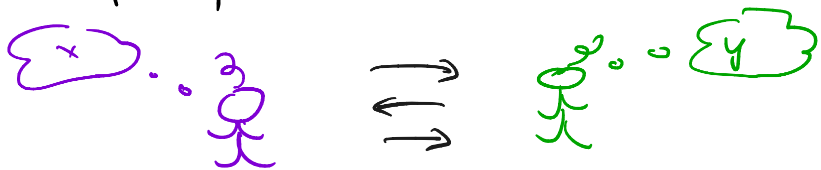
Last Class

(Class Webpage: www.cs.toronto.edu/~toni
go to teaching, 1st link)

1. 2-party basic model (deterministic)



$$P^{cc}(f) = \min_{\Pi \text{ for } f} \max_{\substack{(x,y)\\ |x|=|y|=n}} \#\text{ bits sent on input } (x,y)$$

P^{cc} = class of all functions $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ st $P^{cc}(f) = (\log n)^{O(1)}$

2. Randomized CC: Public vs Private coin model

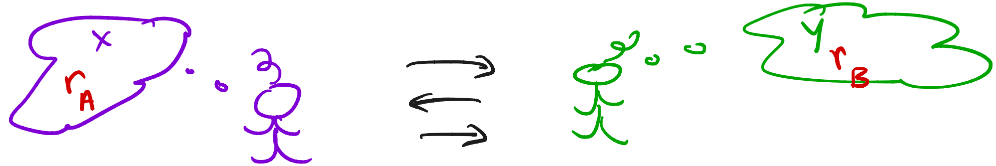
BPP^{cc} : two-sided error

RP^{cc} : one-sided error

ZPP^{cc} : zero sided error.

Randomized CC

(Private Coin Model)



$\boxed{BPP^{cc}}$

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

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

$$BPP^{cc}_{\varepsilon}(f) = \min_{\Pi \text{ for } f} \; \max_{(x,y)} \left[\#\text{ bits sent on } (x,y)\right]$$

$\boxed{RP^{cc}}$

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

$$f(x,y) = 0 \implies \Pr_{r_A, r_B}\left[\Pi(x, r_A; y, r_B) = f(x,y)\right] = 1$$

$$f(x,y) = 1 \implies \Pr_{r_A R_B}\left[\Pi(x, r_A; y, r_B) = f(x,y) \geq 1 - \varepsilon\right.$$

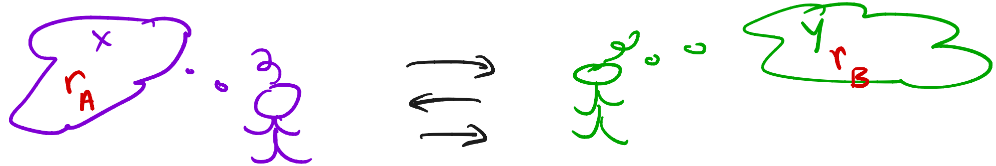
$\boxed{ZPP^{cc}}$

error $\varepsilon = 0$.

$$ZPP^{cc}(f) = \min_{\Pi \text{ for } f} \; \max_{(x,y)} \; \mathop{\mathbb{E}}_{r_A r_B}\left[\#\text{ bits sent on } (x,y)\right]$$

Randomized CC

(Private Coin Model)



$\boxed{BPP^{cc}}$

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

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

Default $\varepsilon = 1/3$

$$BPP^{cc}_{\varepsilon}(f) = \min_{\Pi \text{ for } f} \; \max_{(x,y)} \left[\#\text{ bits sent on } (x,y)\right]$$

$\boxed{RP^{cc}}$

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

$$f(x,y)=1 \implies \Pr_{r_A, r_B}\left[\Pi(x, r_A; y, r_B) = f(x,y)\right] = 1$$

$$f(x,y)=0 \implies \Pr_{r_A R_B}\left[\Pi(x, r_A; y, r_B) = f(x,y)\right] \geq 1-\varepsilon$$

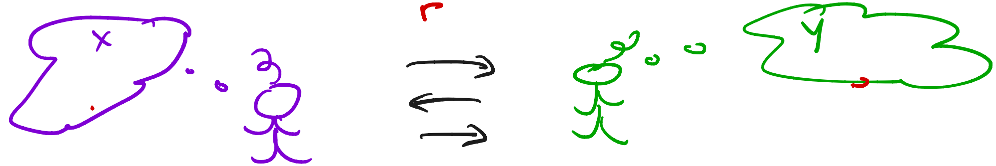
$\boxed{ZPP^{cc}}$

error $\varepsilon = 0$.

