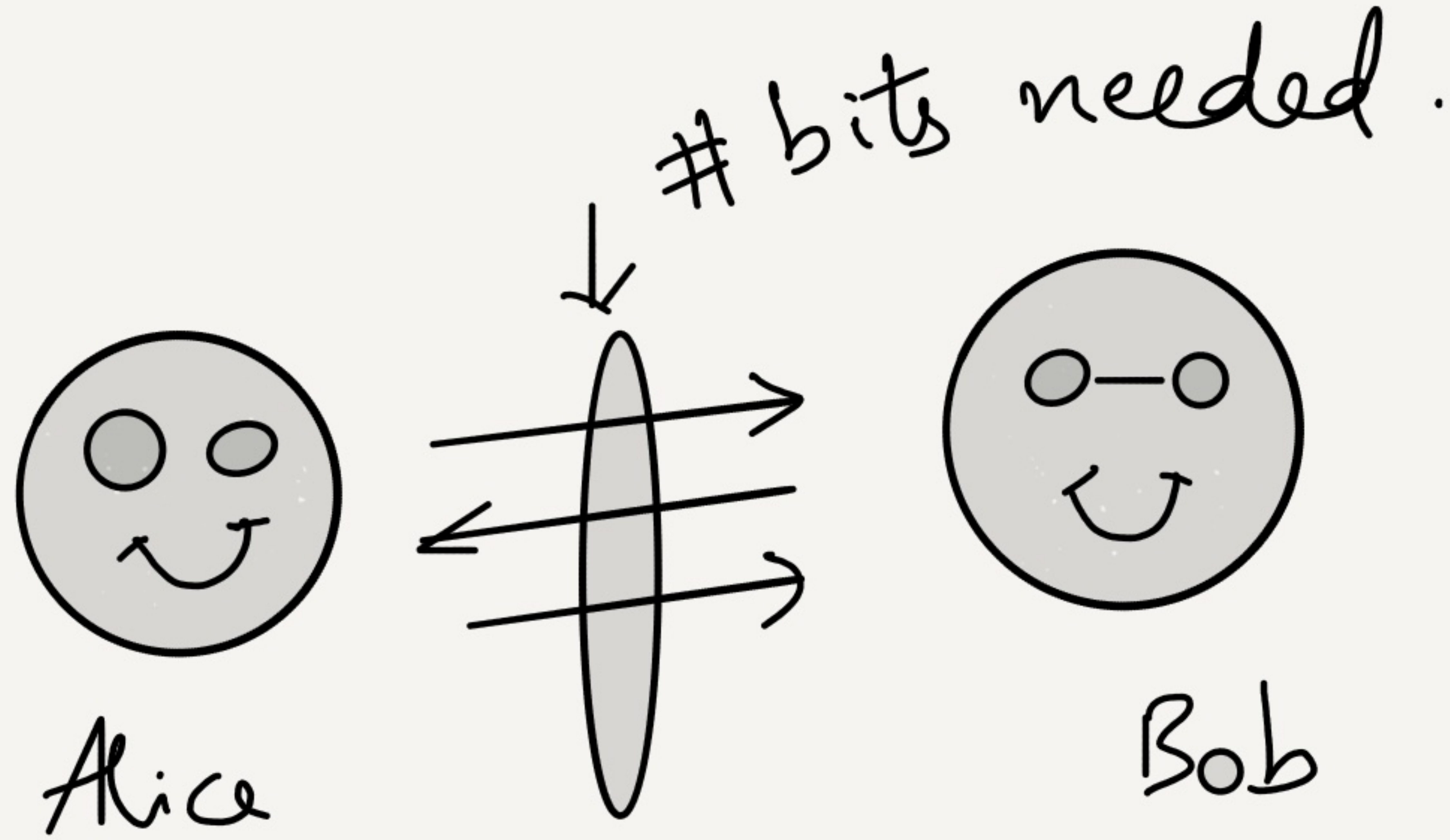
Communication Complexity.

Yao 88:



x $\qquad$ y

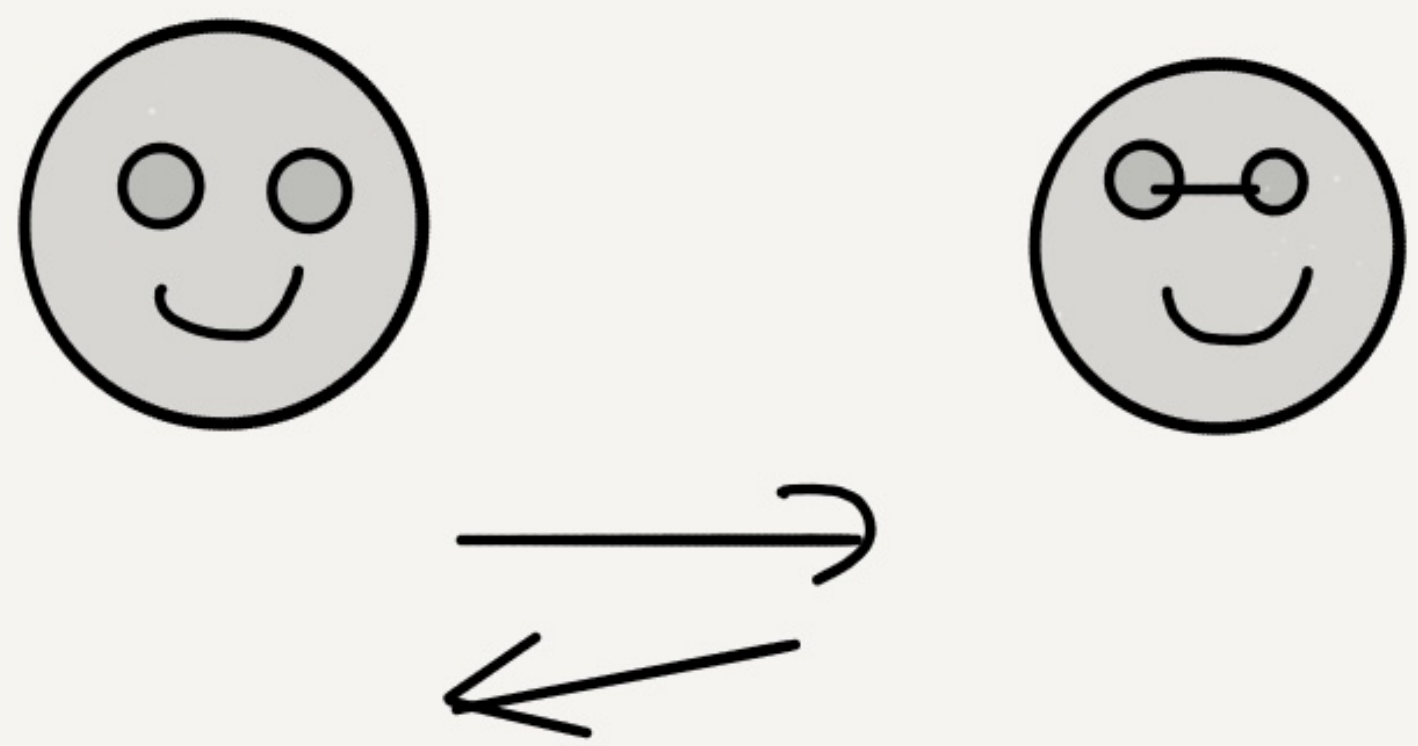
How much Communication?

