Equality Cannot Simulate Randomness

Arkadev Chattopadhyay (TIFR)

Joint with

Shachar Lovett (UCSD)
Marc Vinyals (Technion)

How Powerful is Randomness?

How Powerful is Randomness?

Central Question in Theoretical CS.

How Powerful is Randomness?

Central Question in Theoretical CS.

Theorem: $P \subseteq BPP \subseteq NP^{NP}$

Theorem: Under plausible assumptions $P = BPP$!!

Study Such Questions in Elementary Models.

Study Such Questions in Elementary Models.

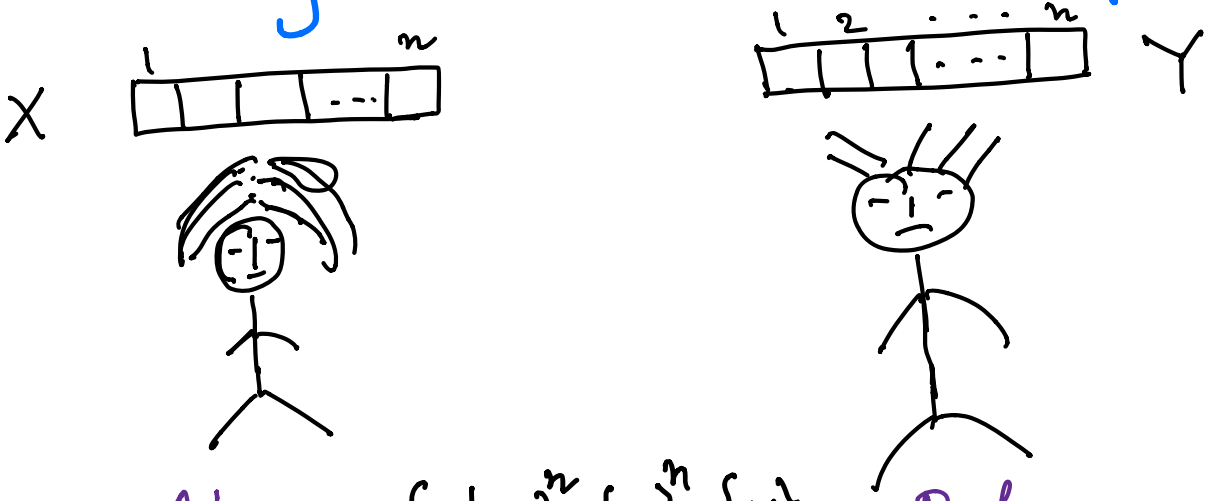
Decision Trees: $P = BPP$ (total functions)

Study Such Questions in Elementary Models.

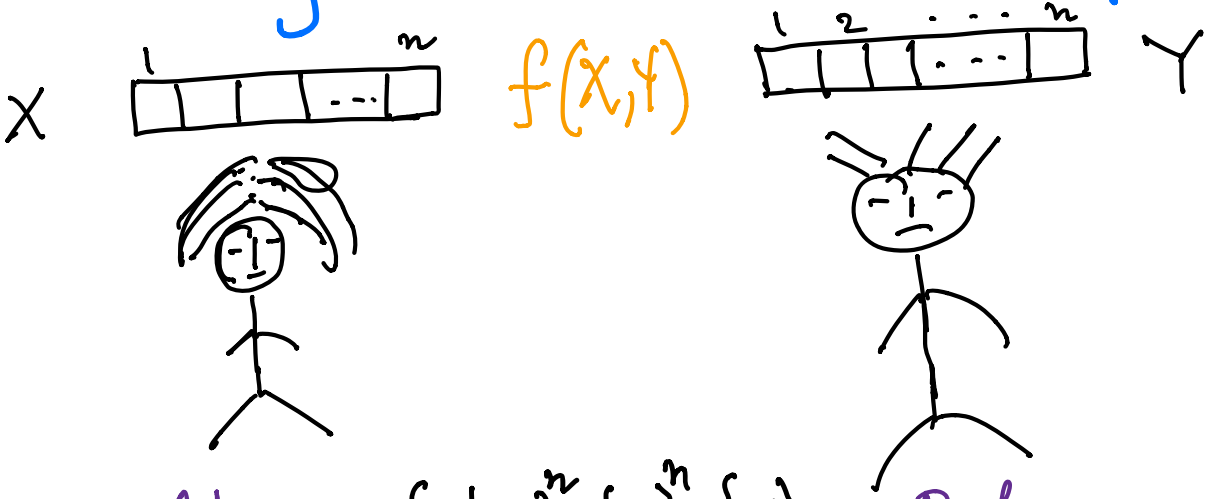
Decision Trees: $P = BPP$ (total functions)

Communication Complexity: $P \subsetneq BPP$.

