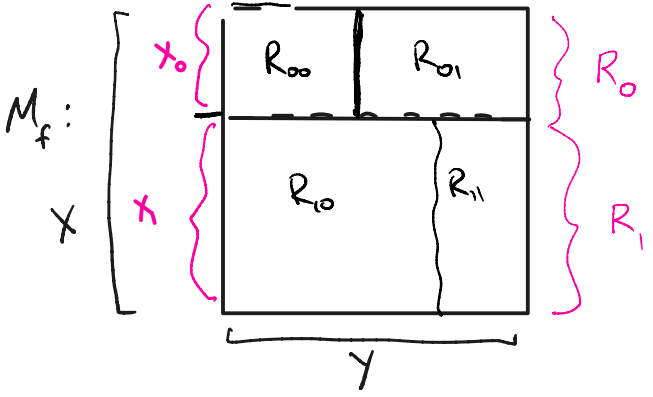
M_{EQ} :  ← Identity matrix

2. Parity(x,y) = 1 iff Number of 1's in x $=_{mod\ 2}$ # 1's in y

M_{PARITY} :

	000	001	010	011	100	101	110	111
000	1	0	0	1	0	1	0	1
001	0	1	1	0	1	0	0	1
010	0	1	1	0	1	0	0	1
011	1	0	0	1	0	1	1	0
100	0	1	1	0	1	0	0	1
101								
110								
111	0	1	1	0	1	0	0	1

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

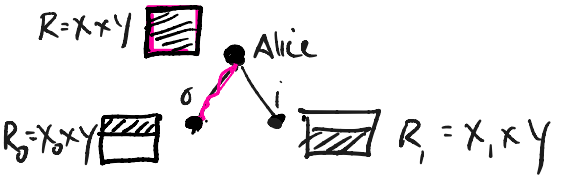


Let $X_0 = \{x \in X \mid$ Alice's 1st bit $= 0\}$
$X_1 = \{x \in X \mid$ " " " $= 1\}$

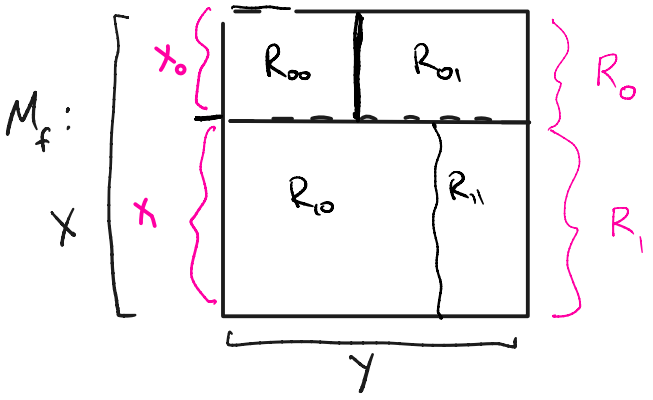
This partitions M_f into 2 disjoint subrectangles: $R_0 = X_0 \times Y$
$R_1 = X_1 \times Y$

Defn A subrectangle R of M has the form $X' \times Y'$ where $X' \subseteq X$, $Y' \subseteq Y$

Say Alice sends 1st bit:



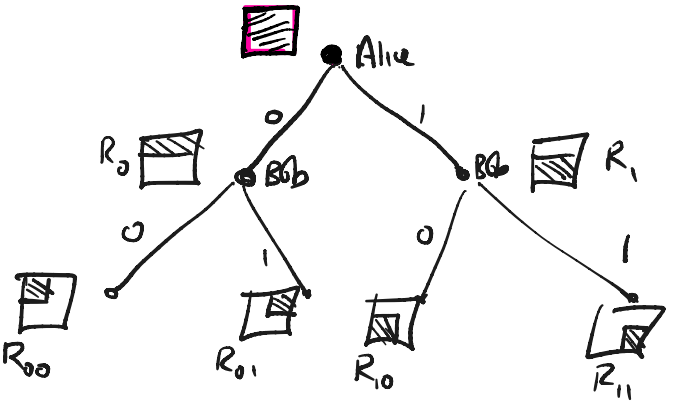
Matrix View of Protocol Π for $f(x,y)$



Let $X_0 = \{x \in X \mid$ Alice's 1st bit is $0\}$
$X_1 = \{x \in X \mid$ " " " " $1\}$