$$f(x,y)$$

Model of Communication.

Deterministic

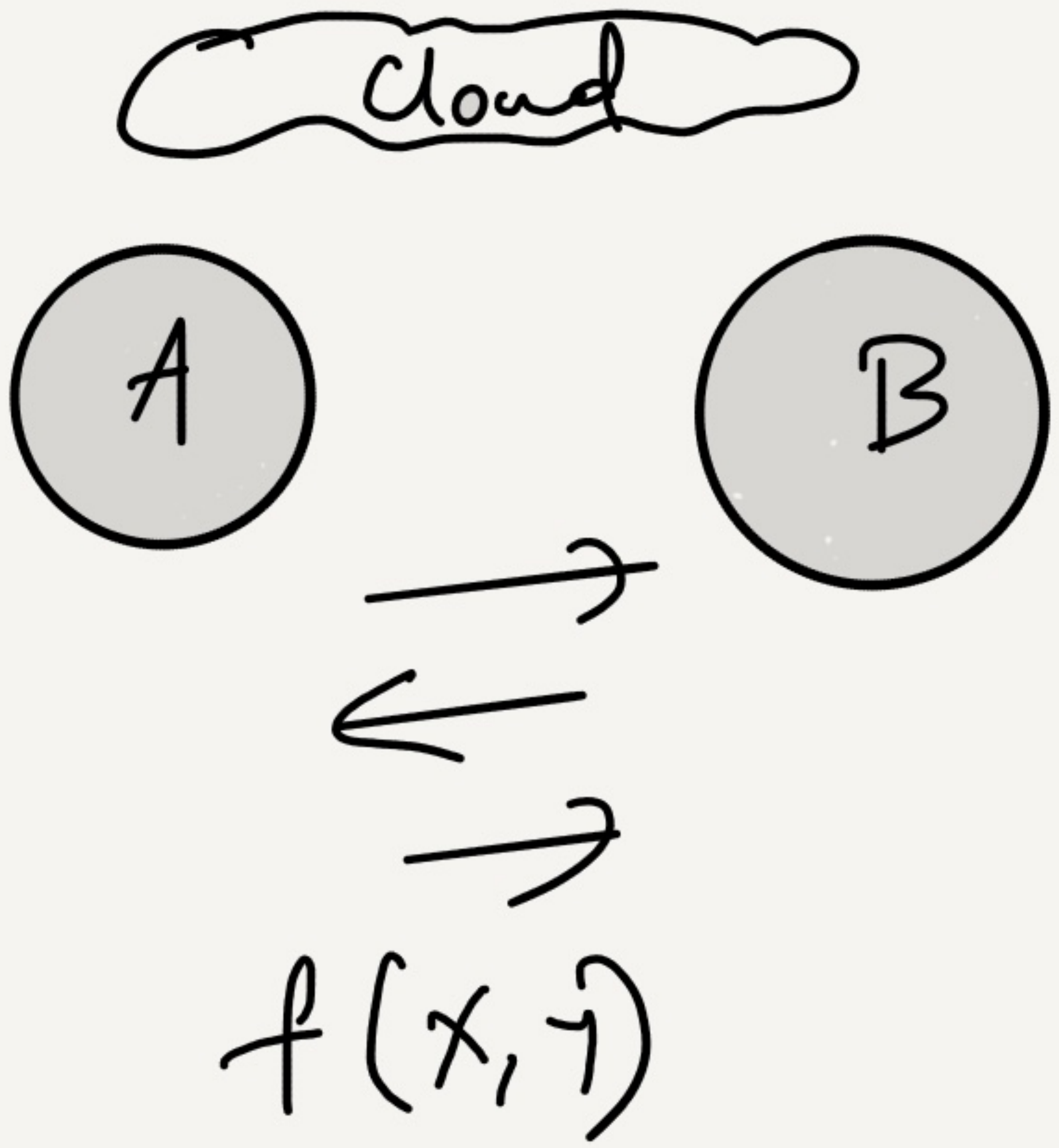
Randomized.



Det : and always output $f(x,y)$.

Rand : output $f(x,y)$ with prob. $\geq 2/3$.

Randomized Public



Randomized Private

$CC(f)$ $\quad R^{\text{Public}}_{1/3}(f)$ $\quad R^{\text{Private}}_{1/3}(f)$.

