Lecture 07

Note Title

Today: Communication Complexity

- Definitions
- Connection to Circuit Depth
- Basic Properties
- Parity Lower Bound.

Setting: Alice & Bob seperated by some distance; & have two portions of the input to a problem they wish to solve.

Alice $\longleftarrow x$

Bob $\longleftarrow y$

wish to compute z s.t. $(x, y, z) \in \underline{\underline{R}}$

PROTOCOL Π computes R if

ALICE		BOB
x		y
	$\xrightarrow{b_1}$	
	$\xleftarrow{b_2}$	
	$\xrightarrow{b_3}$	
	$\xrightarrow{b_4}$	
	$\vdots$	
	$\xleftarrow{b_k}$	

- Π specifies who will speak next as function of $b_1 \dots b_k$.
- Π specifies what will be said
  $f(x, b_1 \dots b_k)$ if ALICE ...
- Π specifies when to stop (fn. of $b_1 \dots b_k$).
- Π specifies $z = f(x, b_1 \dots b_k)$
  $= g(y, b_1 \dots b_k)$.
  & $(x, y, z) \in R$

COMPLEXITY:

- $CC(R) = \min_{\Pi} \max_{x,y} \{\#\text{ bits exchanged}\}$.

for function $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

- $CC(f) = CC\Big(\big(x, y, f(x,y)\big)\Big)$

for "partial" function $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1,?\}$

- $CC(f) = CC(R)$ where $(x,y,1) \in R$ if $f(x,y) \in \{1,?\}$ & $(x,y,0) \in R$ if $f(x,y) \in \{1,?\}$

CC vs. Circuit Complexity

for function $f : \{0,1\}^n \to \{0,1\}$

let $R_f = \{ (x, y, i) \mid f(x) = f(y)$ or $(f(x) \neq f(y)$ & $x_i \neq y_i) \}$

Theorem [KARCHMER - WIGDERSON]

