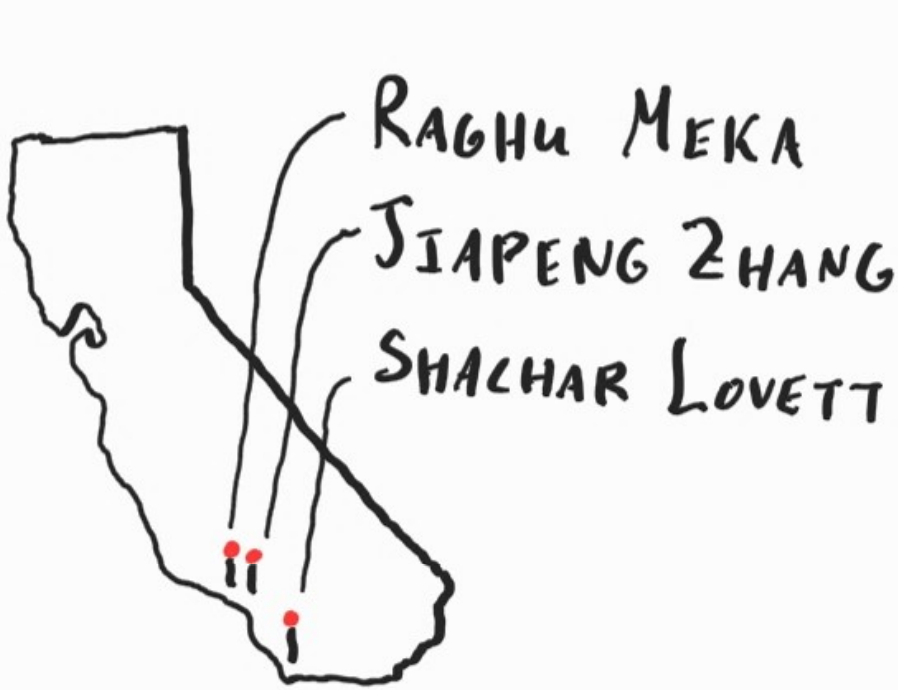
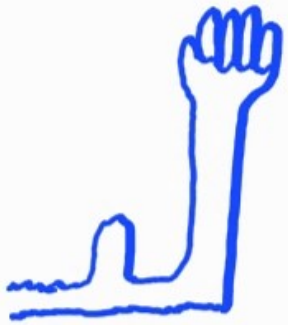
Lifting With Sunflowers

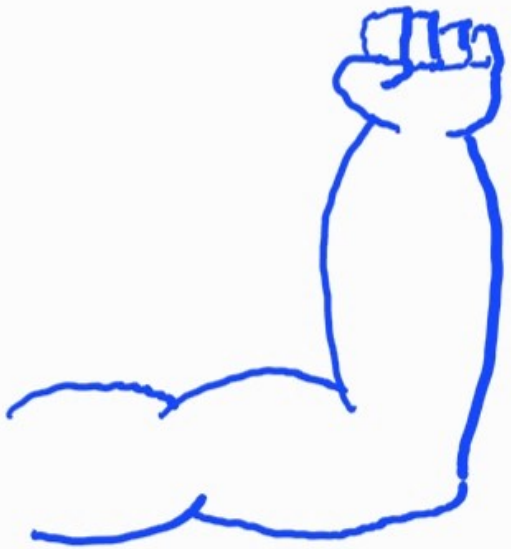
Ian Mertz
University of Toronto
2021.09.06

Joint Work With...