Equality

Alice $\qquad\qquad$ Bob

$x \qquad\qquad y$

$$f(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{else} \end{cases}$$

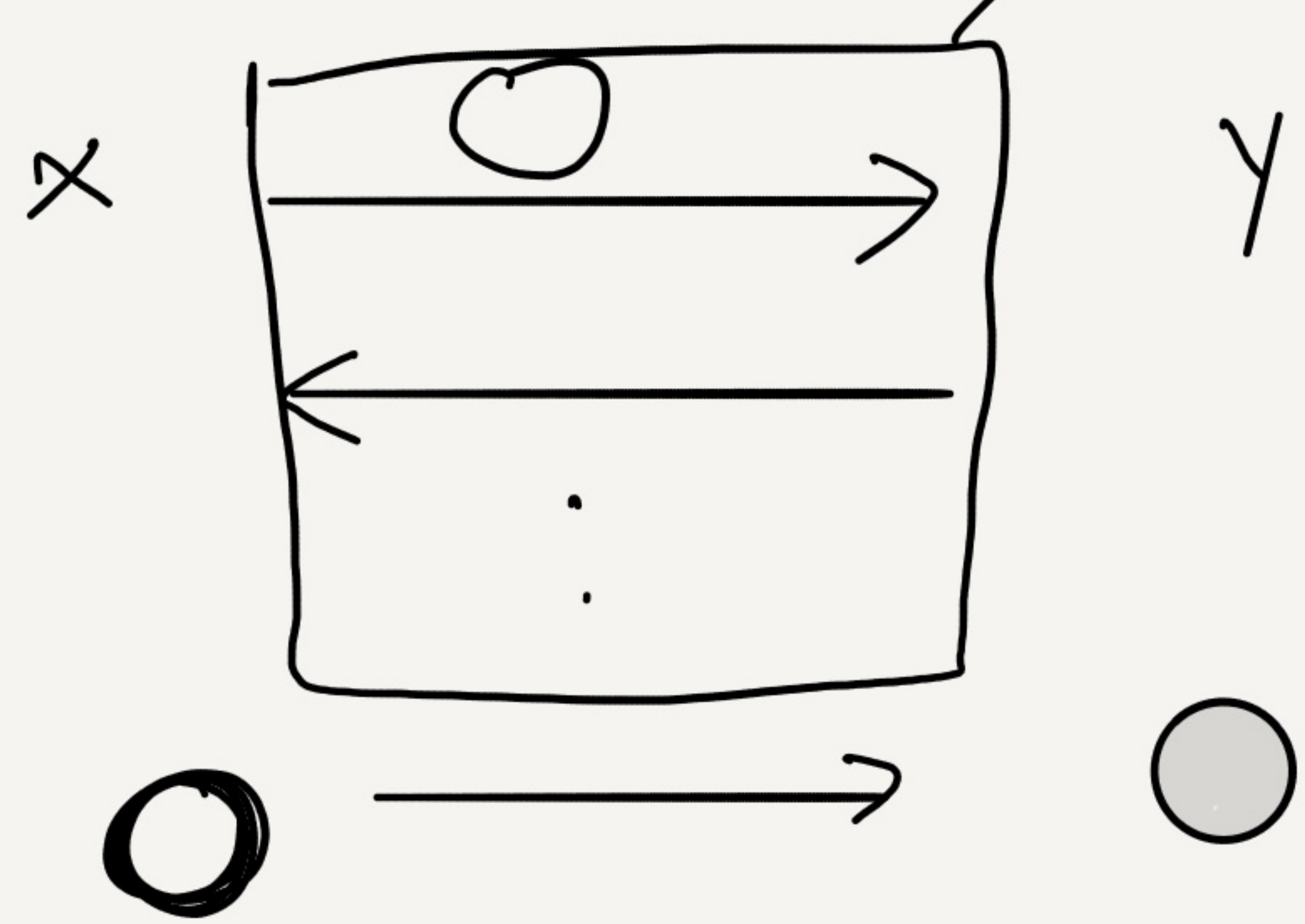
Input space : $\{0,1\}^n$

f is Boolean.

Protocal Communication:

Protocal $\boxed{\Pi}$

Transcript of protocol.



Equality

Alice $\quad\quad$ Bob

$x \quad\quad\quad y$

$$f(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{else} \end{cases}$$

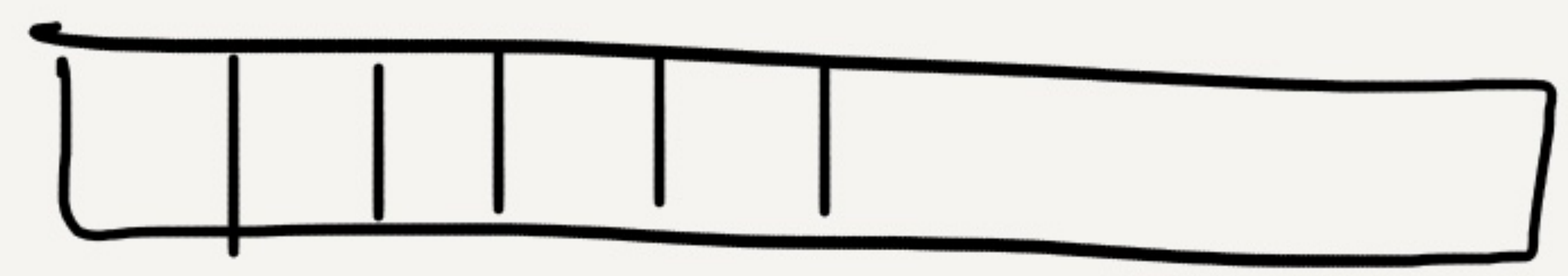
<u>Randomness:</u>

A hash function

$$h : \{0,1\}^n \to [4]$$

$$CC(EQ_n) \leq n.$$

Randomized : $\quad\quad$ Public ??