$$ZPP^{cc}_{\varepsilon}(f) = \min_{\Pi \text{ for } f} \; \max_{(x,y)} \; \mathbb{E}_{r_A r_B}\left[\#\text{ bits sent on } (x,y)\right]$$

Randomized CC

(Public coin model)



BPP^{cc}

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

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

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

$$BPP^{cc}_{\varepsilon}(f) = \min_{\Pi \text{ for } f} \max_{(x,y)} \left[\#\text{ bits sent on } (x,y)\right]$$

RP^{cc}

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

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

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

ZPP^{cc}

error $\varepsilon = 0$.

$$ZPP^{cc}_{\varepsilon}(f) = \min_{\Pi \text{ for } f} \max_{(x,y)} \mathbb{E}_{r}\left[\#\text{ bits sent on } (x,y)\right]$$

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

$$M_{EQ} = \begin{array}{c c} 2^n & \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \\ & 2^n \end{array} = 2^n \times 2^n \text{ Identity matrix}$$

For any deterministic protocol Π for EQ,

- No 2 1 inputs can end up at the same leaf of protocol tree.

Therefore # leaves $\geq 2^n$

$\therefore$ cost $\geq \Omega(n)$

So EQ is maximally hard for det. protocols

But easy for randomized RP^{cc} protocols (public coin)

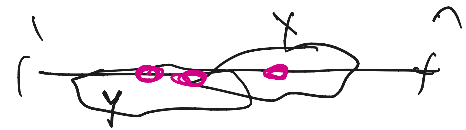
$|r| = n$

Alice

x

Bob

y



view r as a subset of $[n]$.

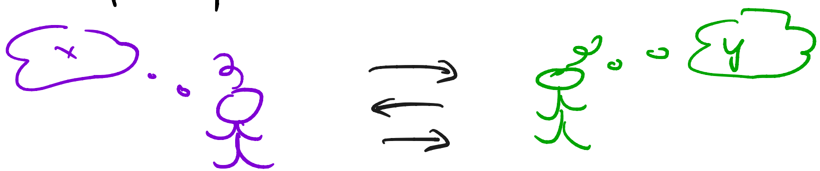
Alice computes $\sum_{i=1}^{n} r_i x_i \mod 2 = b_A$ send to bob.

Bob " $\sum_{i=1}^{n} r_i y_i \mod 2 = b_B$

Bob announces answer $b_A \oplus_2 b_B$

Last Class

1. 2-party basic model (deterministic)



$$P^{cc}(f) = \min_{\Pi \text{ for } f} \; \max_{\substack{(x,y) \\ |x|=|y|=n}} \# \text{ bits sent on input } (x,y)$$

2. Randomized CC : Public vs Private coin model

   BPP^{cc} : two-sided error

   RP^{cc} : one-sided error

   ZPP^{cc} : zero sided error.

3. Nondet cc / coNondet cc

Nondeterministic CC

shared random string r

Π computes f on all (x,y), $|x|=|y|=n$, nondeterministically if

$$f(x,y)=1 \implies \exists r \;\; \Pi(x,y,r)=1$$
$$f(x,y)=0 \implies \forall r \;\; \Pi(x,y,r)=0$$

comm complexity of Π: $\max_{(x,y),r} \left[\# \text{bits sent on } (x,y) + |r| \right]$

$$NP^{cc}(f) = \min_{\substack{\Pi \text{ nondet} \\ \text{protocol for } f}} \max_{(x,y),r} \left[\# \text{bits sent on } (x,y) + |r| \right]$$

Important fxn easy for NP^{cc}, hard for P^{cc}, for BPP^{cc}

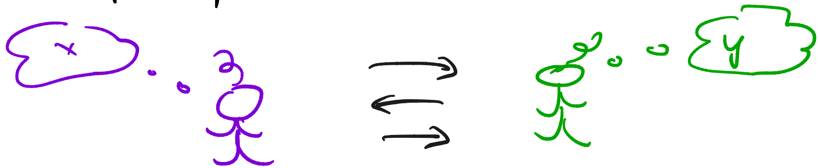
is $\quad DISJ(x,y) = 1$ iff $\exists i \;\; x_i = y_i = 1$

View r as cand $i \in [n]$ $\quad |r| = \log n$

Last Class

1. 2-party basic model (deterministic)

EQ hard



$$P^{cc}(f) = \min_{\Pi \text{ for } f} \max_{\substack{(x,y) \\ |x|=|y|=n}} \#\text{ bits sent on input } (x,y)$$

2. Randomized CC : Public vs Private coin model

EQ easy
DISJ hard

BPP^{cc} : two-sided error

RP^{cc} : one-sided error

ZPP^{cc} : zero sided error.