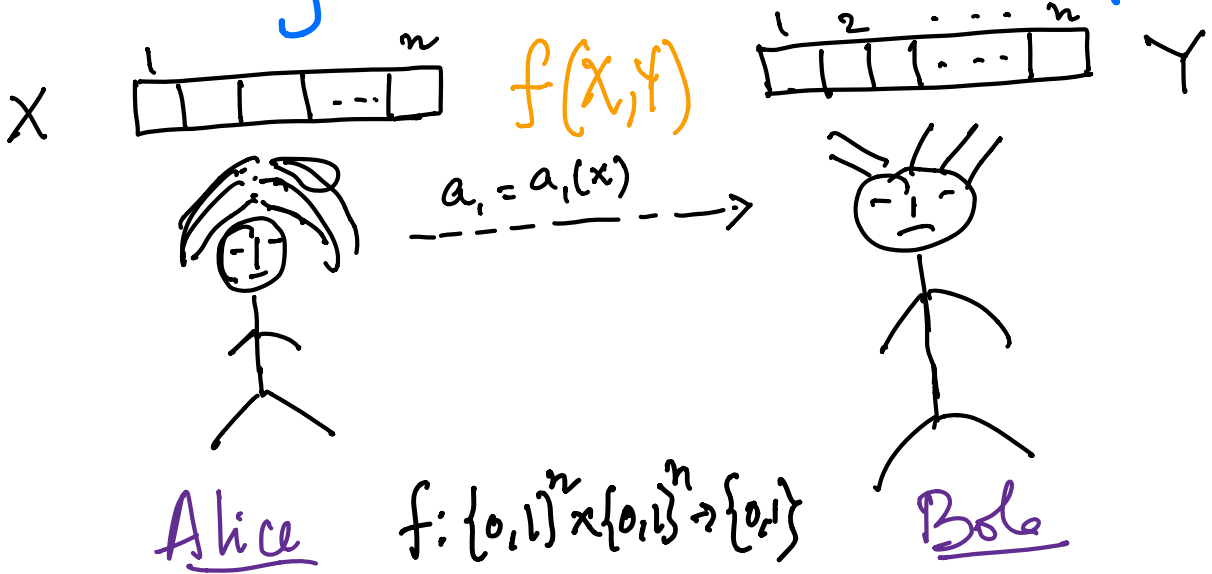
2 - Party Common Model of Yao



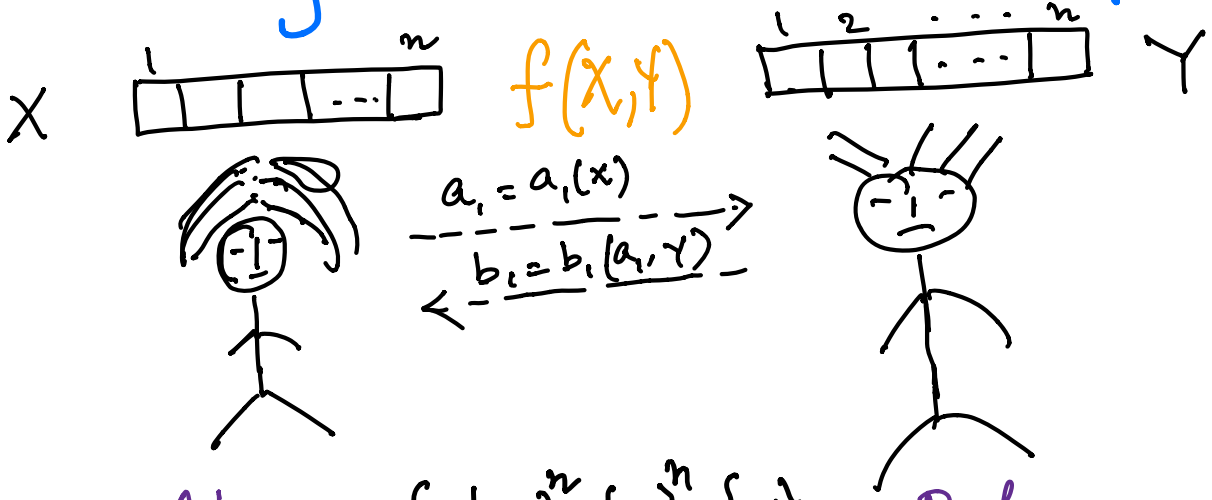
2 - Party Comm. Model of Yao



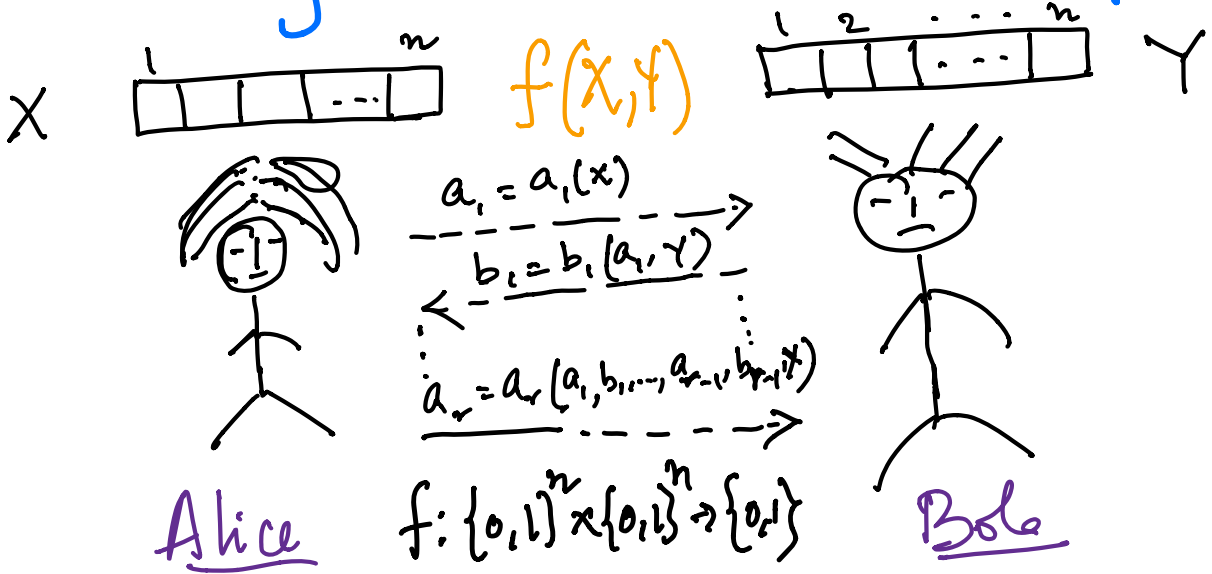
2 - Party Comm. Model of Yao



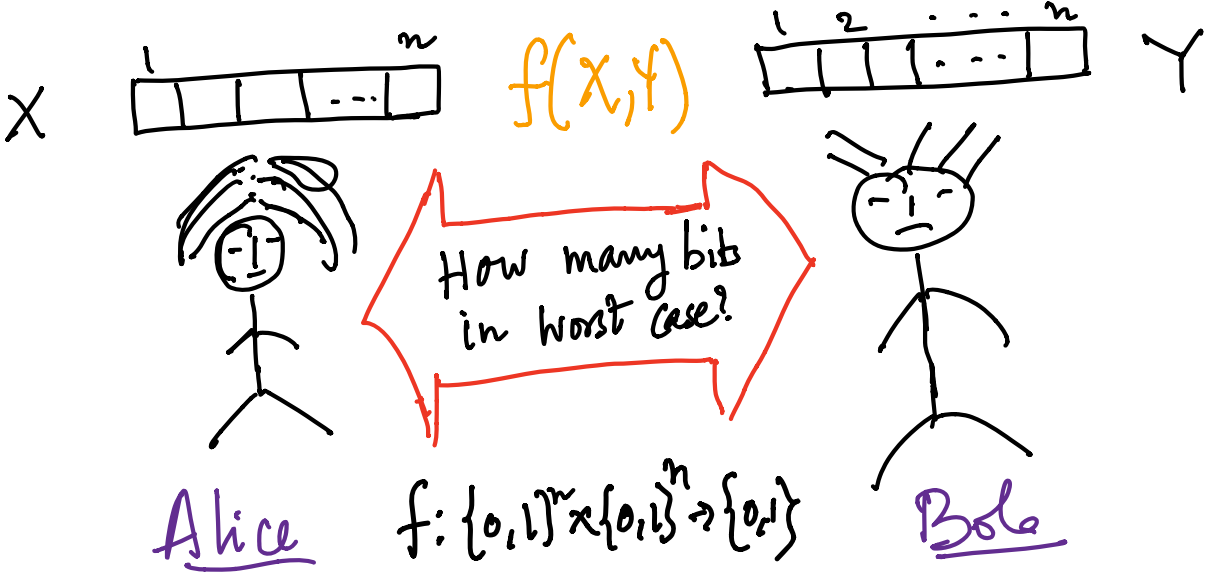
2 - Party Common Model of Yao



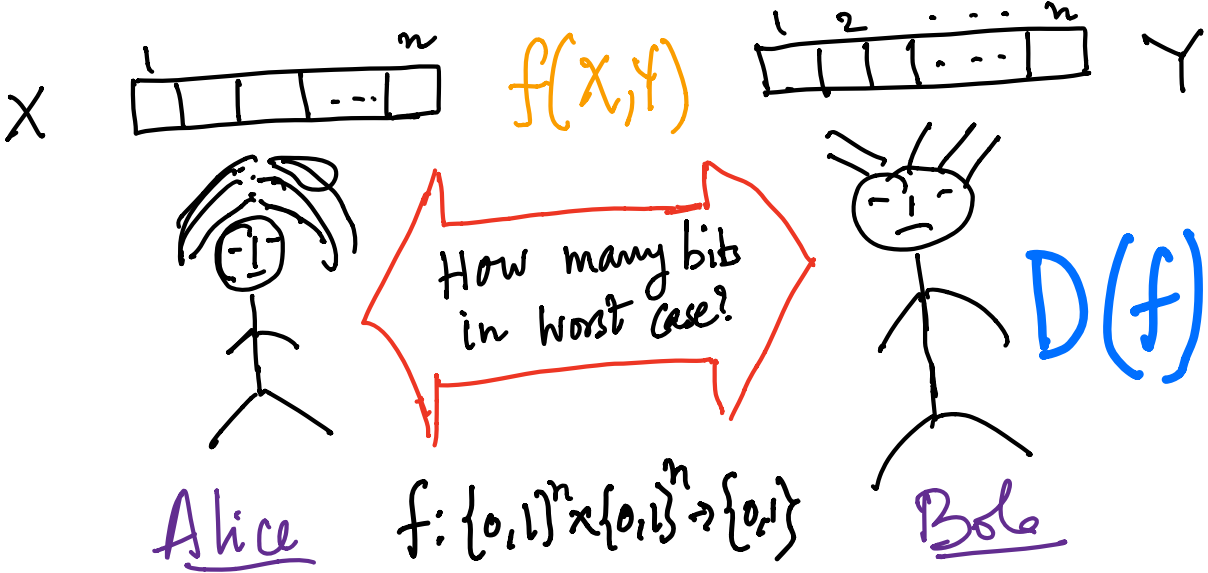
2 - Party Common Model of Yao



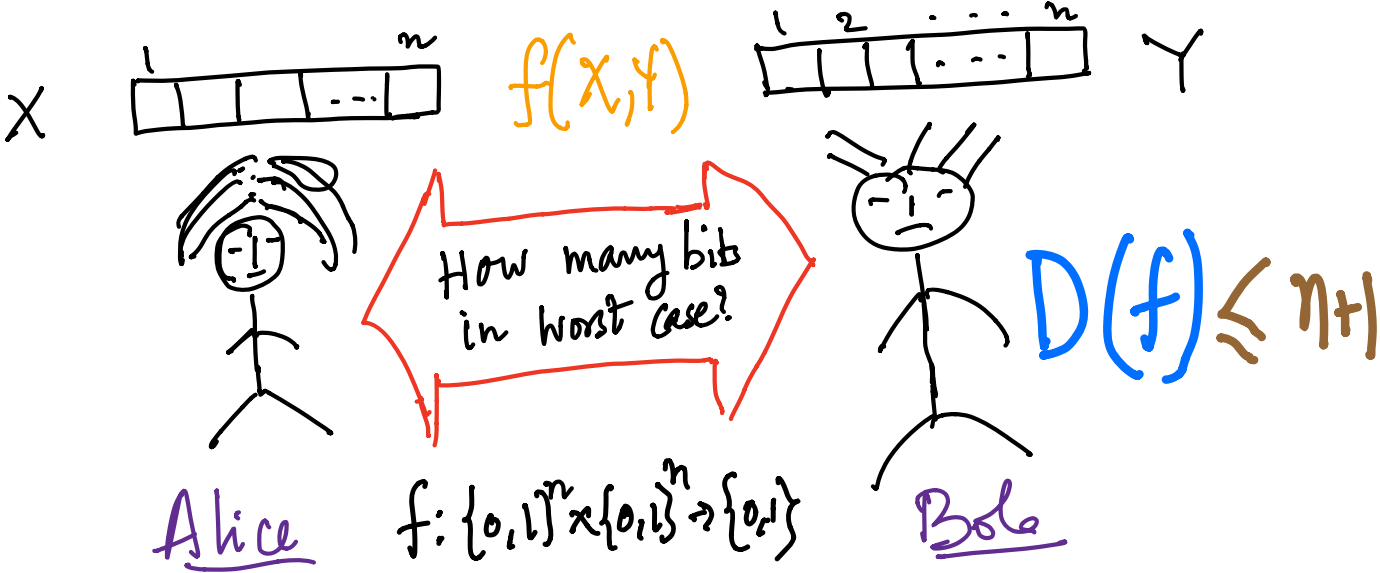
Deterministic Commn. Complexity



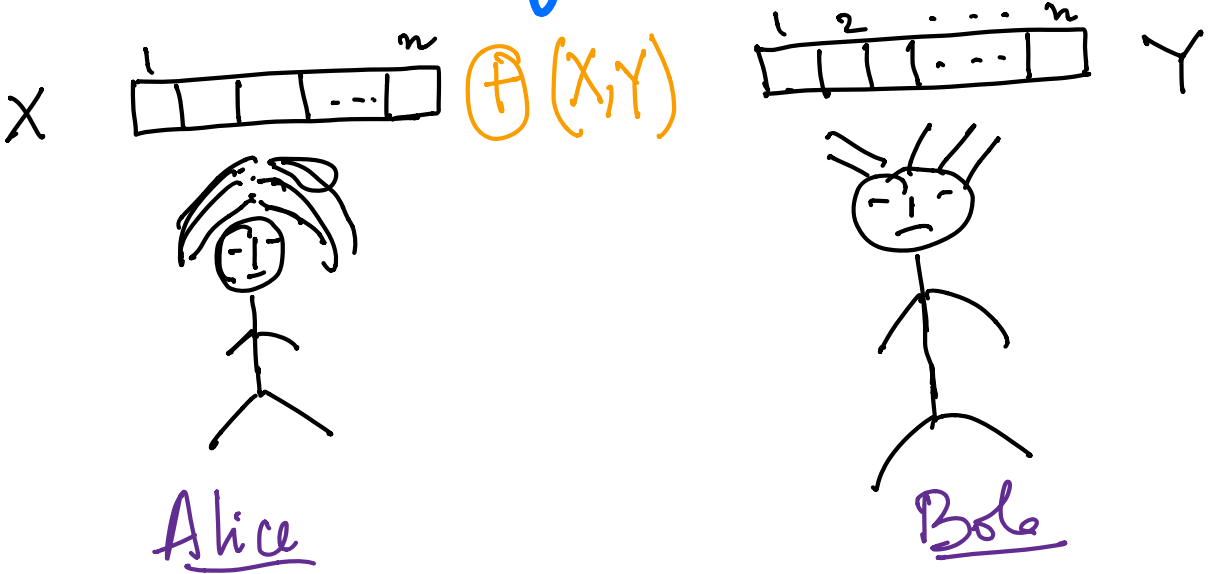
Deterministic Commn. Complexity



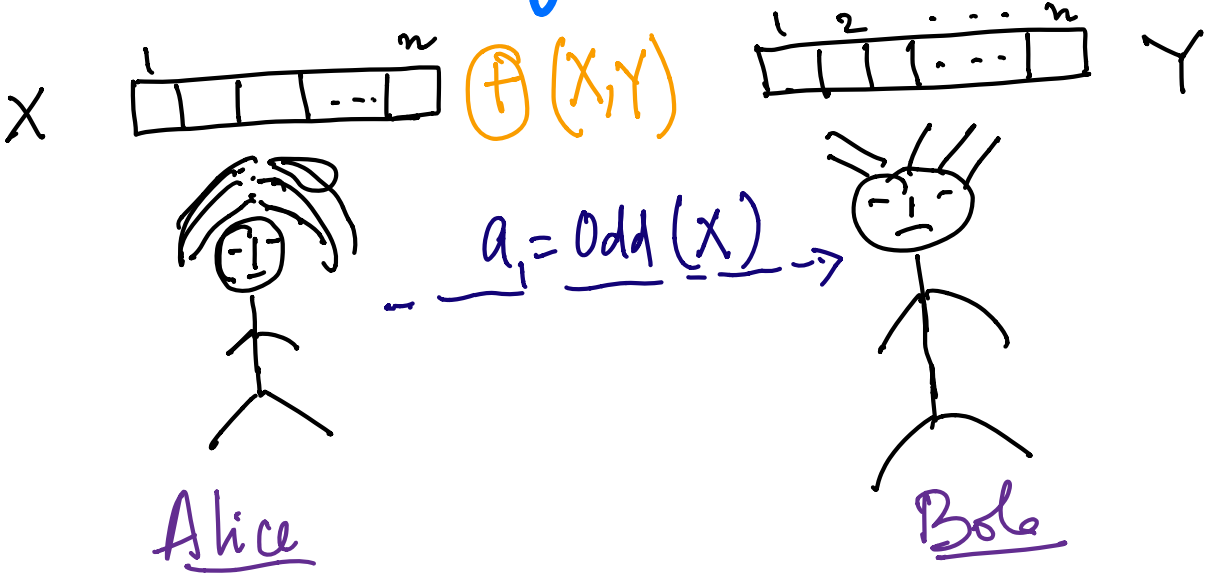
Deterministic Commn. Complexity