$$\underset{x}{\text{Alice}} \xrightarrow{h(x)} \text{Bob}$$

$\downarrow y$

$x = y$ if $h(x) = h(y)$

$$\Pr[\text{Error}] = \frac{1}{4} \quad (\text{if } x \neq y).$$

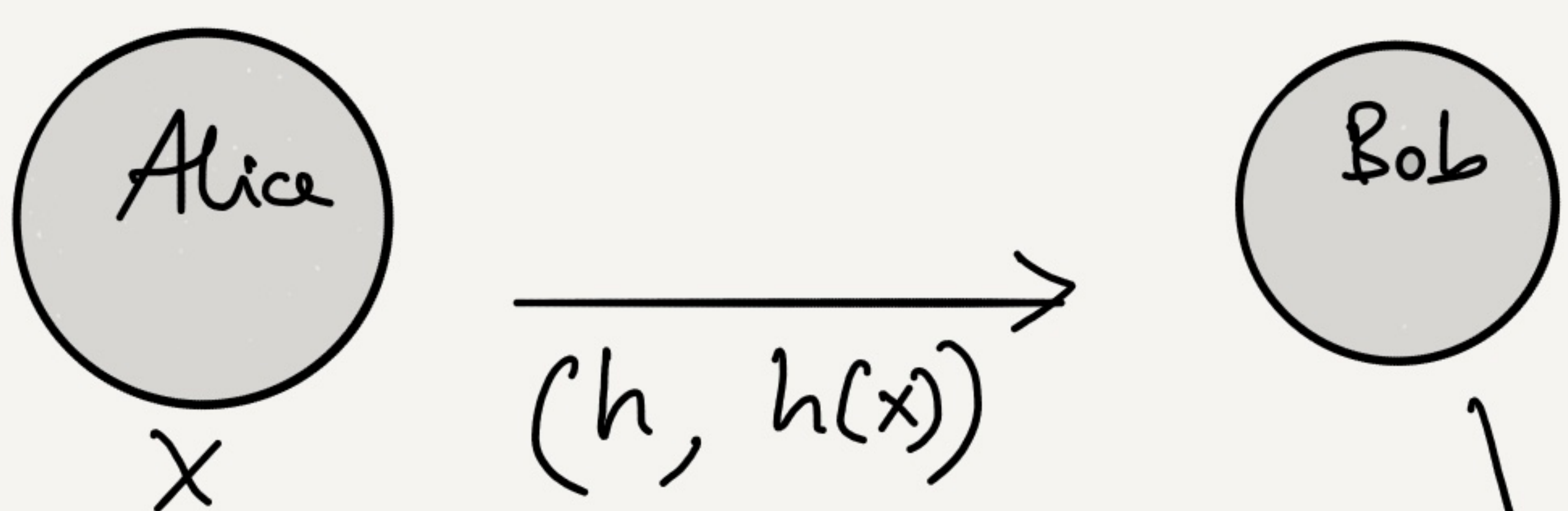
$$\boxed{R^{\text{Public}}_{1/3}(EQ) \leq 2}$$

$R^{\text{Private}}_{1/3}(EQ)$??

You can use "succinct" hash functions.

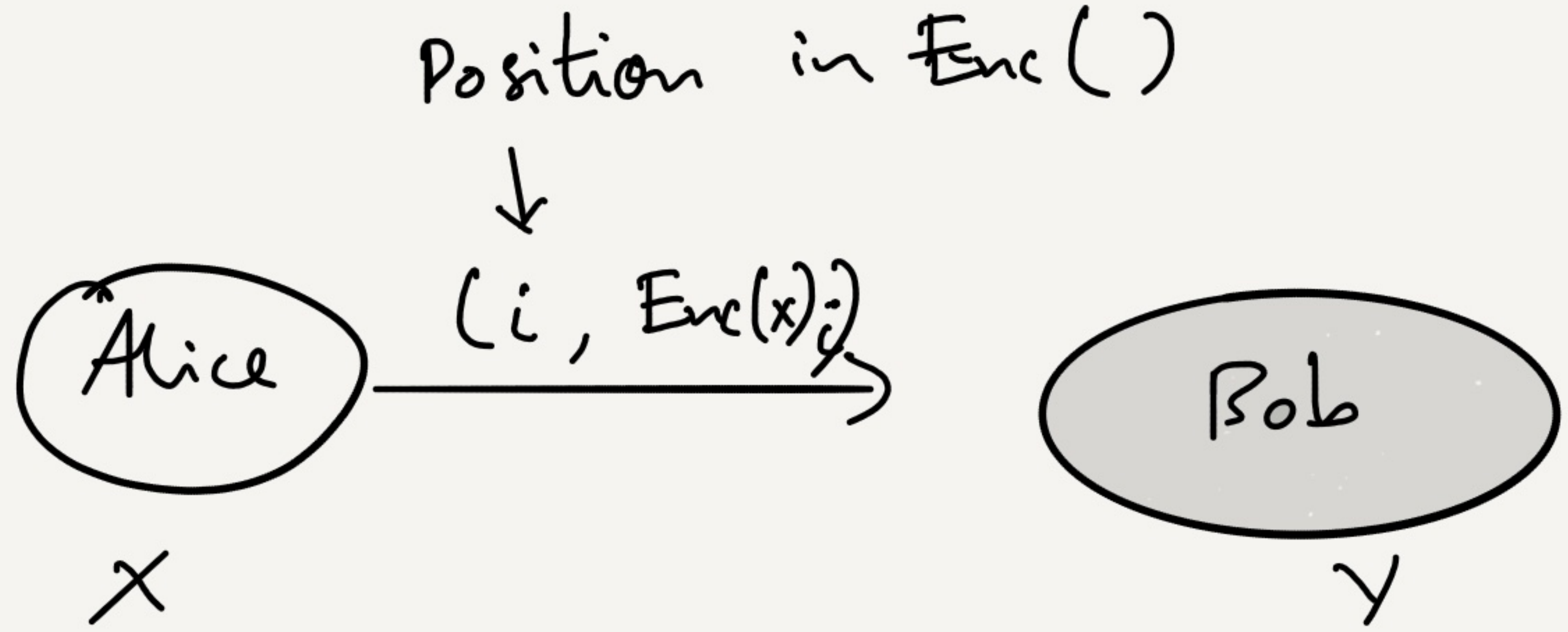
"almost Pairwise indep hash functions"

Cost $< O(\log n)$



$h \in$ Hash family

$x = y$ if $h(x) = h(y)$



Error Correcting Codes:

$$x \longrightarrow Enc(x), \quad |Enc(x)| = O(n).$$

(If $x \neq y$ $Enc(x), Enc(y)$ differ in $\geq \frac{2}{3}$ fraction of bits.)

$$R^{\text{Private}}_{1/3}(EQ) \le \log n + O(1).$$

$$R^{\text{Public}}_{1/3}(EQ) \le 2$$

$$CC(EQ) \boxed{\le} n.$$

Actually $=$.