3. Nondet CC / coNondet CC

DISJ easy nondet

- $IP(x,y) \stackrel{\text{def}}{=} \sum x_i y_i \mod 2$

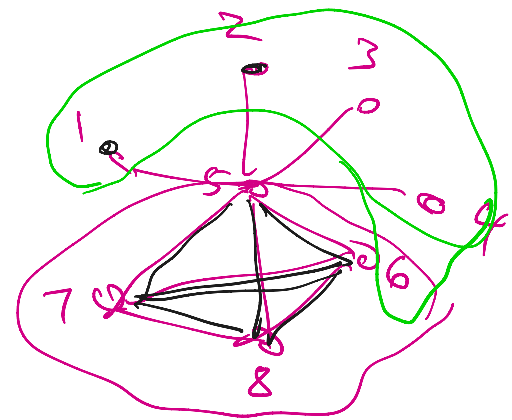
IP hard
Clique/coclique easy

Clique/coclique function

Fixed graph G on n vertices

Alice : given $x \subseteq [n]$ s.t. G has a clique on x

Bob : given $y \subseteq [n]$ s.t. G has indep set on y



ex $x = 00001111$

$y = 11110100$

Output 1 iff $x \cap y$

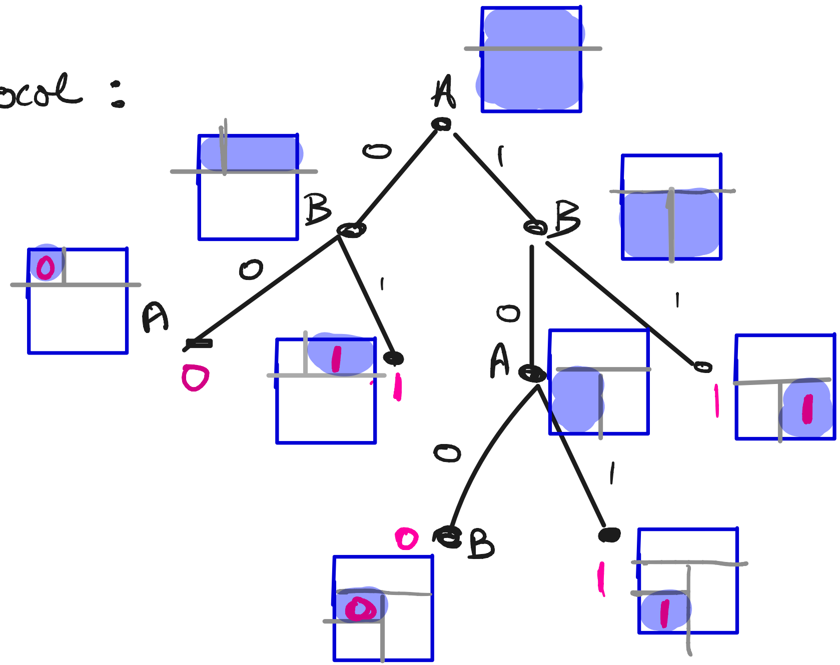
G_x is a clique

$n = 8$

Last class cont'd

f , M_f = cc matrix for f

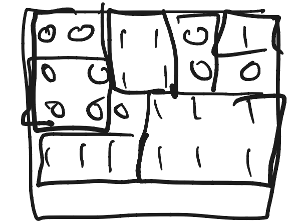
P^{cc} protocol :



