Randomness in Query & Communication

Arkadev Chattopadhyay

Question: How much Computational Advantage does Randomness Provide?

Question: How much Computational Advantage does Randomness provide?

General Algorithms: Unknown !

Complexity Theoretic Evidence Only Polynomial.

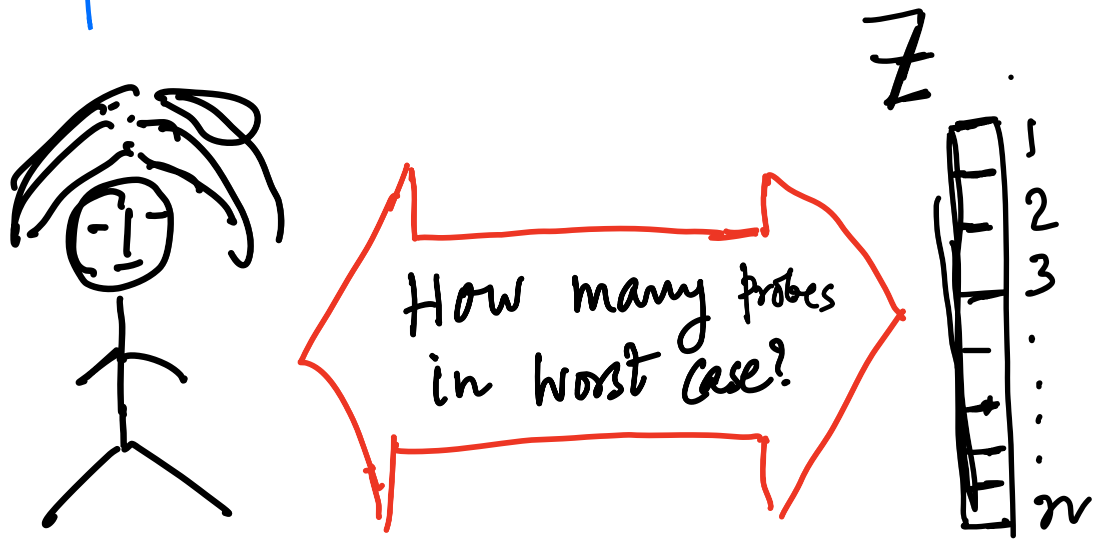
Question: How much Computational Advantage does Randomness Provide?

General Algorithms: Unknown !

Complexity Theoretic Evidence Only Polynomial.

$\boxed{\text{No Known Unconditional Answers!}}$

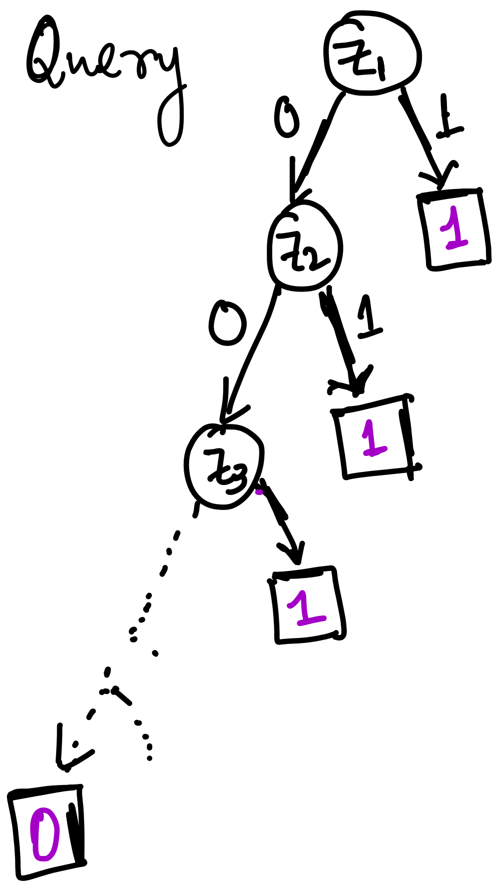
Two Simple Models - I

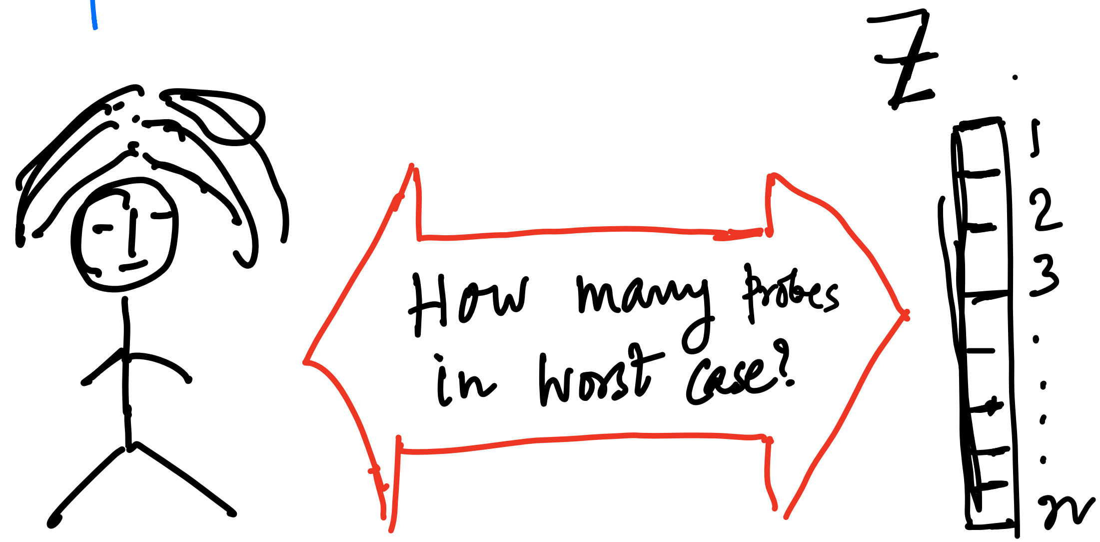


Is there a 1 ?

Two Simple Models - I

1. Query

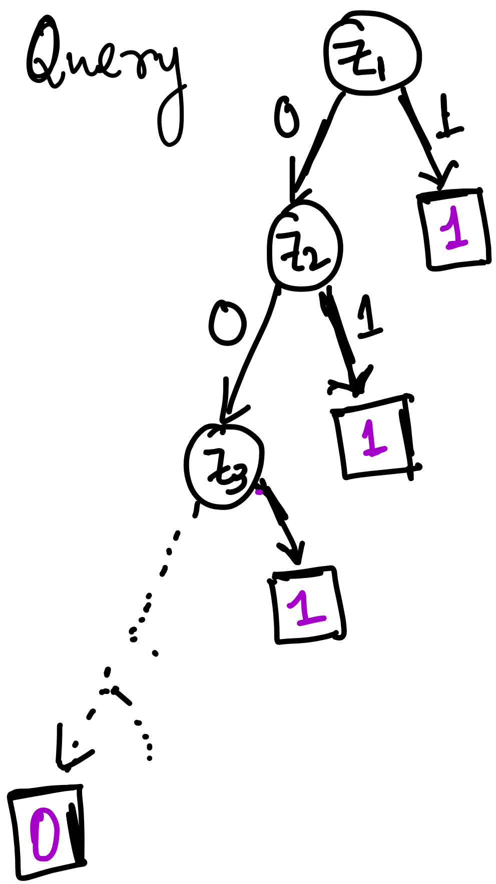


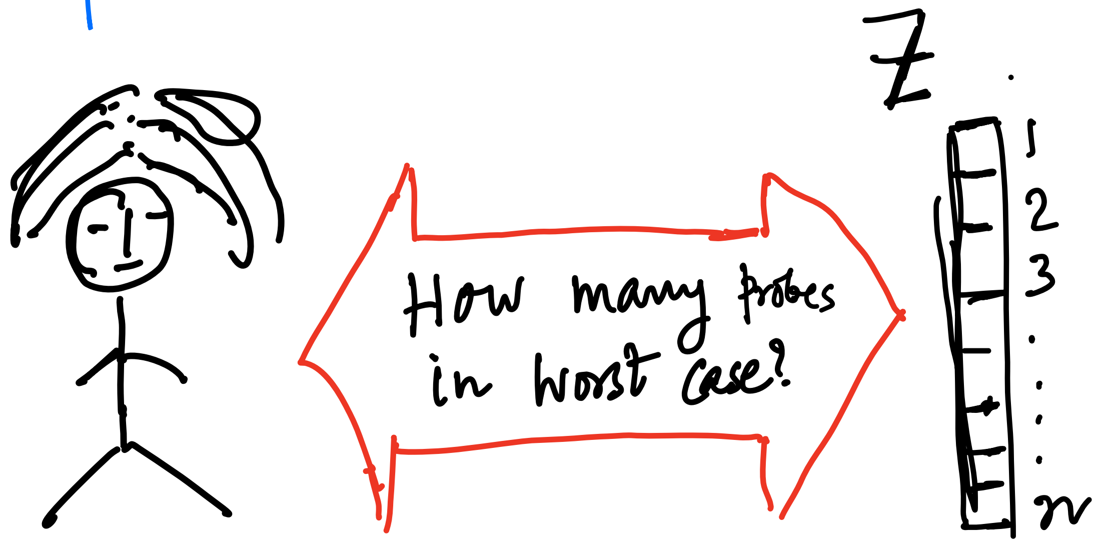


Is there a 1?