Newman 91:

$$R^{\text{Private}}_{1/3}(f) \leq R^{\text{Public}}_{1/3}(f) + O(\log n).$$

$$CC(f) \leq 2^{O\left(R^{\text{Private}}_{1/3}(f)\right)}.$$

DISJOINTNESS:

Alice

Bob

$x \in \{0,1\}^n$

$y \in \{0,1\}^n$.

$$\mathrm{DISJ}(x,y) = \begin{cases} 1 & \text{if } \forall i,\ x_i \wedge y_i = 0 \\ 0 & \text{else.} \end{cases}$$

DISJOINTNESS:

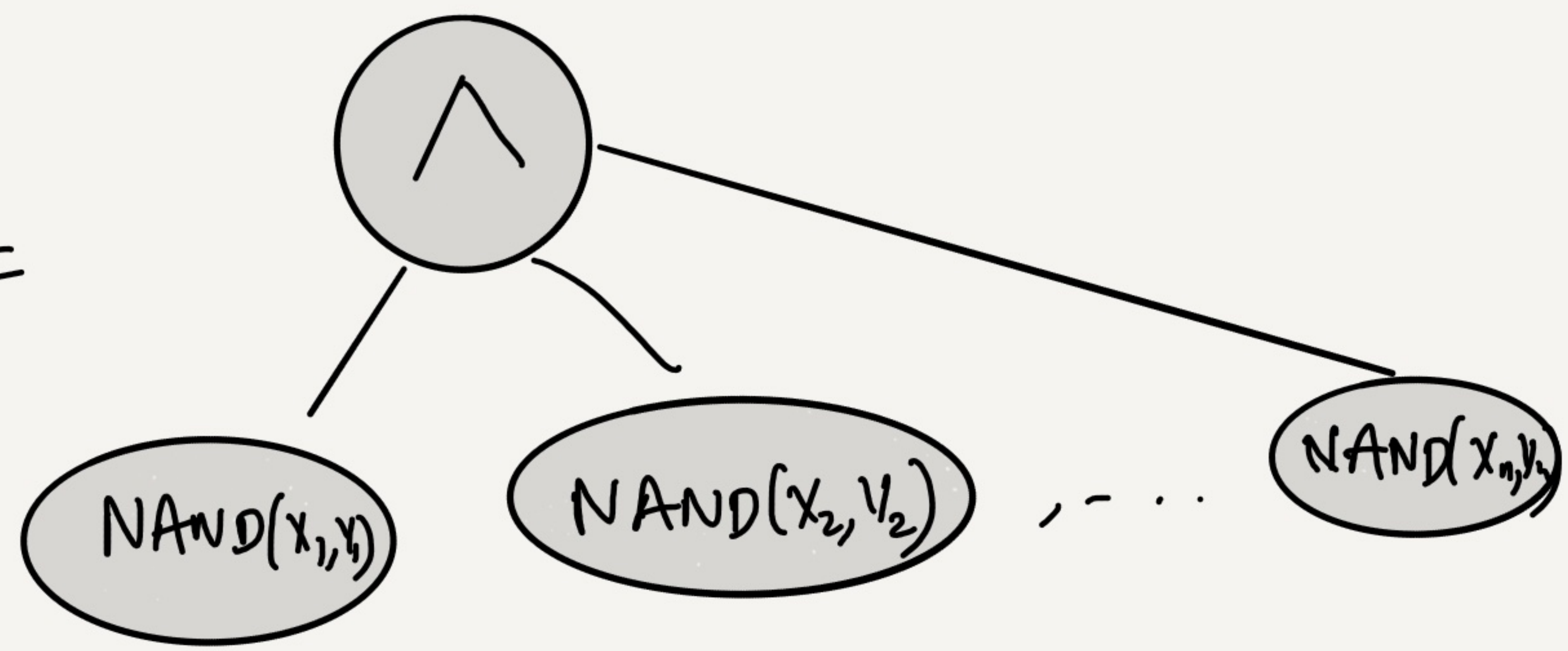
Alice

$x \in \{0,1\}^n$

Bob

$y \in \{0,1\}^n$.

$\mathrm{DISJ}(x,y) =$



$$\boxed{R^{\text{Public}}_{1/3}(\mathrm{DISJ}_n) = \Omega(n).}$$

"Cook-Levin Theorem of CC"!

KS 89

Razborov, 93

BCR 01

BJKS 04

Why Communication Complexity?