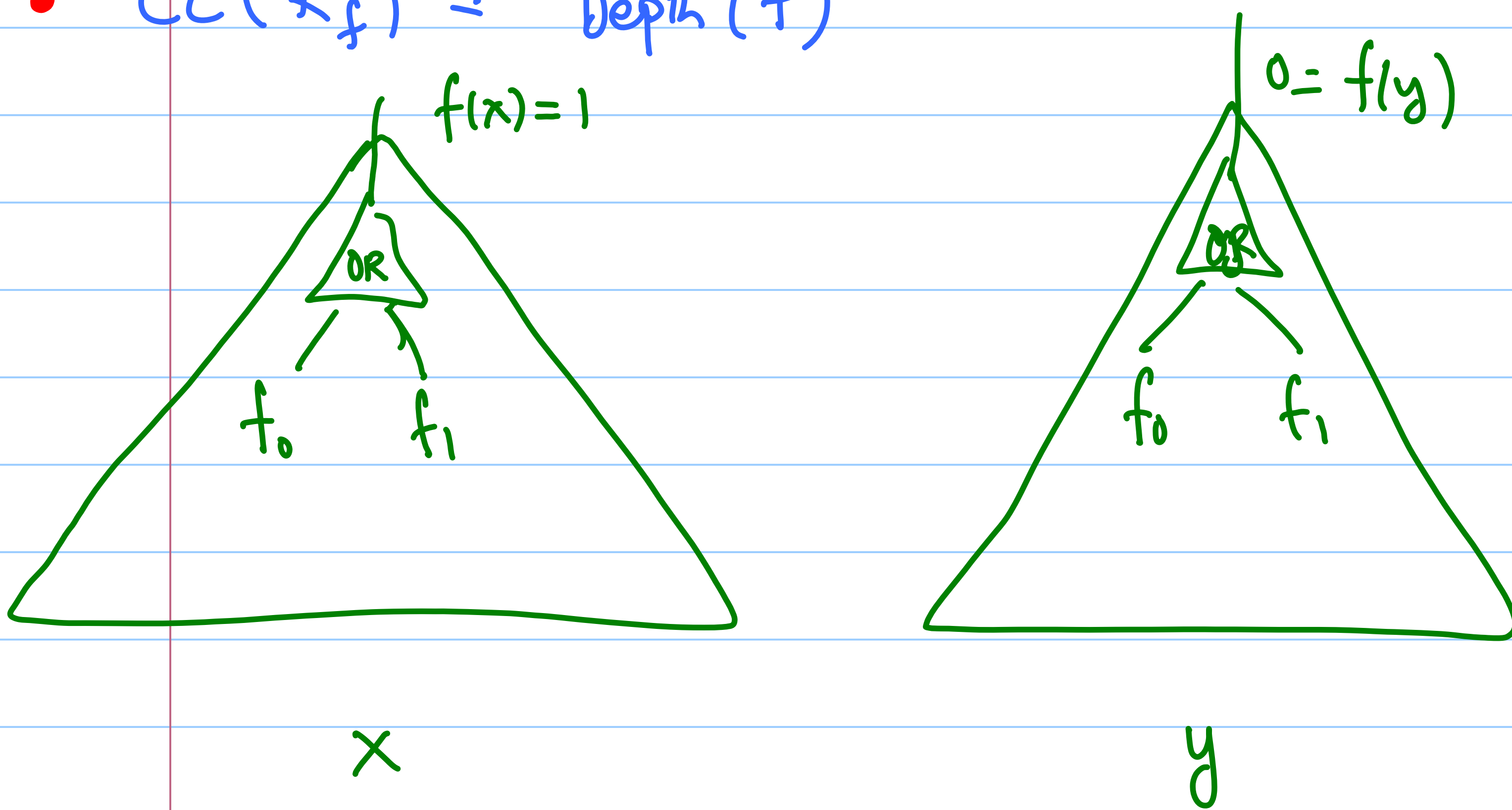
for every f

$$CC(R_f) = \text{Circuit-Depth}(f) + \Theta(1)$$

over {NOT, 2-AND, 2-OR}.

Proof

- $CC(R_f) \leq \text{Depth}(f)$



Know: $f(x)=1$; $f(y)=0$

$\Downarrow$ $\Downarrow$

$f_0(y) = 1$ $f_0(y) = 0$

OR $f_1(y) = 1$ & $f_1(y) = 0$

↑

ALICE knows which one → sends bit to BOB

} Now have f_0 of depth one less

$\text{Depth}(f) \leq CC(R_f)$

Proof by Induction on partial functions f:

Assume Alice has x s.t. $f(x) = 1$

Bob y s.t. $f(y) = 0$

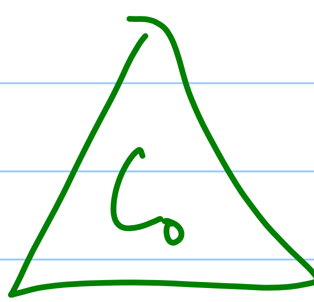
say Alice goes first & sends

$$b_1 = b_1(x)$$

let $f_1 = f(x)\big|_{x \mid b_1(x) = 1 \text{ or } f(x) = 0}$

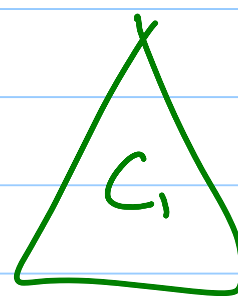
$f_0 = f\big|_{x \mid b_1(x) = 0 \text{ or } f(x) = 0}$