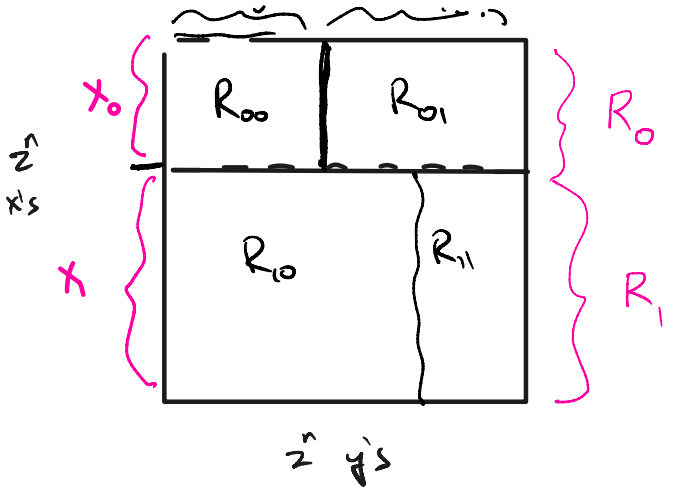
Next bit sent further partitions M into 4 disjoint Rectangles : R_{00}
R_{01}
R_{10}
R_{11}

Say Bob sends 2nd bit :

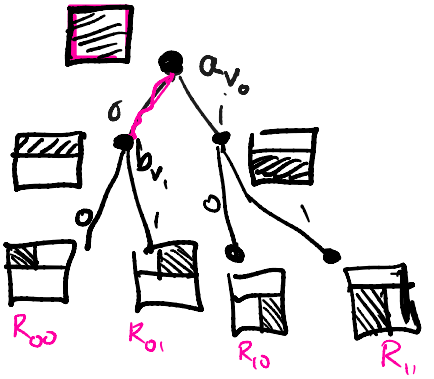


R_{00} = inputs in $X \times Y$ corresponding to transcript 00

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



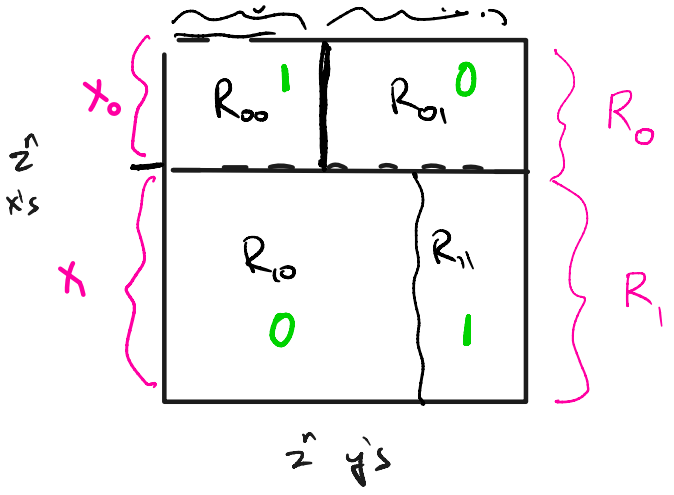
Say Alice sends 1st bit



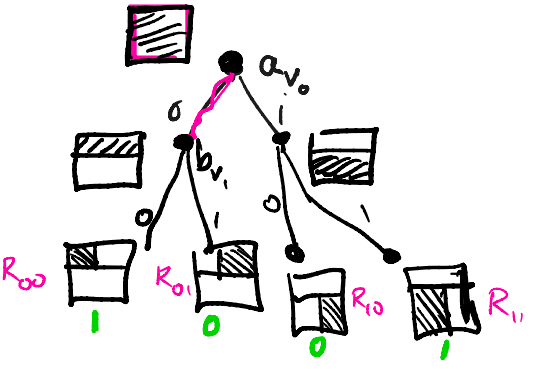
At each leaf ℓ of protocol tree, output is last bit sent. which should equal $f(x,y)$ $\forall (x,y) \in R_\ell$