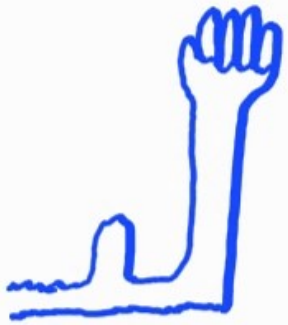


Computation Models





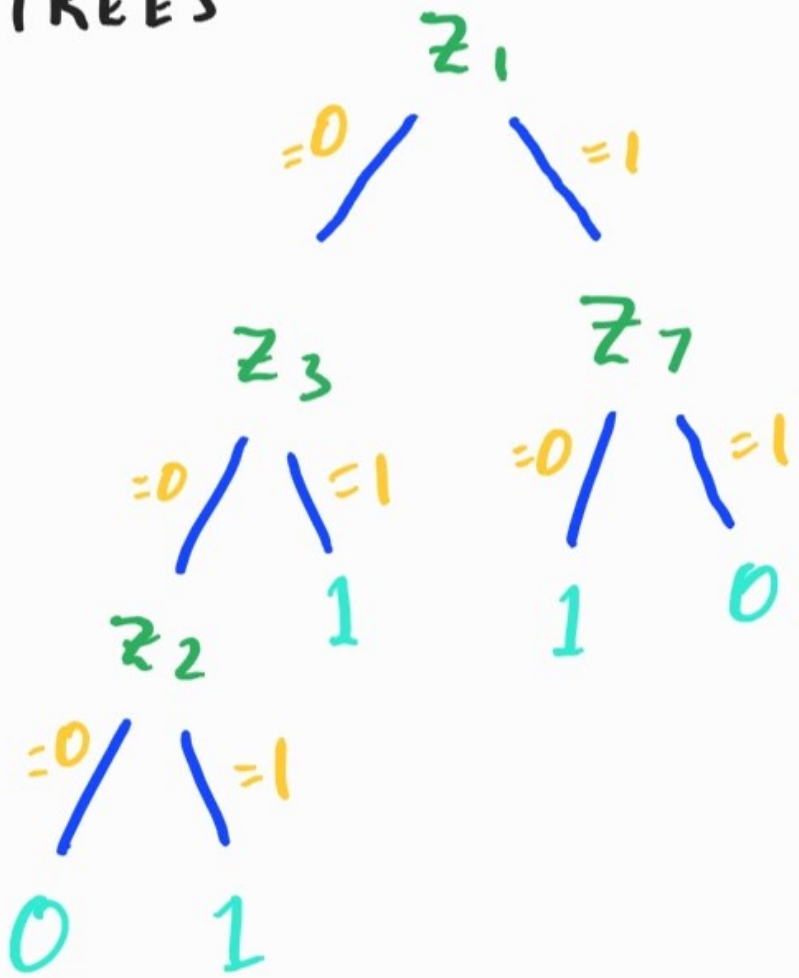
Computation Models



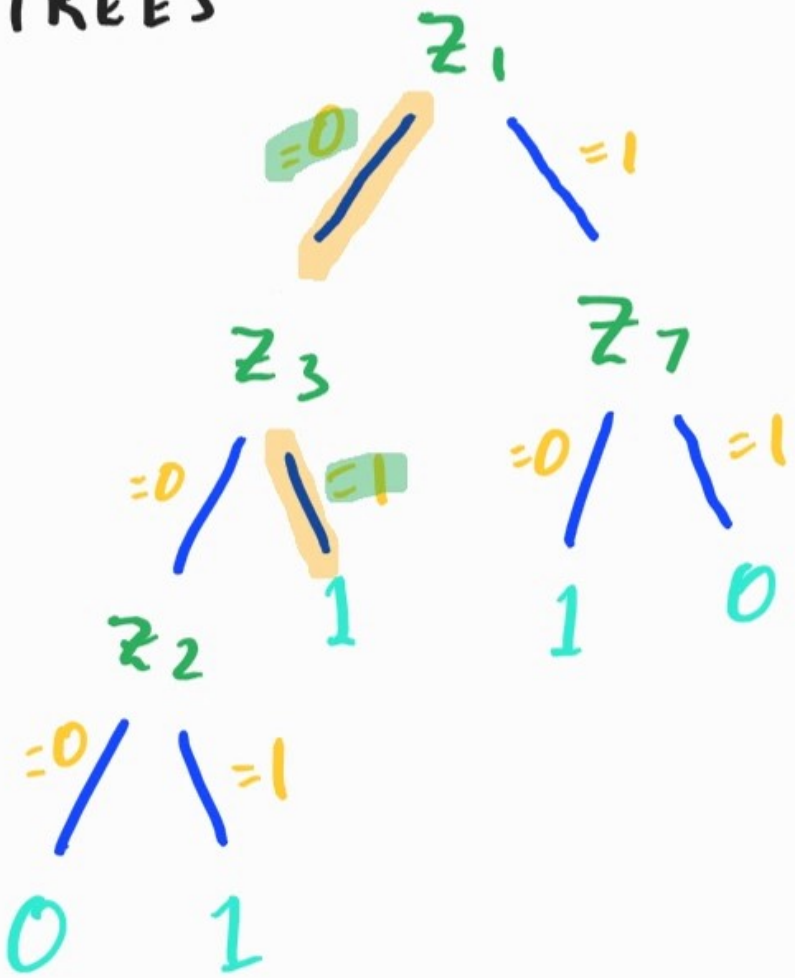
decision trees

communication complexity

Decision Trees

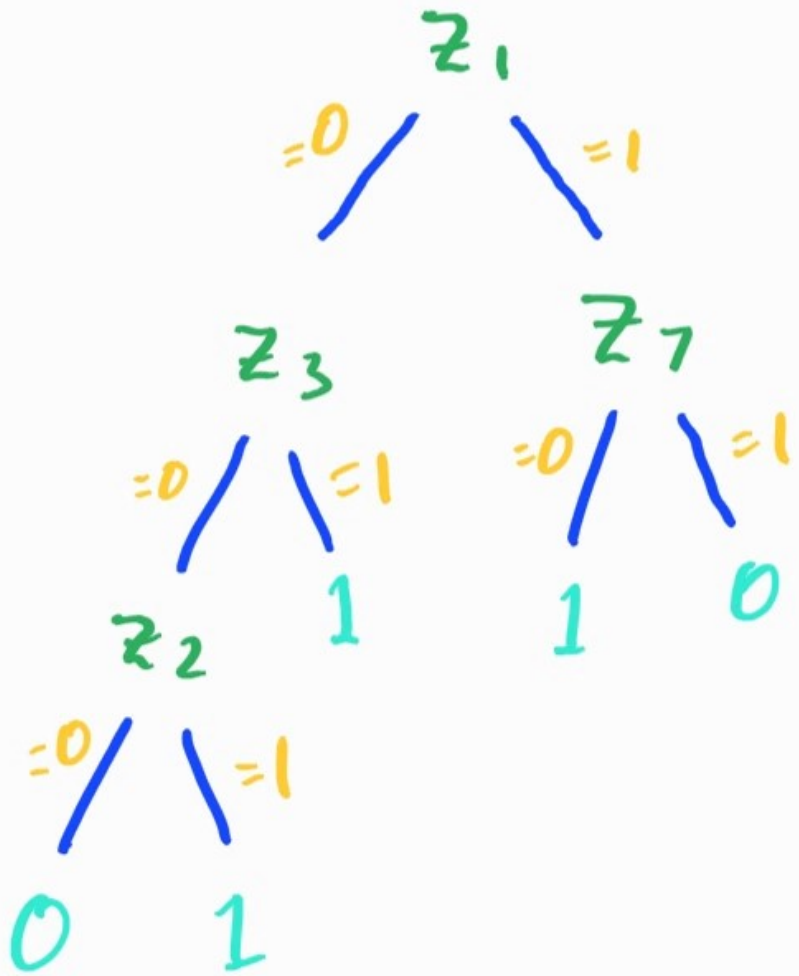


Decision Trees



Decision Trees

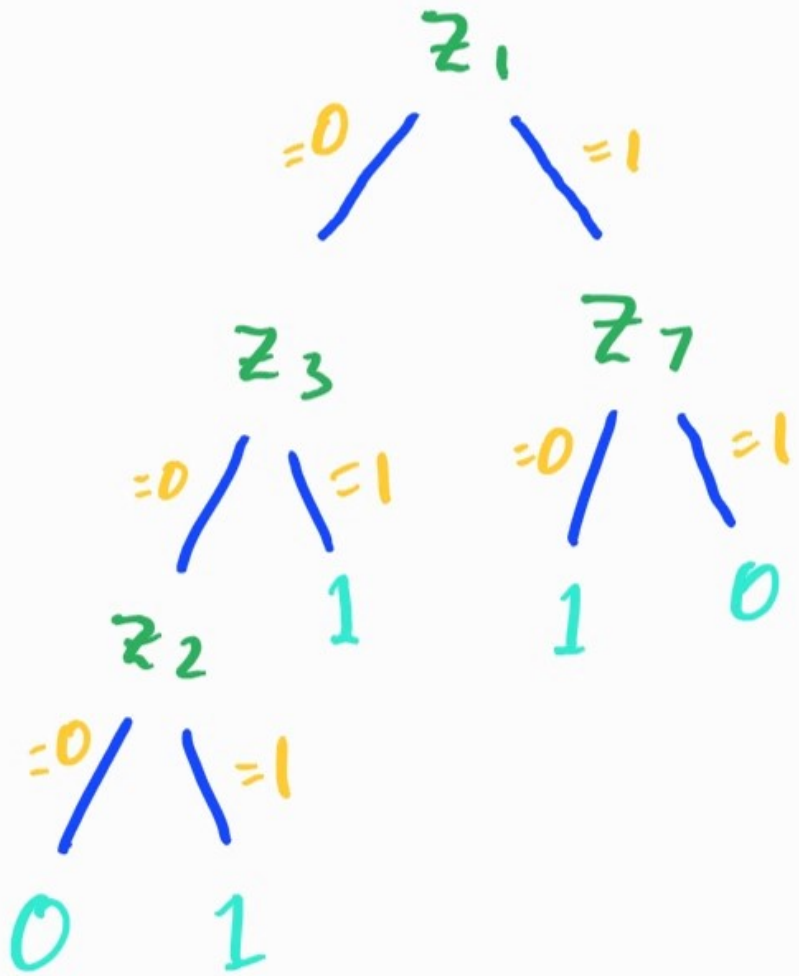
$dt(f(z_1 .. z_n)) = \text{depth}$



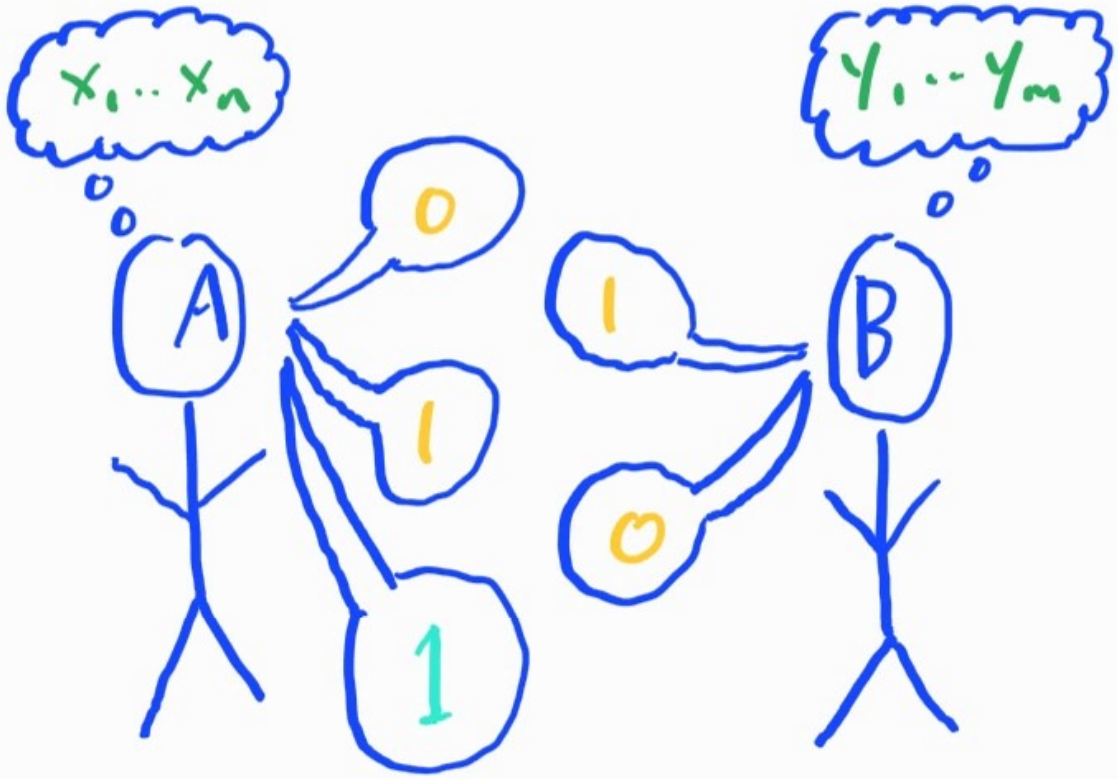
Decision Trees

$dt(f(z_1 .. z_n)) = \text{depth}$

$dt(OR) = n$

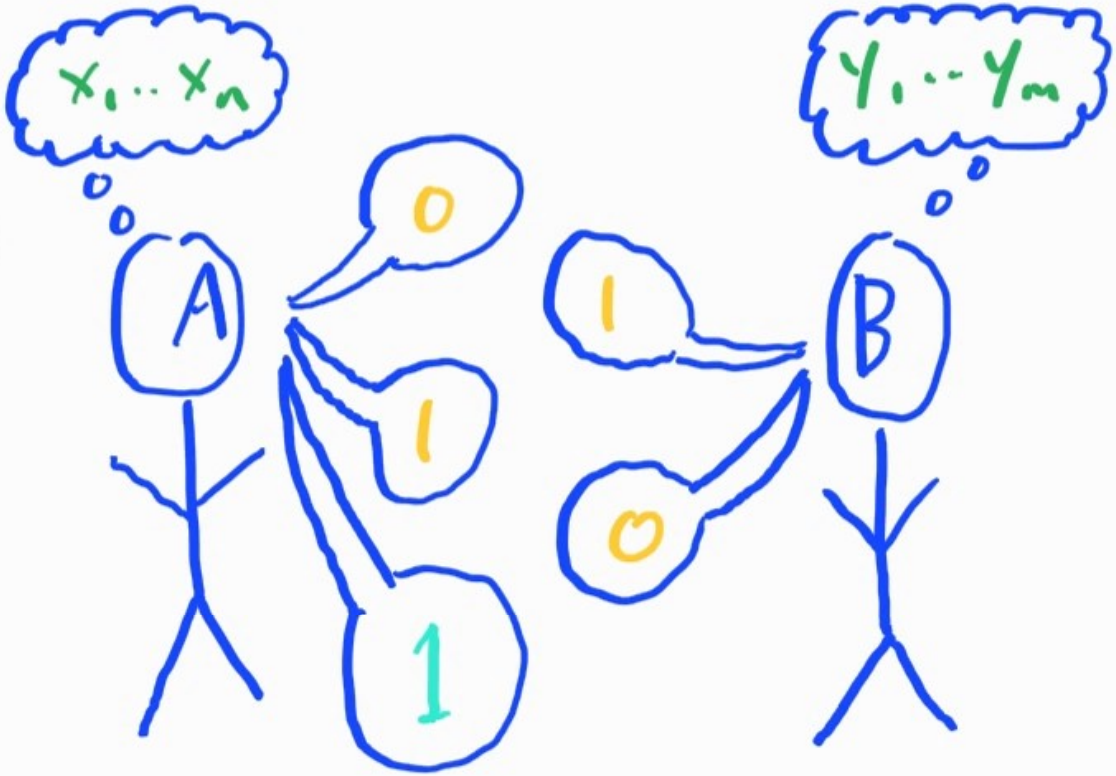


Communication



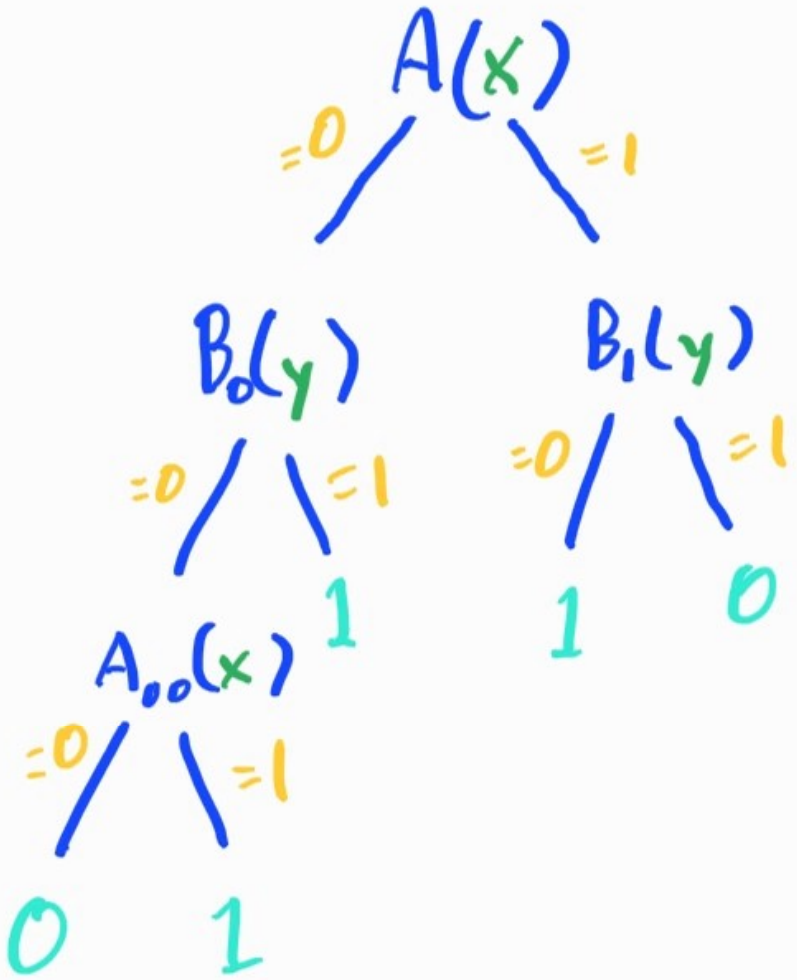
Communication

$cc(F(\begin{smallmatrix} x_1 \dots x_n \\ y_1 \dots y_m \end{smallmatrix})) = \#$ bits sent



Communication

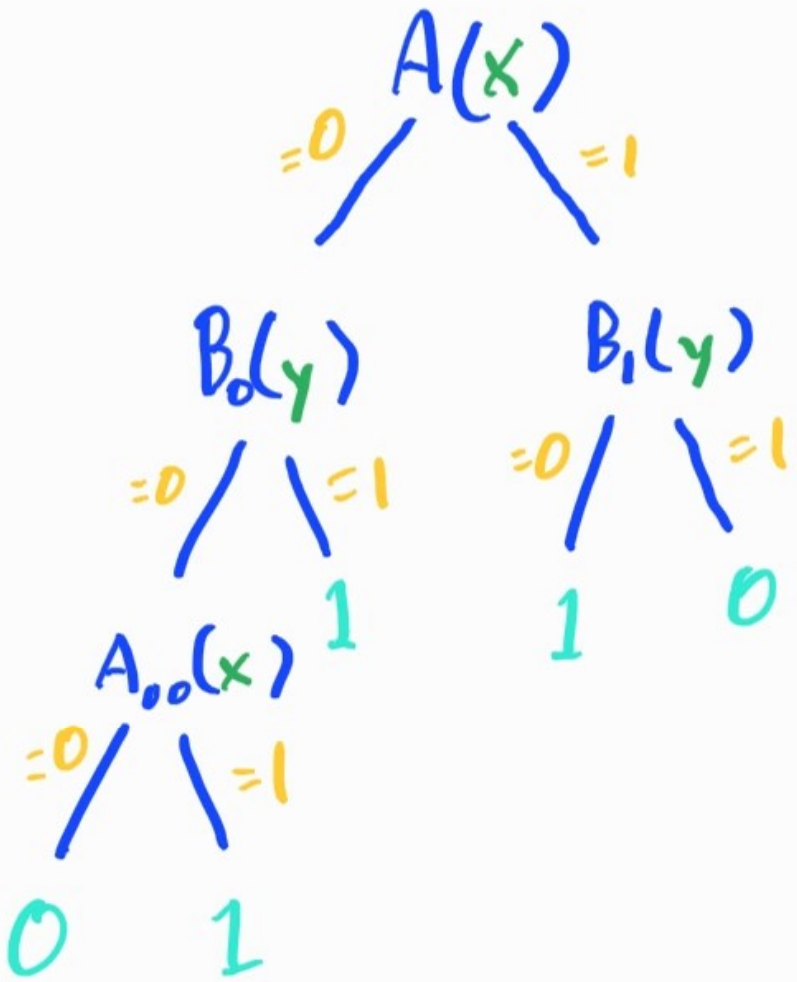
$cc(F(\begin{smallmatrix} x_1 \cdots x_n \\ y_1 \cdots y_m \end{smallmatrix})) = \text{depth}$



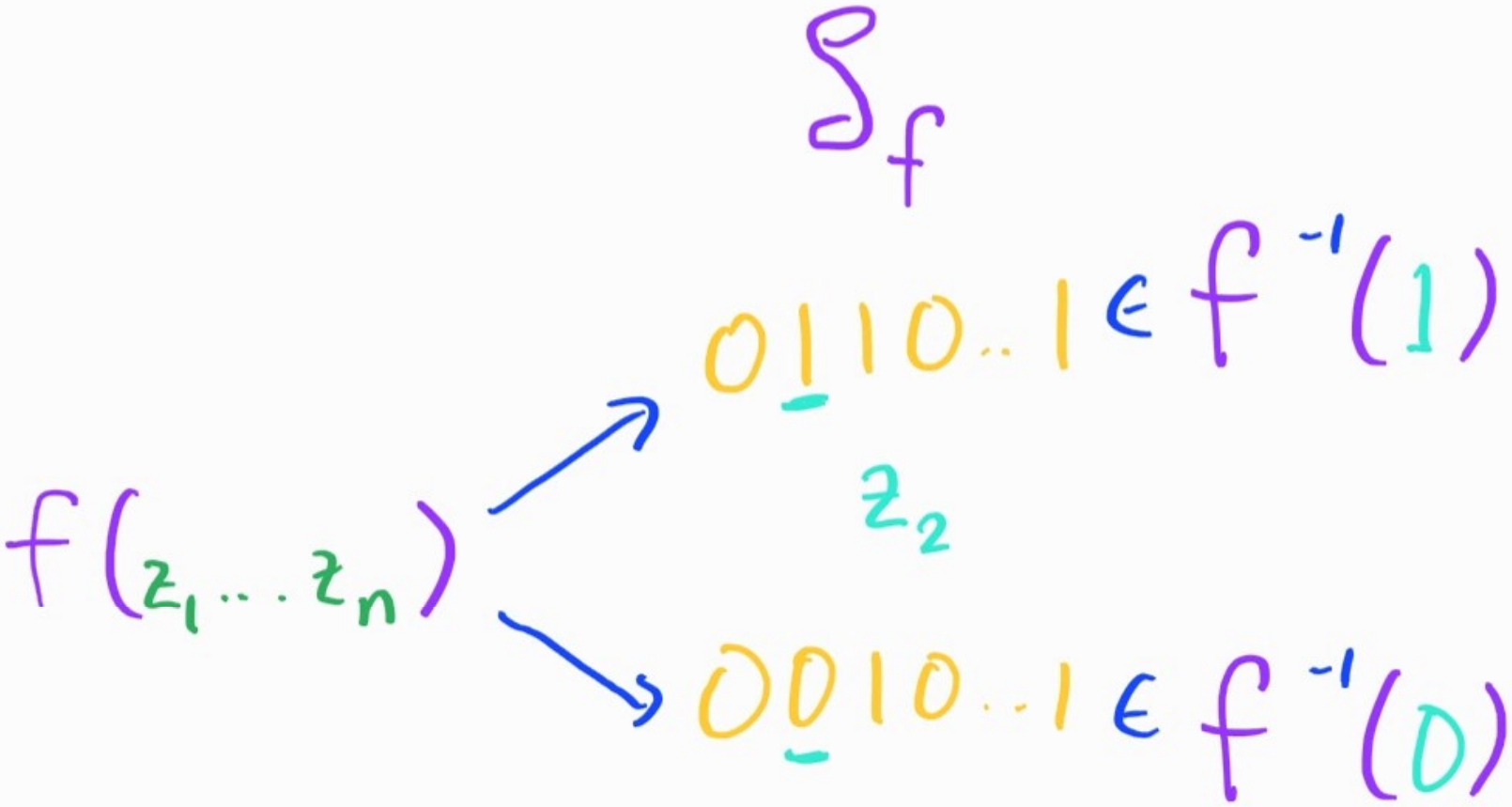
Communication

$cc(F(\begin{smallmatrix} x_1 \cdots x_n \\ y_1 \cdots y_m \end{smallmatrix})) = \text{depth}$