Two Simple Models - I

1. Query



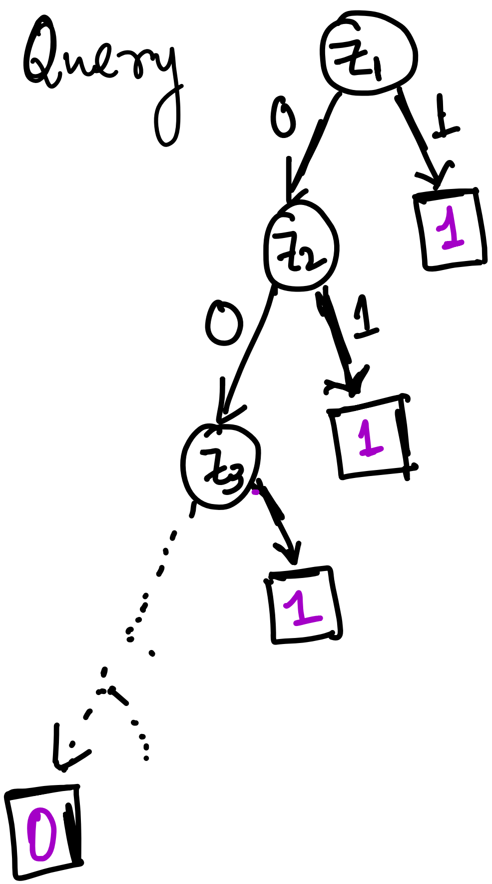


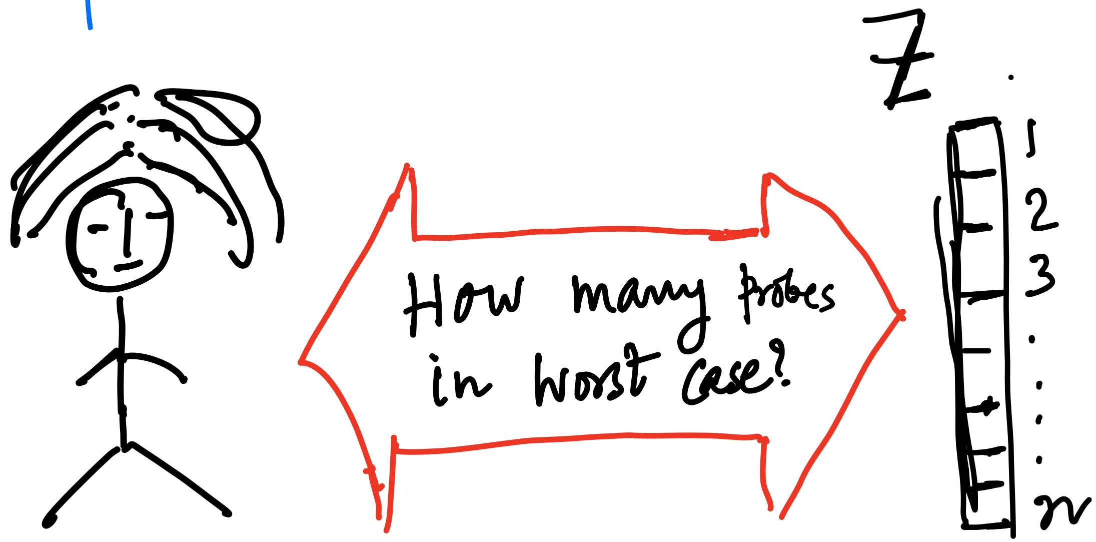
Is there a 1?

$D(OR) = n$ $\quad R(OR) = n$

Two Simple Models - I

1. Query



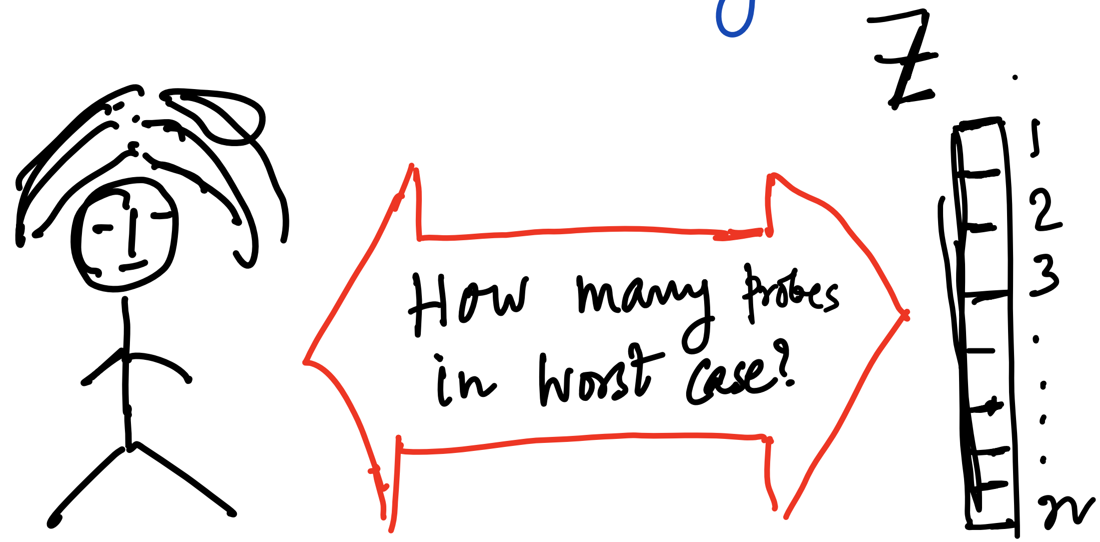


Is there a 1?

$D(OR) = n$ $R(OR) = n$

Does Randomness ever help?

How About Sampling.



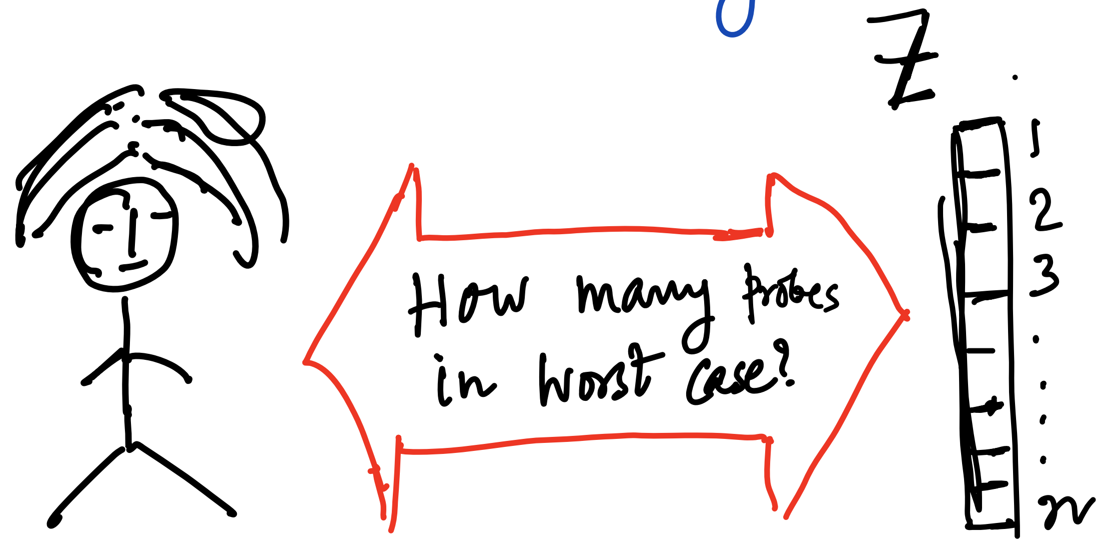
Promise

$$|Z| \geq \frac{1}{2}$$

or

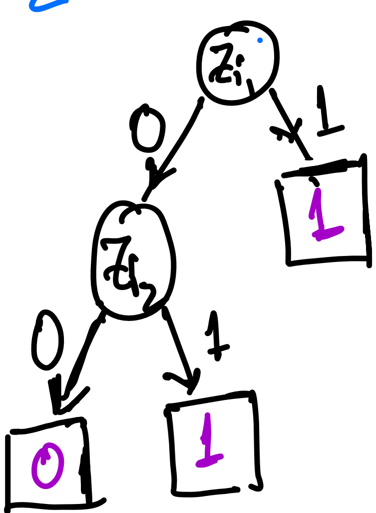
$$|Z| = 0$$

How About Sampling.