$\therefore$ The subrectangles at leaves are all monochromatic

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



Say Alice sends 1st bit



$\therefore$ A deterministic protocol Π partitions M_f into disjoint monochromatic subrectangles

R_{00} = inputs in $X \times Y$ corresponding to transcript 00

R_{01}

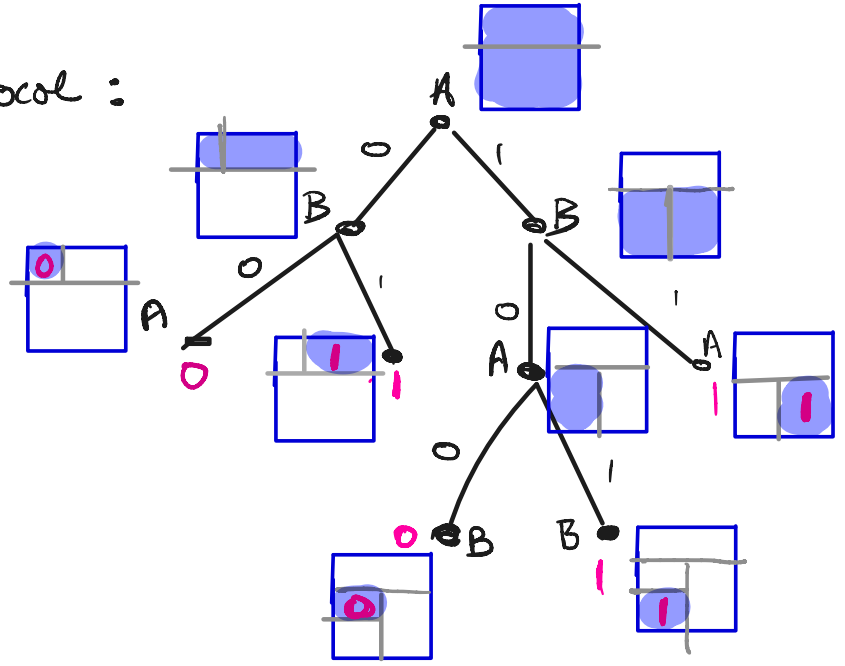
R_{10}

R_{11}

Another visualization:

f , M_f = cc matrix for f

deterministic protocol :

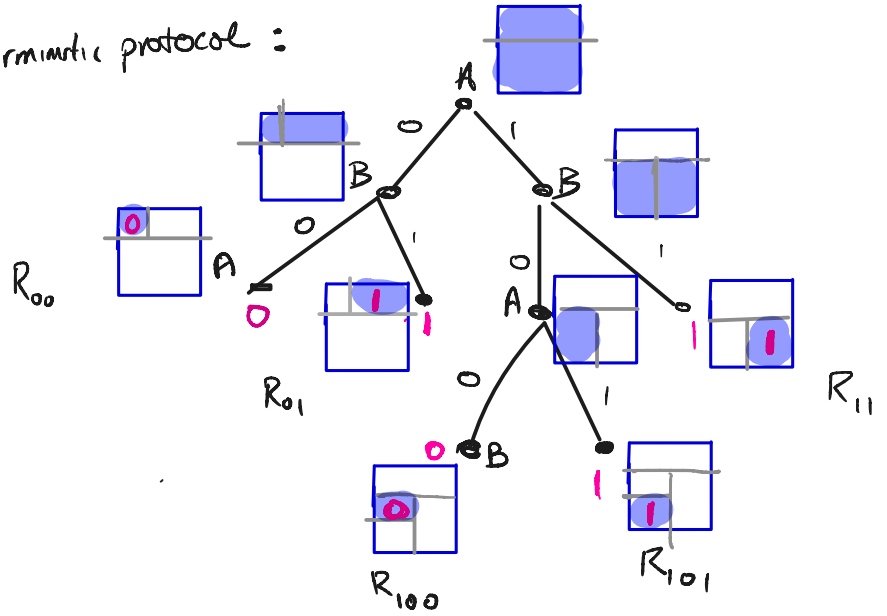


A = Alice speaks
B = Bob "