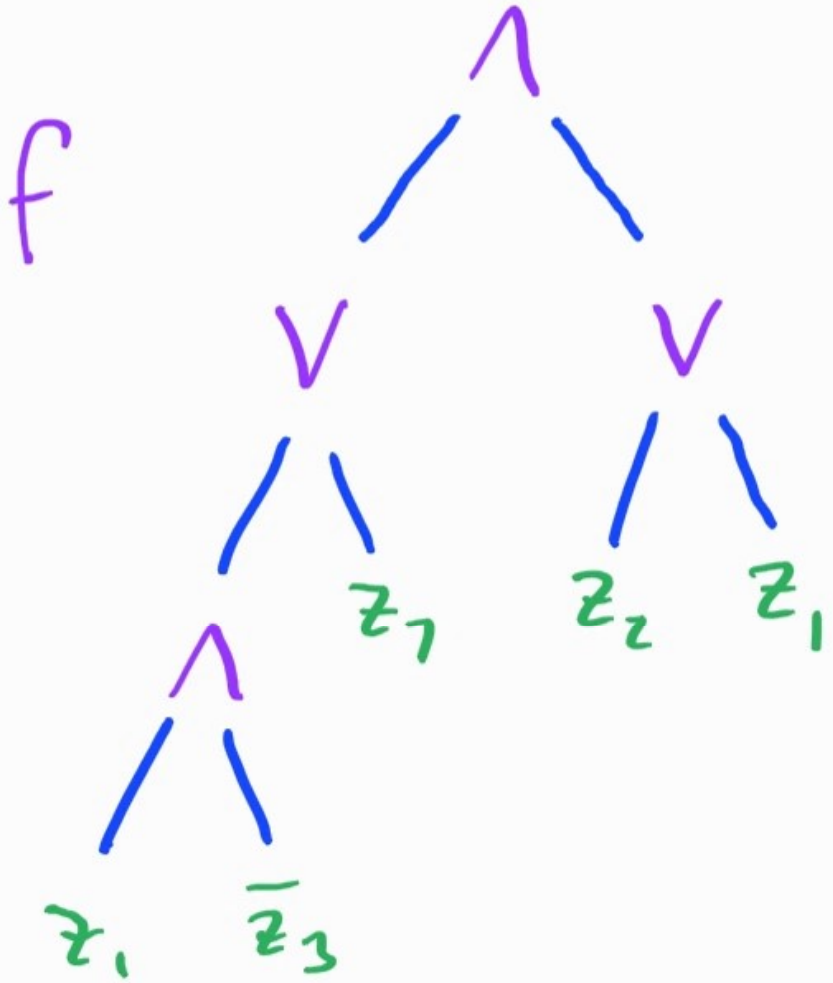
$cc(OR) = 2$

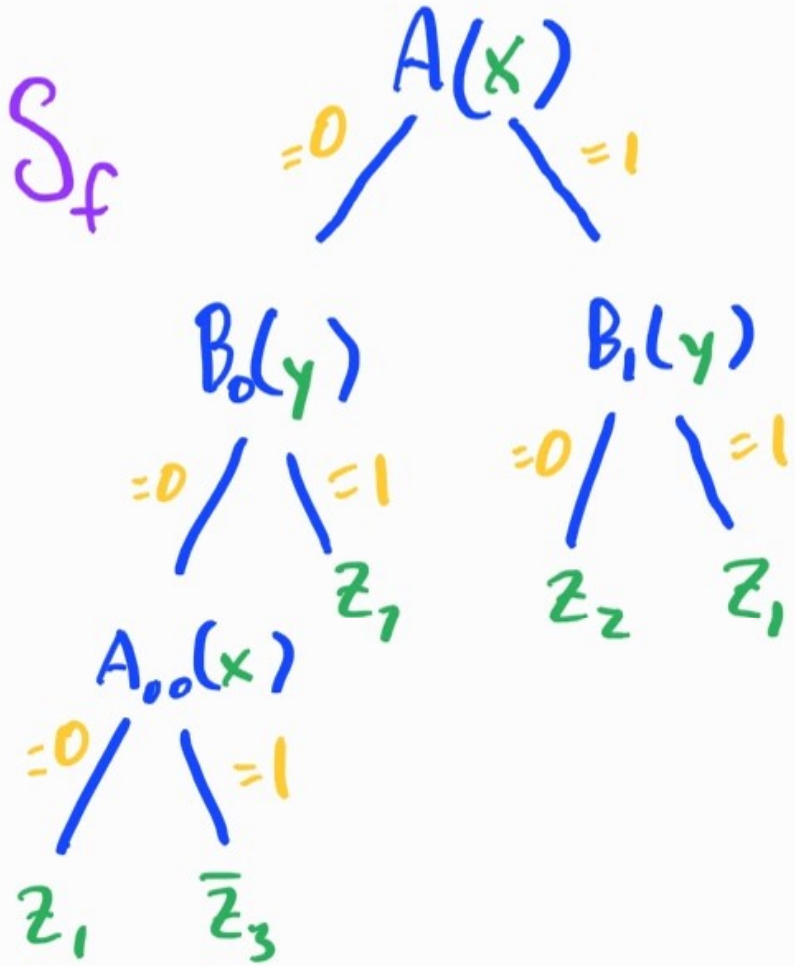


Communication

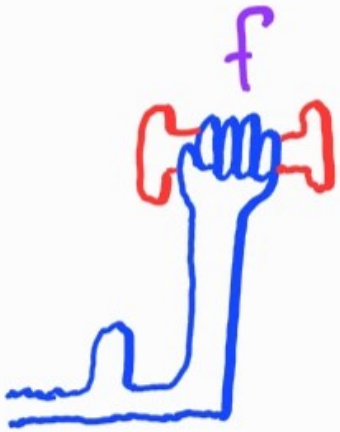


Communication

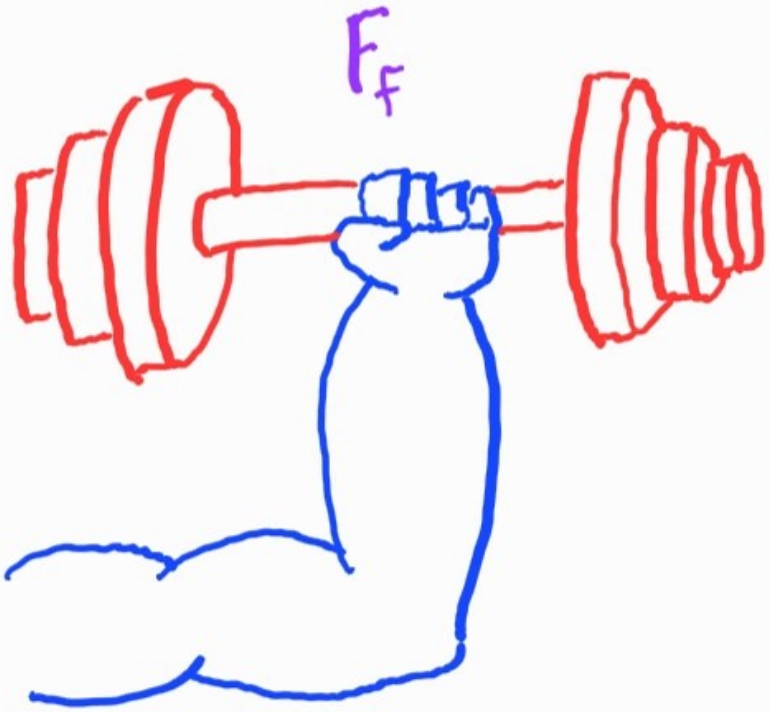




LIFTING



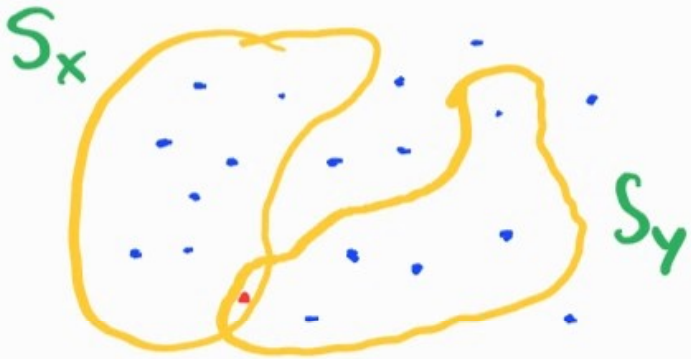
decision trees



communication complexity

LIFTING

$$cc(\overline{DISJ}) = \Omega(n)$$

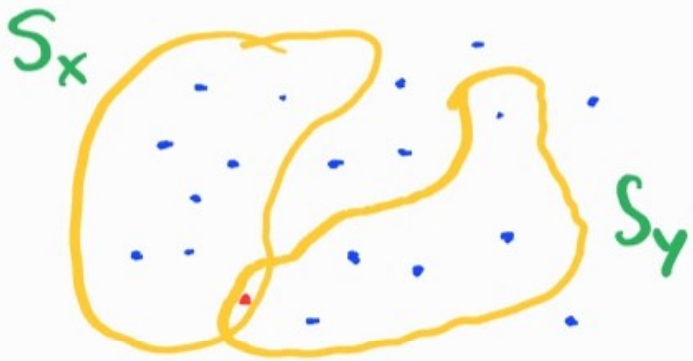


LIFTING

$dt(OR) = n$

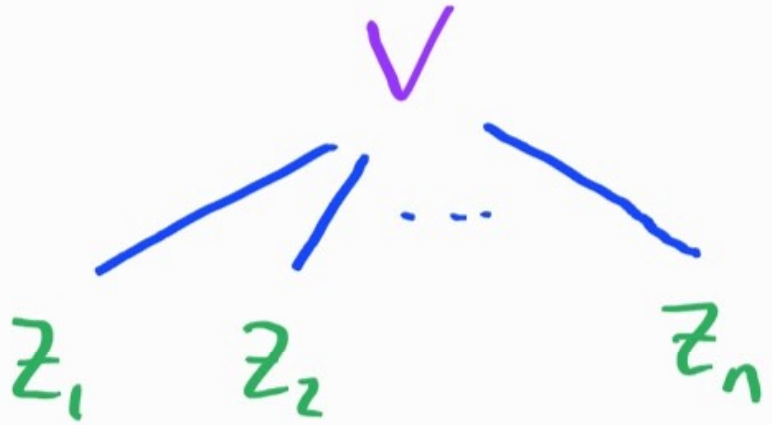
$cc(\overline{DISJ}) = \Omega(n)$

$0\ 0\ 0\ \underline{1}\ \ldots 0$

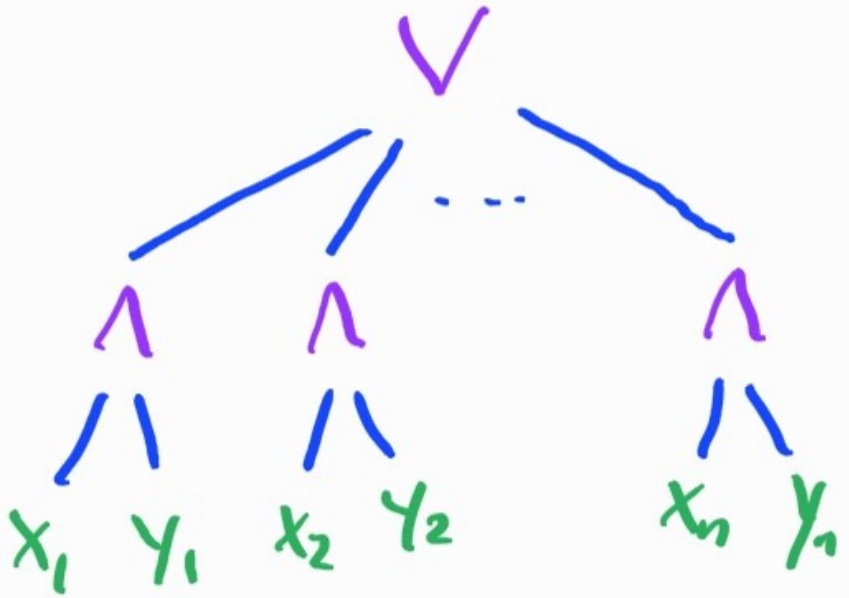


LIFTING

$dt(\mathrm{OR}) = n$



$cc(\overline{\mathrm{DISJ}}) = \Omega(n)$



LIFTING

$$f(z_1 \dots z_n) \longrightarrow f(g(x_1, y_1) \dots g(x_n, y_n))$$

gadget g such that Alice and Bob have to basically solve $g(x_i, y_i)$ to know z_i

LIFTING

index gadget

Alice

Bob

m bits

$\log m$ bits

$x_i = j$

$IND_m(x_i, y_i) = y_i[x_i]$

LIFTING

[RM'99, GPW'15]: for $m = \text{poly}(n)$,

$$cc(f \circ IND_m^n) = dt(f) \cdot \Theta(\log m)$$

LIFTING

[RM'99, GPW'15]: for $m = \text{poly}(n)$,

$$cc(f \circ IND_m^n) = dt(f) \cdot \Theta(\log m)$$

$\leq$: take $\log m + 1$ steps to query z_i

LIFTING

[RM'99, GPW'15]: for $m = \text{poly}(n)$,

$$cc(f \circ IND_m^n) = dt(f) \cdot \Theta(\log m)$$

$\leq$: take $\log m + 1$ steps to query z_i

$\geq$: <u>TODAY!</u>

LIFTING

SOME LIFTING THEOREMS

	CC Model	Query Model
Raz-McKenzie '99	Deterministic CC	Dec Tree
Razborov '03	Quantum CC	approx Degree
Sherstov '07	discrepancy, sign rank	Threshold degree
gLMWZ '15	Nondet CC	approx Junta degree
LRS '15	Semidefinite Rank	SOS degree
RMR '16	Nonneg Rank	Junta degree
P-Robere '17	Algebraic Tiling	Nullstellensatz degree
göös-P-Watson '17	Randomized CC	Randomized dec trees

Applications of Lifting

1. Monotone formula size / circuit lower bounds
2. Cryptography: Lower bounds for Linear secret sharing schemes (and monotone span programs)
3. Linear Programming: Extended formulations
4. game Theory: Nash Equilibrium
5. Graph Theory: Alon-Saks-Seymour Conjecture
6. Proof Complexity
7. Communication Complexity separations
8. Quantum Lower Bounds

Sunflower Technique

1) works for tree-like, dag-like, graduated (and probably many more!)

Sunflower Technique

1) works for tree-like, dag-like, graduated (and probably many more!)
2) simplified proofs: main technical lemma is basically just sunflower lemma

Sunflower Technique

1) works for tree-like, dag-like, graduated (and probably many more!)
2) simplified proofs: main technical lemma is basically just sunflower lemma
3) smaller gadgets! $M = \cancel{n^2}\ n^{1+\varepsilon}$

Sunflower Technique

1) works for tree-like, dag-like, graduated (and probably many more!)
2) simplified proofs: main technical lemma is basically just sunflower lemma
3) smaller gadgets! $m = n^2 \not\to n^{1+\varepsilon}$
   (better sunflowers → even smaller)

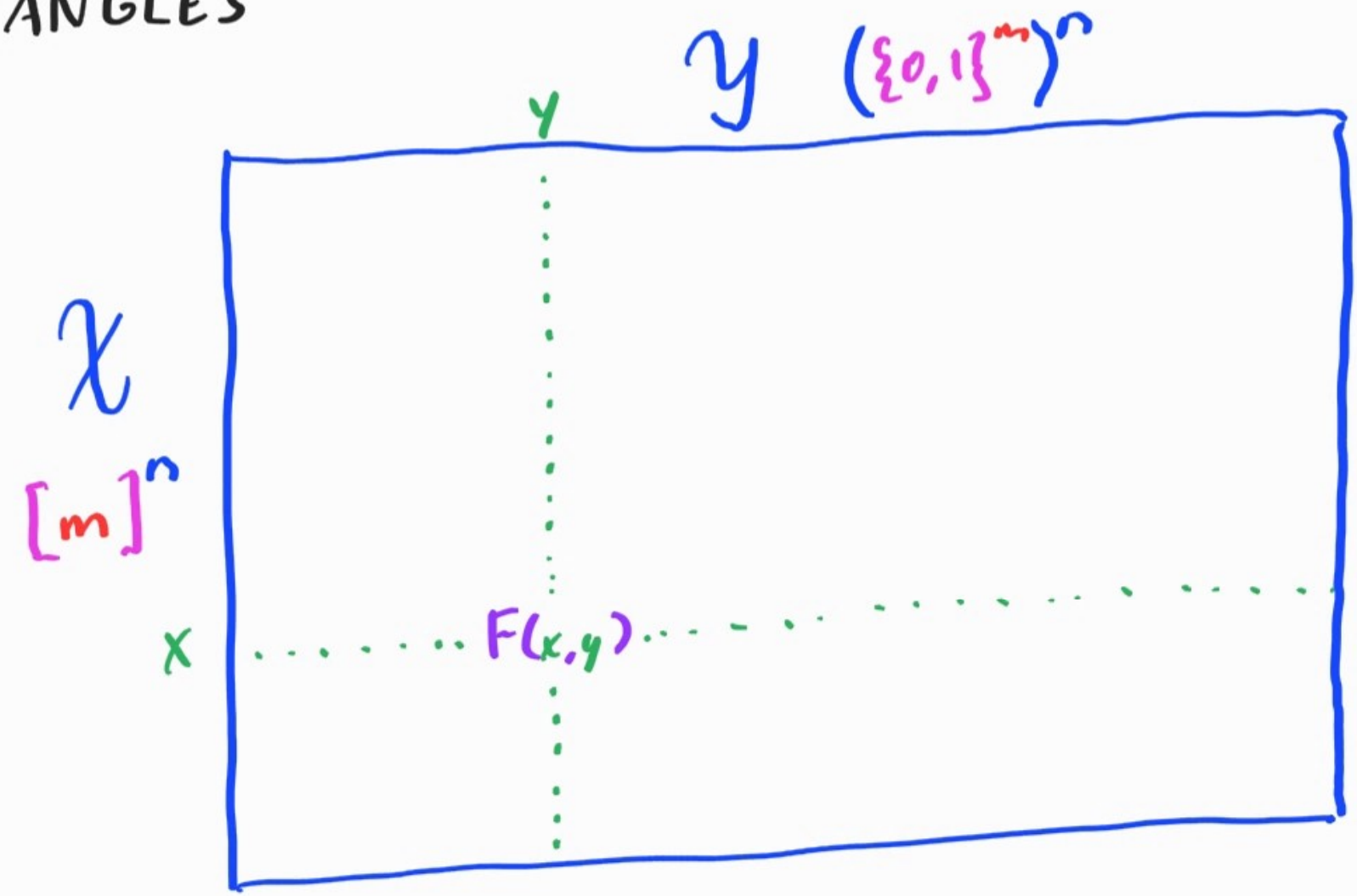
LIFTING

$$cc(f \circ IND_m^n) = dt(f) \cdot \Theta(\log m)$$

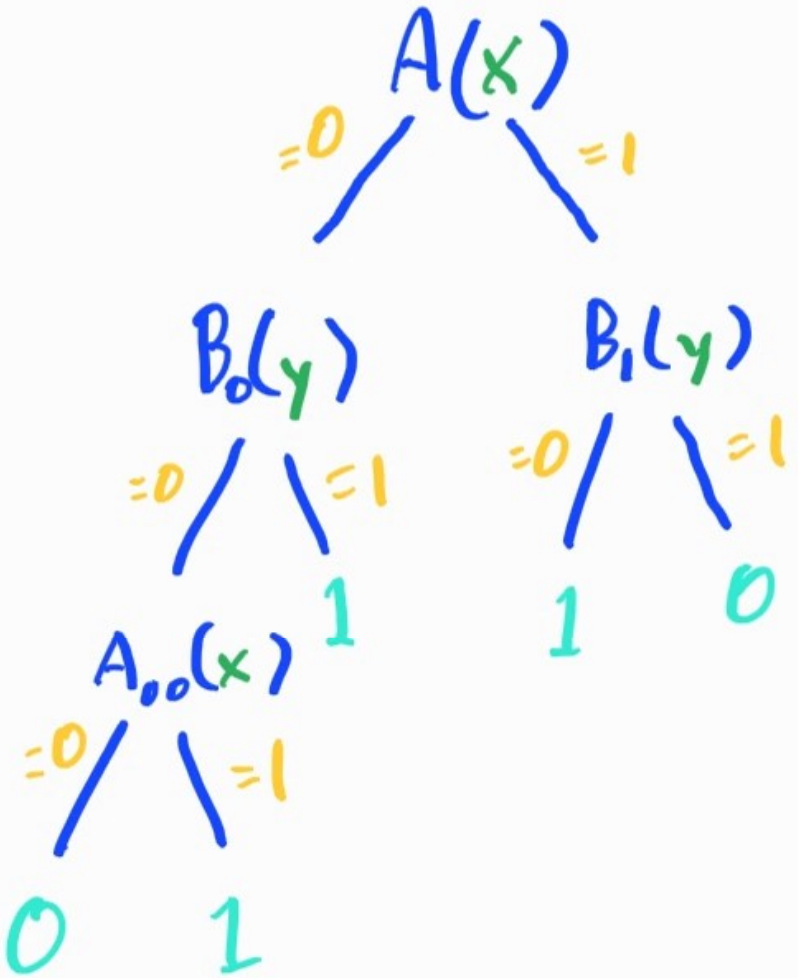
have: Π for $f \circ IND_m^n$, depth $d \log m$