Sample at random 2 bits

i_1, i_2



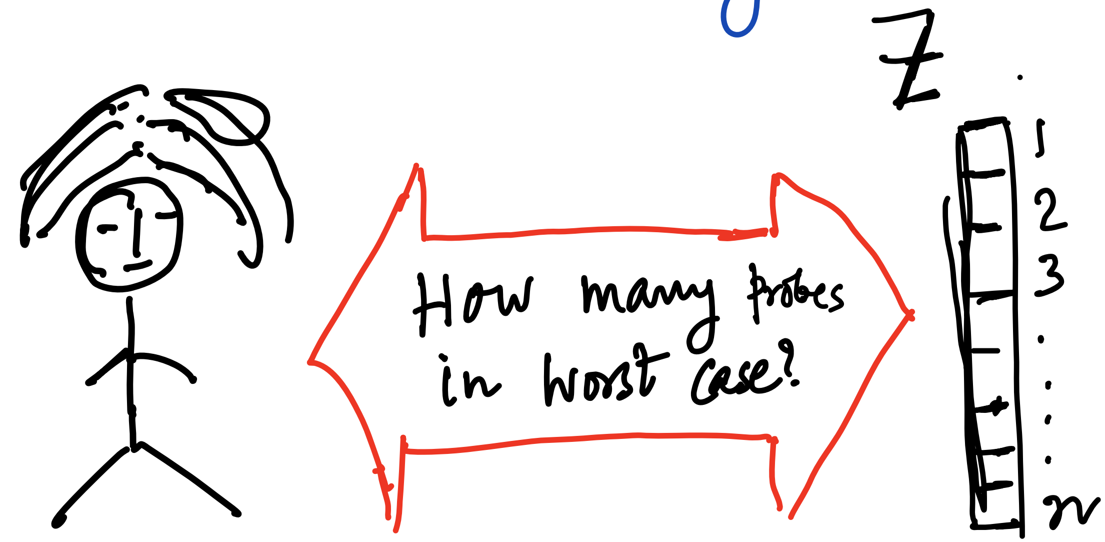
Promise

$$|Z| \geq \frac{1}{2}$$

or

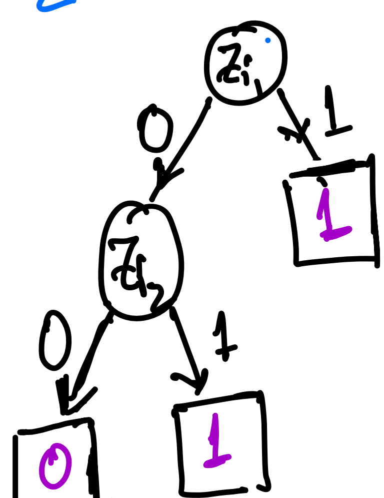
$$|Z| = 0$$

How About Sampling.



Sample at random 2 bits

i_1 , i_2



Promise

$$|Z| \geq \frac{1}{2}$$

or

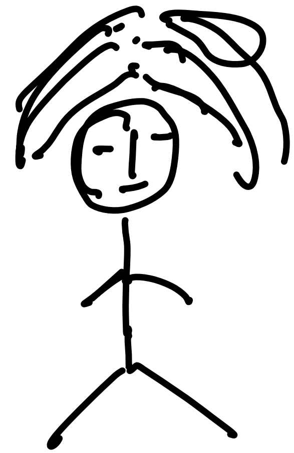
$$|Z| = 0$$

$$D(\text{Promised-OR}) = \Theta(n)$$
$$R(\text{Promised-OR}) = O(1)$$

How About Sampling.

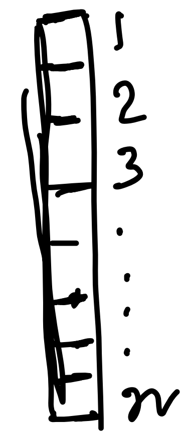
Total functions?

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



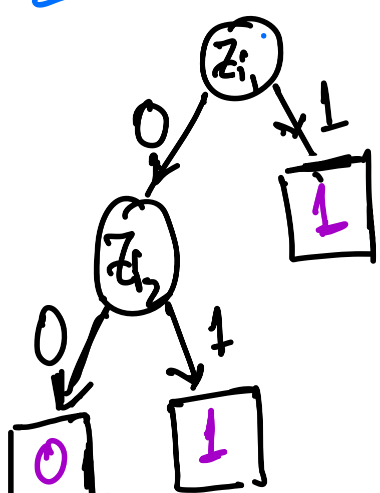
How many probes in worst case?

Z



Sample at random 2 bits

i_1 , i_2



Promise

$$|Z| \geq \frac{1}{2}$$

or

$$|Z| = 0$$

$$\boxed{\begin{aligned} D(\text{Promised-OR}) &= \Theta(n) \\ R(\text{Promised-OR}) &= O(1) \end{aligned}}$$

Limited Power of Randomness

Theorem (Nisan '89):

$$D(f) \leq \overbrace{bs^3(f) \leq R^3(f)}$$

$\forall f_{\text{total}}$

Limited Power of Randomness

Theorem (Nisan '89):

$$R^2(f) \overset{\exists f}{\le} D(f) \overbrace{\le bs^3(f) \le R^3(f)}$$

$\forall f_{\text{total}}$

Mukhopadhyay-Sanyal '15

Ambainis-Balodis-Belovs-Lee-Santha-Smotrovs '16

Limited Power of Randomness

Theorem (Nisan '89):

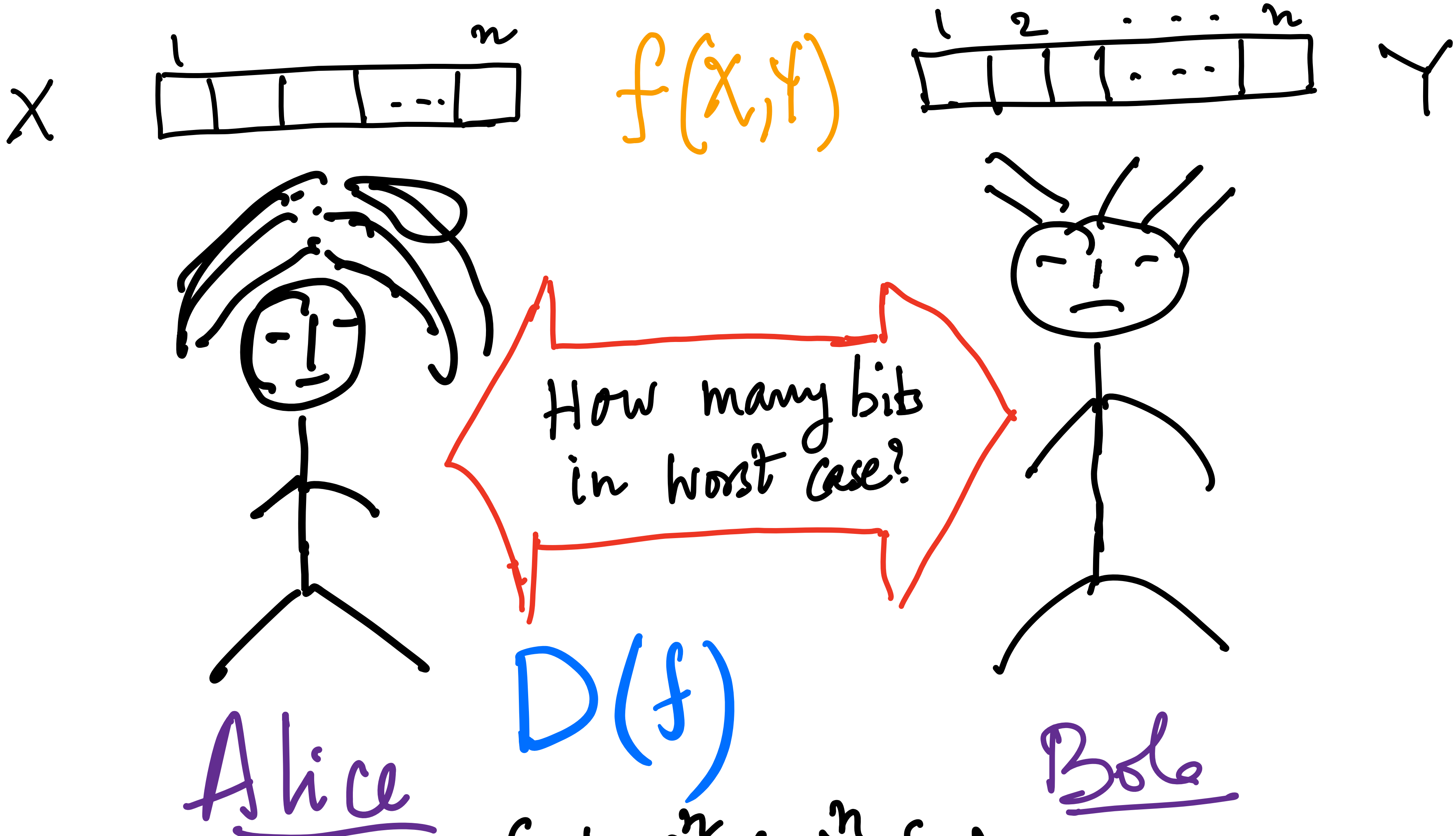
$$R^2(f) \underset{\nexists f}{\leq} D(f) \leq \underbrace{bs^3(f) \leq R^3(f)}_{\forall f_{\text{total}}}$$