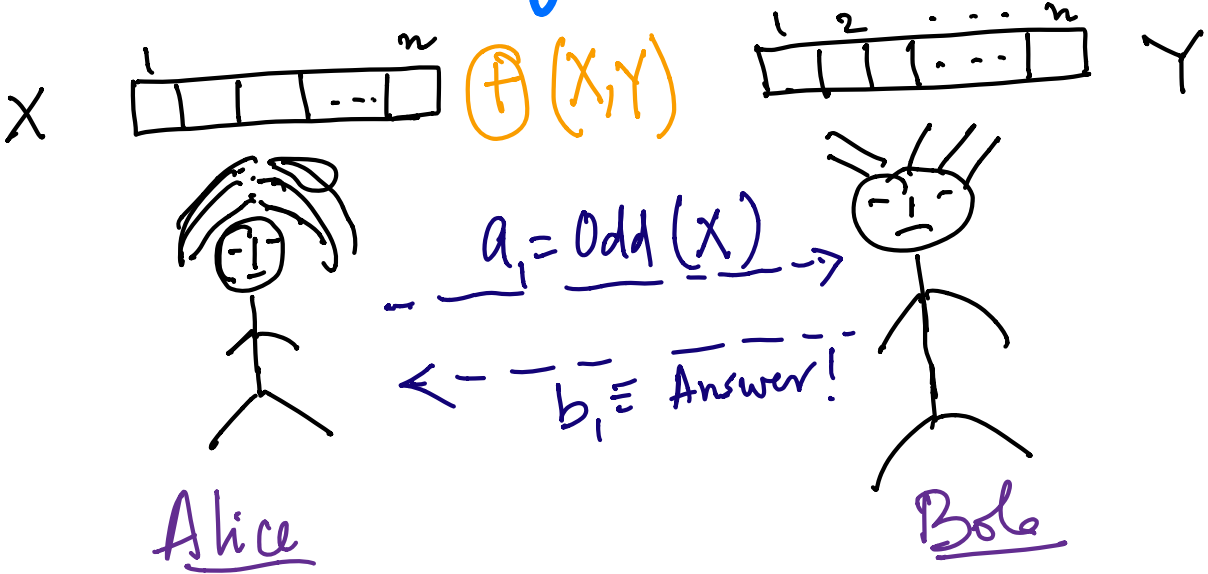
Easy Functions



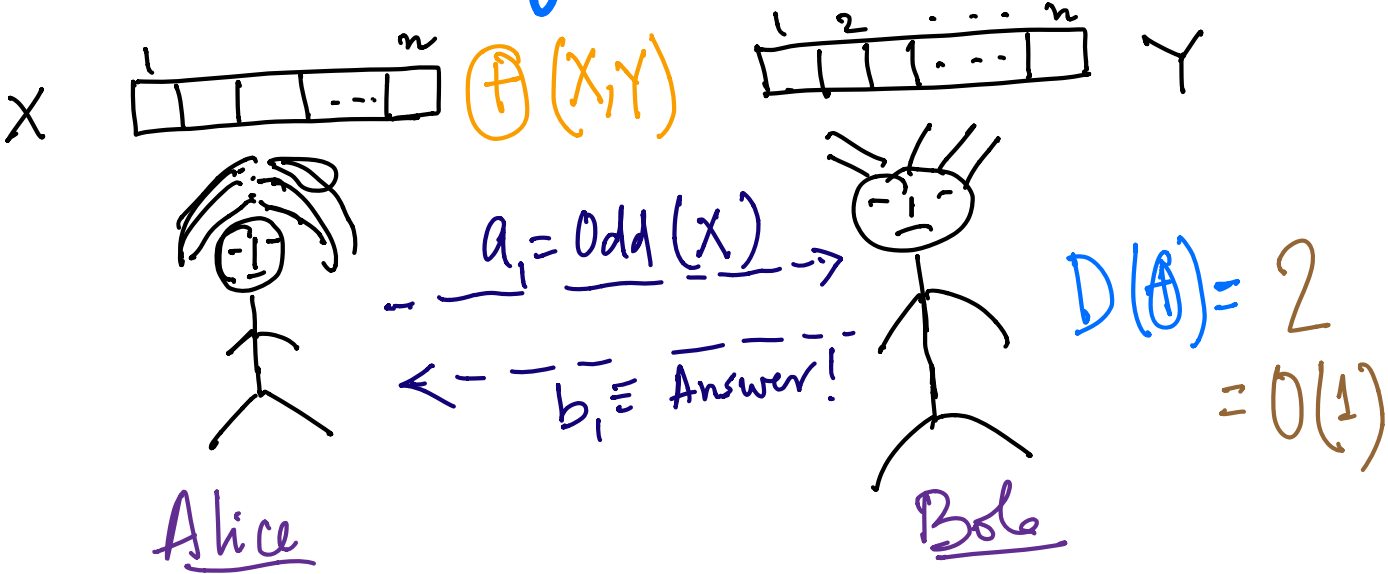
Easy Functions



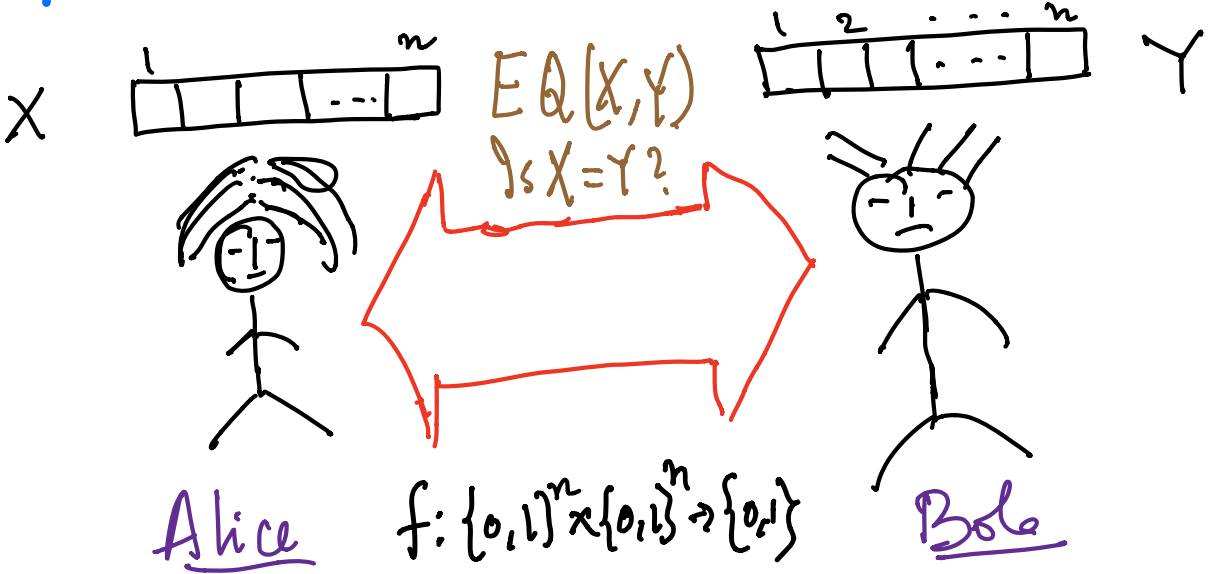
Easy Functions



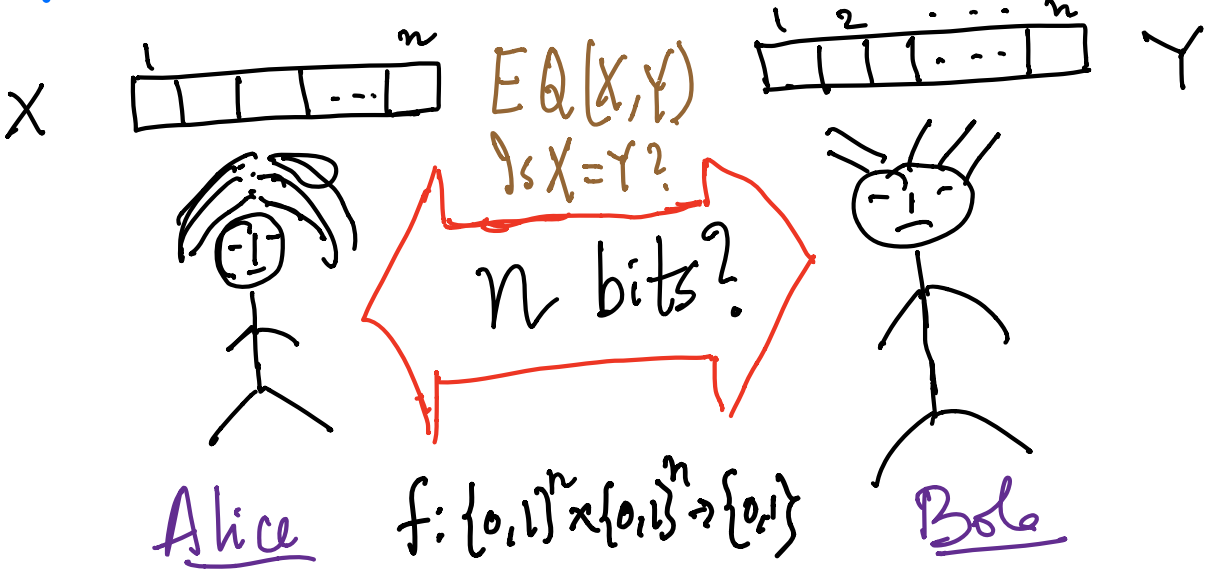
Easy Functions



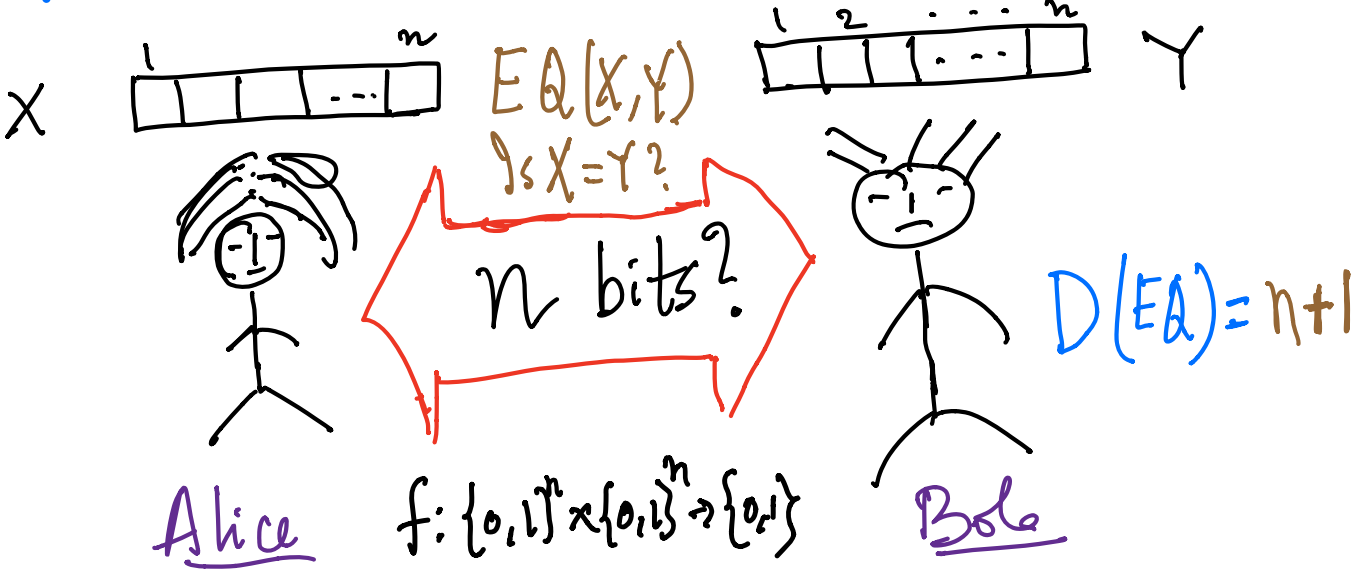
Hardness Of EQUALITY



Hardness Of EQUALITY



Hardness Of EQUALITY



Easy Functions.

$$P \equiv \left\{ f_n \mid D(f_n) = (\log n)^{O(1)} \right\}$$

Easy Functions.

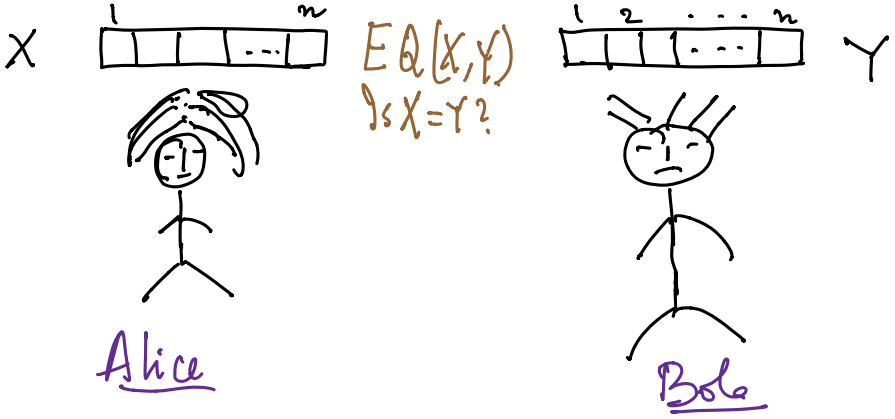
$$P \equiv \left\{ f_n \mid D(f_n) = (\log n)^{O(1)} \right\}$$

Examples:

PARITY, MAJORITY, SYMM....