want: Π for f, depth $O(d)$

Rectangles

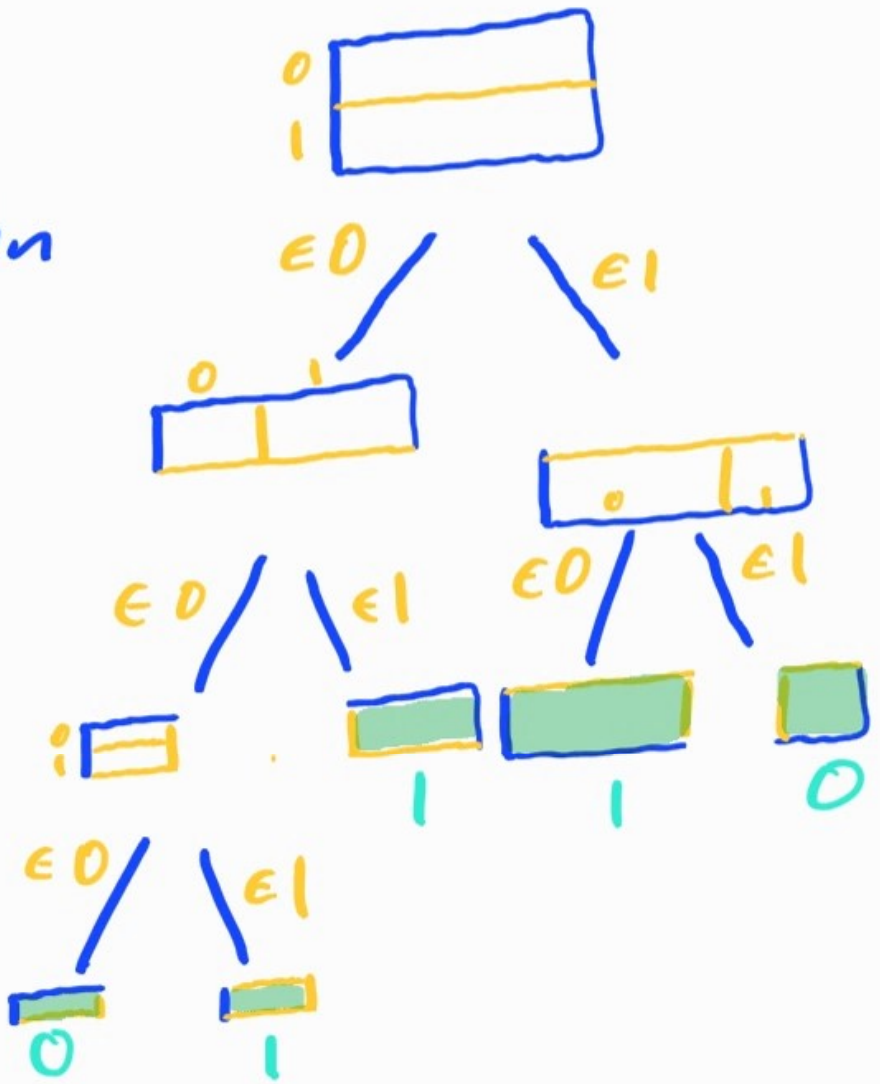


Rectangles



Rectangles

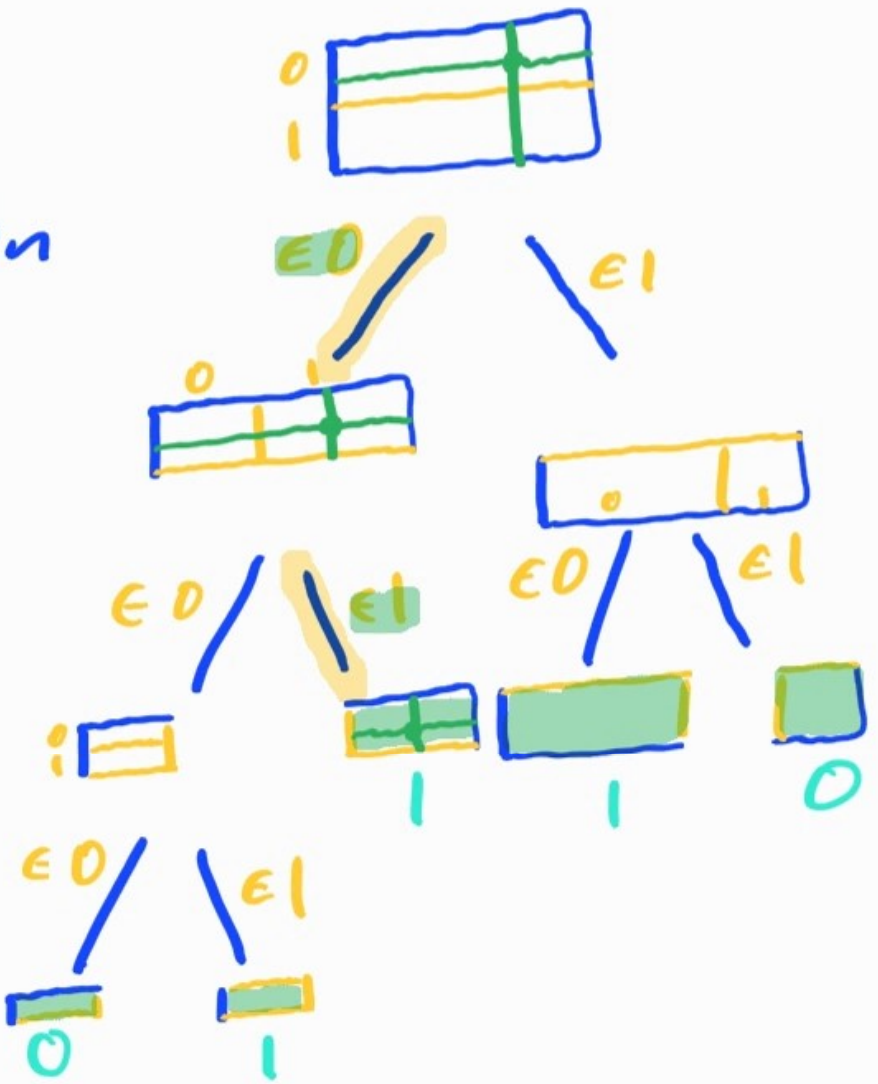
leaves of Π partition R_F into monochromatic rectangles



Rectangles

leaves of Π partition $\mathcal{R}_F$ into monochromatic rectangles

(x, y) follows the rectangles it's in



Important Coordinates

- index gadget obfuscates z_i

Important Coordinates

- index gadget obfuscates z_i
- they can figure z_i out in $\log m + 1$ rounds: Alice sends x_i

Important Coordinates

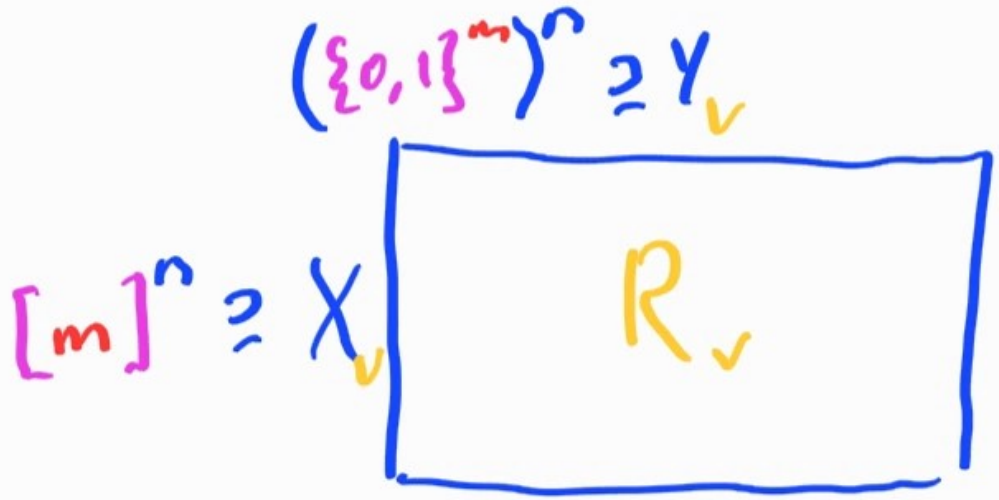
- index gadget obfuscates z_i
- if they send $\Omega(\log m)$ bits "trying to learn about z_i", we're satisfied

Important Coordinates

- index gadget obfuscates z_i
- if they send $\Omega(\log m)$ bits "trying to learn about z_i", we're satisfied

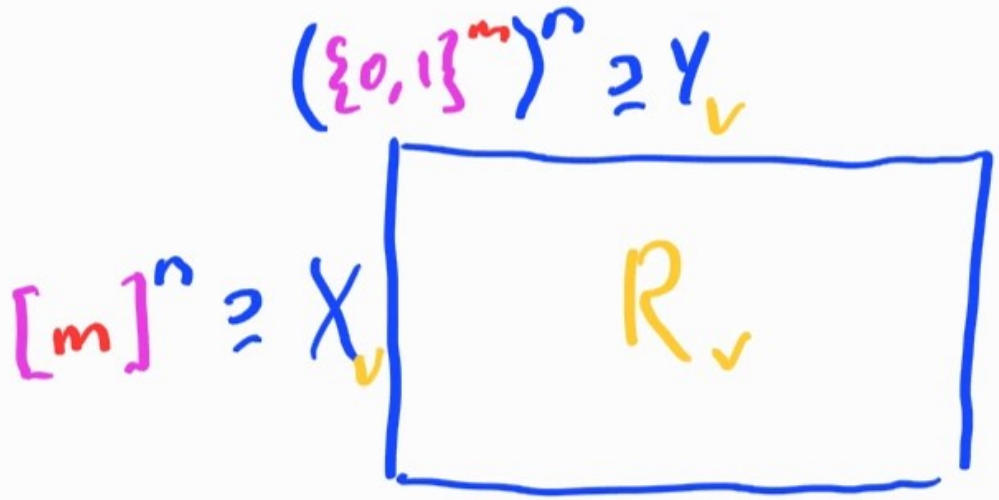
- if they <u>haven't</u> sent $\Omega(\log m)$ bits "trying to learn about z_i", they know basically <u>nothing</u> about z_i

Important Coordinates



Q: how much do they know about z_i?

Important Coordinates



A: depends on X_v restricted to x_i

(ignore Y for now)

Important Coordinates

Def: min-entropy of X ($H_\infty(X)$) is

$$\min_{i,\alpha_i} \left\{ -\log \Pr_{x \sim X} [x[i] = \alpha_i] \right\}$$

Important Coordinates

Def: min-entropy of X ($H_\infty(X)$) is

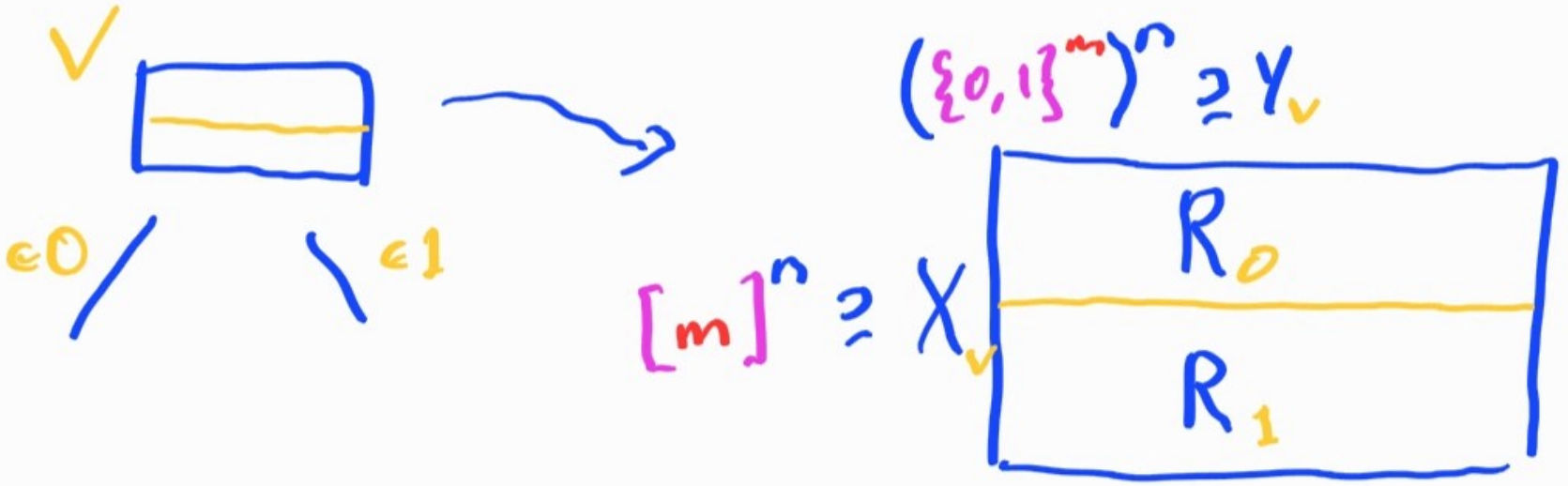
$$\min_{i,\alpha_i} \left\{ -\log \Pr_{x \sim X} [x[i] = \alpha_i] \right\}$$

$$H_\infty(X) \in [0, \log m]$$

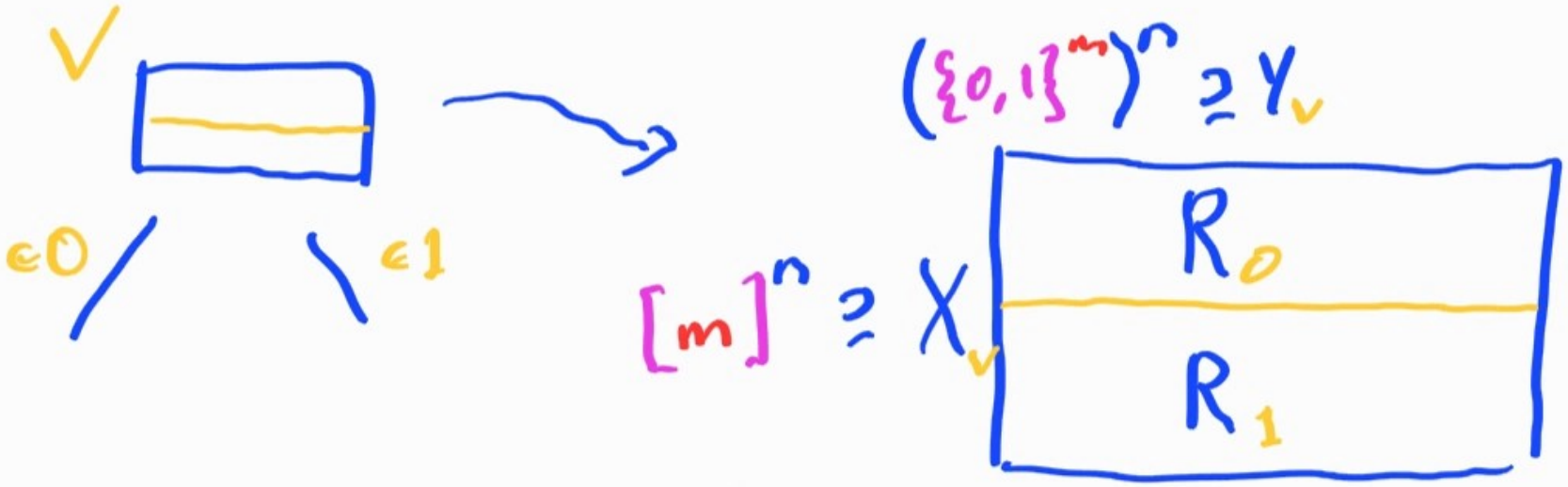
0: x_i known

$\log m$: x_i uniform

Important Coordinates



Important Coordinates



if $|X_b| \geq |X_v|/2$, then

$$H_\infty(X_b) \geq H_\infty(X_v) - 1$$

- at X_v, always pick the larger side of X_0, X_1

- at X_v, always pick the larger side of X_0, X_1
- since min-entropy goes down by at most 1 in each step, takes $\Omega(\log n)$ steps before $H_\infty(X_v) \leq (1 - \Omega(1)) \log n$

