Last Class

1. Deterministic Protocols & partition number vs det. cc partition balancing protocols

2. Randomized cc Protocols

- Error ε can be amplified with little cost

  We did amplification for 1-sided error protocols
  See Rao-Yehudayoff for 2-sided error amplification

EQ_n : has $O(1)$ cost public coin RP"" protocol

Today

(2) Randomized CC Protocols

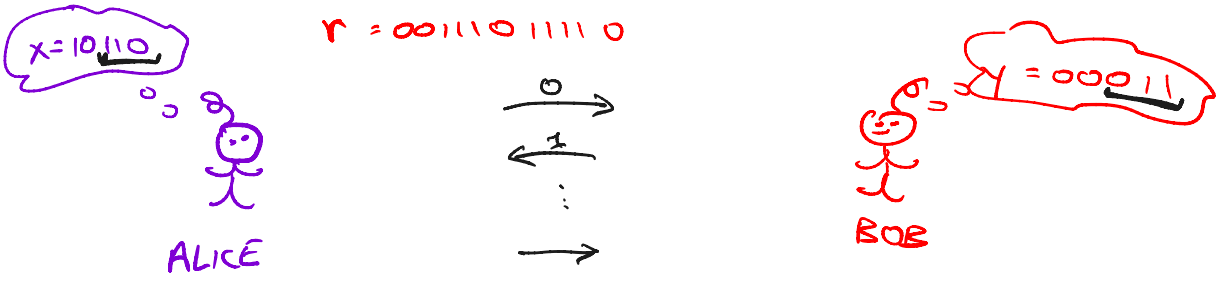
- Examples EQ_n, GT_n
- Public Coin CC $\approx$ Private Coin CC

  Main Lemma (Newman)

  Can assume wlog #random bits used in randomized protocol is $O(\log n)$
- Distributional View of randomized protocols

  Yao's Minimax for randomized CC

Randomized COMMUNICATION COMPLEXITY (public coin)



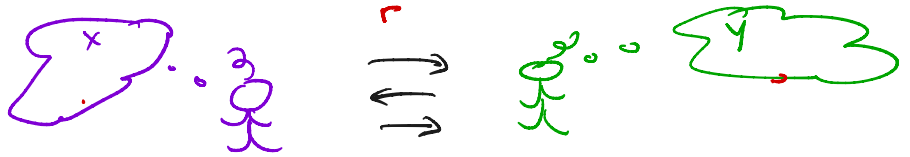
Π computes $f: X \times Y \to \{0,1\}$ with prob $\geq 1-\varepsilon$ if:

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

cc of (randomized) $\Pi := \max_r (cc(\Pi_r))$ ← we'll see soon that wlog $|r| \leq$ 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)]

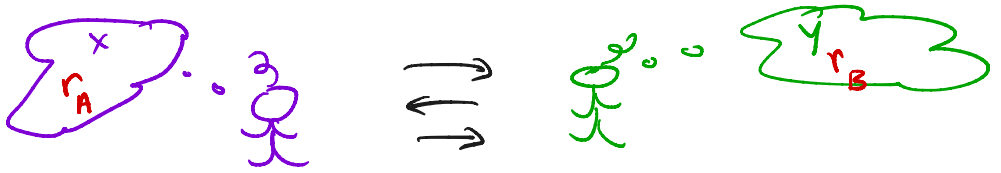
Sometimes we'll also use

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

to denote the comm complexity of f in that model.

Randomized CC

(Private coin Model)



BPP^{cc} Π computes f with error ε if: $\forall (x,y)$ $|x| = |y| = n$

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

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

RP^{cc} Π computes f with 1-sided error ε if $\forall (x,y)$

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

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

ZPP^{cc} error $\varepsilon = 0$.

Randomized CC : Private vs Public Coin

Private coin Protocol $\Rightarrow$ Public coin Protocol

Public coin $\overset{?}{\Rightarrow}$ Private ?