Power Of Randomness

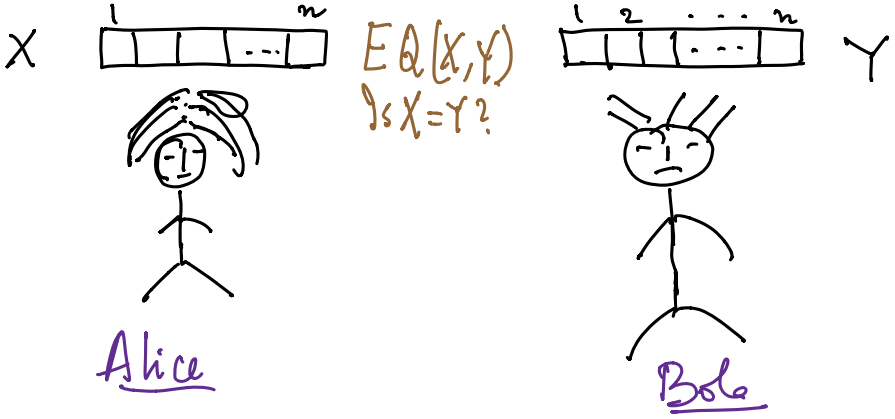
$D(EQ) = n+1$



Power Of Randomness

Randomness: 

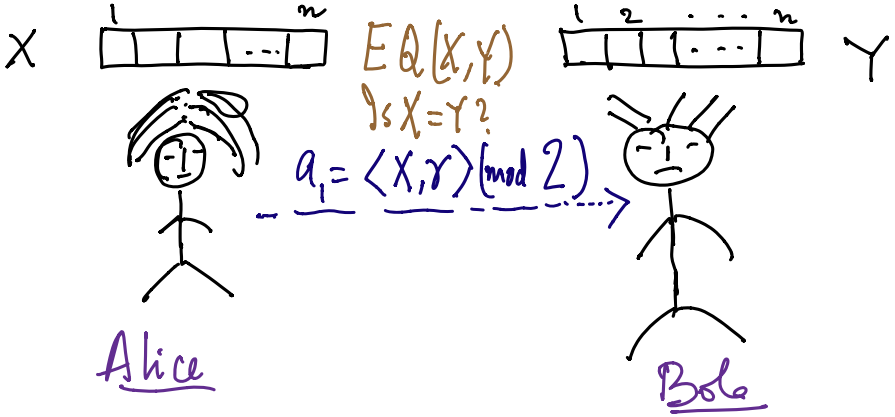
$D(EQ) = n+1$



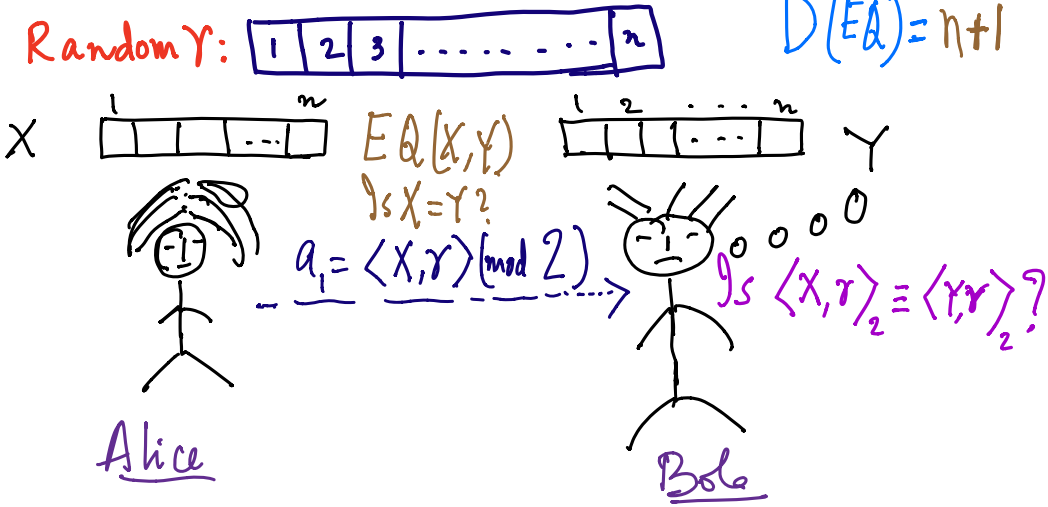
Power Of Randomness

Randomness: 

$D(EQ) = n+1$



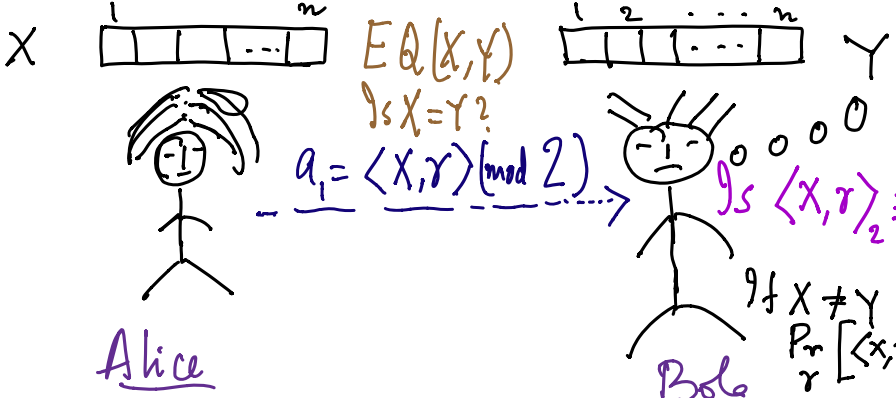
Power Of Randomness



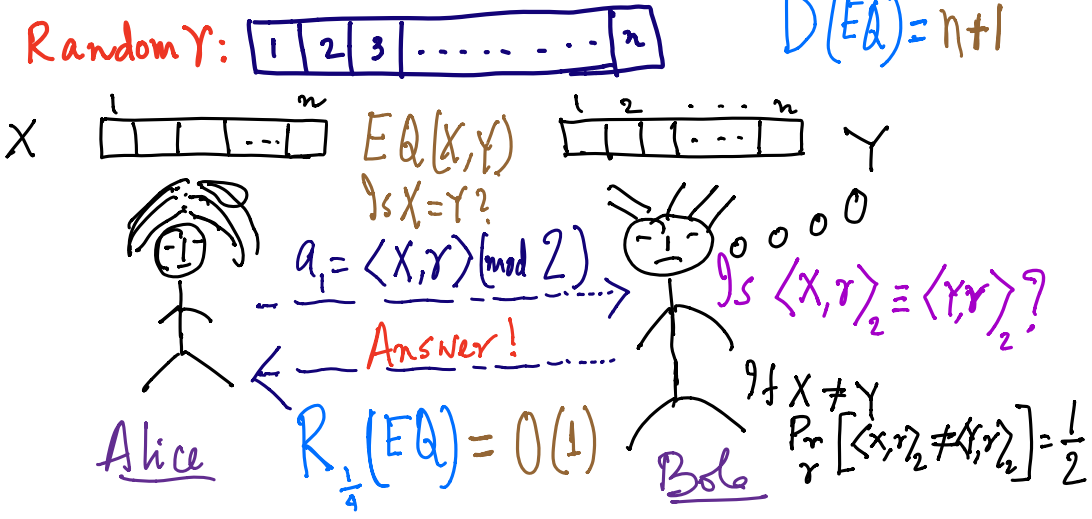
Power Of Randomness

Random r: 

$D(EQ) = n+1$



Power Of Randomness



A Class Separation

$$BPP \equiv \left\{ f_n \mid R(f_n) = (\log n)^{O(1)} \right\}$$

A Class Separation

$$BPP \equiv \left\{ f_n \mid R(f_n) = (\log n)^{O(1)} \right\}$$

Fact: $P \subsetneq BPP$

A Class Separation

$$BPP \equiv \left\{ f_n \mid R(f_n) = (\log n)^{O(1)} \right\}$$

Fact: $P \subsetneq BPP$

(via EQUALITY).

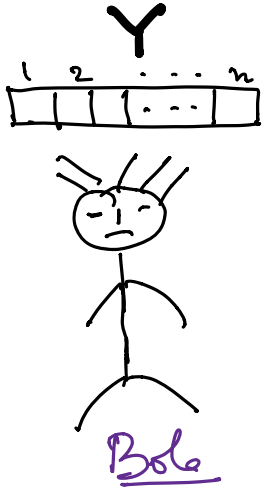
EQUALITY For Free

$$P^{EQ} \equiv \{ f_n \mid D^{EQ}(f_n) = (\log n)^{O(1)} \}$$

What else can be done?