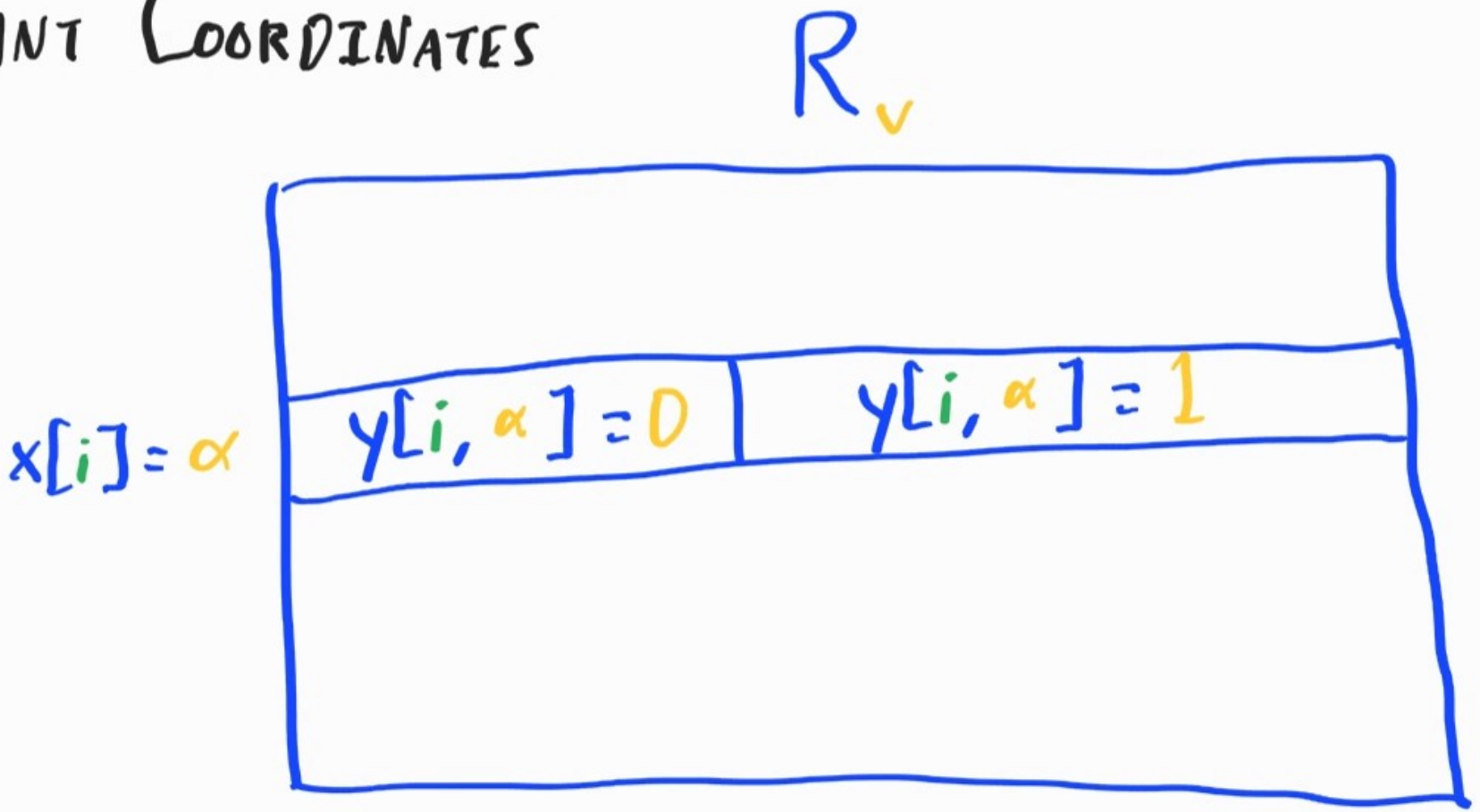
- at X_v, always pick the larger side of X_0, X_1
- since min-entropy goes down by at most 1 in each step, takes $\Omega(\log n)$ steps before $H_\infty(X_v) \leq (1 - \Omega(1)) \log m$
- free to query z_i for i witnessing