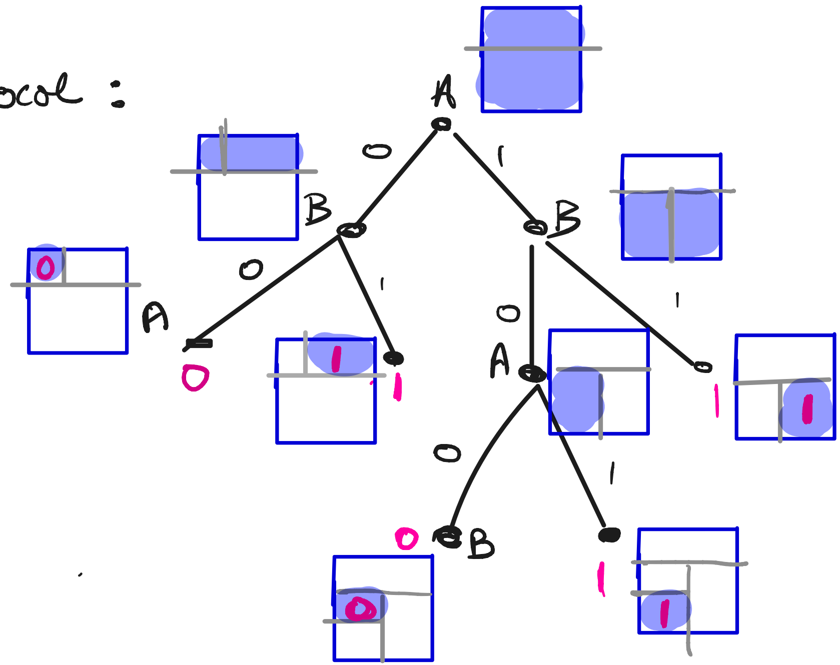
Last Class cont'd

f , M_f = cc matrix for f

M_f



P^{cc} protocol :



TODAY

✓ 1. Protocols can be balanced

✓ 2. Error ε can be amplified with little cost

✓ 3. Can assume $|r|$ is $O(\log n)$ for randomized protocols] Newman's Thm

$\therefore$ Public coin & private coin randomized comm. nearly the same

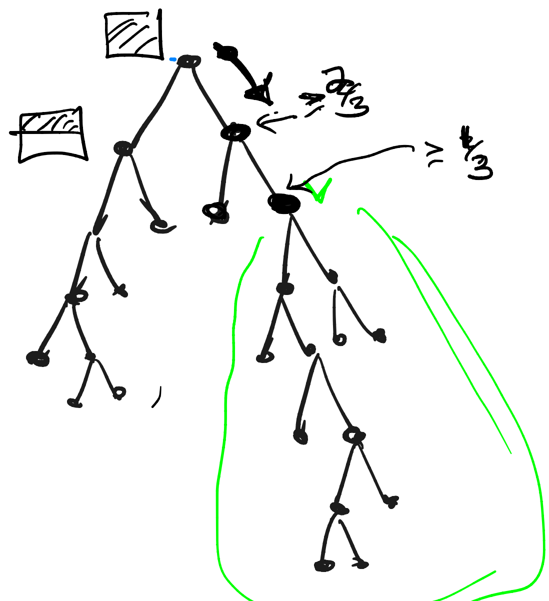
4. $P^{cc}(f) \leq NP^{cc}(f) \cdot coNP^{cc}(f)$ [Yannakakis] postpone

5. Log Rank conjecture (time permitting)]

BALANCING PROTOCOLS

Theorem If f has a deterministic protocol Π with ℓ leaves, then f has a det protocol of height/cost $O(\log \ell)$

$\frac{1}{3}$-$\frac{2}{3}$ Lemma Any binary tree T with $\ell > 1$ leaves contains a vertex v st T_v has between $\frac{\ell}{3}$ and $\frac{2\ell}{3}$ leaves



BALANCING PROTOCOLS

Theorem If f has a deterministic protocol Π with ℓ leaves, then f has a det protocol of height/cost $O(\log \ell)$

$\frac{1}{3}$-$\frac{2}{3}$ Lemma Any binary tree T with $\ell > 1$ leaves contains a vertex v st T_v has between $\frac{\ell}{3}$ and $\frac{2\ell}{3}$ leaves

given Π, with ℓ leaves:

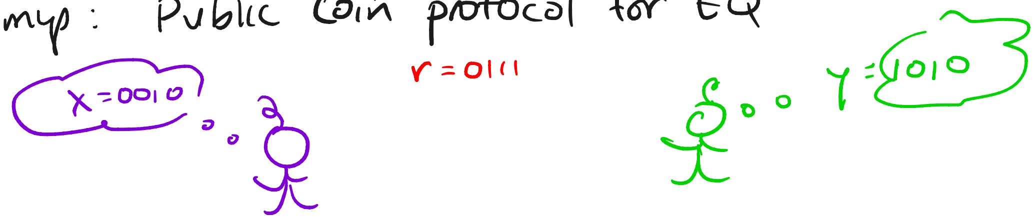
1. Players (no communication) find $\frac{1}{3}$-$\frac{2}{3}$ vertex v
2. Alice sends one bit – 1 iff $x \in R_v$
   Bob " " – 1 iff $y \in R_v$
3. If alice + Bob both send 1 then recurse on T_v
   ow delete T_v from T + recurse on $T - T_v$

at each round # leaves in current tree shrinks by at least $\frac{2}{3}$ factor

so # bits $\leq 2 \cdot \log_{3/2} \ell = O(\log \ell)$

Newman's theorem & Application to Public/Private Randomness

Warmup: Public coin protocol for EQ



Alice: computes $a = \sum_{i=1}^{n} x_i r_i \mod 2$ & sends a to Bob

Bob: computes $b = \sum y_i r_i \mod 2$

Output 1 iff $a = b \mod 2$

Claim ① If $x = y$ protocol always outputs correct answer

② If $x \neq y$ with prob $\frac{1}{2}$ $\Pi(x, y, r) = 1$ (is incorrect)

repeat c times: error on 0-inputs is $\frac{1}{2^c}$

error on 1-inputs is 0

Lemma (Newman)

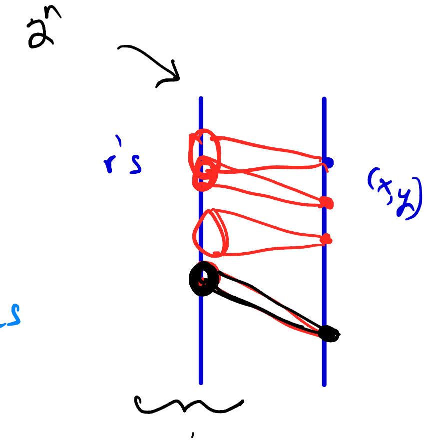
Let Π be a ~~public~~ coin protocol for f with error ε.
$\forall \delta > 0$ there is another protocol Π' such that:

1. cc of Π = cc of Π'
2. error of Π' is $\leq \varepsilon + \delta$
3. Π' uses $O(\log n + \log \frac{1}{\delta})$ random bits

given the above Lemma, we can convert a public coin protocol Π for f (error ε) to a private coin protocol for f (error $\varepsilon + \delta$), with cost $= cc(\Pi) + \underbrace{O(\log n + \log \frac{1}{\delta})}_{K}$.

To simulate public coin protocol by private coin one
Alice sends ~~to~~ 1st K bits of r_A to Bob. Then they both use this as public random string

Proof of Lemma $(|x| = |y| = n)$



Idea: $\forall (x,y)$ only an ε fraction of r's are bad

so there exists a small number of r's s.t. $\forall (x,y)$ Π makes $< \varepsilon + \delta$ mistakes on these r's

Let $Z(x,y,r) = \begin{cases} 1 & \text{if } \Pi(x,y,r) \neq f(x,y) \\ 0 & \text{ow} \end{cases}$

$\forall x,y \quad \mathbb{E}_r [Z(x,y,r)] \le \varepsilon$ since Π has error ε

Let $r_1 \dots r_t$ be random strings, $t = O(n/\delta^2)$

Define $\Pi_{r_1 \dots r_t}(x,y)$: Alice & Bob choose $i \in [t]$ at random and run $\Pi(x,y,r_i)$

Say $R = \{r_1 \dots r_t\}$ of good r_i's

Π': $|r| = \log t$

pick random $r_i \in R$

run $\Pi(x,y,r_i)$

<u>Claim</u> $\exists r_1 \dots r_t$ st $\mathbb{E}_i [Z(x,y,r_i)] \le \varepsilon + \delta \quad \forall x,y$]

For this choice of $r_1 \dots r_t$, $\Pi_{r_1 \dots r_t}(x,y)$ will be Π'

Proof of Lemma, cont'd

Chernoff Bound: $X_1, \ldots, X_N$ i.i.d rv's in $\{0,1\}$, $\varepsilon = \mathbb{E}[X_i]$, $\delta > 0$