Last Class cont'd

f , M_f = cc matrix for f

deterministic protocol :



$\therefore$ M_f = R_{00} + R_{01} + R_{100} + R_{101} + R_{11}

Rank of M Lower bounds CC

By the previous argument, a deterministic CC protocol of cost d for $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ gives a partition of M_f into 2^d disjoint monochromatic subrectangles:

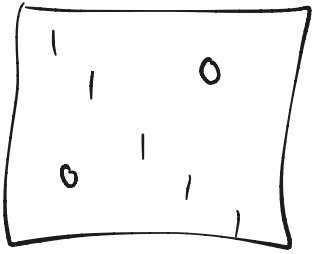
That is $M = \sum_{\alpha \in \{0,1\}^d} R_\alpha$ α : transcript of protocol

Each R_α has rank ≤ 1 (since all-0 outside M and inside R_α either all 1 or all 0)

$\therefore$ $\text{Rank}(M) \leq \sum_\alpha \text{Rank}(R_\alpha) \leq 2^d$

Observation $CC(EQ_n) = \Omega(n)$

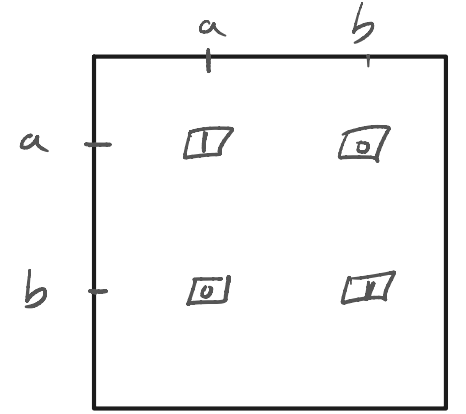
M_{EQ_n} :



Pf 1 M_{EQ_n} is identity matrix which has full rank $= 2^n$

$\therefore CC(EQ_n) = \Omega(n)$

Observation $CC(EQ_n) \geq \log(n)$

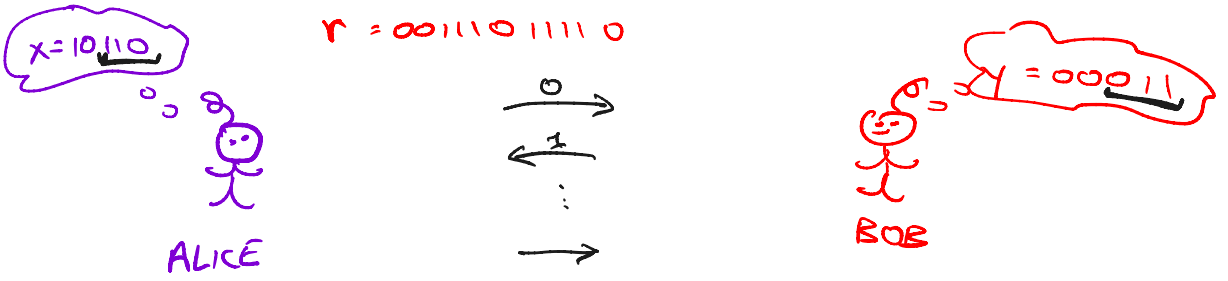


Pf 2 "Fooling set" argument.

Claim: For any 2 distinct diagonal entries (a,a), (b,b) any protocol for EQ_n has (a,a) and (b,b) in different leaves.