Example: EQUALITY

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

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

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) if parities are the same
ow output 0

Public coin
n bits of randomness

Repeat k times to get error $1/2^k$

$k = 2 \rightarrow \varepsilon = 1/4$, communication $O(1)$

$k = \log n \rightarrow \varepsilon = 1/n$, communication $O(\log n)$

Another public coin protocol (easier but even more random bits)

Alice / Bob sample a random function $h: \{0,1\}^n \to \{0,1\}^k$

1. Alice sends $h(x)$ to Bob.
2. Bob: If $h(x) = h(y)$ Bob outputs 1
   ow " 0

Analysis:

If $x = y$: $\forall h \quad h(x) = h(y)$

If $x \neq y$: $\Pr_h [h(x) = h(y)] \leq 2^{-k}$

for $k = 1$ this gives error $1/2$.] cost 1-bit

general k: error $\frac{1}{2^k}$, cost k

A Private Coin Randomized Protocol for EQ_n

Encode sets x, y as $X = Y = \{1, 2, \cdots, 2^n\}$

Protocol

1. Alice samples a random prime p in $[M, 2M]$

   Then she computes $a = x \pmod p$ and send a, p to Bob

2. Bob sends 1 iff $a = y \pmod p$

We will pick $M = n^2$

$\therefore$ complexity $O(\log n)$

since $|p|, |a| = O(\log n)$

A Private Coin Randomized Protocol for EQ_n

Encode sets X, Y as $X = Y = \{1, 2, \dots, 2^n\}$

Correctness:

If $x = y$: $\forall p,\ x \pmod p = y \pmod p$ so protocol outputs 1 w.p. 1

If $x \neq y$: Let $D = |x - y| \in \{1, 2, \dots, 2^n - 1\}$

If Bob says $x = y$: then $x \bmod p = y \bmod p \iff |x - y| = 0 \bmod p$

$\therefore$ protocol errs on (x, y, p) iff p is a prime factor of $|x - y|$

$$\therefore \varepsilon = \frac{\#\text{ primes in } [M, 2M] \text{ that divide } |x-y|}{\#\text{ primes in } (M, 2M]} \quad \frac{①}{②}$$

① : say $p_1, \dots, p_k \in [M, 2M]$ are prime factors of D

Then $P = p_1 \times \cdots \times p_k$ also divides D

But each $p_i \geq M$ so $M^k \leq P \leq D < 2^n$ $\therefore k \leq n / \log M$

② #. primes between M & $2M$ is $\Theta\left(\frac{M}{\log M}\right)$ (density of primes)

By ①, ② $\varepsilon \leq \frac{n}{\log M} \cdot \Theta\left(\frac{\log M}{M}\right)$ pick $M = n^2$ gives $\varepsilon \ll 1$

Ex $GT_n(x,y) = 1$ iff $x > y$ (as binary numbers)

Deterministic CC of $GT_n = \Omega(n)$ [rank lb or fooling set]

Idea of randomized protocol (we'll do public coin):

Find lexicographically 1^{st} index i

such that $x_i \neq y_i$ (using binary search + EQ protocol)

If $x_i = 1$ & $y_i = 0$ $\Rightarrow$ output 1

ow output 0

FIND-FIRST-NEQ-INDEX (x, y, i, j) $\quad [0 < i \le j \le n]$

If $i = j$: If $x_i \neq y_i \Rightarrow$ output i
Else $\Rightarrow$ output 0

Else : If $EQ(x[i,j], y[i,j]) = 1 \Rightarrow$ output 0

Else: If $EQ(x[i, j/2], y[i, j/2]) = 0$:

call FIND-FIRST-NEQ-INDEX $(x, y, i, j/2)$

Else call FIND-FIRST-NEQ-INDEX $(x, y, j/2 + 1, j)$

Let $x[i,j] = x_i, \ldots, x_j$

$\in CC \leq$

$2 + \log n \, (CC(EQ))$

$GT(x, y)$:

Call Find-First-NEQ-INDEX $(x, y, 1, n)$

If if returns $0 \Rightarrow$ output 0

Else suppose it returns i, $1 \le i \le n$:

If $x_i = 1$ and $y_i = 0 \Rightarrow$ output 1

Else $\Rightarrow$ output 0

CC Complexity

Need to call EQ with $\varepsilon \approx \frac{1}{3\log n}$ (so overall error $\leq \frac{1}{3}$)

$CC(EQ_\varepsilon) = O\left(\frac{1}{\log \varepsilon}\right)$, so cost per EQ call is $O(\log \log n)$

We call EQ $\log n$ times

$\therefore$ cost $= O(\log n \cdot \log \log n)$

Is protocol 2-sided or 1-sided error?

What about private coin protocol?

Next we'll show Public & Private coin Protocols are nearly equivalent.

1. Easy Direction: $\forall \varepsilon$ If f has a randomized private coin protocol Π of cost $CC(\Pi) = c$, error ε then f has a public coin protocol of cost c, error ε

$$BPP_{\varepsilon}^{pub}(f) \leq BPP_{\varepsilon}^{priv}(f)$$

Π': Let $r' = r_1 r_2$.
Alice runs Π on (x, r_1)
Bob runs Π on (y, r_2)

2. Harder Direction: $\forall \varepsilon, \delta$ If f has public coin protocol cost c, error ε then f has private coin protocol of cost $c + O(\log n) + O(\log 1/\delta)$

$$BPP_{\varepsilon+\delta}^{priv}(f) \leq BPP_{\varepsilon}^{pub} + O(\log n + 1/\delta)$$

Theorem (Newman)

Let Π be a public coin protocol for f with error ε.
$\forall \delta > 0$ there is another (public coin) 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 = $CC(\Pi) + O(\log n + \log \frac{1}{\delta})$:

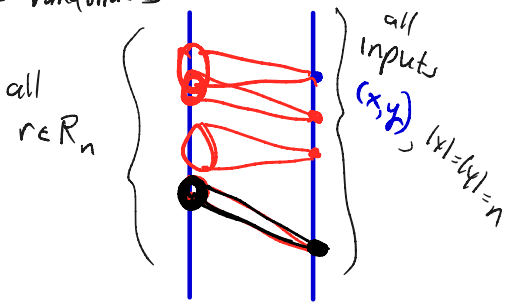
(i) Construct Π' from Π using Newman's thm

Π': public coin, $CC(\Pi') = CC(\Pi)$, error $\varepsilon + \delta$, # random bits $\overbrace{O(\log n) + \log(\frac{1}{\delta})}^{K}$

(ii) construct Π^{priv} from Π': Alice draws K random bits $r = r_1 \ldots r_K$ & sends them to Bob
Then they run Π' on r

Proof of Newman's Thm

$(|x| = |y| = n)$ Let Π_n use R_n bits of randomness



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

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

Let $r_1 \dots r_t$ be strings from $\{0,1\}^{R_n}$ $\quad t = O(\frac{n}{\delta^2})$

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

Claim $\exists r_1 \dots r_t$ s.t. $\mathop{\mathbb{E}}_{i}[Z(x,y,r_i)] \leq \varepsilon + \delta \quad \forall x,y$

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

$\left[\Pi' \text{ uses } \log t = O(\log n + \log \frac{1}{\delta}) \text{ bits of randomness}\right]$

Claim $\exists r_1 \ldots r_t$ s.t. $\mathbb{E}_i[Z(x,y,r_i)] \le \varepsilon + \delta \quad \forall x,y$

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

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

Fix (x,y). Pick $r_1 \ldots r_t \in \{0,1\}^{R_n}$ at random

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

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

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

IN general this is tight (as evidenced by EQ_n):