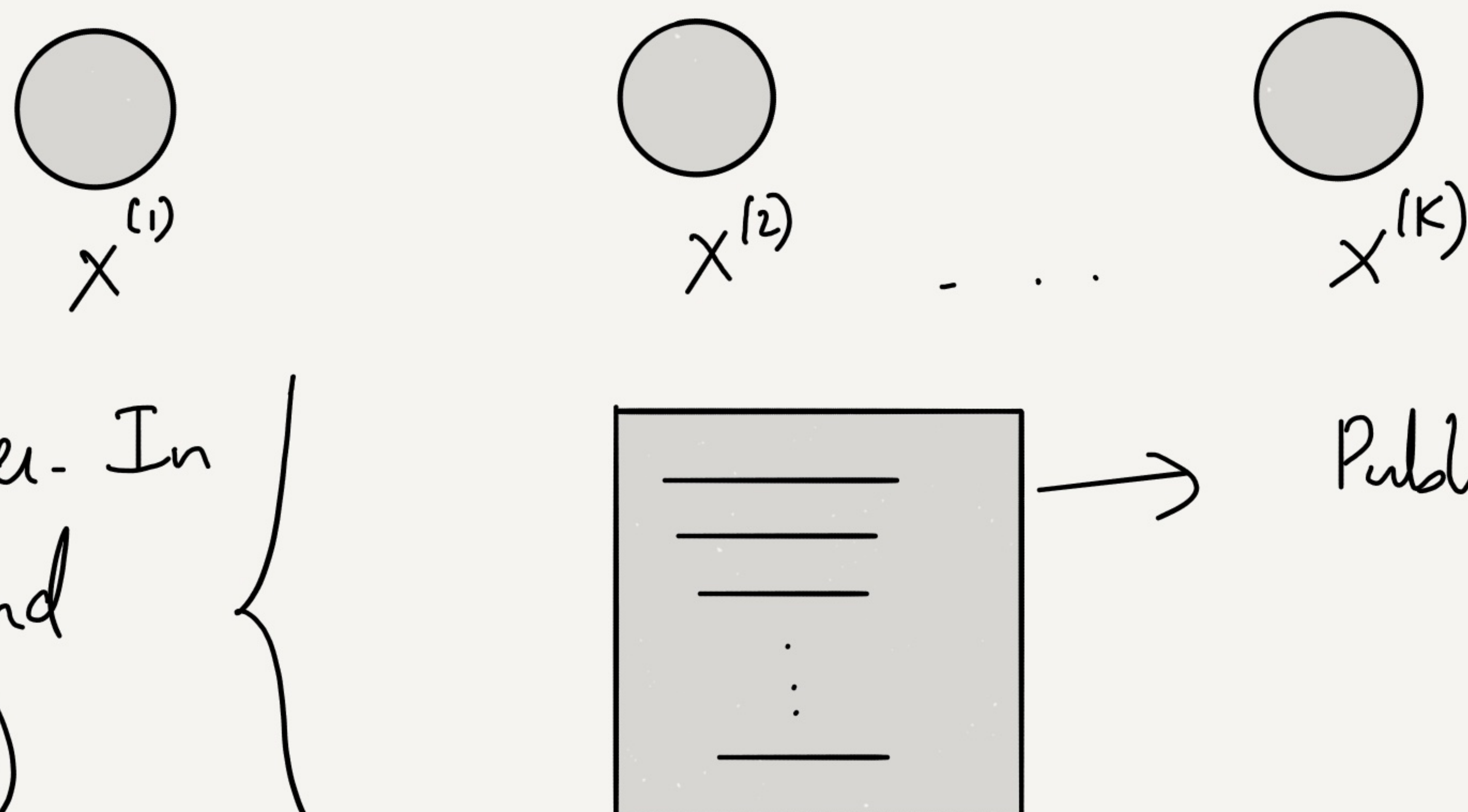
Applications:

- → Circuit Complexity?
- → Streaming algorithms
- → Data Structures
- → Optimization
- → Combinatorics

Number-On-Forehead

Chandra, Furst, Lipton 83:

Multi-party Communication:



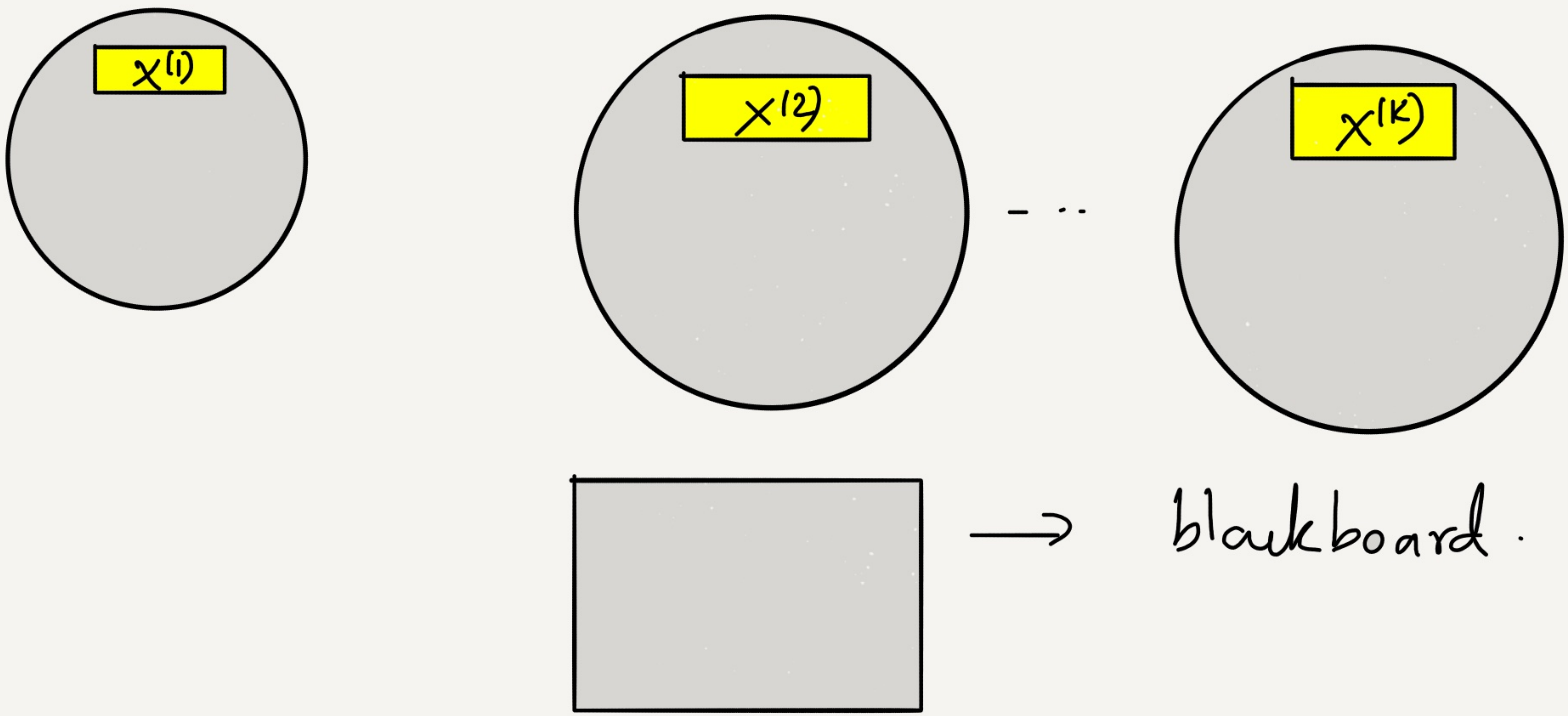
Number-In-Hand (NIH)

Public blackboard

Number-On-Forehead

Chandra, Furst, Lipton 83:

Multi-party Communication:



NOF on 3 parties.