Mukhopadhyay-Sanyal '15

Ambainis-Balodis-Belovs-Lee-Santha-Smotrovs '16

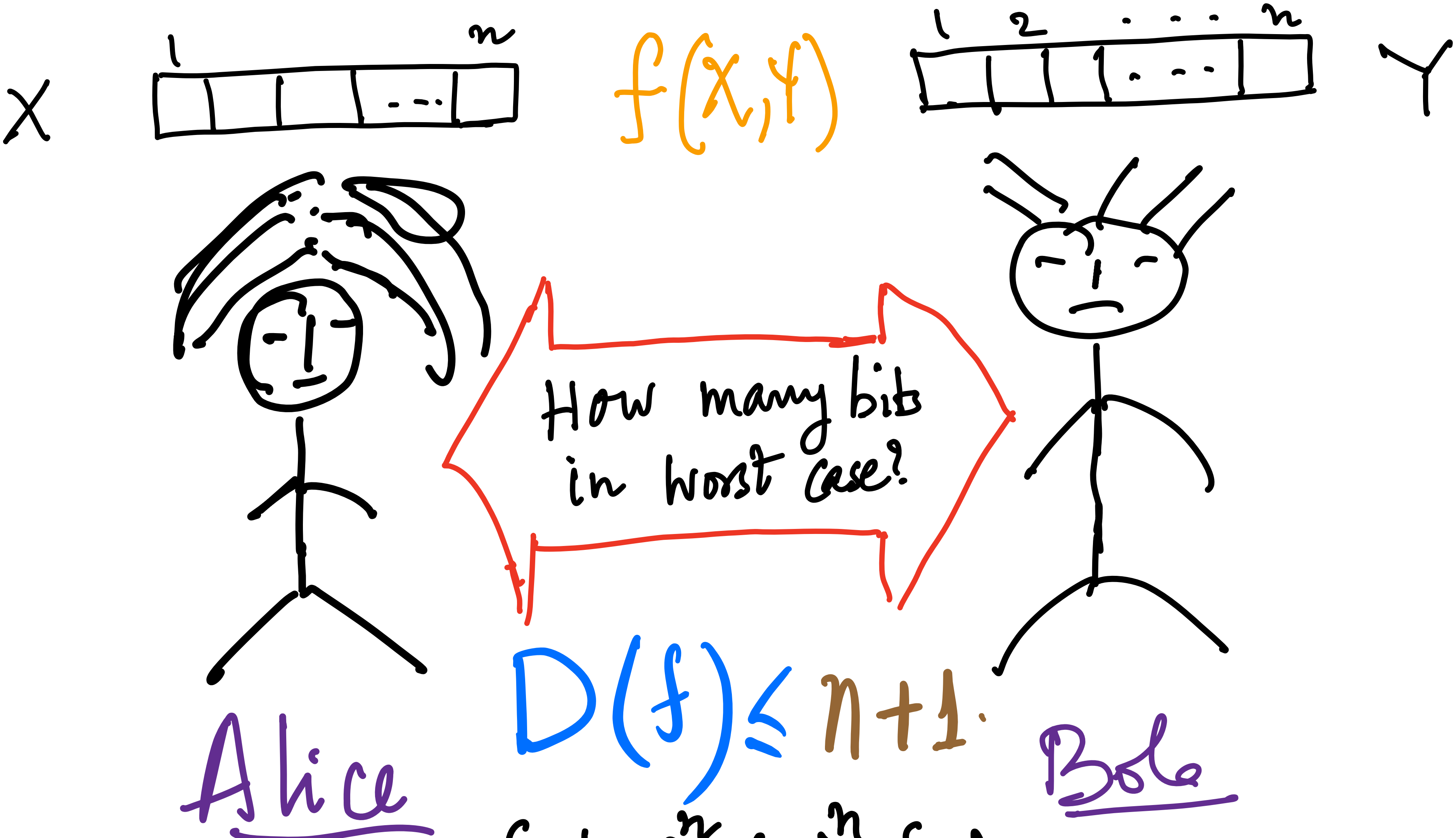
Open: What is the right exponent $2 \leq \alpha \leq 3$?

Simple Model - II



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

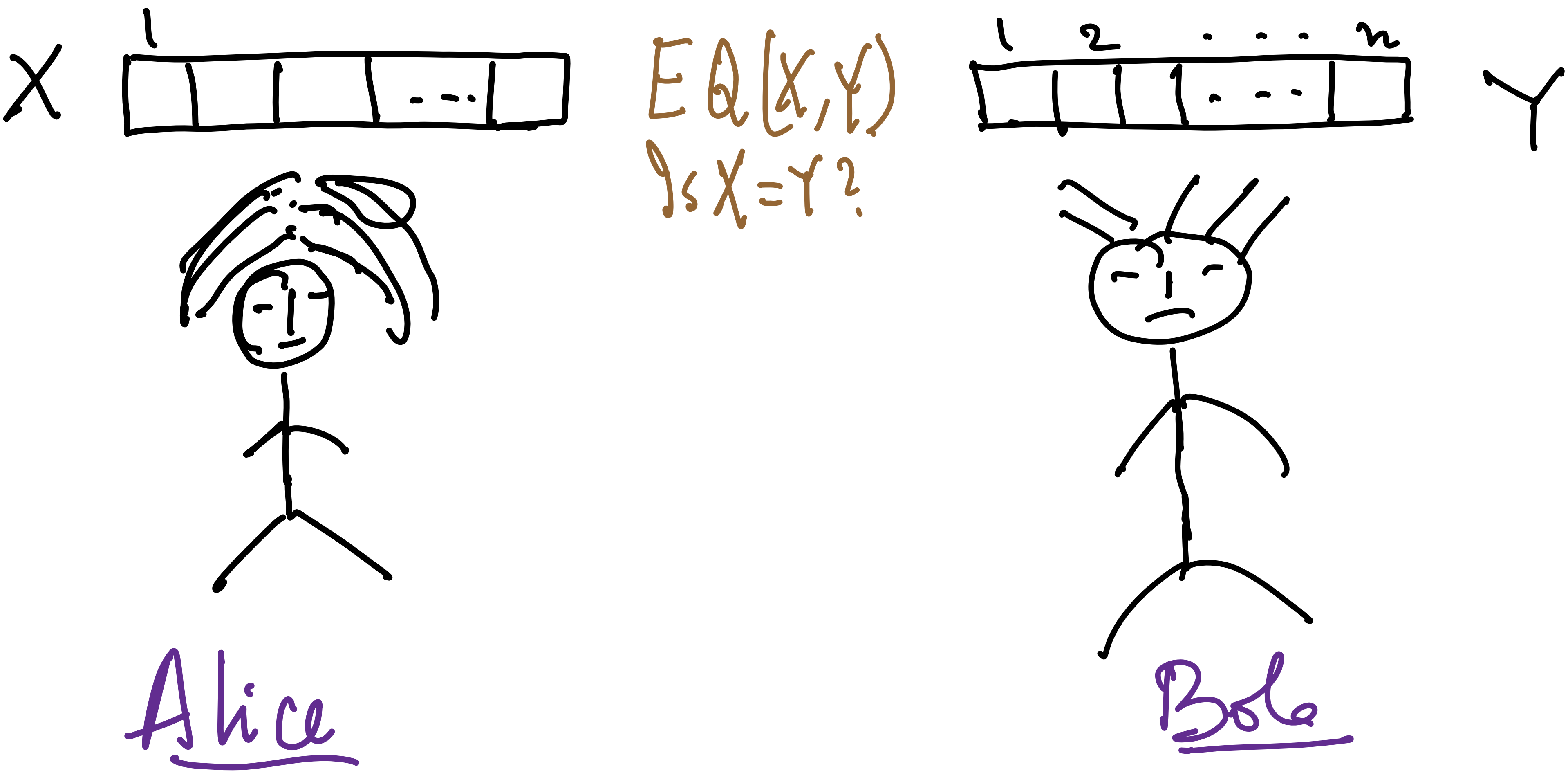
Simple Model - II



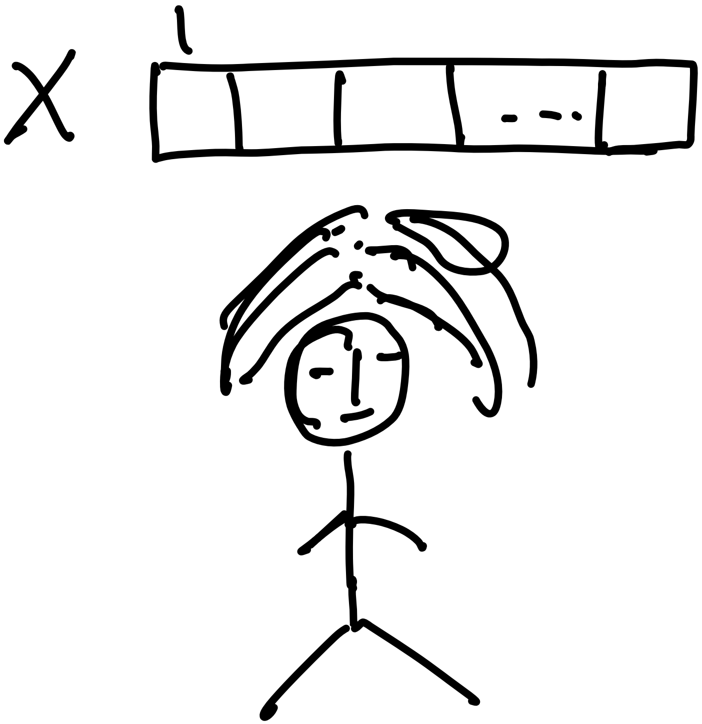
$D(f) \leq n+1$.

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

Equality: Analog of OR



Equality: Analog of OR

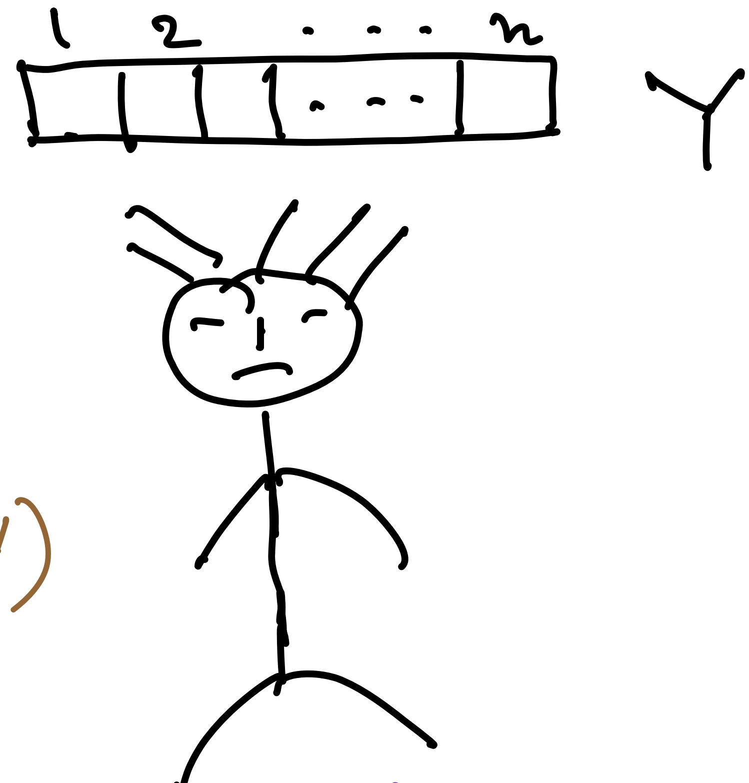


EQ(X, Y)

Is X = Y ?