Important Coordinates

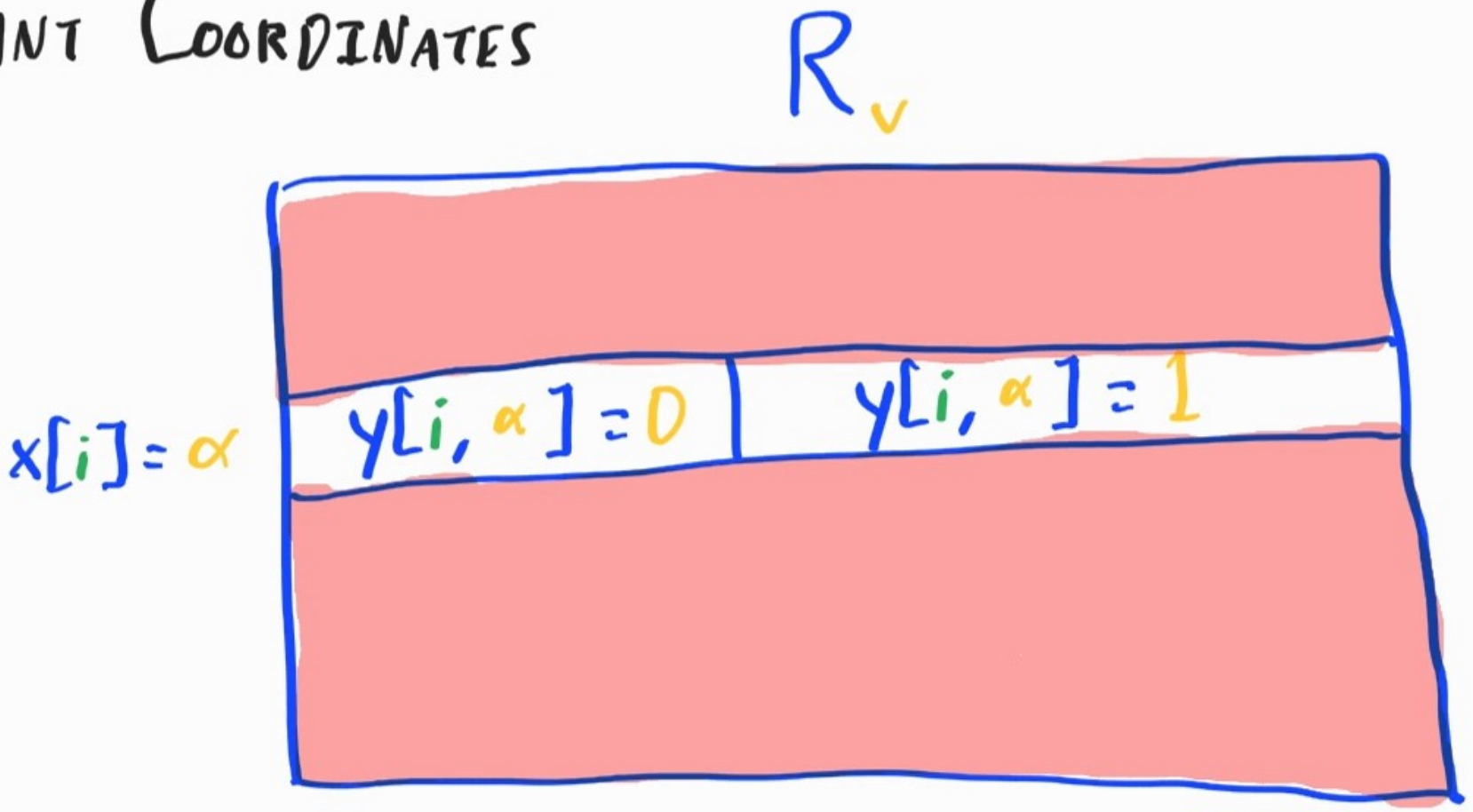
$H_\infty(X_{\bar{5}})$ and $|Y|$ large

$\longrightarrow IND_m^{\bar{5}}(X, Y)$ has all possibilities free

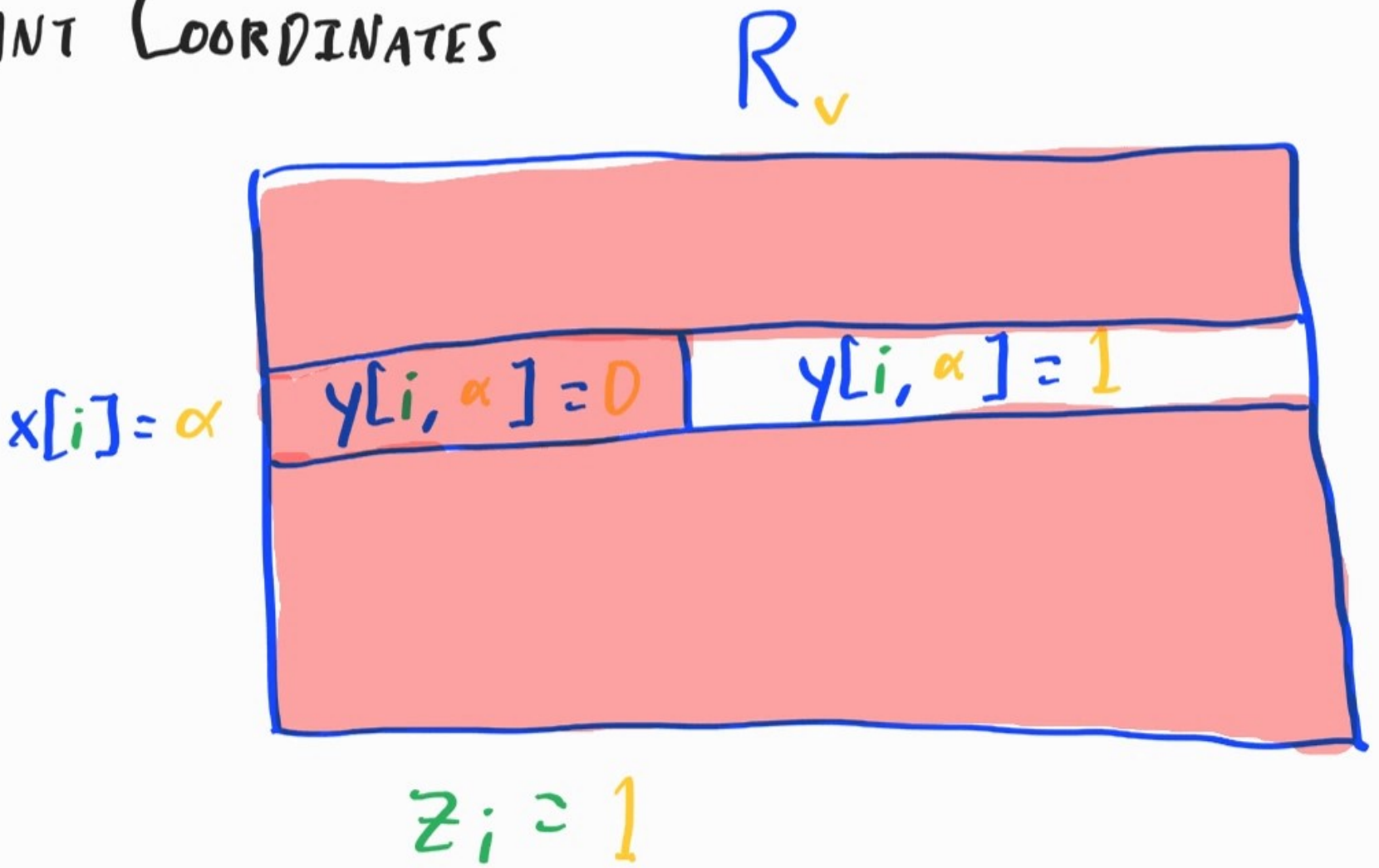
Important Coordinates



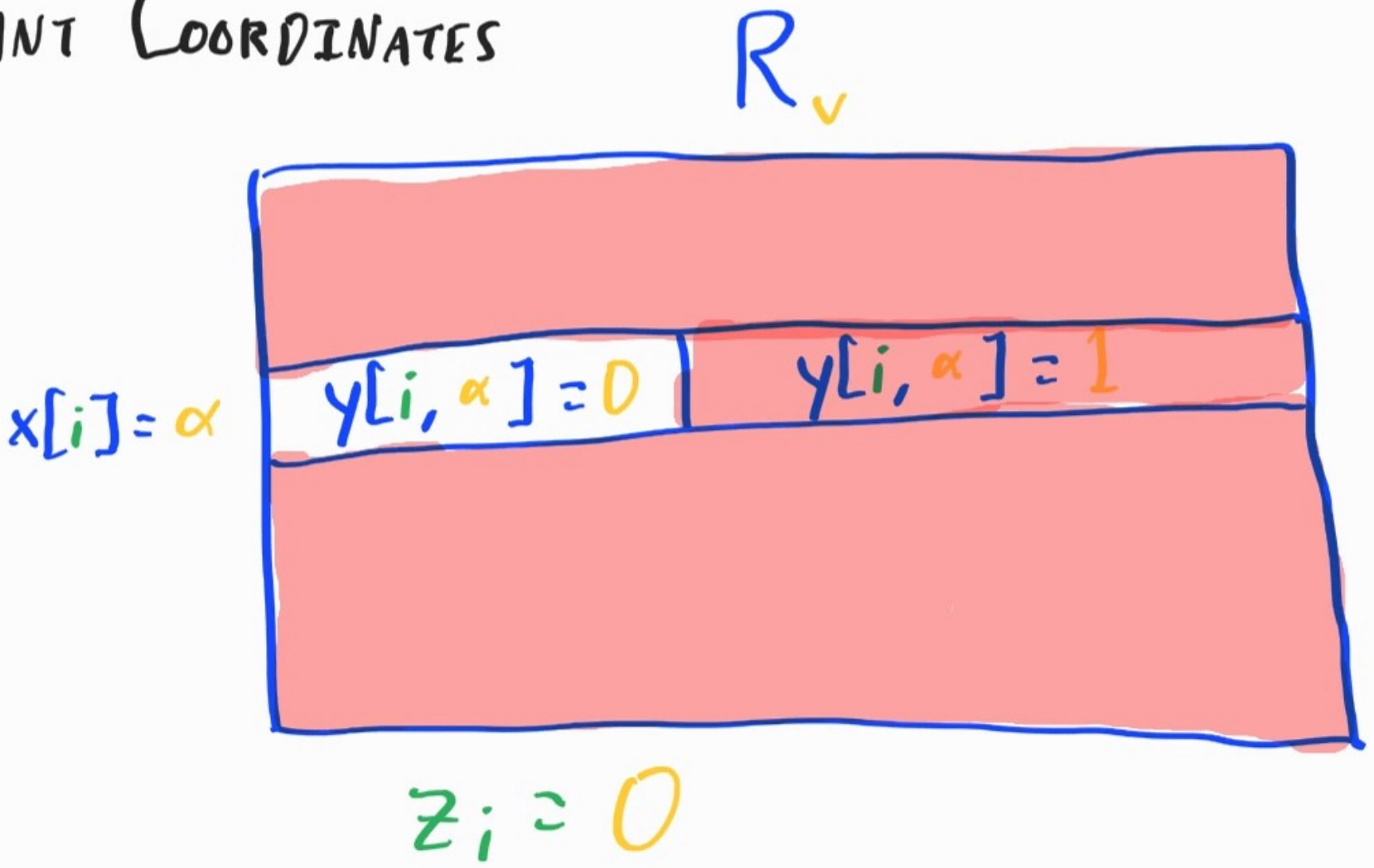
Important Coordinates



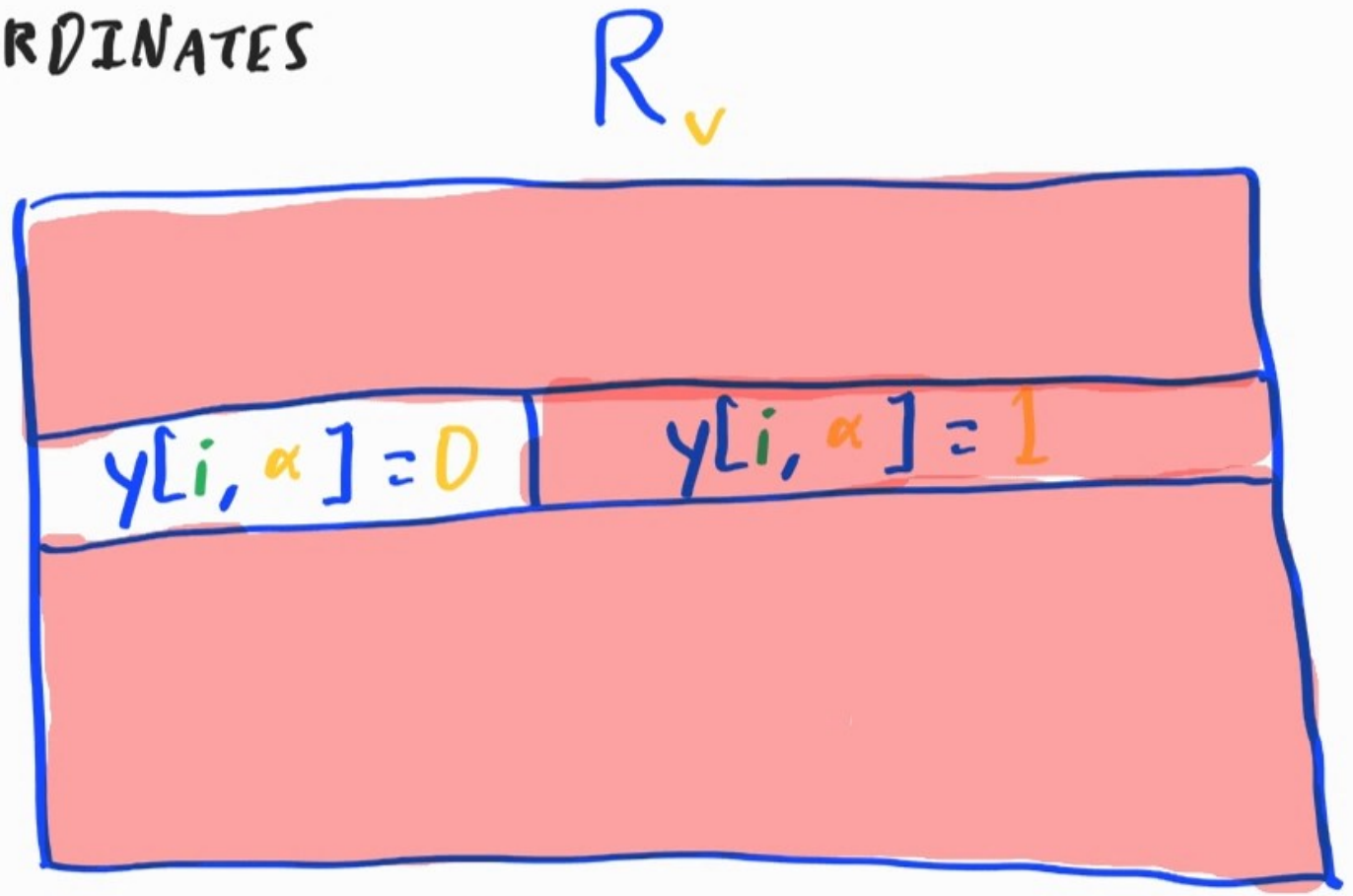
Important Coordinates



Important Coordinates



Important Coordinates



$H_\infty(X_{\bar{J}})$ and $|Y|$ large

$\rightarrow$ $IND_m^{\bar{J}}(X, Y)$ has all possibilities free

Important Coordinates

- maintain $R \subseteq R_v$ such that

  1) $(x, y) \in R$ gives the same answers as our decision tree T on all z_i queried thus far ($:= J$)

Important Coordinates

- maintain $R \subseteq R_v$ such that

1) $(x, y) \in R$ gives the same answers as our decision tree T on all z_i queried thus far ($:= J$)

2) $H_\infty(X) \geq 0.95 \log m$ on $\overline{J}$

Important Coordinates

- maintain $R \subseteq R_v$ such that

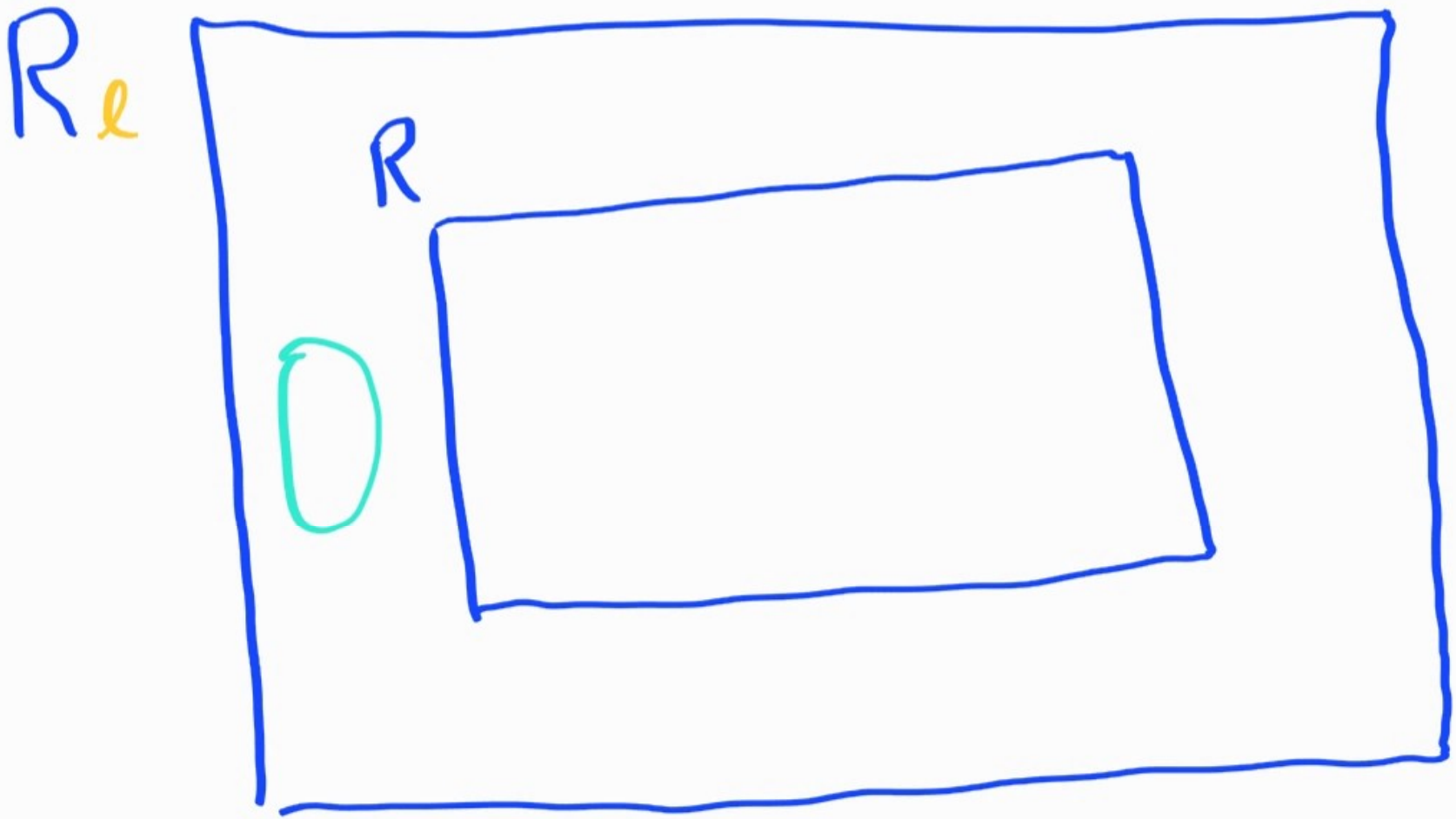
1) $(x, y) \in R$ gives the same answers as our decision tree T on all z_i queried thus far ($:= J$)

2) $H_\infty(X) \geq 0.95 \log m$ on $\overline{J}$

(3) $|Y|$ big)

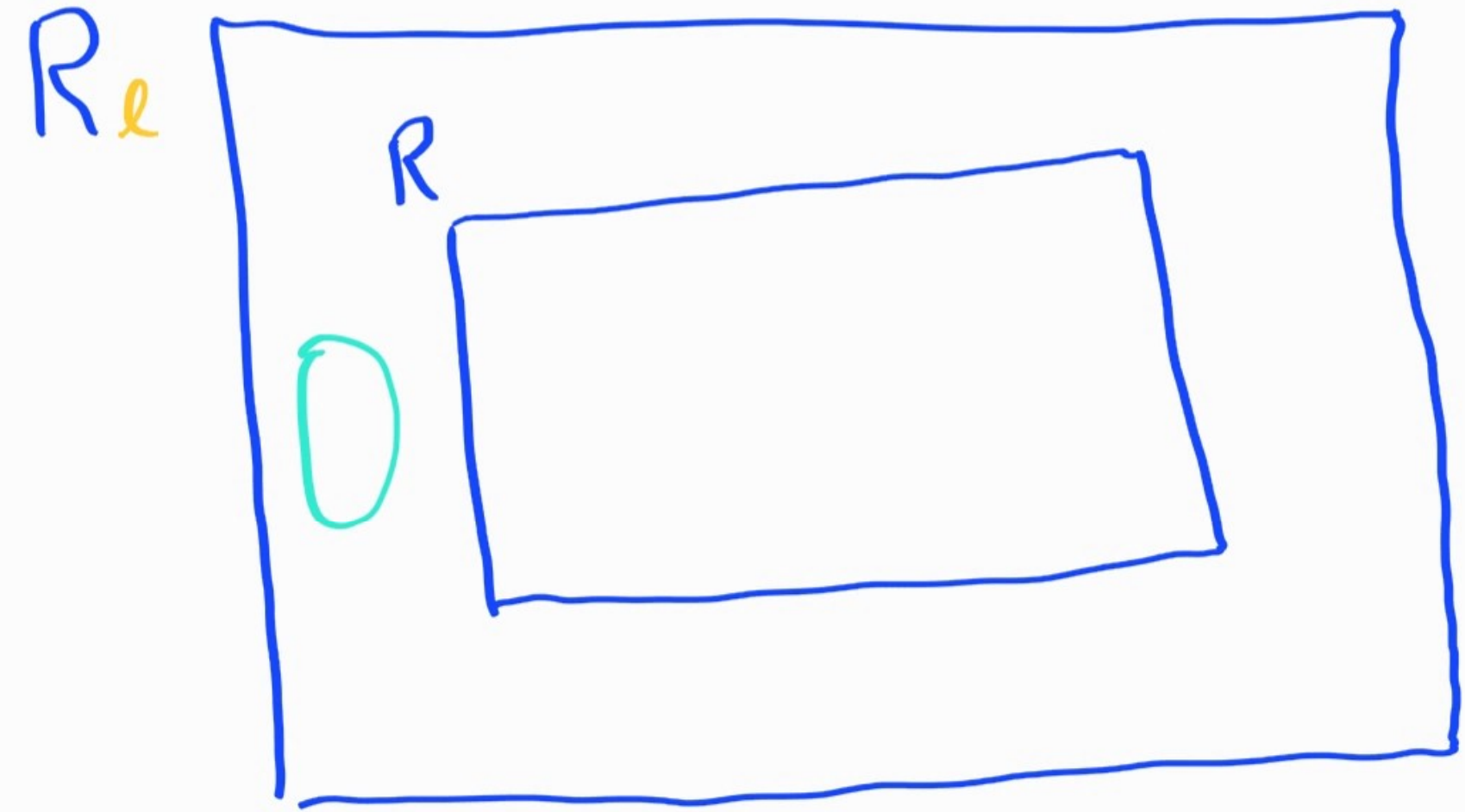
LEAVES

$z = * * 0 * 0 1 \ldots$



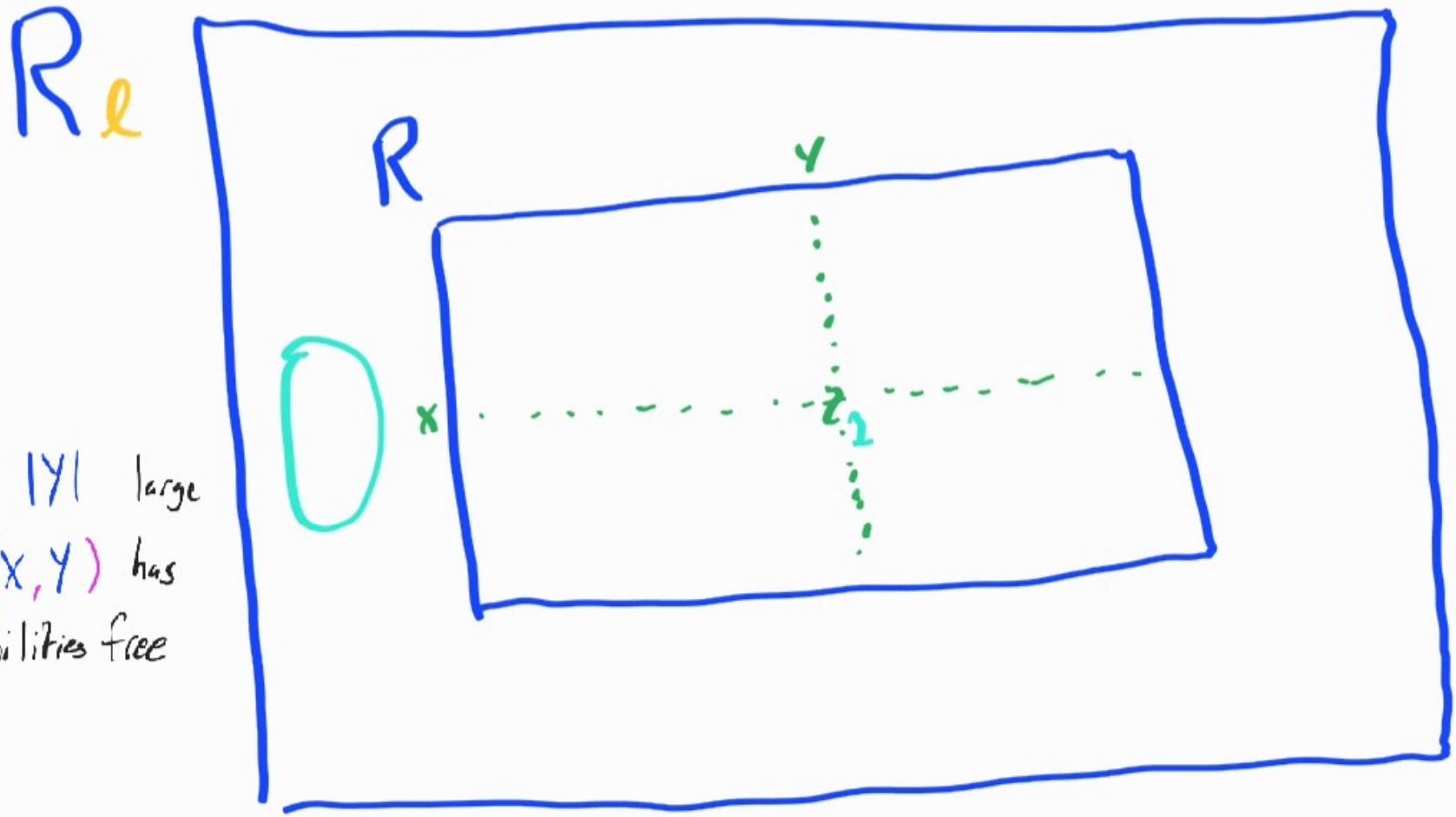
LEAVES

$z_1 = 1\ 1\ 0\ 0\ 0\ 1\ \ldots$



LEAVES

$z_1 = 1\ 1\ 0\ 0\ 0\ 1\ \ldots$



$H_\infty(X_{\bar{J}})$ and $|Y|$ large

$\rightarrow$ $IND^{\bar{J}}_m(X,Y)$ has all possibilities free

Important Coordinates

Q: what if fixing x_i causes x_j to violate $0.95 \log m$ min-entropy?

Important Coordinates

Q: what if fixing x_i causes x_j to violate $0.95 \log m$ min-entropy?