Pf If not then since each leaf associated with a rectangle if (a,a), (b,b) both in some leaf rectangle R_x then (a,b), (b,a) also in R_x. But then R_x can't be monochromatic

Randomized COMMUNICATION COMPLEXITY (public coin)



Alice / Bob have shared access to a random string $r \in \{0,1\}^R$

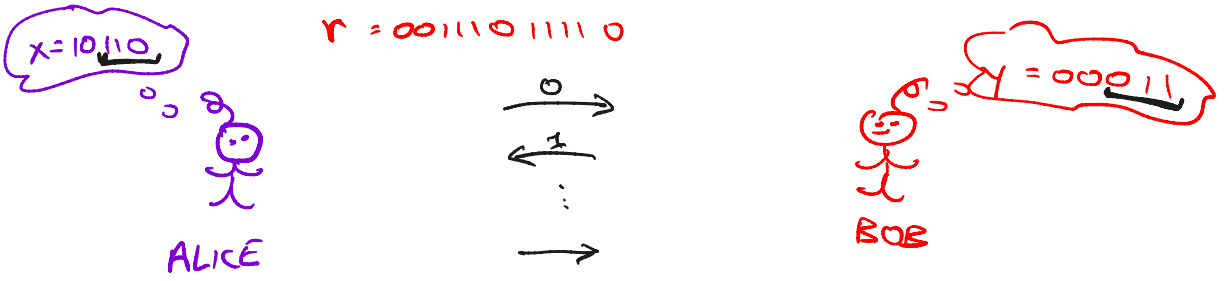
For each $r \in \{0,1\}^R$, have a deterministic protocol Π_r (depends on r)

So randomized protocol Π is a distribution over deterministic protocols $\{\Pi_r\}_{r \in \{0,1\}^R}$

Π computes $f: X \times Y \to \{0,1\}$ with prob $\geq 1-\varepsilon$ if:

$\forall (x,y) \in f^{-1}(1) \quad \Pr_r [\Pi_r(x,y) = f(x,y)] \geq 1-\varepsilon$

Randomized COMMUNICATION COMPLEXITY (public coin)



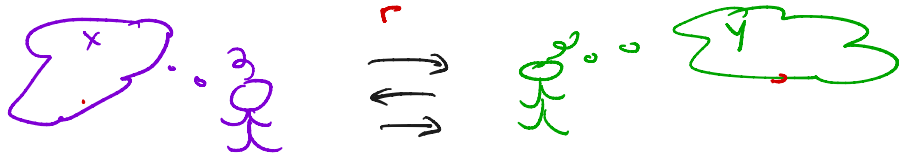
Π computes $f: X \times Y \to \{0,1\}$ with prob $\geq 1-\varepsilon$ if:

$\forall (x,y) \in f^{-1}(1) \quad \Pr_r [\Pi_r(x,y) = f(x,y)] \geq 1-\varepsilon$

cc of (randomized) $\Pi := \max_r (cc(\Pi_r))$ ← we'll see that wlog $|r| \leq \text{poly} \log n$

Randomized CC

(Public Coin Model)



BPP^{cc}

Π computes f_n with error ε if: $\forall (x,y)$ $|x|=|y|=n$

$$\Pr_{r_A, r_B}\left[\Pi(x, y, r) = f_n(x,y)\right] \geq 1-\varepsilon$$

Default $\varepsilon = \frac{1}{3}$

$f \in BPP^{cc}_{\varepsilon}(f)$ if randomized CC of $f = O(\text{polylog } n)$

RP^{cc}

Π computes f with 1-sided error ε if $\forall (x,y)$ $|x|=|y|=n$

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

$$f(x,y)=0 \Rightarrow \Pr_r\left[\Pi(x, y, r)\right] = f(x,y) \geq 1-\varepsilon$$

$f \in RP^{cc}(f)$ if randomized cc of $f = O(\text{polylog } n)$

ZPP^{cc}

error $\varepsilon = 0$.