$EQ(0^n, Y)$

$= NOR(Y)$

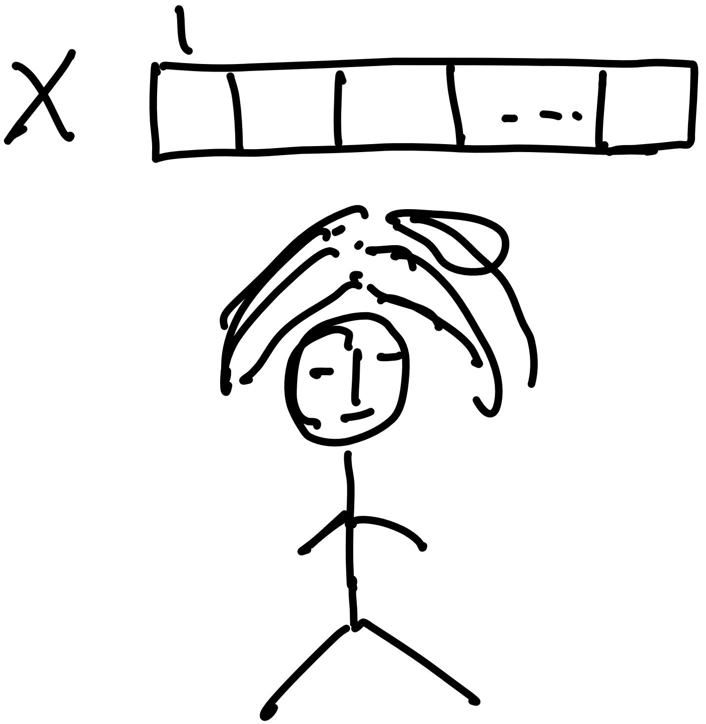


Alice

Bob

Equality: Analog of OR

$D(EQ) = n+1$



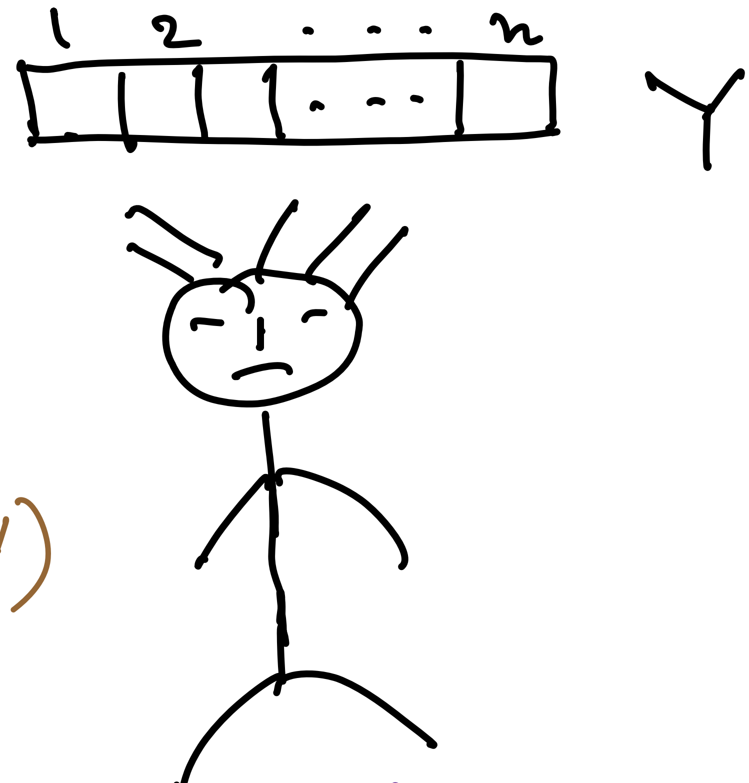
Alice

$EQ(X, Y)$

Is $X = Y$?

$EQ(0^n, Y)$

$= NOR(Y)$



Bob

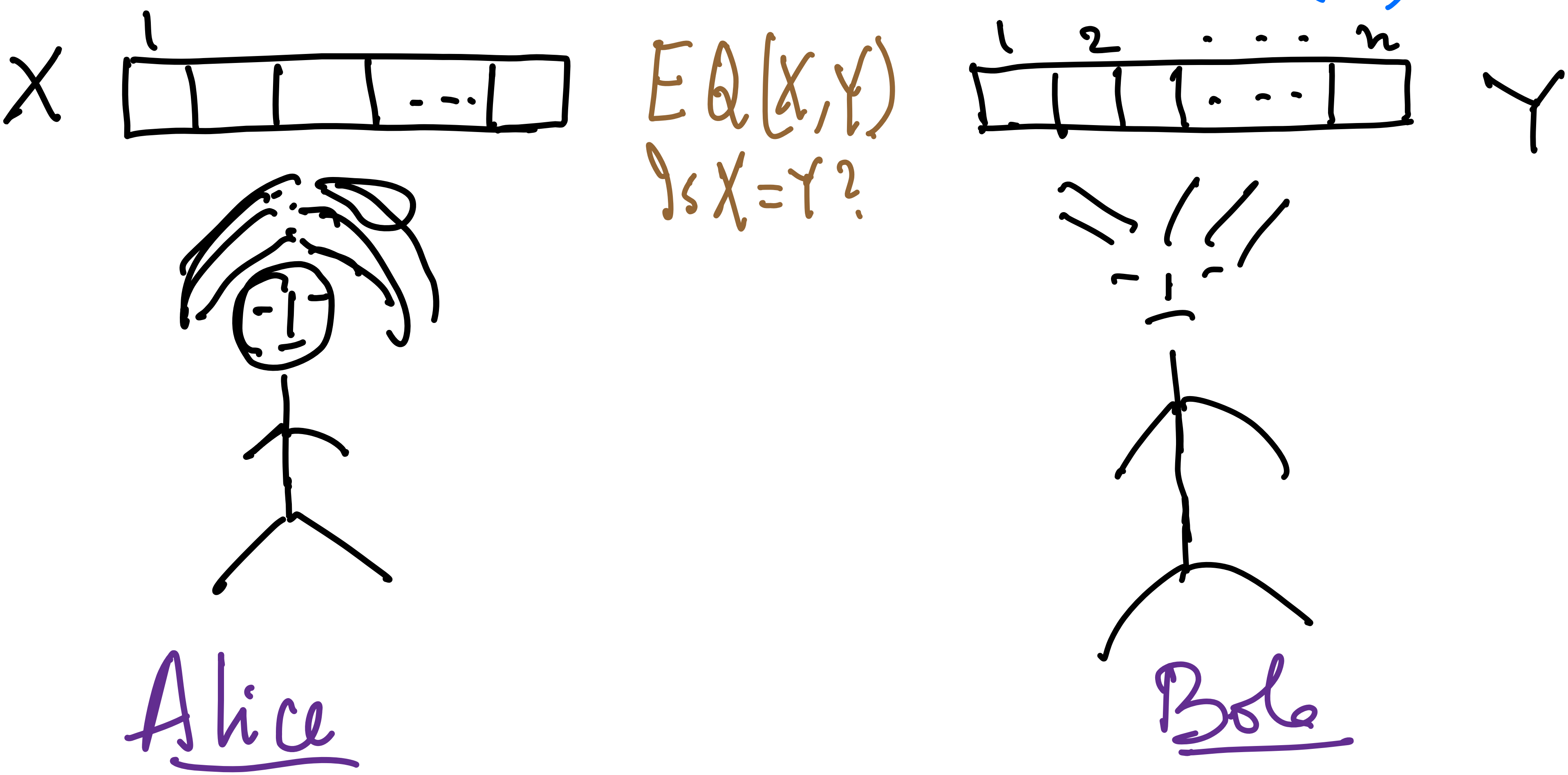
Power Of Randomness

Random $r \in \{0,1\}^n$

$D(EQ) = n+1$

$EQ(X,Y)$

Is $X = Y$?