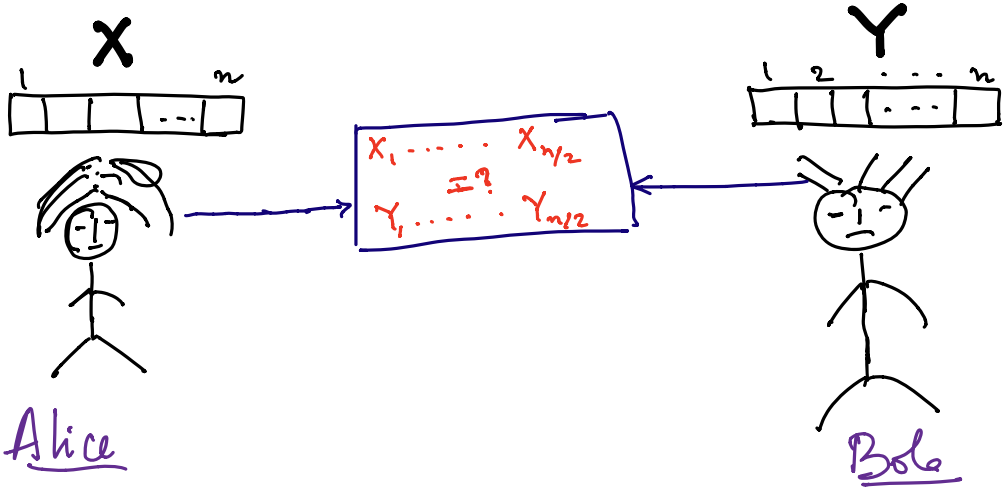
Power of EQ

$GT(X,Y) \equiv \neg(X \geq Y)$



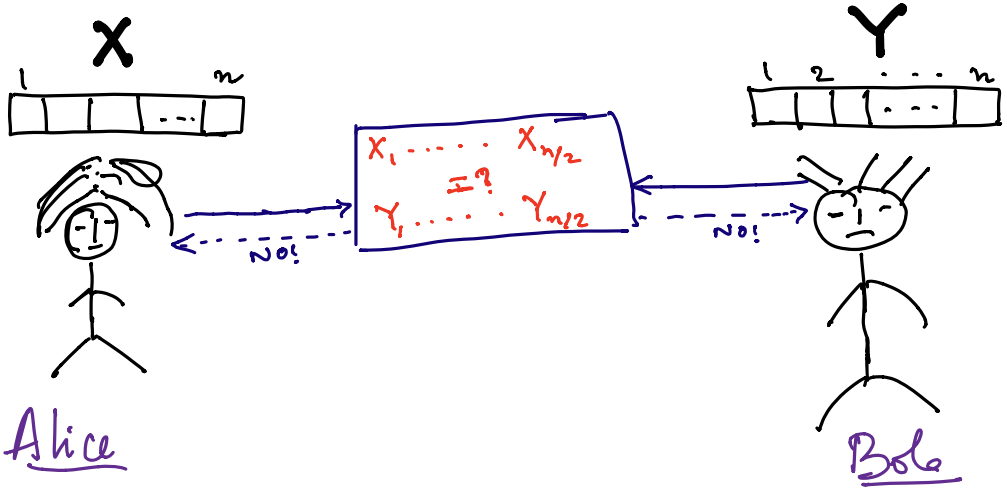
Power Of EQ

$GT(X,Y) \equiv ?\ X \gtrless Y$



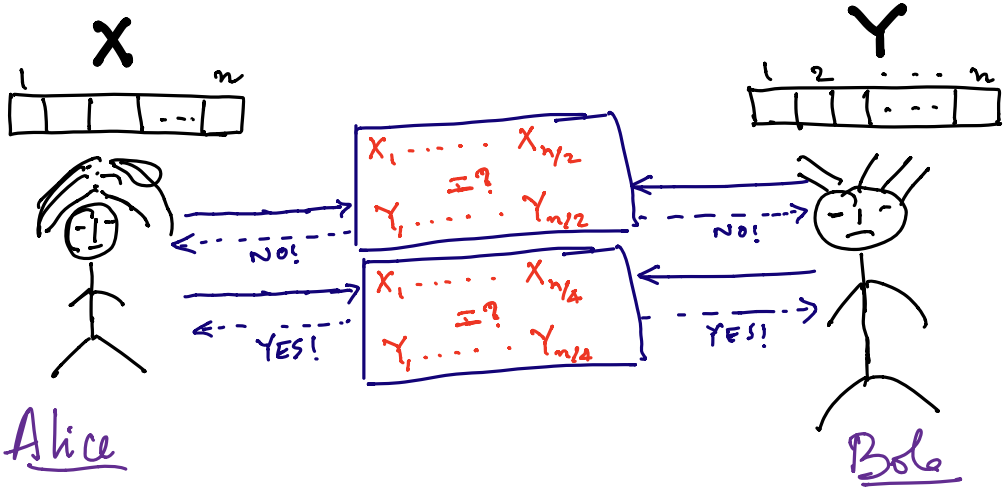
Power Of EQ

$GT(X,Y) \equiv \neg(X=Y)$



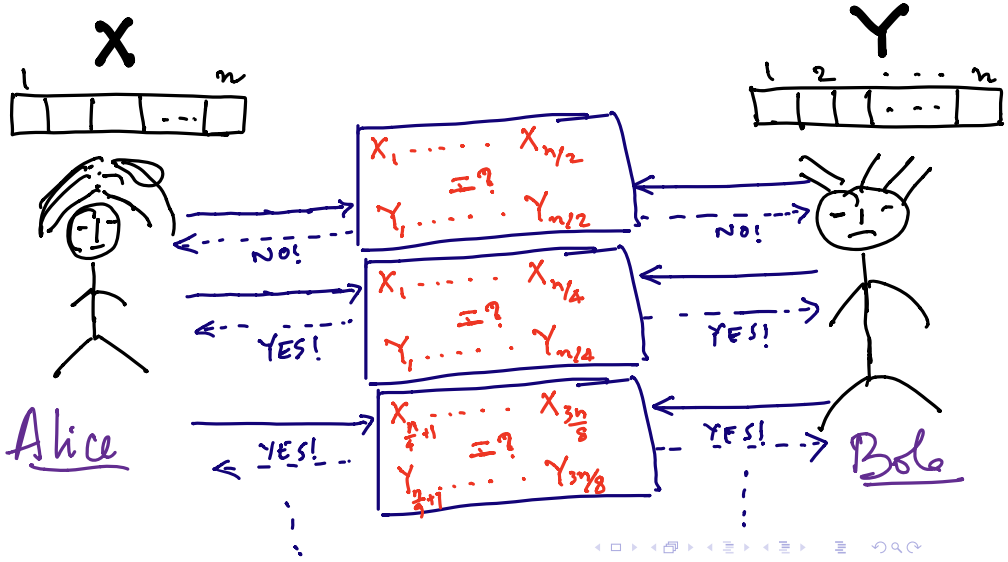
Power Of EQ

$GT(X,Y) \equiv \neg(X \geq Y)$



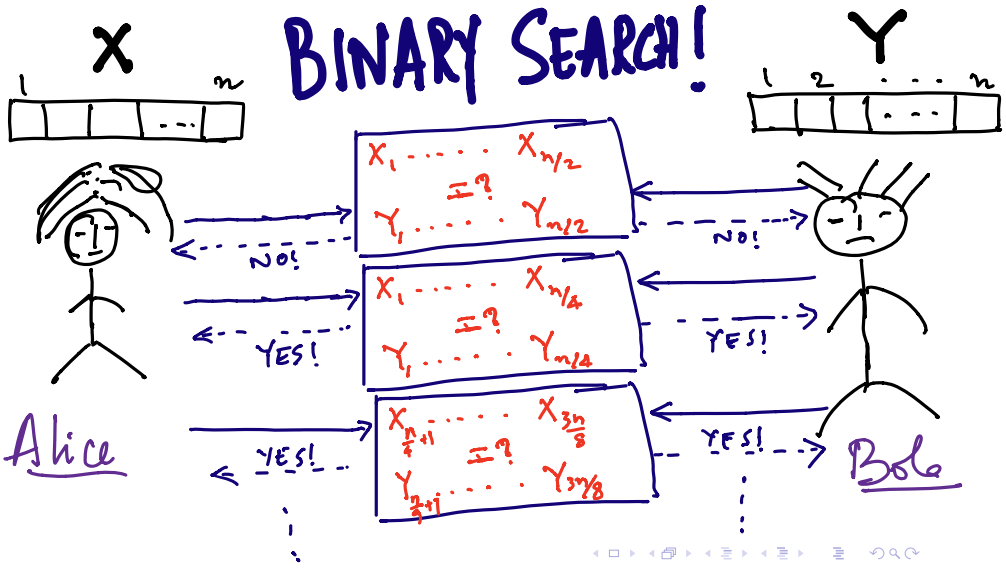
Power Of EQ

$GT(X,Y) \equiv \neg(X \geq Y)$



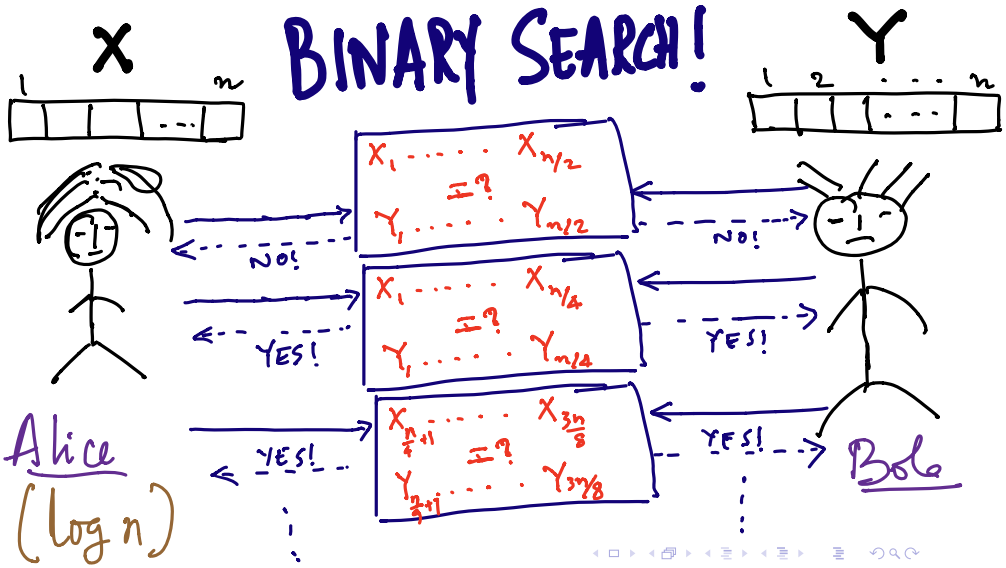
Power Of EQ

$GT(X,Y) \equiv ?\ X > Y$



Power Of EQ

$GT(X,Y) \equiv ?\ X > Y$



$D^{EQ}(GT) = O(\log n)$

EQUALITY vs. Randomness

$$P^{EQ} \equiv \left\{ f_n \mid D^{EQ}(f_n) = (\log n)^{O(1)} \right\}$$

Fact: $P^{EQ} \subseteq BPP$.

EQUALITY vs. Randomness

$$P^{EQ} \equiv \{ f_n \mid D^{EQ}(f_n) = (\log n)^{O(1)} \}$$

Fact: $P^{EQ} \subseteq BPP$.

Question: Is $P^{EQ} = BPP$?

Total vs. Partial

Fact: $P^{EQ} \not\subseteq BPP$. (Partial. Gap-Hamming)

Total vs. Partial

Fact: $P^{EQ} \not\subseteq BPP$. (Partial. Gap-Hamming)

Question: Is $P^{EQ} = BPP$? (Total Functions)

Our Result

Theorem: $P^{EQ} \not\subseteq BPP$ (Total fns.)

Our Result

Theorem: $P^{EQ} \not\subseteq BPP$ (Total fns.)

Theorem:

$$P^{EQ} = P^{\Pi P_2} \not\subseteq P^{\Pi P_5} \subseteq P^{\Pi P_9} \subseteq \underbrace{\cdots}_{\text{Infinite}} \subseteq BPP$$

Integer Inner Product

Let $t \in \mathbb{Z}_+$; $X_1, \ldots, X_t, Y_1, \ldots, Y_t \in \{-N, -N+1, \ldots 0, \ldots +N\}$

Integer Inner Product

Let $t \in \mathbb{Z}_+$; $X_1, \dots, X_t, Y_1, \dots, Y_t \in \{-N, -N+1, \dots 0, \dots +N\}$

Definition:

$$IIP(X_1, \dots, X_t, Y_1, \dots, Y_t) = \begin{cases} 1 \text{ if } \sum_{i=1}^{t} X_i Y_i = 0 \\ 0, \text{ Otherwise} \end{cases}$$

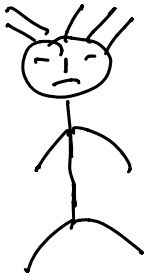
Randomized Protocol For IIP

$X_i, Y_i \in [-N, N]$

$N = 2^n$.

$X_1 \dots X_t$

$Y_1 \dots Y_t$ Y



Randomized Protocol For IIP

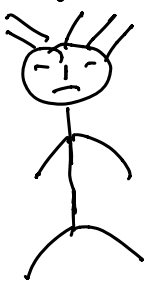
Random prime $p \in [n^2]$

$X_i, Y_i \in [-N, N]$

$N = 2^n$.

$X_1 \dots X_t$

$Y_1 \dots Y_t$



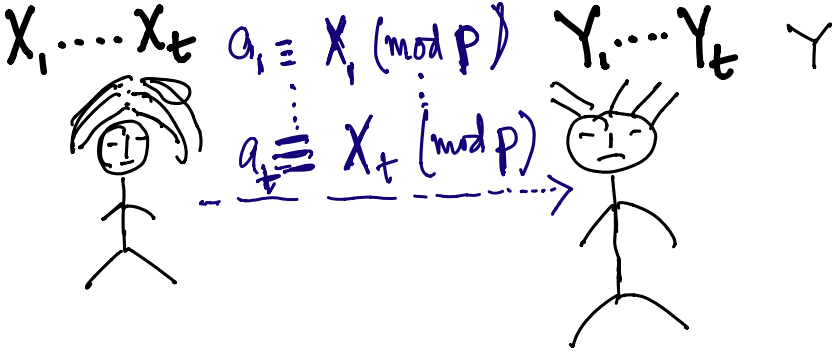
Y

Randomized Protocol For IIP

Random prime $p \in [n^2]$

$X_i, Y_i \in [-N, N]$

$N = 2^n$.

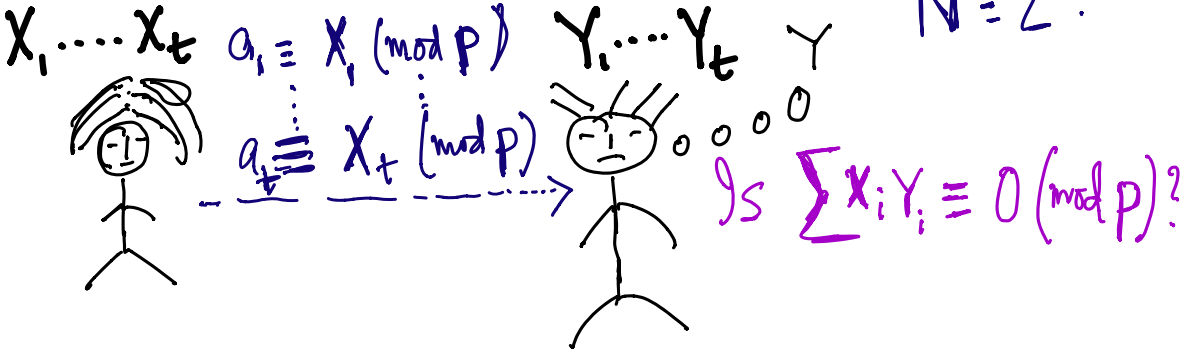


Randomized Protocol For IIP

Random prime $p \in [n^2]$

$X_i, Y_i \in [-N, N]$

$N = 2^n$.

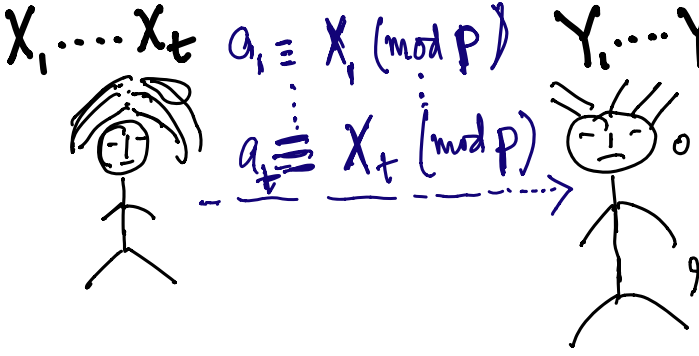


Randomized Protocol For IIP

Random prime $p \in [n^2]$

$X_i, Y_i \in [-N, N]$

$N = 2^n$.