Def: blockwise min-entropy of X ($H_\infty(X)$) is

$$\min_{I, \alpha_I} \frac{1}{|I|} \left\{ - \log \Pr_{x \sim X} [x[I] = \alpha_I] \right\}$$

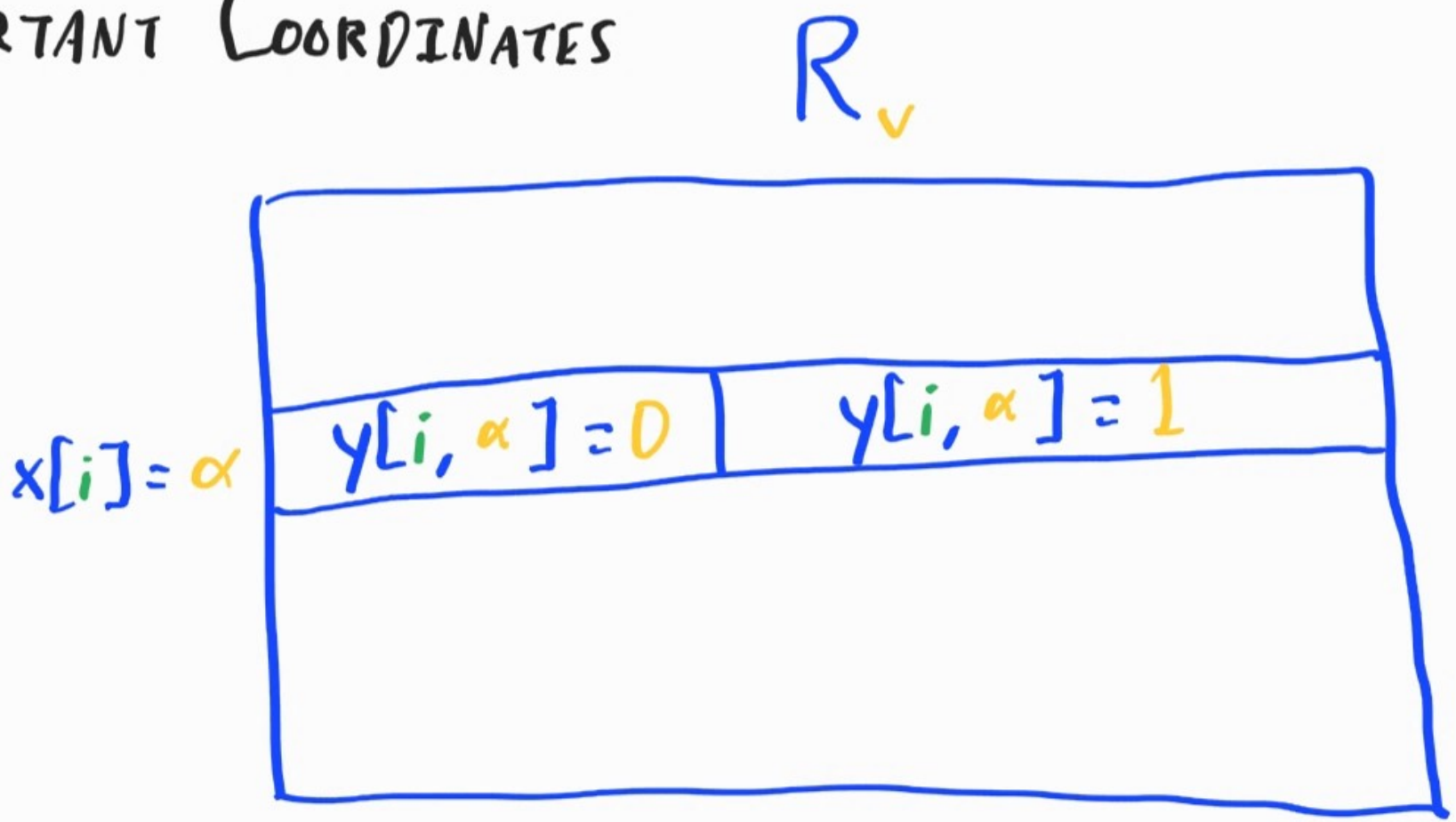
Important Coordinates

pick maximal I, α_I, remaining

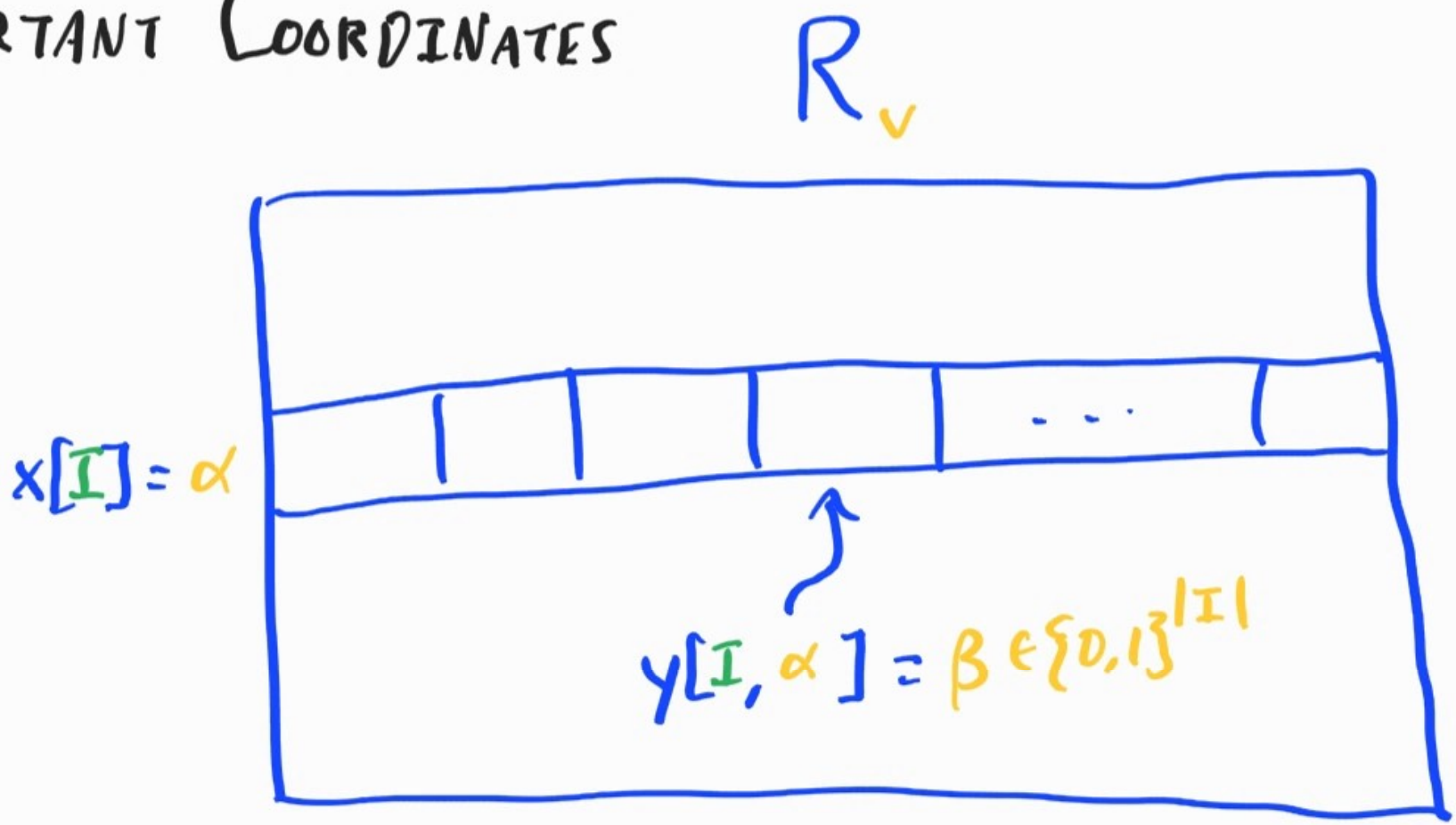
X retains $0.95 \log m$ blackwise

min-entropy on free coordinates

Important Coordinates



Important Coordinates



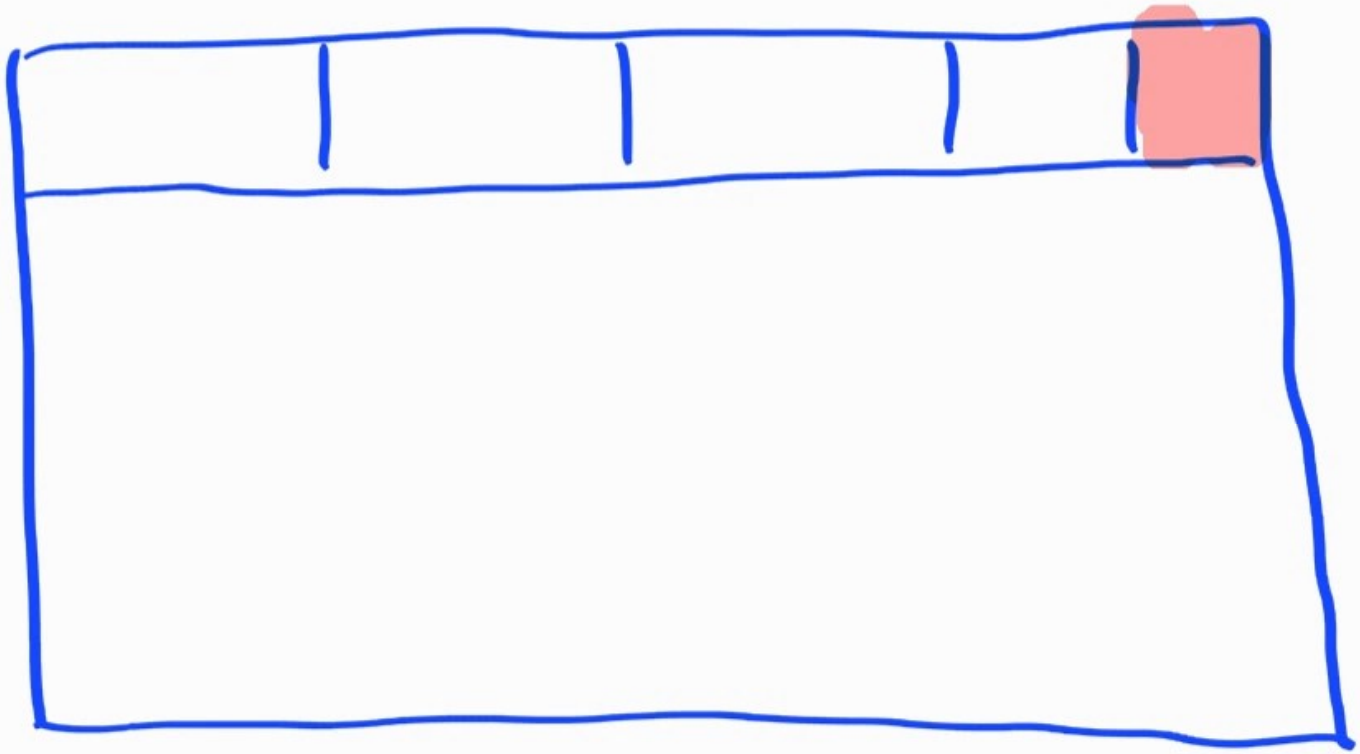
Y SIDE

Q: what if $|\{y[I, \alpha] = \beta\}|$ is small?

Y SIDE

Q: what if $|\{y[I, \alpha] = \beta\}|$ is small?

$x[I] = \alpha$



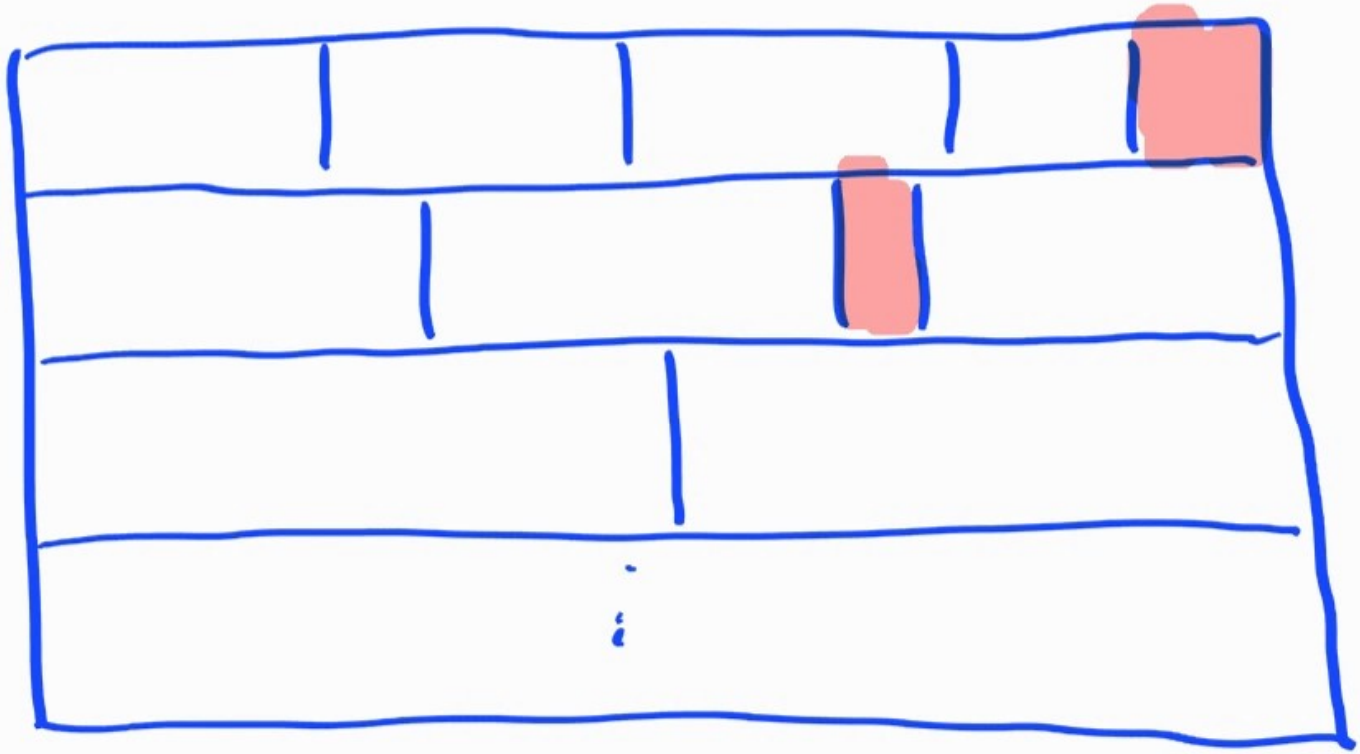
Y Side

Q: what if $|\{y[I, \alpha] = \beta\}|$ is small?

$x[I_1] = \alpha_1$

$x[I_2] = \alpha_2$

$x[I_3] = \alpha_3$



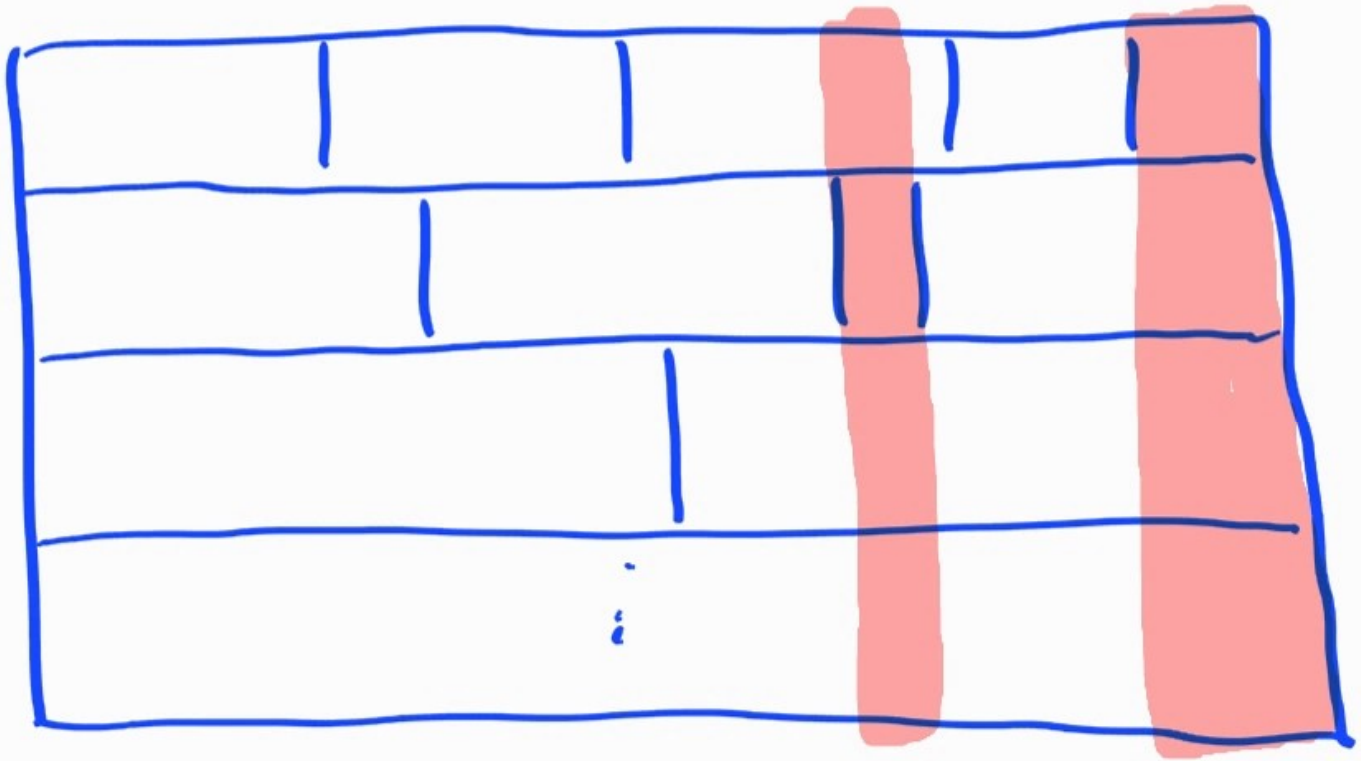
Y Side

Q: what if $|\{y[I, \alpha] = \beta\}|$ is small?