Power Of Randomness

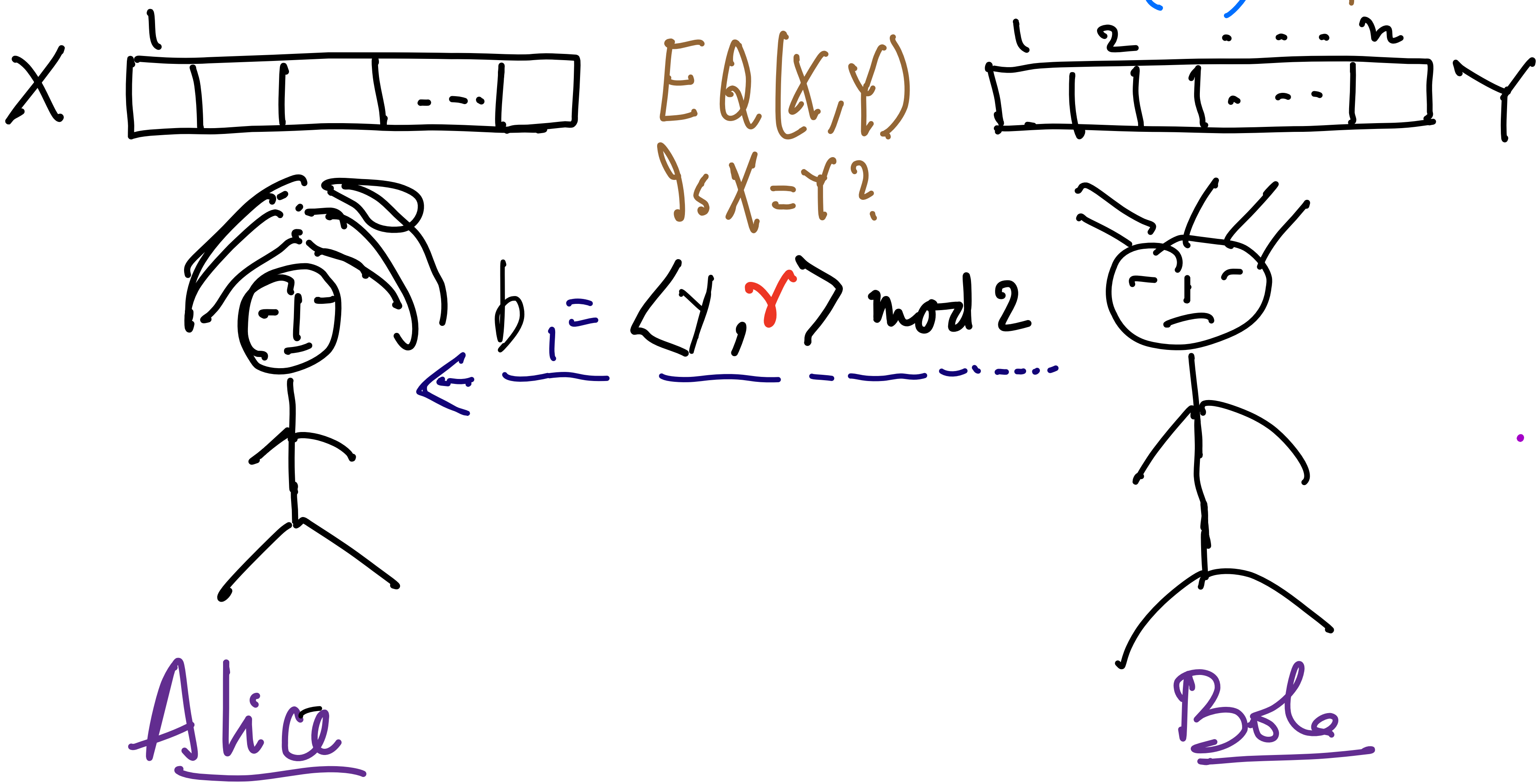
Random $r \in \{0,1\}^n$

$D(EQ) = n+1$

$EQ(X,Y)$

Is $X = Y$?

$b_1 = \langle Y, r \rangle \bmod 2$



Power Of Randomness

Random $r \in \{0,1\}^n$

$D(EQ) = n+1$

X: $[\,1 \mid \;\mid \;\mid \cdots \mid \;]$

Y: $[\,1 \mid 2 \mid \;\mid \cdots \mid n\,]$

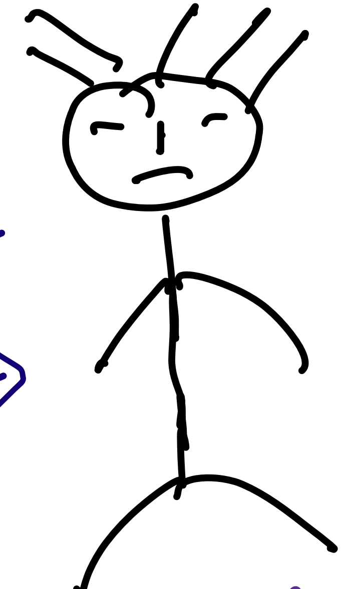
$EQ(X,Y)$

Is $X = Y$?

$b_1 = \langle Y, r \rangle \bmod 2$

Answer!

Is $b_1 = \langle X, r \rangle \bmod 2$



Bob

Power Of Randomness

Random $r \in \{0,1\}^n$ $\quad D(EQ) = n+1$

X $\quad$ 1 $\quad$ . . . $\quad\quad$ $EQ(X,Y)$ $\quad\quad$ 1 $\quad$ 2 $\quad$ . . . $\quad$ n $\quad$ Y

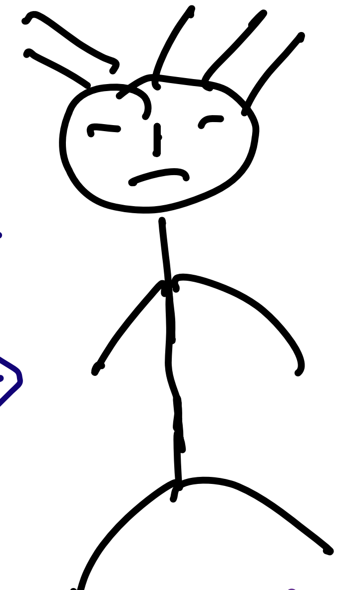
Is $X=Y$?

o o o o

Is $b_1 = \langle x, r \rangle \bmod 2$

$b_1 = \langle y, r \rangle \bmod 2$

Answer!



Alice $\quad\quad$ Bob

If $X \neq Y$

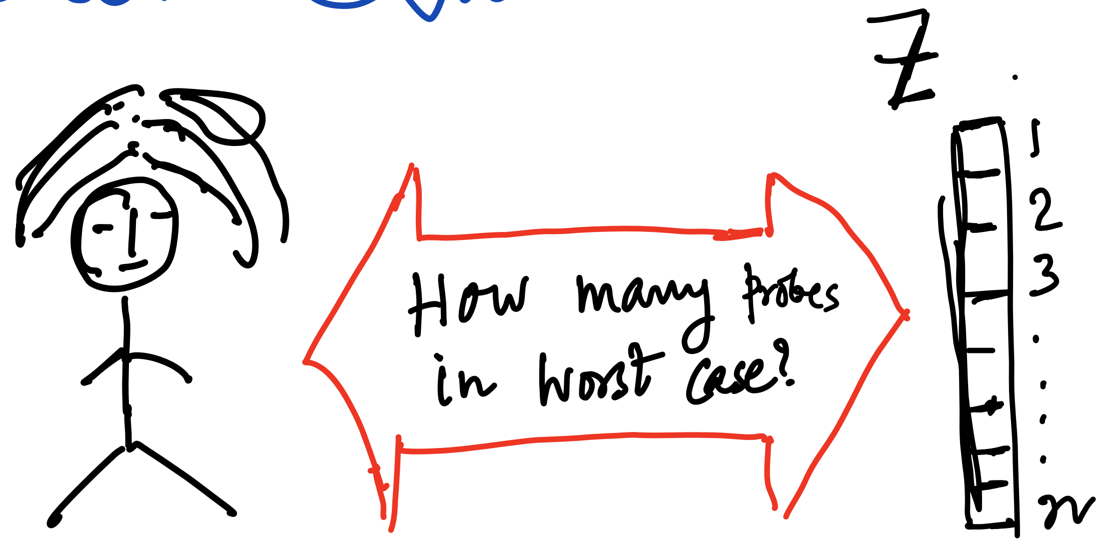
$$\Pr_{r}\left[\langle x,r \rangle \not\equiv \langle y,r \rangle \bmod 2\right] = \frac{1}{2}$$

Richer Queries.

Query fns.

$$Q := \left\{ \bigoplus_{i \in S} Z_i \;\middle|\; S \subseteq [n] \right\}$$

Parity Decision Tree



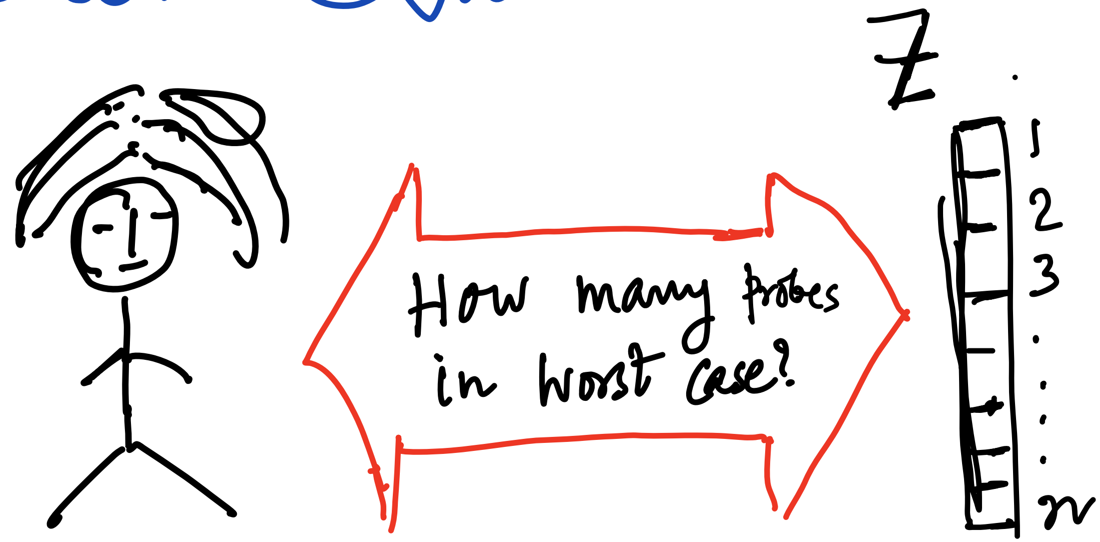
Is there an i s.t. $Z_i = 1$.