Is $\sum X_i Y_i \equiv 0 \pmod p$?

If $IIP(X,Y) \neq 0$

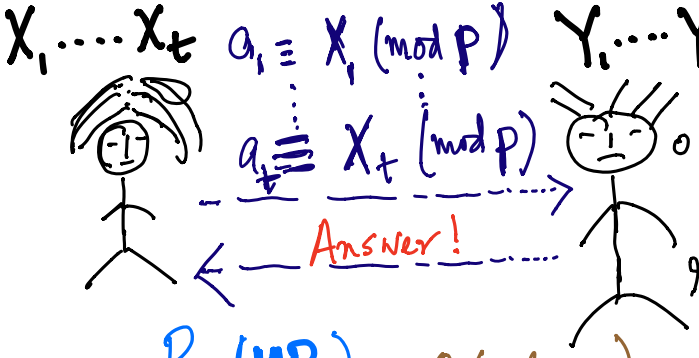
$\Pr_p\left[\sum X_i Y_i \neq 0 \pmod p\right] \geq 1 - o(1)$

Randomized Protocol For IIP

Random prime $p \in [n^2]$

$X_i, Y_i \in [-N, N]$

$N = 2^n$.



Is $\sum X_i Y_i \equiv 0 \pmod p$?

If $IIP(X,Y) \neq 0$

$R_{\frac{1}{4}}(IIP_t) = O(t \log n)$

$\Pr_p\left[\sum X_i Y_i \neq 0 \pmod p\right] \geq 1 - o(1)$

Our Result

Theorem: $D^{EQ}(\Pi P_t) = \Omega(n), t \approx 6$

Our Result

Theorem: $D^{EQ}(\|P_t) = \Omega(n)$, $t \geq 6$.

$(RP \not\subseteq P^{EQ})$

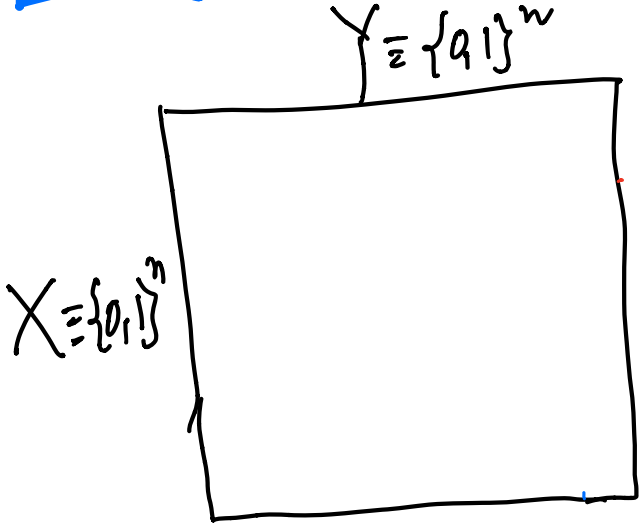
Our Result

Theorem: $D^{EQ}(\Pi P_t) = \Omega(n)$, $t \neq 6$.

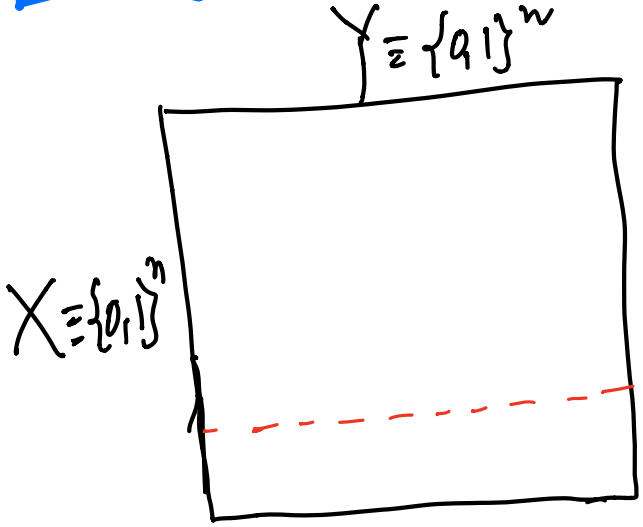
$(RP \not\subseteq P^{EQ})$

Theorem: $P \subsetneq P^{EQ} \subsetneq P^{\Pi P_{t_1}} \subsetneq P^{\Pi P_{t_2}} \subsetneq \dots \subsetneq P^{\Pi P_{t_i}} \subsetneq \dots \subseteq BPP$