$x[I_1] = \alpha_1$

$x[I_2] = \alpha_2$

$x[I_3] = \alpha_3$



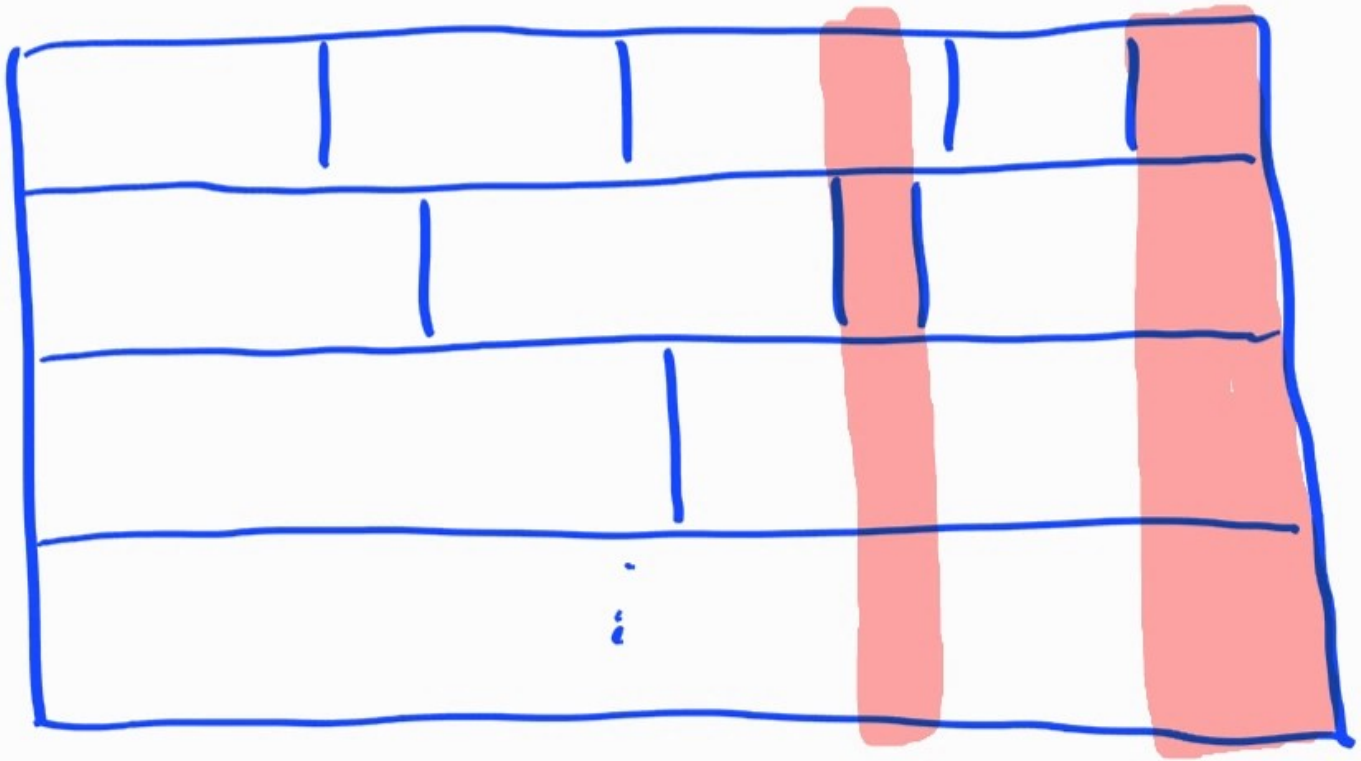
Y SIDE

UNION BOUND: $|Y^{err}| \ll |Y|/2$

$x[I_1] = \alpha_1$

$x[I_2] = \alpha_2$

$x[I_3] = \alpha_3$



Y Side

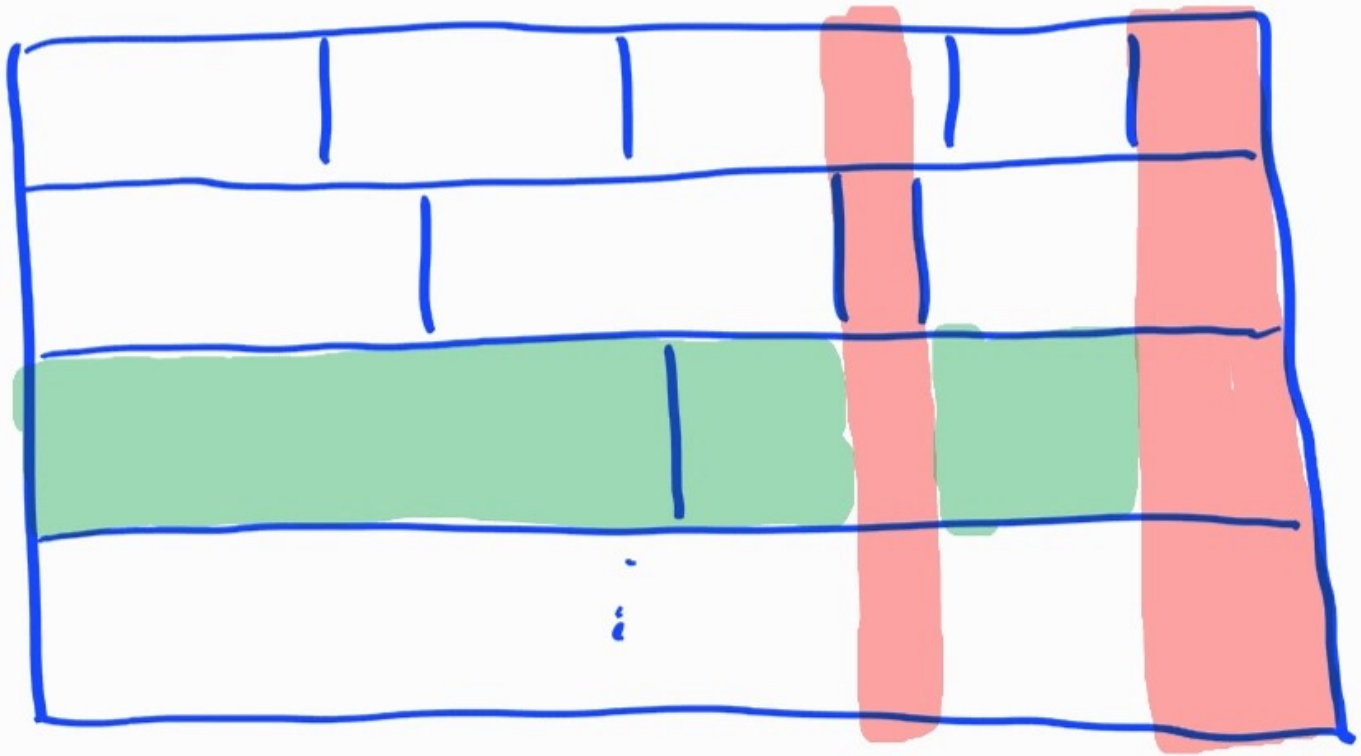
$H_\infty(X_{\bar{J}})$ and $|Y|$ large

$\longrightarrow$ $IND_m^{\bar{J}}(X, Y)$ has all possibilities free

$x[I_1] = \alpha_1$

$x[I_2] = \alpha_2$

$x[I_3] = \alpha_3$



Full Range

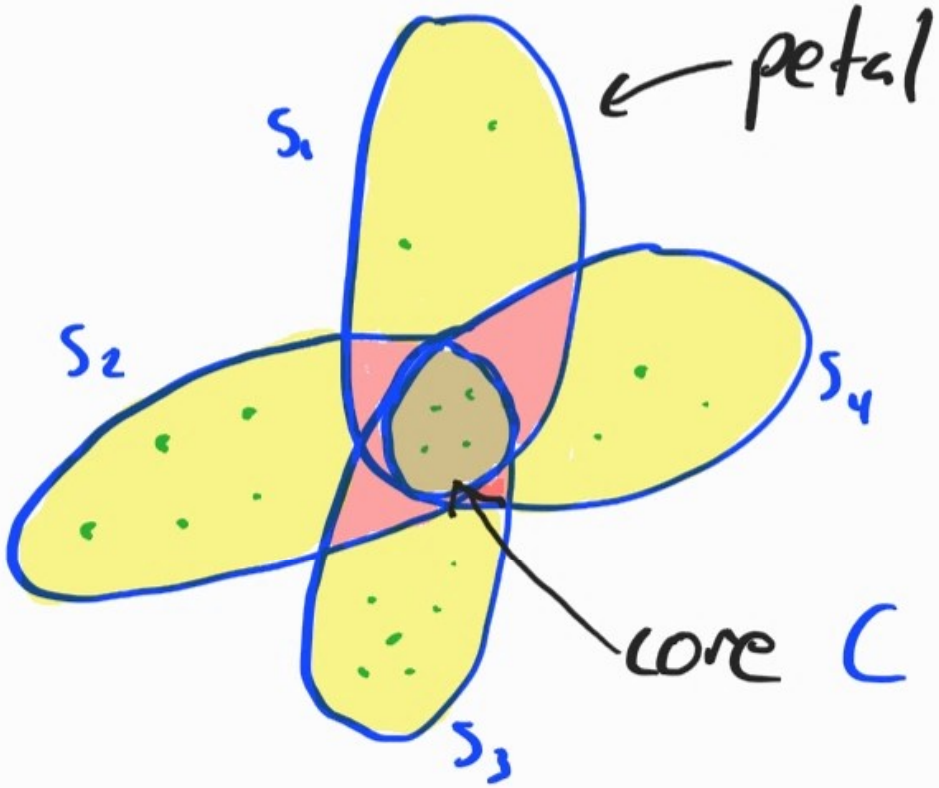
if $H_\infty(X_{\bar{J}}) \geq 0.95 \log m - O(1)$

and $|Y| \geq 2^{mn - n \log m}$

then $\exists x^* \in X$ such that

$$IND_m^{\bar{J}}(x^*, Y) = \{0,1\}^{\bar{J}}$$

Sunflowers



$$S_i \cap S_j = C$$

$$\forall S_i, S_j \in \mathcal{S}$$

Sunflowers

$$[\text{ER}'60]: |S| \leq d \qquad \forall S \in \mathcal{F}$$

$$|\mathcal{F}| \geq d!\, k^d$$

$$\longrightarrow \exists \text{ sunflower } \mathcal{S} \subseteq \mathcal{F}, \quad |\mathcal{S}| \geq k$$

Sunflowers

Proof : what's the max # of disjoint sets?

Sunflowers

Proof: what's the max # of disjoint sets?

$\geq k$: S = that collection ($C = \emptyset$)

Sunflowers

Proof: what's the max # of disjoint sets?

$\geq k$: S = that collection ($C = \emptyset$)

$< k$: some element i is in at least

$$|F| / dk \geq (d-1)!\, k^{d-1} \text{ sets}$$

$\rightarrow$ add i to C, recurse

Sunflowers

[ER'60]: $|\mathcal{F}| \geq d!\, k^d$

[ALWZ'19]: $|\mathcal{F}| \geq (k \log kd)^d$

: $|\mathcal{F}| \geq (ck)^d$

Sunflowers

Proof: does some set T appear at least $r^{|T|}$ times?

Sunflowers

Proof: does some set T appear at least $r^{|T|}$ times?

no: can find a collection of disjoint sets S

yes: recurse on T

Sunflowers

Proof: does F have blockwise min-entropy at most $\log r$?

no: can find a collection of disjoint sets S

yes: recurse on T

Sunflowers

[ALWS '19]: if $\mathcal{F}$ has blockwise min-entropy $\geq \log K \log(n/\varepsilon)$ (where K is an absolute constant and $|\mathcal{U}| = n$), then

$$\Pr_{Y \subseteq \mathcal{U}}\left(\forall x \in \mathcal{F},\ x \not\subseteq Y\right) < \varepsilon$$

Full Range

Full Range

$$\text{no } x^* \rightarrow \forall x \; \exists \beta_x \notin IND_m^{\overline{J}}(x, y)$$

Full Range

no x^* $\rightarrow \forall x \; \exists \beta_x \notin \overline{IND_m^{\mathcal{F}}}(x, Y)$

worst case: $\beta_x = 11..1$ (DNF counting)

Full Range

$$\text{no } x^* \rightarrow \forall x \; \exists \beta_x \notin \overline{IND_m^{\mathcal{J}}}(x, Y)$$

$$\mathcal{U} : [mn]$$

$$x \subseteq \mathcal{U}, \quad |x| = n$$

$$H_\infty(X) \geq 0.95 \log m \geq \log K \log mn \, 2^{n \log m}$$

$$-O(1)$$

Full Range

no x^* $\rightarrow \forall x \; \exists \beta_x \notin IND_m^{\overline{J}}(x, Y)$

$\mathcal{U} : [mn]$

$x \subseteq \mathcal{U}, \quad |x| = n$

$m^{0.95} > n \log m$

$H_\infty(X) \geq 0.95 \log m \geq \log\log 2^{n \log m}$

Full Range

$$\Pr_{Y \subseteq U}(\forall x \in X,\ x \notin y) < 2^{-n \log m}$$

Full Range

$$\Pr_{y \subseteq U}\left(\forall x \in X,\ x \notin y\right) < 2^{-n \log m}$$

$$\Pr_{y \sim (\{0,1\}^m)^n}\left(\forall x \in X,\ y[x] \neq \beta^x\right) < 2^{-n \log m}$$

Full Range

$$\Pr\left(\forall x \in X,\ y[x] \neq \beta^x\right) < 2^{-n \log m}$$

$y \sim (\{0,1\}^m)^n$

Full Range

$$\Pr_{y}\left(\forall x \in X,\ y[x] \neq \beta^{x}\right) < 2^{-n \log m}$$

$y \sim (\{0,1\}^m)^n$

$$\left|\{y : \forall x \in X,\ y[x] \neq \beta^{x}\}\right| < 2^{mn - n \log m}$$

$$< |Y| \qquad \square$$

- $X \times Y = R \subseteq R_v$, $IND_m^J(X, Y)$ fixed

- $X \times Y = R \subseteq R_v$, $IND_m^J(X,Y)$ fixed
- go to bigger $R \cap R_b$, partition
  $X := \bigsqcup_j X^j$ where $X^j = \{x \in X : x[I_j] = \alpha_j\}$
  for (I_j, α_j) maximally violating $H_\infty \geq 0.95 \log m$

- $X \times Y = R \subseteq R_v$, $IND_m^J(X,Y)$ fixed
- go to bigger $R \cap R_b$, partition
  $X := \bigsqcup_j X^j$ where $X^j = \{x \in X : x[I_j] = \alpha_j\}$
  for (I_j, α_j) maximally violating $H_\infty \geq 0.95 \log m$
- remove all small $Y^{j,\beta}$, apply Full Range
  to find some $x^* \in X^j$

- $X \times Y = R \subseteq R_v$, $IND_m^J(X,Y)$ fixed
- go to bigger $R \cap R_b$, partition
  $X := \bigsqcup_j X^j$ where $X^j = \{x \in X : x[I_j] = \alpha_j\}$
  for (I_j, α_j) maximally violating $H_\infty \geq 0.95 \log m$
- remove all small $Y^{j,\beta}$, apply Full Range
  to find some $x^* \in X^j$
- query z_i for all $i \in I_j$, set $R = X^j \times Y^{j,\beta}$
  for the resulting β, add I_j to J

□

Connections

[LLZ'18]: better lifting → better sunflowers

[LMMPZ'21]: better sunflowers → better lifting

Connections

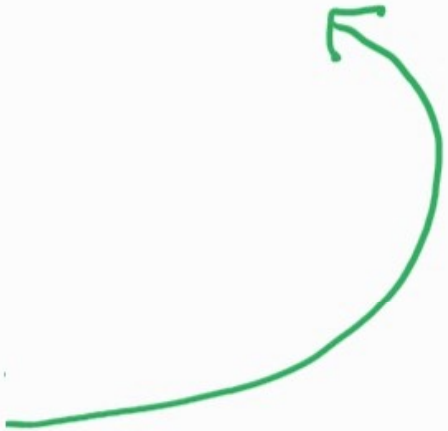
[LLZ'18]: better lifting → better sunflowers

[LMMPZ'21]: better sunflowers → better lifting

$$H_\infty \geq \cancel{0.95}^{1-\delta} \log m$$

$$\rightarrow m^{1-\delta} \geq n \log m$$

$$\rightarrow m := n^{1+\varepsilon}$$



Open Problems

$m = o(n)$? $O(1)$?

$g = IP$