By induction



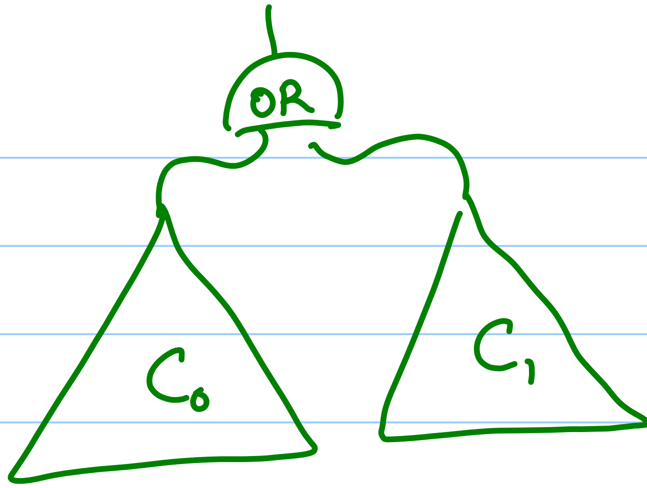
computes f_0

&



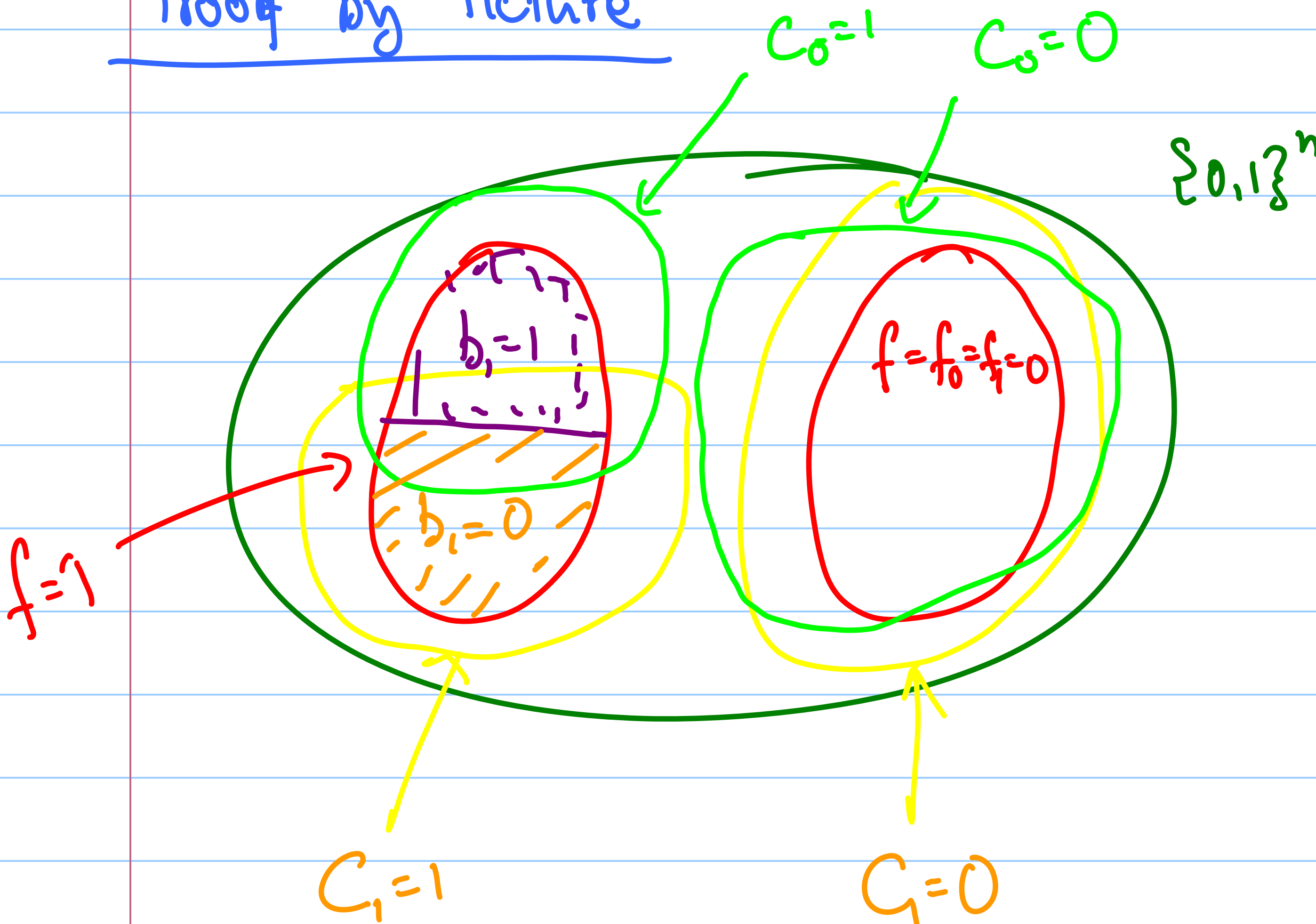
computes f_1

Claim:



computes f.

Proof by Picture



LOWER BOUNDS BASED ON $CC(R_f)$.