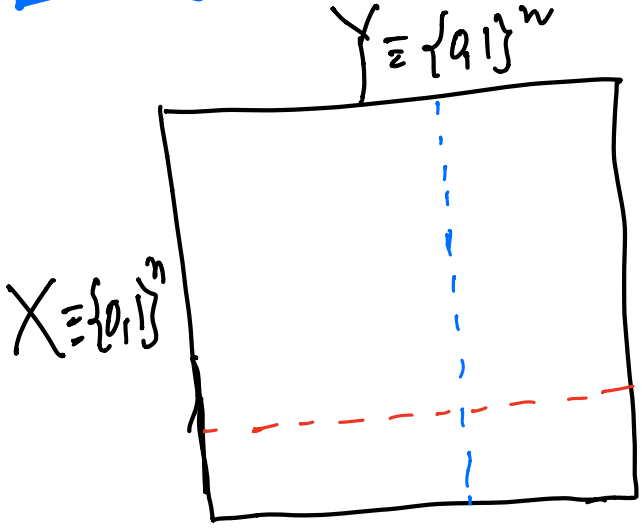
Lower Bounds



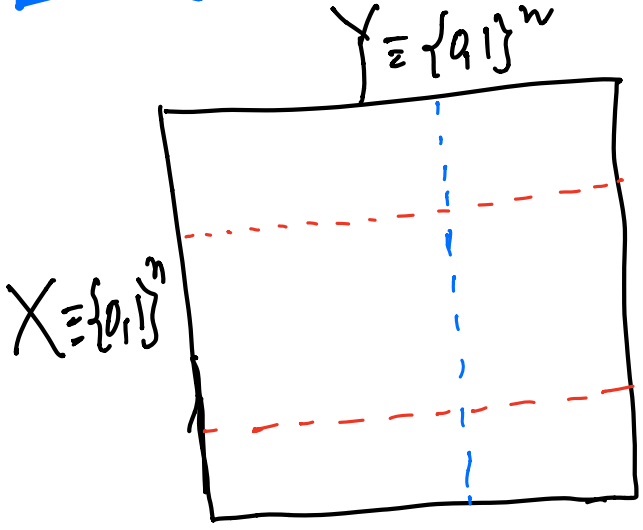
Lower Bounds



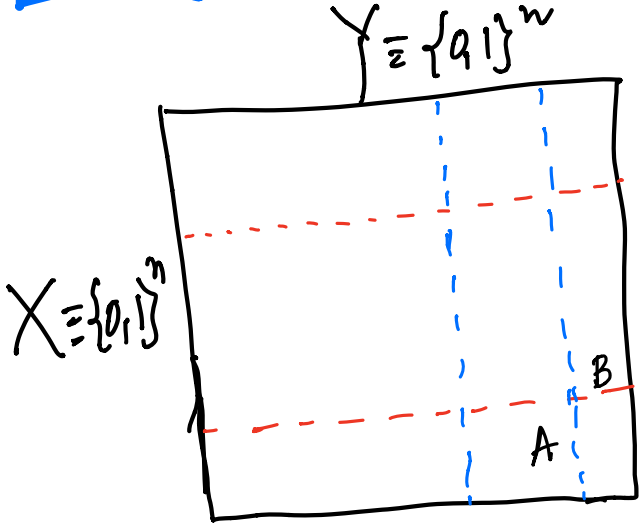
Lower Bounds



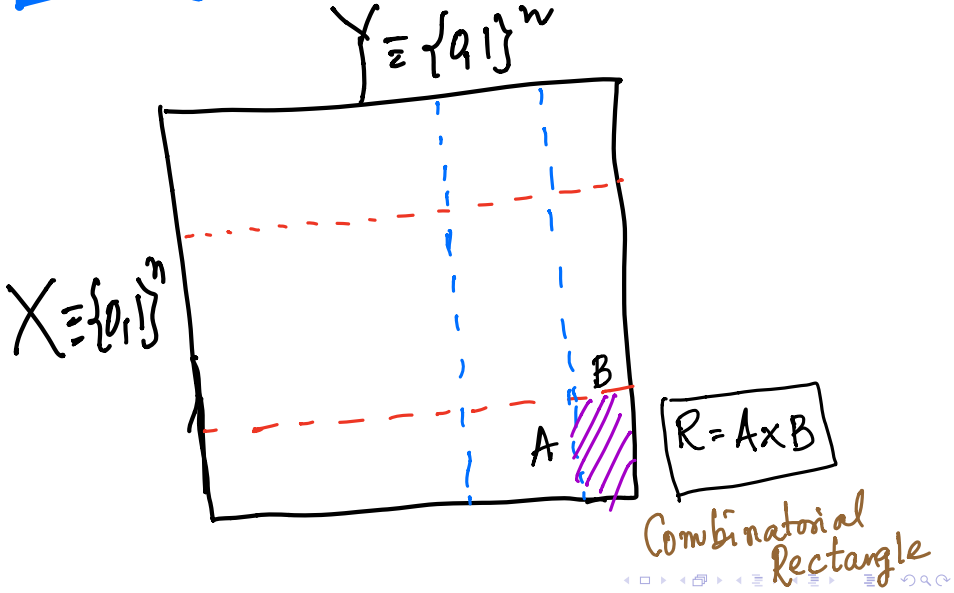
Lower Bounds



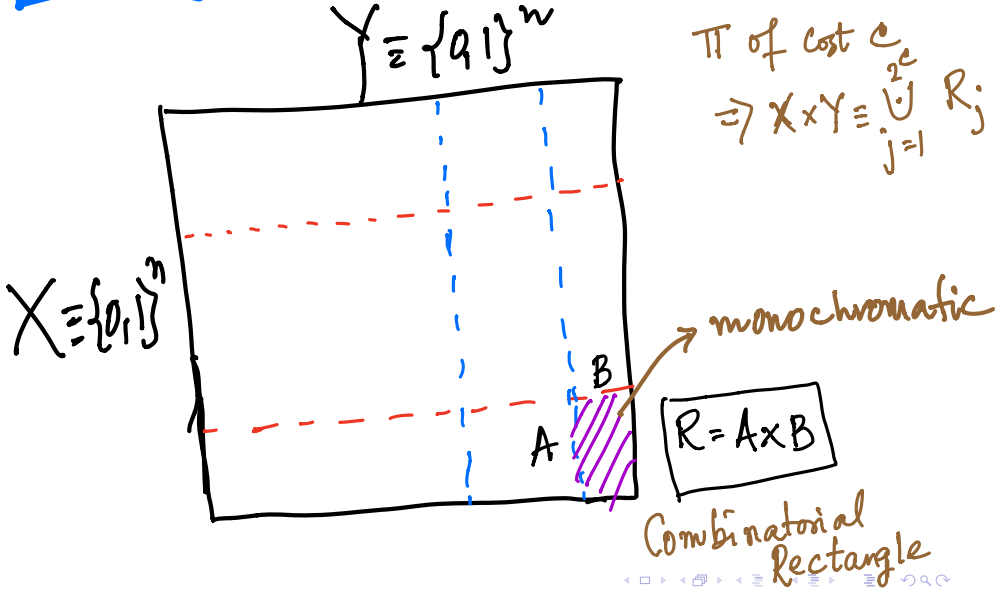
Lower Bounds



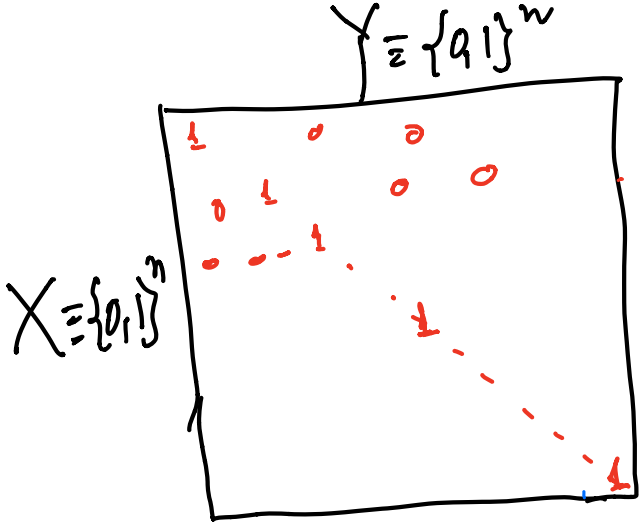
Lower Bounds



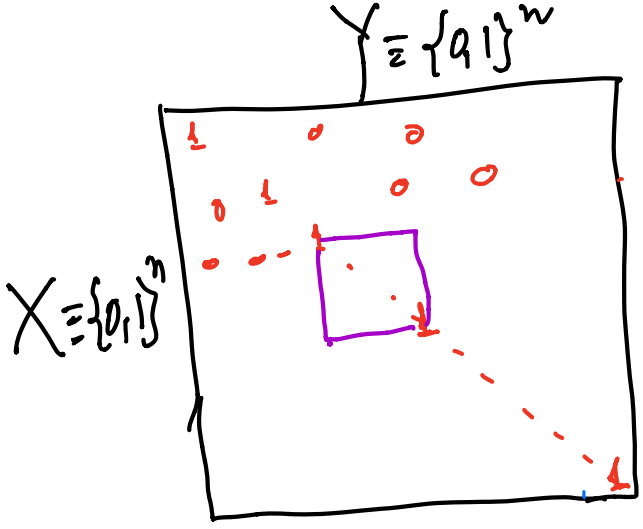
Lower Bounds



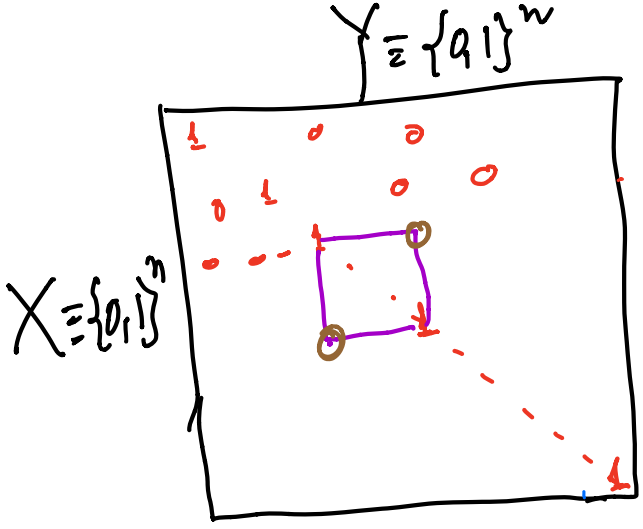
Lower Bound Fn EQUALITY



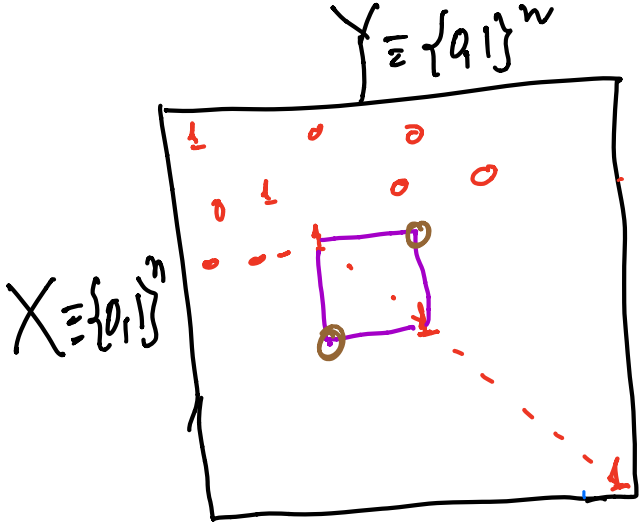
Lower Bound Fn EQUALITY



Lower Bound Fn EQUALITY

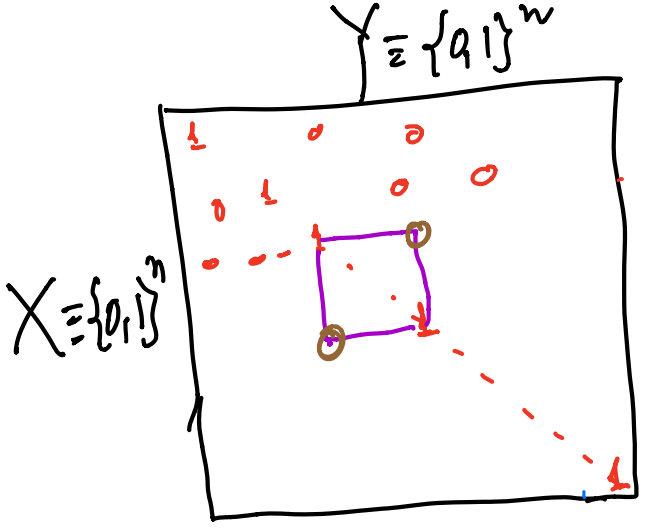


Lower Bound Fn EQUALITY



$2^c \geq 2^n + 1$

Lower Bound Fn EQUALITY



$$2^c \geq 2^n + 1$$

$$\Rightarrow c \geq n+1$$

$$\therefore \boxed{D(EQ) = n+1}$$

How Do We Lower Bound Cost of π^{EQ} Protocols?

How Do We Lower Bound Cost of π^{EQ} Protocols?

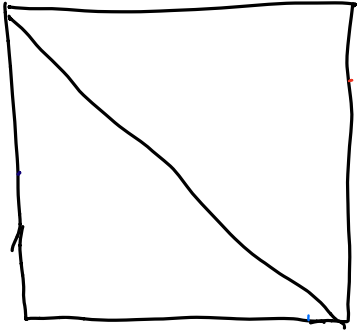
Consider π^{GT} protocols.

How Do We Lower Bound Cost of π^{EQ} Protocols?

Consider π^{GT} protocols.

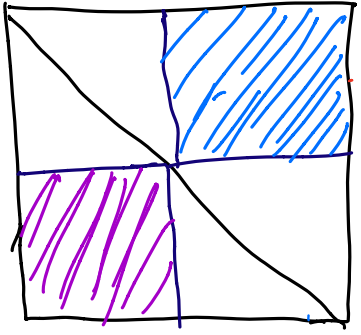
$D^{GT}(f) \leq 2 \cdot D^{EQ}(f)$.

Perimeter of EQUALITY is Small.



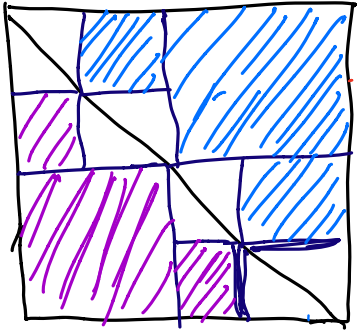
Difficulty:
No small partition into monochrom rectangles.

Perimeter of EQUALITY Is Small.



Difficulty:
No small partition into monochrom rectangles.

Perimeter of EQUALITY is Small.

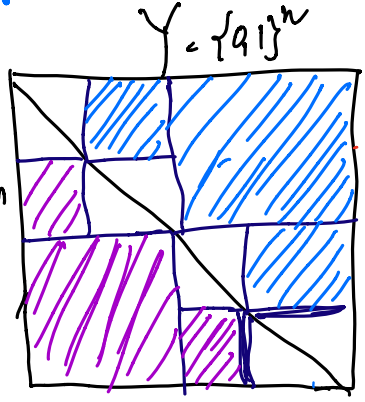


Difficulty:
No small partition into monochrom. rectangles.

Perimeter of EQUALITY Is Small.

Observation:

Average mon. rect size is large.



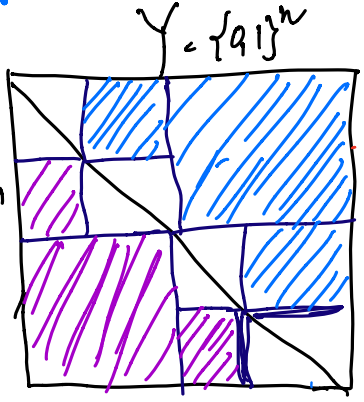
Difficulty:

No small partition into monochrom rectangles.

Perimeter of EQUALITY Is Small.

Observation:

Average mon. rect size is large. $X = \{0,1\}^n$



Difficulty:

No small partition into monochrom rectangles.

Definition: -

$R = A \times B$.

$\mathrm{Per}(R) = |A| + |B|$

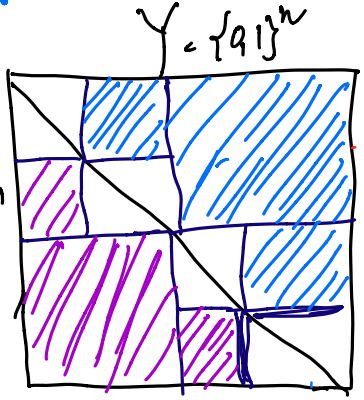
$\mathcal{R} = \bigcup_i (R_i = A_i \times B_i)$

$\mathrm{Per}(\mathcal{R}) = \sum_i (|A_i| + |B_i|)$

Perimeter of EQUALITY Is Small.

Observation:

Average mon. rect size is large. $X = \{0,1\}^n$



Difficulty:

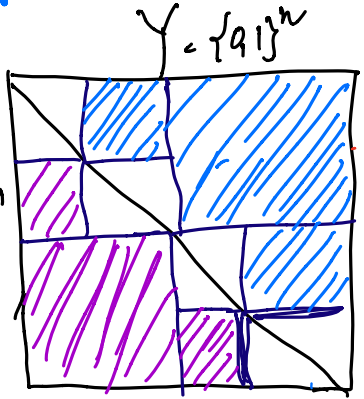
No small partition into monochrom rectangles.

$$Per(EQ_n) \leq 2 \cdot (2^{n-1} + 2^{n-1}) + 2 \cdot Per(EQ_{n-1})$$

Perimeter of EQUALITY Is Small.

Observation:

Average mon. rect size is large. $X = \{0,1\}^n$

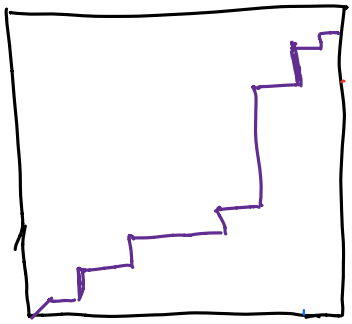


Difficulty:

No small partition into monochrom rectangles.

$$\begin{aligned} Per(EQ_n) &\leq 2\cdot(2^{n-1}+2^{n-1}) + 2\cdot Per(EQ_{n-1}) \\ &= 4\cdot 2^{n-1} + 2\cdot Per(EQ_{n-1}) \leq 4\cdot 2^{n-1} + 4\cdot 2^{n-2} + \cdots \\ &= 2n\cdot 2^{n-1} = 2n\cdot 2^{n}. \end{aligned}$$

Perimeter of Greater-than is Small.

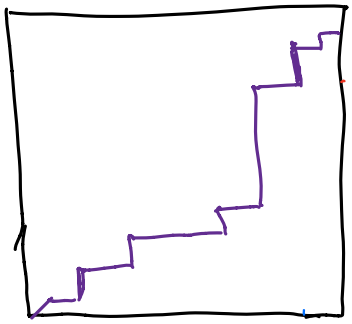


Permute rows & columns.

Perimeter of Greater-than is Small.

Monotone matrix

$i_1 \le i_2$
$j_1 \le j_2$
$\Rightarrow M(i_1, j_1) \le M(i_2, j_2)$

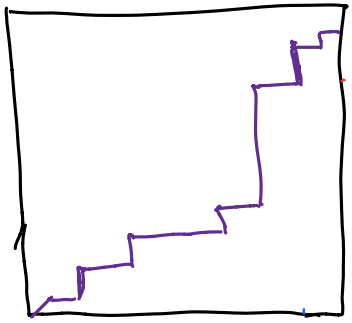


Permute rows & Columns.

Perimeter of Greater-than is Small.

Monotone matrix

$i_1 \le i_2$
$j_1 \le j_2$
$\Rightarrow M(i_1, j_1) \le M(i_2, j_2)$



Permute rows & columns.

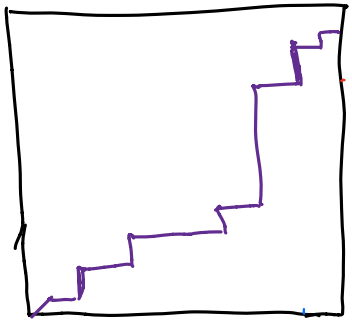
Fact: Let $R = A \times B$ be monotone.

$$\beta_{er}(R) \le (|A| + |B|) \log_2(|A| \cdot |B|)$$

Perimeter of Greater-Than Is Small.