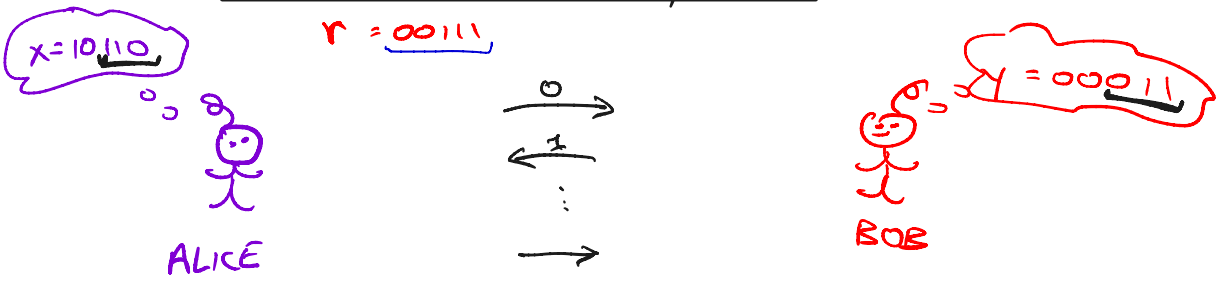
$f \in ZPP^{cc}$: $\min_{\Pi \text{ for } f} \max_{(x,y)} \mathbb{E}_r$ [# bits sent on (x,y)]

Sometimes we'll also use

$P^{cc}(f)$, $BPP^{cc}(f)$, $RP^{cc}(f)$, etc

to denote the comm complexity of f in that model.

Example: EQUALITY



We saw last lecture: deterministic cc of $EQ_n = \Omega(n)$

RP^{cc} EQ protocol ($\varepsilon = \frac{1}{2}$)

View 1st n bits of r as selecting a subset of $1 \ldots n$.
Alice sends parity of $x|_{\cdot}$
Bob sends parity of $y|_r$
Accept (output 1) if parities are the same
ow output 0

Repeat $O(\log n)$ times to get $O(\log n)$-cost protocol with $\varepsilon \sim \frac{1}{n}$

Amplification of error in Randomized Protocols

RP^{cc} protocols:

Say Π is an RP^{cc} protocol for f with error ε

To decrease $\varepsilon \longrightarrow \varepsilon^k$:

Repeat Π k times using $r_1, \ldots r_k$

Output 1 if $\forall$ k runs, Π output 1

Else output 0

If $f(x,y) = 1$ $\quad Pr\left(\Pi_{r_1} = 1 \wedge \Pi_{r_2} = 1 \wedge \ldots \wedge \Pi_{r_k} = 1\right) = 1$

If $f(x,y) = 0$ $\quad Pr\left(\Pi(x,y) = 1\right) \wedge Pr\left(\Pi_{r_1}(x,y) = 1\right) \wedge \ldots \wedge Pr_{r_k}(x,y) = 1\big)$

$$= \varepsilon^k$$

$$\therefore Pr\left(\Pi(x,y) = f(x,y)\right) = 1 - \varepsilon^k$$

Amplification of error in Randomized Protocols

BPP^{ϵ} protocols:

Say Π is an RP^{cc} protocol for f with error ε

To decrease $\varepsilon \rightarrow \varepsilon^k$:

Repeat Π k times using $r_1, \ldots r_k$

Output majority answer

Nondeterministic CC

Protocol Π: Shared string w ("nondet. "witness")

Alice: x $\rightleftharpoons$ Bob: y

Π computes $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ if

$\forall x, y \in \{0,1\}^n$:

$f(x,y) = 1 \Rightarrow \exists w$ s.t. $\Pi(x, y, w) = 1$

$f(x,y) = 0 \Rightarrow \forall w \quad \Pi(x, y, w) = 0$

Comm complexity of Π on x, y of length n:

$\max_{x,y}$(# bits sent) + $\max_{w}$ ($|w|$)

why do we add length of w to cost?

Nondeterministic CC – Set Disjointness

$DISJ(x, y) := 1$ iff $\exists i \in \{1, \ldots, n\}$ s.t. $x_i = y_i = 1$

DISJ has NP^{cc} protocol of cost $O(\log n)$

What is P^{cc}, BPP^{cc} cc of DISJ ?