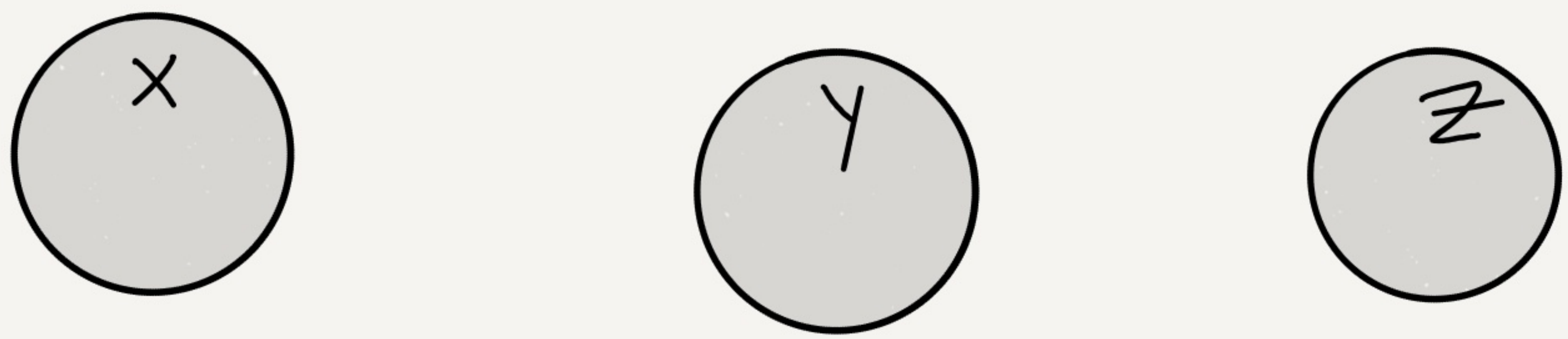
$$EQ(X, Y, Z) = \begin{cases} 1 & \text{if } X = Y = Z \\ 0 & \text{else.} \end{cases}$$

$$CC(EQ) \leq 2.$$

$$\boxed{R^{\text{Public}}_{1/3}(\text{DISJ}) = \quad ??} \rightarrow$$

We don't know.

$$\geq \sqrt{n}.$$



Inputs are numbers from

$\{-N, -N+1, \dots, 0, 1, 2, \dots, N\}$.

$$\mathrm{ZERO}(x, y, z) = \begin{cases} 1 & \text{if } x+y+z=0 \\ 0 & \text{else} \end{cases}$$

$$CC(\mathrm{ZERO}) = ??$$

$$\le \log N.$$

<u>CFL 83:</u>

$$CC(\mathrm{ZERO}) \le O\left(\sqrt{\log N}\right).$$

$$\left(\underline{\text{Ex:}} \quad R^{\text{Public}}_{1/3}(\mathrm{ZERO}) = O(1) \right)$$

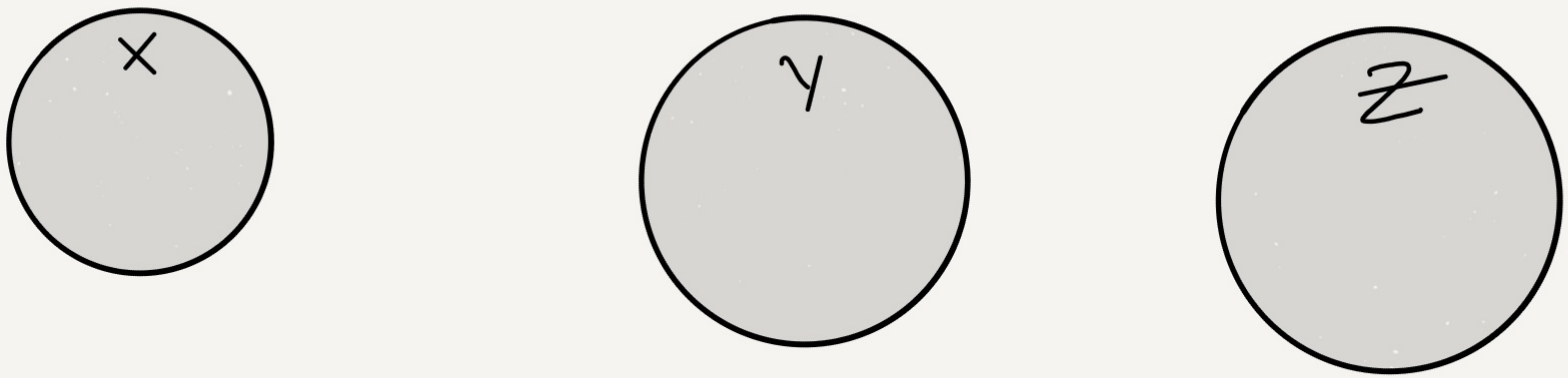
(Ref: Rao, Yehudayoff textbook)

AP-Free Coloring of $\mathbb{Z}_{2N}$.

$$\mathbb{Z}_{2N} = \{-N, -N+1, \ldots, 0, 1, 2, \ldots, N\}.$$

Color numbers with 1 through p, such that $\nexists$ no monochromatic 3-term arithmetic progression.