Monotone matrix

$i_1 \le i_2$
$j_1 \le j_2$
$\Rightarrow M(i_1, j_1) \le M(i_2, j_2)$



Permute rows & Columns.

Corollary:
$D^{pr}(GT_n) \le 2^{n+1} \cdot (2n)$

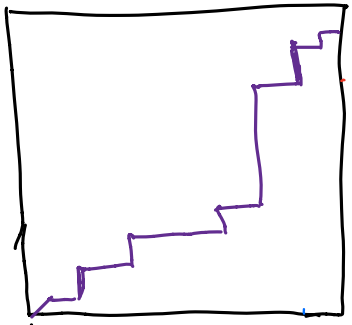
Fact: Let $R \subseteq A \times B$ be monotone.

$$D^{pr}(R) \le (|A| + |B|) \log_2(|A| \cdot |B|)$$

Perimeter of Greater-Than Is Small.

Monotone matrix

$i_1 \le i_2$
$j_1 \le j_2$
$\Rightarrow M(i_1, j_1) \le M(i_2, j_2)$



Permute rows & Columns.

Corollary:
$Per(GT_n) \le 2^{n+1} \cdot (2n)$

Fact: Let $R = A \times B$ be monotone.
$Per(R) \le (|A| + |B|) \log_2(|A| \cdot |B|)$

Lemma: Let $D^{GT}(f) \le c$. Then $Per(f) \le 2^{n+1} \cdot (2n)^c$

Functions With High Perimeter

Lemma 3.3. *Let f be an n-bit function with a corresponding $2^n \times 2^n$ communication matrix M. Assume that:*

1. *The number of entries i, j with $M_{i,j} = 1$ is $\alpha 2^{2n}$.*
2. *For any 1-monochromatic rectangle R in M it holds that $|R| \leq \beta 2^{2n}$.*

Then, $\mathrm{Per}(f) \geq 2^{n+1} \cdot \lfloor \alpha/\beta \rfloor \cdot \sqrt{\beta}$

High Perimeter

Proof: $f^{-1}(1) \equiv \mathcal{R} = \bigcup_i R_i = \bigcup_i A_i \times B_i$

$$\mathrm{Per}(\mathcal{R}) = \sum_i |A_i| + |B_i| \geq 2 \sum_i \sqrt{|A_i| |B_i|}$$

High Perimeter

Proof: $f^{-1}(1) \equiv \mathcal{R} = \bigcup_i R_i = \bigcup_i A_i \times B_i$

$$Per(\mathcal{R}) = \sum_i |A_i| + |B_i| \geq 2 \sum_i \sqrt{|A_i||B_i|}$$

$$\Rightarrow Per(\mathcal{R}) \geq 2^{n+1} \min \sum \sqrt{x_i}$$

$$x_i \equiv \frac{|A_i||B_i|}{2^{2n}}$$

$$0 \leq x_i \leq \beta$$

$$\sum x_i = \alpha$$

Lower Bounding Perimeter

$$\mathrm{Per}(R) \geq 2^{n+1} \min \sum_i \sqrt{x_i}$$

$$0 \leq x_i \leq \beta$$

$$\sum_i x_i = \alpha$$

$$x_i \equiv \frac{|A_i||B_i|}{2^{2n}}$$

Lower Bounding Perimeter

$$\mathrm{Per}(R) \geq 2^{n+1} \min \sum_i \sqrt{x_i}$$

$$0 \leq x_i \leq \beta$$

$$\sum_i x_i = \alpha$$

$$x_i \equiv \frac{|A_i||B_i|}{2^{2n}}$$

Concave function attains minm. on vertex of polytope.

Lower Bounding Perimeter

$$Per(R) \geq 2^{n+1} \cdot \min \sum_i \sqrt{x_i}$$

$$0 \leq x_i \leq \beta$$

$$\sum_i x_i = \alpha$$

$$x_i \equiv \frac{|A_i||B_i|}{2^{2n}}$$

Concave function attains minm. on vertex of polytope.

Vertex: $\lfloor \frac{\alpha}{\beta} \rfloor$ co-ordinates $:= \beta$.

1 co-ordinate $= \alpha - \lfloor \frac{\alpha}{\beta} \rfloor \beta$.

Lower Bounding Perimeter

$$OPT \geq 2^{n+1}\left\lfloor \frac{\alpha}{\beta} \right\rfloor \sqrt{\beta}.$$

$$Per(R) \geq 2^{n+1} \min \sum_i \sqrt{x_i}$$

$$0 \leq x_i \leq \beta$$

$$\sum_i x_i = \alpha$$

$$x_i \equiv \frac{|A_i||B_i|}{2^{2n}}$$

$$\simeq 2^{n+1}\left(\frac{\alpha}{\sqrt{\beta}}\right)$$

Concave function attains minm. on vertex of polytope.

Vertex: $\left\lfloor \frac{\alpha}{\beta} \right\rfloor$ co-ordinates $:= \beta$.

1 co-ordinate $= \alpha - \left\lfloor \frac{\alpha}{\beta} \right\rfloor \beta$.

Perimeter of $\mathbb{1}_P$ is High.

Lemma 1: Let t be even. $\Pr_{x,y}\left[\mathbb{1}_{P_{n,t}}(x,y)=1\right] = \Omega\left(\frac{1}{tN^2}\right)$

Perimeter of $\mathbb{1}_P$ is High.

Lemma 1: Let t be even. $\Pr_{x,y}\left[\mathbb{1}_{P_{n,t}}(x,y)=1\right] = \Omega\left(\frac{1}{tN^t}\right)$

$x = (x', -x'')$

$y = (y', y'')$

x', x'', y', y'' are i.i.d $\sim_r [-N, N]^{t/2}$

Perimeter of IIP is High.

Lemma 1: Let t be even.

$$\Pr_{x,y}\left[IIP_{n,t}(x,y)=1\right]=\Omega\left(\frac{1}{tN^{2}}\right)$$

$$x=(x',-x'')$$

$$y=(y',y'')$$

x', x'', y', y'' are i.i.d $\sim_r [-N, N]^{t/2}$

$$\langle x,y\rangle=\underbrace{\langle x',y'\rangle}-\underbrace{\langle x'',y''\rangle}$$

range: $O(tN^{2})$

Perimeter of 1P is High.

Lemma 1: Let t be even.

$$\Pr_{x,y}\left[1P_{n,t}(x,y)=1\right]=\Omega\left(\frac{1}{tN^{\nu}}\right)$$

$x = (x', -x'')$

$y = (y', y'')$

x', x'', y', y'' are i.i.d $\sim_{\nu} [-N, N]^{t/2}$

$\langle x, y\rangle = \langle x', y'\rangle - \langle x'', y''\rangle$

range: $O(tN^{\nu})$

Collision probability $= \Omega\left(\frac{1}{tN^{\nu}}\right)$

Perimeter of $\mathbb{1}_P$ is High.

Lemma 1: Let t be even. $\Pr_{x,y}\left[\mathbb{1}_{P_{n,t}}(x,y)=1\right] = \Omega\left(\frac{1}{tN^2}\right)$

Perimeter of $\mathbb{1}\mathbb{P}$ is High.

Lemma 1: Let t be even. $\Pr_{x,y}\left[\mathbb{1}\mathbb{P}_{n,t}(x,y)=1\right]=\Omega\left(\frac{1}{tN^2}\right)$

Lemma 2: Rectangle $R \subseteq \mathbb{1}\mathbb{P}_{n,t}^{-1}(1) \Rightarrow |R| \leq (4N)^t$

Perimeter of $\mathbb{1}P$ is High.

Lemma 1: Let t be even. $\Pr_{x,y}\left[\mathbb{1}P_{n,t}(x,y)=1\right]=\Omega\left(\frac{1}{tN^2}\right)$

Lemma 2: Rectangle $R \subseteq \mathbb{1}P_{n,t}^{-1}(1) \Rightarrow |R| \leq (4N)^t$

$R = A \times B$.

Prime P, $2N+1 \leq P \leq 4N$

Perimeter of $\mathbb{1}P$ is High.

Lemma 1: Let t be even. $\Pr_{x,y}\left[\mathbb{1}P_{n,t}(x,y)=1\right]=\Omega\left(\frac{1}{tN^2}\right)$

Lemma 2: Rectangle $R \subseteq \mathbb{1}P_{n,t}^{-1}(1) \Rightarrow |R| \leq (4N)^t$

$R = A \times B$.

$A \subseteq F_p^t$, $W = \text{span}(A)$

Prime p, $2N+1 \leq p \leq 4N$ $B \subseteq F^t$ $V = \text{span}(B)$

Perimeter of $\mathbb{1}_P$ is High.

Lemma 1: Let t be even. $\Pr_{x,y}\left[\mathbb{1}_{P_{n,t}}(x,y)=1\right]=\Omega\left(\frac{1}{tN^2}\right)$

Lemma 2: Rectangle $R \subseteq \mathbb{1}_{P_{n,t}}^{-1}(1) \Rightarrow |R| \le (4N)^t$

$R = A \times B$.

$A \subseteq F_p^t$, $W = \mathrm{span}(A)$ $W \perp V$

Prime p, $2M+1 \le p \le 4M$ $B \subseteq F^t$ $V = \mathrm{span}(B)$ $\Rightarrow \dim(W)+\dim(V) \le t \le (4N)^t$

Perimeter of $\mathbb{1}\mathbb{P}$ is High.

Lemma 1: Let t be even. $\Pr_{x,y}\left[\mathbb{1}\mathbb{P}_{n,t}(x,y)=1\right]=\Omega\left(\frac{1}{tN^2}\right)$

Lemma 2: Rectangle $R \subseteq \mathbb{1}\mathbb{P}_{n,t}^{-1}(1) \Rightarrow |R| \leq (4N)^t$

$\alpha = \Omega\left(\frac{1}{tN^2}\right)$, $\beta \leq \frac{(4N)^t}{(2N+1)^{2t}} \leq \frac{1}{N^t}$

Perimeter of Π_P is High.

Lemma 1: Let t be even. $\Pr_{x,y}\left[\Pi_{P_{n,t}}(x,y)=1\right] = \Omega\left(\frac{1}{tN^2}\right)$

Lemma 2: Rectangle $R \subseteq \Pi_{P_{n,t}}^{-1}(1) \Rightarrow |R| \leq (4N)^t$

$\alpha = \Omega\left(\frac{1}{tN^2}\right)$, $\beta \leq \frac{1}{N^t}$

$$\text{Per}\left(\Pi_{P_{n,t}}\right) \geq N^t \cdot \left(\frac{\alpha}{\sqrt{\beta}}\right) \geq N^t \cdot N^{t/2-2}$$

D^{EQ} Cost of IIP

Let $D^{EQ}(IIP_{n,t}) = c$

$$N^t \cdot N^{t/2-2} \leq Per(IIP_{n,t}) \leq (2t \log N)^c \cdot (2N^t)$$

D^{EQ} Cost of IIP

Let $D^{EQ}(IIP_{n,t}) = c$

$$N^t \cdot N^{t/2-2} \leq Per(IIP_{n,t}) \leq (2t \log N)^c \cdot (2N^t)$$

$$\Rightarrow c \geq \Omega\left(\frac{t \log N}{\log t \log N}\right) = \Omega\left(\frac{tn}{\log n}\right).$$

Conclusion.

$RP \not\subseteq P^{EQ} \Rightarrow P^{EQ} \subsetneq BPP$

$D^{EQ}(11P_{t,n}) = \Omega\left(\frac{n}{\log n}\right)$ → improves $\Omega(n)$.

Conclusion.

$RP \not\subseteq P^{EQ} \Rightarrow P^{EQ} \subsetneq BPP$

$D^{EQ}(IIP_{t,n}) = \Omega\left(\frac{n}{\log n}\right)$ → improves $\Omega(n)$.

$D^{EQ}(DISJ_n) = \Omega(n)$.

Conclusion.

$RP \not\subseteq P^{EQ} \Rightarrow P^{EQ} \subsetneq BPP$

$D^{EQ}(IIP_{t,n}) = \Omega\left(\frac{n}{\log n}\right)$ → improves $\Omega(n)$.

$D^{EQ}(DISJ_n) = \Omega(n)$.

Consequence:

TC^0 circuits need $\Omega(n)$ size for $DISJ_n$.