- Mostly for monotone functions with monotone circuits

- Simple proof that $\underbrace{\text{depth(parity)} \geq \log(n^2)}_{\Uparrow}$

  formula size $(\oplus) \geq n^2$

- <u>Proof:</u> Pick random x s.t. $\oplus(x) = 0$
  Pick random $i \in [n]$

  $x \to$ ALICE

  $y = x \oplus i \to$ BOB

By PHP: Bob must receive $\geq \log n$ bits from ALICE

Alice must also ...

total $\geq 2 \log n = \log(n^2)$

General Results in CC

- Not well-developed for relations,
  partial functions.

- Functions are quite well-understood
  [Yao, Kushilevitz-Nisan]

Lower Bounds by Tiling

- Fix protocol Π & bits exchanged
  $\bar{b} = 0110\ldots0$

- What does the set

$$S_{\bar{b}} = \{(x,y) \mid \Pi(x,y) = \bar{b}\}$$

look like?

- Claim: $\exists\ S_A \subseteq \{0,1\}^n$ & $S_B \subseteq \{0,1\}^n$

  s.t. $S_{\bar{b}} = S_A \times S_B$

- **Proof**: S_A = projection of $S_{\bar{b}}$ to 1^{st} coord.

  S_B = " 2^{nd} ".

  $\forall\ (x,y) \in S_A \times S_B$

  $\Pi(x,y) = \bar{b}$:

  Why? Suppose $(x, y') \in S_{\bar{b}}$

  $(x', y) \in S_{\bar{b}}$

  then for all Alice knows, Bob might have y' ... & so should be consistent with $\bar{b}$ ... ...

Conclusion: Let

$N_0 =$ min # "rectangles" needed to tile $f^{-1}(0)$

$N_1 =$ " $f^{-1}(1)$

thus $CC(f) \geq \log N_0 , \log N_1$.

Example: $EQ?(x, y) = 1$ if $x = y$
$= 0$ o.w.

f-Matrix

$$\begin{array}{c|c} & \longleftarrow y \longrightarrow \\ \hline \begin{array}{c} \uparrow \\ x \\ \downarrow \end{array} & \begin{bmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ 0 & & & & 1 \end{bmatrix} \end{array}$$

$N_1 = 2^n$

$\Rightarrow CC(f) \geq n$

Rank Lower Bound

Thm: Let
$$M_f = \begin{array}{cc} & y \rightarrow \\ x \downarrow & \begin{bmatrix} \\ \quad f(x,y) \quad \\ \\ \end{bmatrix} \end{array}$$

Then $CC(f) \geq \log \operatorname{rank}(M_f)$

Proof: Follows from $\operatorname{rank}(M_f) \leq N_1$

N_1 : Express $M_f = \sum$ rank one matrices.

$$\operatorname{rank}(A+B) \leq \operatorname{rank}(A) + \operatorname{rank}(B).$$

(Which field? Any one ......

or Rationals ....)

EXAMPLE

Inner Product function:

$$\langle x, y \rangle = \sum x_i y_i \pmod 2$$

$$\text{Rank}(M_f) = ?$$

Lets use **fundamental trick of Complexity**

$$M_f \longrightarrow N_f$$
$$0 \longrightarrow 1$$
$$1 \longrightarrow -1$$
$$M_f \longrightarrow J - 2M_f$$

all 1's matrix ; rank (1)

Claim: $\text{Rank}(N_f) = 2^n$

Proof:
$$N_f \cdot N_f^T = \underbrace{2^n \cdot I}_{\text{rank} = 2^n}$$

$$\text{rank}(AB) \leq \text{rank}(A)\ \text{rank}(B)$$

$$\Rightarrow \text{rank}(N_f) \geq 2^n \qquad \boxtimes$$

Claim: $\text{Rank}(M_f) \geq 2^n - 1$

Proof: $N_f = J - 2M_f$

$$\Rightarrow \text{rank}(N_f) \leq \text{rank}(J) + \text{rank}(M_f)$$

$$\Rightarrow \text{rank}(M_f) \geq 2^n - 1 \qquad \boxtimes$$

Note: Proof doesn't work over GF(2)?