Then $\Pr\left[\frac{1}{N} \sum X_i > \varepsilon + \delta\right] \leq 2 \cdot e^{-2\delta^2 N}$

Fix (x,y). Pick $\underbrace{r_1 \ldots r_t}$ at random

$$\Pr_{r_1 \ldots r_t}\left[\mathbb{E}_i [Z(x,y,r_i)] > \varepsilon + \delta \right] = \Pr_{r_1 \ldots r_t}\left[\underbrace{\frac{1}{t} \sum_{i=1}^{t} Z(x,y,r_i)} > \varepsilon + \delta\right]$$

- By Chernoff: $\Pr_{r_1 \ldots r_t}\left[\frac{1}{t} \sum_{i=1}^{t} Z(x,y,r_i) > \varepsilon + \delta\right] \leq 2e^{-2\delta^2 t} < 2^{-2n}$ (for $t = O(n/\delta^2)$)
- By union Bd, $\exists\, r_1 \ldots r_t$ s.t. $\forall (x,y)$ the error of $\Pi_{r_1 \ldots r_t}(x,y)$ is $\leq \varepsilon + \delta$

Proof of Lemma, cont'd

Idea: $\forall (x,y)$ an ε-fraction of r's are bad

Fix $r_1 \ldots r_t, x, y$

- $E_i\left[Z(x,y,r_i) \right] = \frac{1}{t}\sum_{i=1}^{t} Z(x,y,r_i)$

  So $Pr\left[E_i(z,y,r_i) \right] > \varepsilon + \delta$ equals the prob. that

  $$\frac{1}{t}\sum_{i=1}^{t} Z(x,y,r_i) > \varepsilon + \delta$$

- By chernoff: $\Pr_{r_1 \ldots r_t}\left[\frac{1}{t}\sum_{i=1}^{t} Z(x,y,r_i) - \varepsilon > \delta \right] \leq 2e^{-2\delta^2 t} < 2^{-2n}$ (for $t = O(n/\delta^2)$)

- By union Bd, $\exists r_1 \ldots r_t$ s.t. $\forall (x,y)$ the error of $\Pi_{r_1 \ldots r_t}(x,y)$ is $\leq \varepsilon + \delta$

\# bits used by Π': $\log t \approx \log\left(n/\delta^2\right) = O\left(\log n + \log \frac{1}{\delta}\right)$ ∎

Log Rank Lower Bounds Deterministic CC

Recall from last time we said $P^{cc}(EQ) = n$,

since $M_{EQ} = \begin{bmatrix} 1 & & & \\ & 1 & & 0 \\ & & 1 & \\ 0 & & & 1 \\ & & & & 1 \end{bmatrix}$

rank is 2^n

So no 2 1 inputs can end up at same leaf of protocol tree

$\therefore$ # leaves $\geq 2^n$ so $CC \geq \Omega(n)$

Log Rank Lower Bounds Det. CC

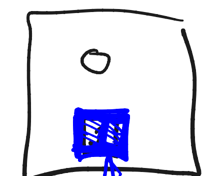
Lemma $\forall f$ $\quad P^{cc}(f) \geq \log_2 \text{rank}(M_f)$ $\qquad$ rank is over Reals

Pf Let L_1 be the leaves of Π that output 1. (L = all leaves)

For each $\ell \in L_1$, we have associated 1-mono subrectangle M_ℓ

$$M_f = \sum_{\ell \in L_1} M_\ell$$

M_f



say this 1-mono subrect assoc with leaf $\ell \in L_1$

since Rank is subadditive

$$\text{Rank}(M_f) \leq \sum_{\ell \in L_1} \text{Rank}(M_\ell) = |L_1| \leq |L|$$

$$\therefore \log \text{rank}(M_f) \leq P^{cc}(f)$$

LOG RANK CONJECTURE

States that the converse holds

$$\boxed{\text{LRC}: \quad \forall f \quad \underbrace{P^{cc}(f)}_{} = \log^{O(1)} \operatorname{rank}(M_f)}$$

Best known:

$$P^{cc}(f) \leq \underbrace{\sqrt{\operatorname{rank}(f)}}_{}\ \underbrace{\log \operatorname{rk}(f)}_{} \qquad \text{Lovett}$$

$$\exists f \quad P^{cc}(f) \gtrsim \log^{3/2} \operatorname{rk}(f)$$