Richer Queries.

Query fns.

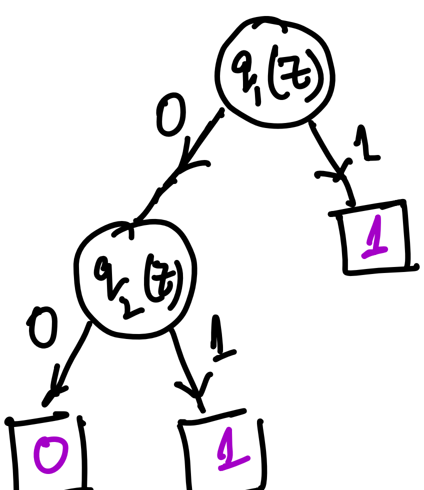
$Q := \{ \bigoplus_{i \in S} z_i \mid S \subseteq [n] \}$

Parity Decision Tree



Is there an i s.t. $z_i = 1$.

Sample randomly $q_1, q_2 \in Q$.



$R_\oplus(OR) = O(1)$

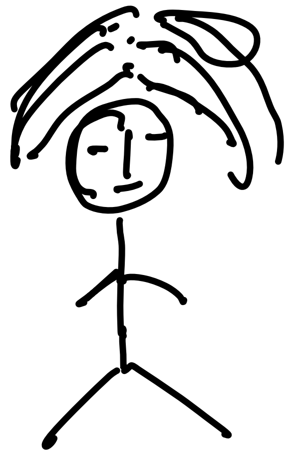
$D_\oplus(OR) = n$

Richer Queries

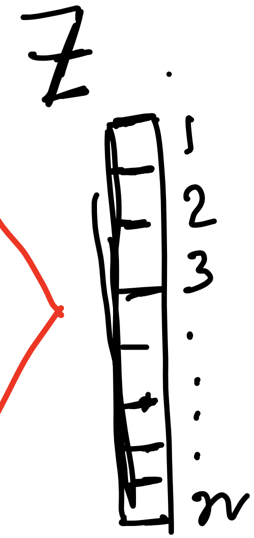
Query fns:

$$Q := \left\{ \bigoplus_{i \in S} z_i \;\middle|\; S \subseteq [n] \right\}$$

Parity Decision Tree



How many probes in worst case?

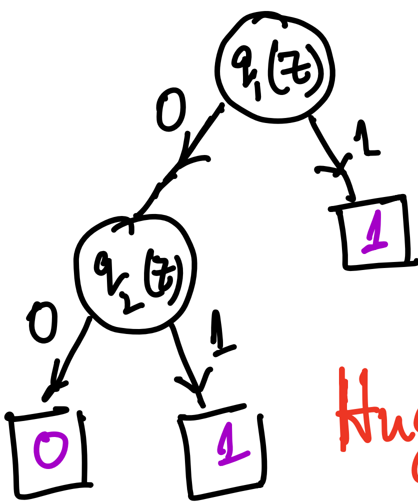


Is there an i s.t. $z_i = 1$.

Sample randomly $q_1, q_2 \in Q$.

$$R_\oplus(OR) = O(1)$$

$$D_\oplus(OR) = n$$



Huge power of Randomness!

AND Decision Trees

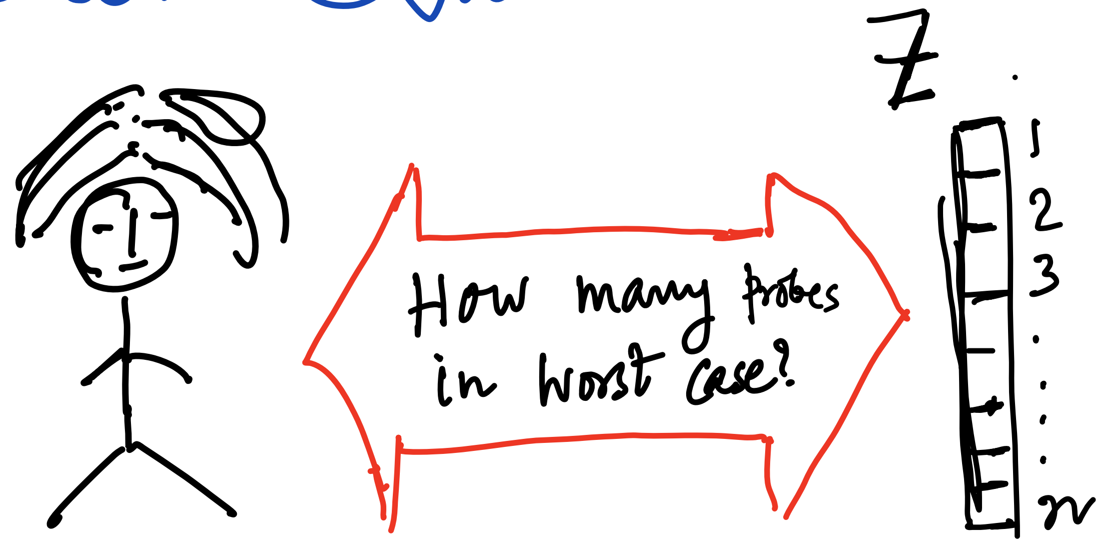
$$Q = \left\{ \bigwedge_{i \in S} z_i \;\middle|\; S \subseteq [n] \right\}$$

Richer Queries.

Query fns.

$$Q := \left\{ \bigoplus_{i \in S} z_i \;\middle|\; S \subseteq [n] \right\}$$

Parity Decision Tree

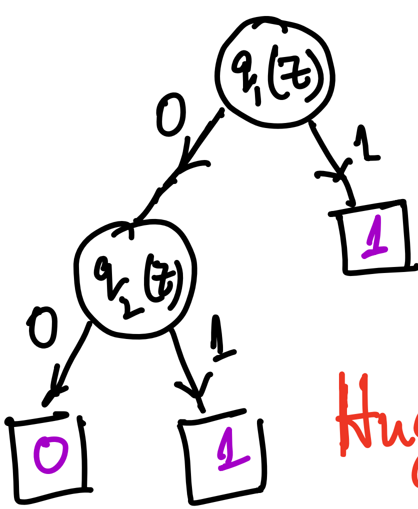


Is there an i s.t. $z_i = 1$.

Sample randomly $q_1, q_2 \in Q$.

$R_{\oplus}(OR) = O(1)$

$D_{\oplus}(OR) = n$



Huge power of Randomness!

AND Decision Trees

$$Q = \left\{ \bigwedge_{i \in S} z_i \;\middle|\; S \subseteq [n] \right\}$$

What is the power of Randomness in ADT?

Knop-Lovett-McGuire-Yuan-2021

Question: How much Computational Advantage does Randomness Provide for ADT's?

Knop-Lovett-McGuire-Yuan-2021

Question: How much Computational Advantage does Randomness provide for ADT's?

Theorem (C-Dahiya-Mande-Radhakrishnan-Sanyal-23)

For every total f,
$$D_{\wedge}(f) = \tilde{O}\left(R_{\wedge}^{3}(f)\right)$$
$$D_{\vee}(f) = \tilde{O}\left(R_{\vee}^{3}(f)\right)$$
$$D_{\vee,\wedge}(f) = \tilde{O}\left(R_{\vee,\vee}^{4}(f)\right)$$

Some Intuition & Observations.

Computing $\vee$ by ADT:

OR: $\boxed{0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0} \to 0$

- Adversary keeps answering 0
- Fixes one bit to 0/query.

$$D_{\wedge}(OR) = n$$

$$R_{\wedge}(OR) = n.$$

Some Intuition & Observations.

Computing $\vee$ by ADT:

OR: $\boxed{0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0} \to 0$

OR: $\boxed{1\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0} \to 1$

Adversary keeps answering 0

Fixes one bit to 0/query.

$D_\wedge(OR) = n$

$R_\wedge(OR) = n$.

Some Intuition & Observations.

Computing $\vee$ by ADT:

OR:

0	0	0	0	0	0	0	0	0	$\to 0$

OR:

1	0	0	0	0	0	0	0	0	$\to 1$

⋮

OR:

0	0	0	0	0	0	0	0	1	$\to 1$

Adversary keeps answering 0

Fixes one bit to 0/query.

$D_\wedge(OR) = n$

$R_\wedge(OR) = n$.

Some Intuition & Observations.

Computing $\vee$ by ADT:

OR: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $\rightarrow 0$

0-sensitive blocs.

OR: | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $\rightarrow 1$

$\vdots$

OR: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | $\rightarrow 1$

Adversary keeps answering 0
Fixes one bit to 0/query.

$$D_\wedge(OR) = n$$

$$R_\wedge(OR) = n.$$

Some Intuition & Observations.

Computing $\vee$ by ADT:

OR: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $\rightarrow 0$

0-Sensitive blocks.

OR: | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $\rightarrow 1$

⋮

OR: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | $\rightarrow 1$

Adversary keeps answering 0

Fixes one bit to 0/query.

$D_\wedge(OR) = n$

$R_\wedge(OR) = n$.

$HSC_0(x)$ - hitting set complexity of 0 blocks.

Some Intuition & Observations.

Computing $\vee$ by ADT:

OR: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $\to$ 0

0-sensitive blocks.

OR: | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $\to$ 1

$\vdots$

OR: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | $\to$ 1

Adversary keeps answering 0

Fixes one bit to 0/query.

$D_\wedge(OR) = n$

$R_\wedge(OR) = n$.