We saw EQ has $O(1)$ public coin protocol

By previous result this implies a private coin

RP protocol of cost $O(\log n)$ [error $\varepsilon = \frac{1}{3}$]

It is known that any private coin protocol for EQ has cc $\Omega(\log n)$

Nondeterministic Communication Complexity

$f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ Players share random string r

Nondeterministic NP^{cc} protocol Π for $f : \{0,1\}^n \to \{0,1\}$

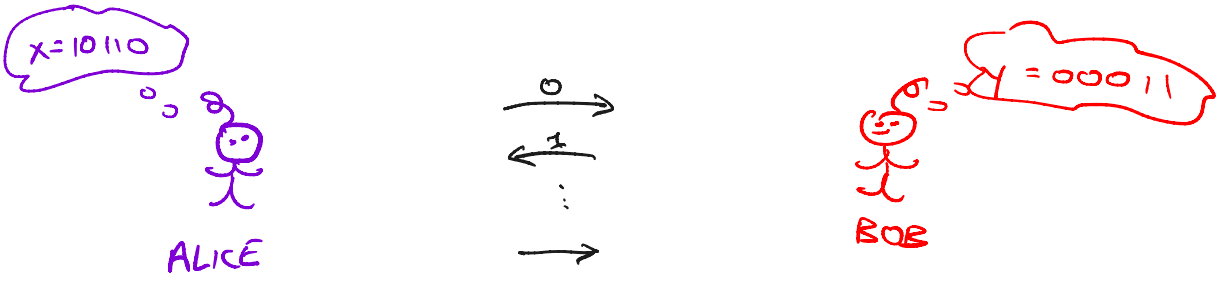
$\forall x \in f^{-1}(1) \quad \exists r \quad \Pi_r(x) = 1$

$\forall x \in f^{-1}(0) \quad \forall r \quad \Pi_r(x) = 0$

Comm. Complexity of Π $= \max_{\substack{x,y,r \\ |x|=|y|=n}} \left(\|\Pi_r\| + |r| \right)$ ← Note $|r|$ should be polylogn for protocol to be "efficient"

$f \in NP^{cc}$ if Nondet cc of Π is $O(\text{polylog}n)$

EXAMPLE: DISJOINTNESS



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

↑ communication complexity

analog of SATISFIABILITY problem

NP complete

DISJ requires $\Omega(n)$ CC (det + randomized)

But easy Nondeterministically

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

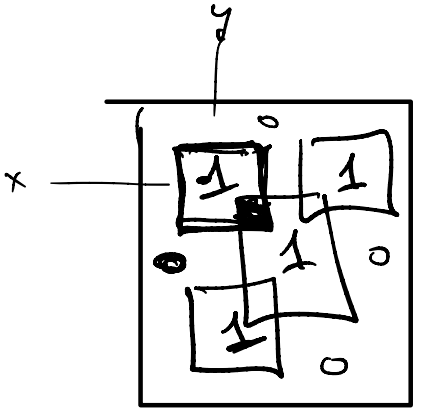
We'll soon see that DISJ while easy for nondet protocols, is maximally hard for randomized protocols.

↑

Nontrivial + very important LB.

Now has several proofs (None are easy)

Nondeterministic Protocol Π for f: Induces a covering of the 1's of M_f by all-1 rectangles (can be overlapping)



If Π has cc b, then size of covering $\leq 2^b$

(Recall in contrast a deterministic protocol Π of cost b partitions M_f into disjoint monochrom Rectangle (Non overlapping)

co - Nondeterministic CC shared random string r

Π computes f on "all" (x,y), $|x|=|y|=n$, co-Nondeterministically if

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

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

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

A co-nondet protocol Π for f induces a covering of the 0's of f into all-0 rectangles (can be overlapping)

Yannakakis Theorem 2

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ have

a Nondeterministic protocol Π^1 of cc c_1

and a conondet. protocol Π^0 of cc c_0

Then f has a deterministic protocol of cc $O(c_0 \cdot c_1)$.