Other Interesting Topics in Communication Complexity

- Multiparty Communication:

  [Chandra, Furst, Lipton; Babai, Nisan, Szegedy]

  k-players ; k inputs $x_1 \dots x_k \in \{0,1\}^n$

  Catch: P_i has all inputs except x_i.

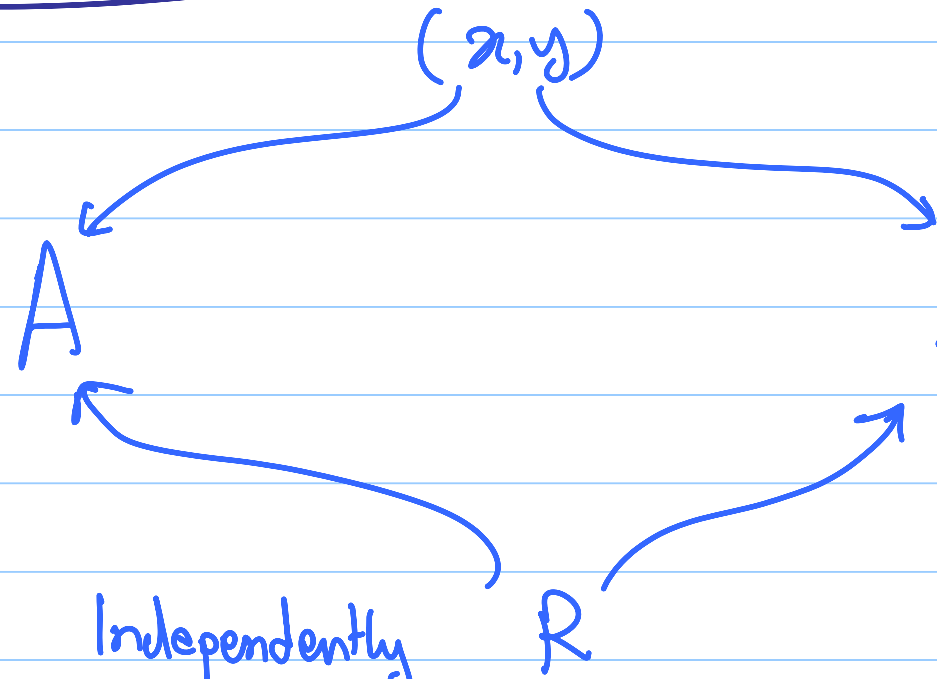
  Compute : $f(x_1 \dots x_k)$

  Example Result (without proof) :

  $$GIP(x_1 \dots x_k) = \sum_{j=1}^{n} \prod_{i=1}^{k} (x_i)_j \pmod 2$$

  $$CC(GIP) \geq \frac{n}{f(k)} \dots$$

- # PROBABILISTIC COMMUNICATION COMPLEXITY



(shared common ind. random string)

$$P_{x,y} = \operatorname*{Prob}_{R}\left[\ \Pi_R(x,y) \text{ outputs } 1\ \right]$$

Want : $\forall\ x, y$

$$\left| f(x,y) - P_{x,y} \right| \leq \frac{1}{2} - \epsilon$$

$\uparrow$

$CC_\epsilon(f)$ ....

__Example:__

Set disjointness $DISJ(x,y) = 1$

$\iff$ if $\forall i \quad x_i \wedge y_i = 0$.

$\forall \epsilon > 0 \quad CC_\epsilon(DISJ) \geq \Omega(n)$.

__Example__

$CC_\epsilon(EQ?) = O(1)$.

__Proof:__ Pick error correcting code

$$E : \{0,1\}^n \to \{0,1\}^{n^2}$$

with $\Pr_j\left[E(x)_i = E(y)_i\right] \leq .9$

Π_R : A sends $E(x)_R$ to B.

Open Questions

- Obvious ones due to $CC(R_f)$.
- Log-rank Conjecture

$$\forall f \qquad CC(f) \leq \text{poly}(\log(\text{rank}(M_f)))$$

- Direct Sum Questions:

How does $CC(f_1 + f_2)$ depend on f_1, f_2?

$$\left[f_1 + f_2 \rightarrow \text{compute } f_1(x_1, y_1) \text{ \& } f_2(x_2, y_2) \right]$$

$\vdots$