$HSC_0(x)$ - hitting set complexity of 0 blocks.

$FHSC_0(x) \to$ fractional relaxation

Some Intuition & Observations.

Computing $\vee$ by ADT:

OR: $\boxed{0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0} \to 0$

0-sensitive blocks.

OR: $\boxed{1\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0} \to 1$

$\vdots$

OR: $\boxed{0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,0\,|\,1} \to 1$

maximize over x: HSC_0 $FHSC_0$

Adversary keeps answering 0

Fixes one bit to 0/query.

$D_\wedge(OR) = n$

$R_\wedge(OR) = n$.

$HSC_0(x)$ - hitting set complexity of 0 blocks.

$FHSC_0(x) \to$ fractional relaxation

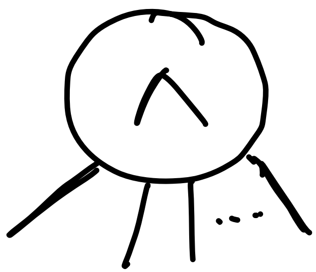
Some Intuition & Observations.

Lemma: $\Omega\left(FHSC_0(f)\right) \leq R_\Lambda(f)$

:

Some Intuition & Observations.

Lemma: $\Omega(\mathrm{FHSC}_0(f)) \leq R_\wedge(f)$

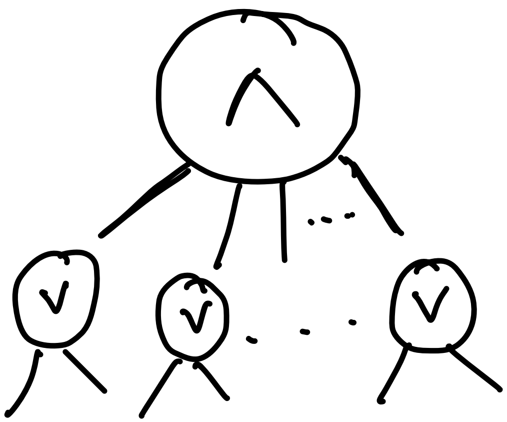


$\mathrm{FHSC}_0(\wedge) = 1$.

Some Intuition & Observations.

Lemma: $\Omega\left(FHSC_0(f)\right) \leq R_\wedge(f)$

:

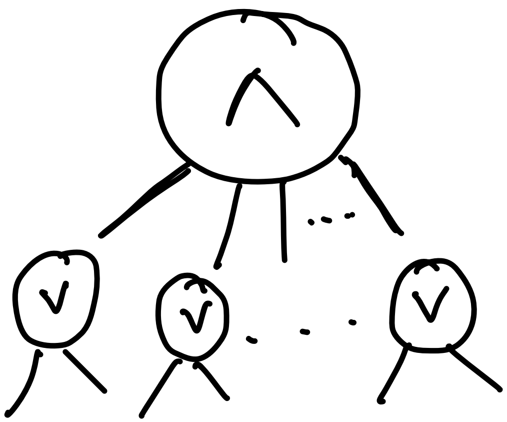


$$FHSC_0\left(\wedge_n \circ \vee_2\right) = 2$$

Some Intuition & Observations.

Lemma: $\Omega(FHSC_0(f)) \leq R_{\wedge}(f)$.

:

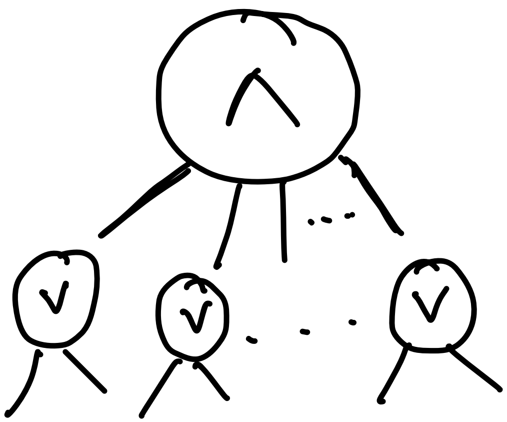


$FHSC_0(\wedge_n \circ \vee_2) = 2$

$R_{\wedge}(\wedge_n \circ \vee_2) = \Omega(n)$.

Some Intuition & Observations.

Lemma: $\Omega(FHSC_0(f)) \leq R_\wedge(f)$



$FHSC_0(\wedge_n \circ \vee_2) = 2$

$R_\wedge(\wedge_n \circ \vee_2) = \Omega(n).$

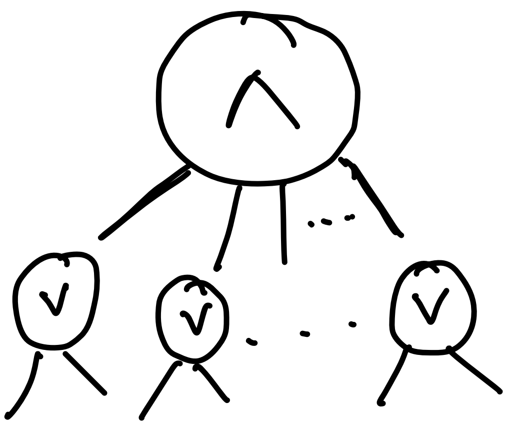
Observation 1: # of min terms $= 2^n$.

Observation 2: Sub-cube cover # of 1's $= 2^n$,

Some Intuition & Observations.

Lemma: $\Omega(FHSC_0(f)) \leq R_\wedge(f)$

:



$$FHSC_0(\wedge_n \circ \vee_2) = 2$$

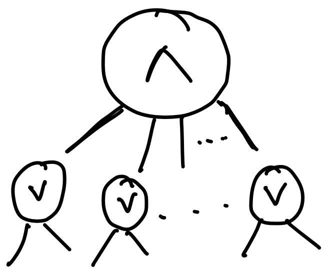
$$R_\wedge(\wedge_n \circ \vee_2) = \Omega(n).$$

Observation 1: # of min terms $= 2^n$.

Observation 2: $\boxed{\text{Sub-cube cover \# of 1's}} = 2^n,$ $\longrightarrow N_1$

Some Intuition & Observations.

Lemma: $\Omega\left(\text{FHSC}_0(f)\right) \leq R_\wedge(f)$



$\text{FHSC}_0(\wedge_n \circ \vee_2) = 2$

$R_\wedge(\wedge_n \circ \vee_2) = \Omega(n)$.

Observation 1: # of min terms $= 2^n$.

Observation 2: $\boxed{\text{Sub-cube Cover \# of 1's}} = 2^n, \quad \to N_1$

Observation 3: $\begin{matrix} N_1(f) \\ N_0(f) \end{matrix} \leq \text{DSize}(f) \leq n^{D_\wedge(f)}$

Cover Number

Lemma: $\tilde{\Omega}\left(\sqrt{\log N(f)}\right) \leq R_{\wedge}(f)$.

Cover Number

Lemma: $\tilde{\Omega}\left(\sqrt{\log N(f)}\right) \leq R_\wedge(f)$.

Matching Upper Bound.

Lemma: $D_\wedge(f) = O\left(\mathrm{FHSC}_0(f) \cdot \log N(f)\right)$

Mystery - I: Parity Decision Tree

Recall: $D_{\oplus}(OR) = n, \quad R_{\oplus}(OR) = O(1).$

What if OR is free?

Mystery - I: Parity Decision Tree

Recall: $D_{\oplus}(OR) = n$, $R_{\oplus}(OR) = O(1)$.

What if OR is free?

i.e. Affine space detection is free!

Mystery-I: Parity Decision Tree

Recall: $D_{\oplus}(OR) = n$, $R_{\oplus}(OR) = O(1)$.

What if OR is free?

i.e. Affine space detection is free!

Conjecture: $D_{\text{Affine}}(f) = \left(R_{\oplus}(f)\right)^{O(1)}$

Basic Question on PDT.

$N^1_\oplus(f)$: Affine cover of 1's of f

$N^0_\oplus(f)$: Affine cover of 0's of f

Conjecture:

$$D^\perp_\oplus(f) \leq n^{\text{poly-log}(N^1_\oplus(f), N^0_\oplus(f))}$$

Theorem (Ehrenfeucht–Haussler '80's)

$$D^\perp(f) \leq n^{O(\log(N^1(f)) \cdot \log(N^0(f)))}$$

Mystery - II: Communication

Question: How powerful are randomized protocols?

Question: What if we give EQ for free?

Solves GT, Halfspaces, several others.

Question (Implicit in BFS'89): Does EQ simulate Randomness? (total fns).

Equality is not Enough

Theorem: (C-Lovett-Vinyals)

EQ does not efficiently simulate Randomness.

Equality is not Enough

Theorem: (C-Lovett-Viruyals)

EQ does not efficiently simulate Randomness.

$$\|P_t\left(x_1, x_2, \dots, x_t, y_1, y_2, \dots, y_t\right); \quad x_i, y_i \in \mathbb{Z}$$

$$= \begin{cases} 1 & \text{if } \langle x_i, y_i \rangle = 0 \\ 0, & \text{otherwise} \end{cases}$$

$t \geq 5$ is a constant.

Question : What if we give Set-Disjointness for free?

Is $BPP \subseteq P^{NP}$?

Question: What if we give Set-Disjointness for free?

Is $BPP \subseteq P^{NP}$?

Is $BPP^{O} \subseteq P^{NP}$?

Question: What if we give Set-Disjointness for free?

Is $BPP \subseteq P^{NP}$?

Is $BPP^0 \subseteq P^{NP}$?

Is $BPP^0 \subseteq P^{EQ}$?

Thank You!