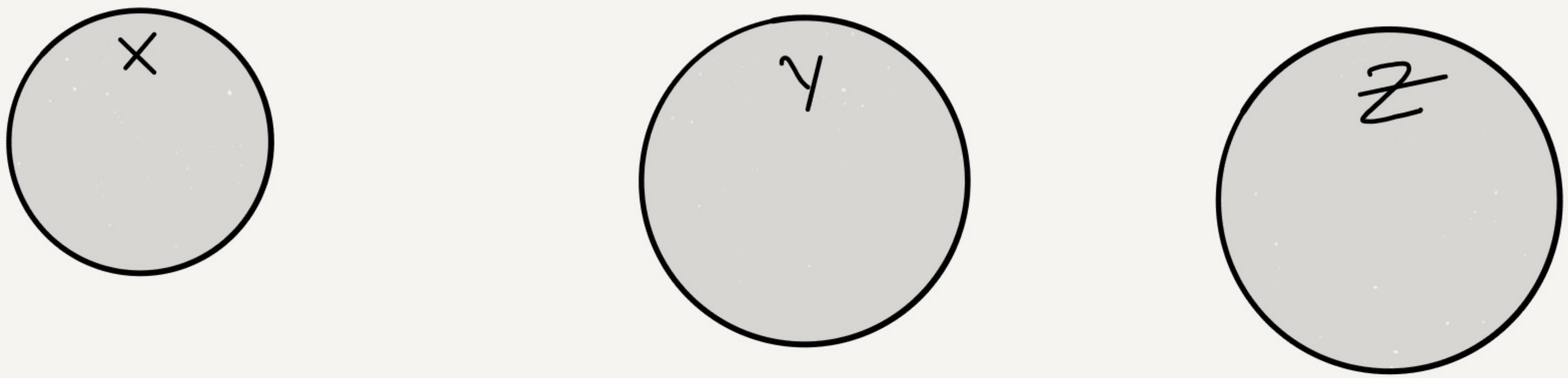
$$\boxed{\text{\underline{No} } a, b, c \text{ Same color and } b-a = c-b}$$



$$-y-2z = a \qquad x-z = b \qquad 2x+y = c$$

$$b-a = x+y+z$$

$$c-b = x+y+z$$



$a = -Y - 2Z \qquad b = X - Z \qquad c = 2X + Y$

$\mathrm{ZERO}(X, Y, Z) = 1 \Rightarrow$ a, b, c form a trivial AP

$= 0 \Rightarrow$ a, b, c form a non-trivial AP.

Protocal: Write down colorings of a, b, c.

Cost of protocol $= O(\log p)$

$\mathrm{ZERO}(x, y, z) = 0 \Rightarrow$ Colors are different

$= 1 \Rightarrow$ Colors are same.

CFL: Behrend (1946) (implicit)

AP-free Coloring with $p = 2^{O(\sqrt{\log N})}$ Colors.

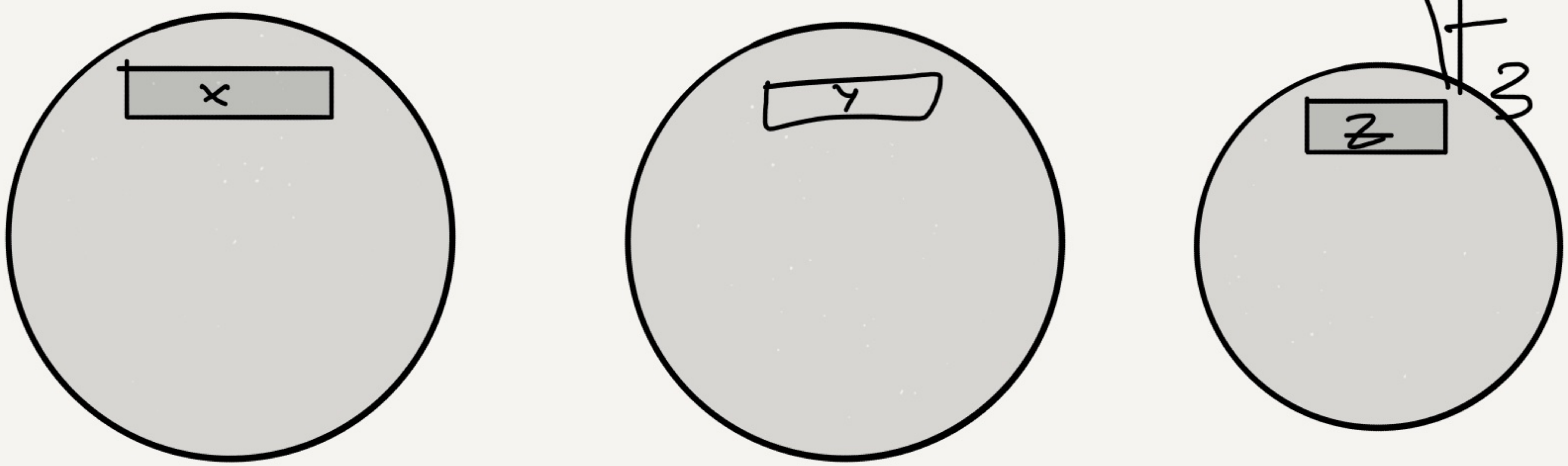
$$CC(\mathrm{ZERO}) \le \Theta\left(\sqrt{\log N}\right).$$

$$= \underline{\underline{??}}.$$

ZERO(x, y, z)

$\mathbb{Z}_{2N}$

$\mathbb{F}_3^n$.



$\boxed{??} \le CC(\text{ZERO}) \le n.$

CAP-SET (Ellenberg, Gijswijt 2016) $\geqslant c^n$ Colors

when $c > 1$.

No - Polynomial lower bounds for NOF with $> \log n$ players.

Babai, Nisan, Szegedy 89: $> \frac{n}{4^k}$

LECTURE 2 : CC

Recap:

→ Defined $CC(f)$, $R^{Public}(f)$, $R^{Private}(f)$

→ Equality, Disjointness, etc;

→ Number-On-Forehead model

- "ZERO" problem for 3 parties on $\mathbb{Z}_N$
- How about on $\mathbb{F}_3^n$??

LECTURE 2 : CC

Recap:

→ Defined $CC(f)$, $R^{\text{Public}}(f)$, $R^{\text{Private}}(f)$

→ Equality, Disjointness, etc;

→ Number-On-Forehead model

- "ZERO" problem for 3 parties on $\mathbb{Z}_N$

Clarification: $\Omega\left(\frac{\log\log N}{\log\log\log N}\right) \leq CC(\text{ZERO}_{\mathbb{Z}_N}) \leq O\sqrt{\log N}$

REF: Comm. Complexity by Rao & Yehudayoff.

Lower bounds on Communication.

→ Covering Number
→ Fooling Set Method
→ Discrepancy

} Combinatorial

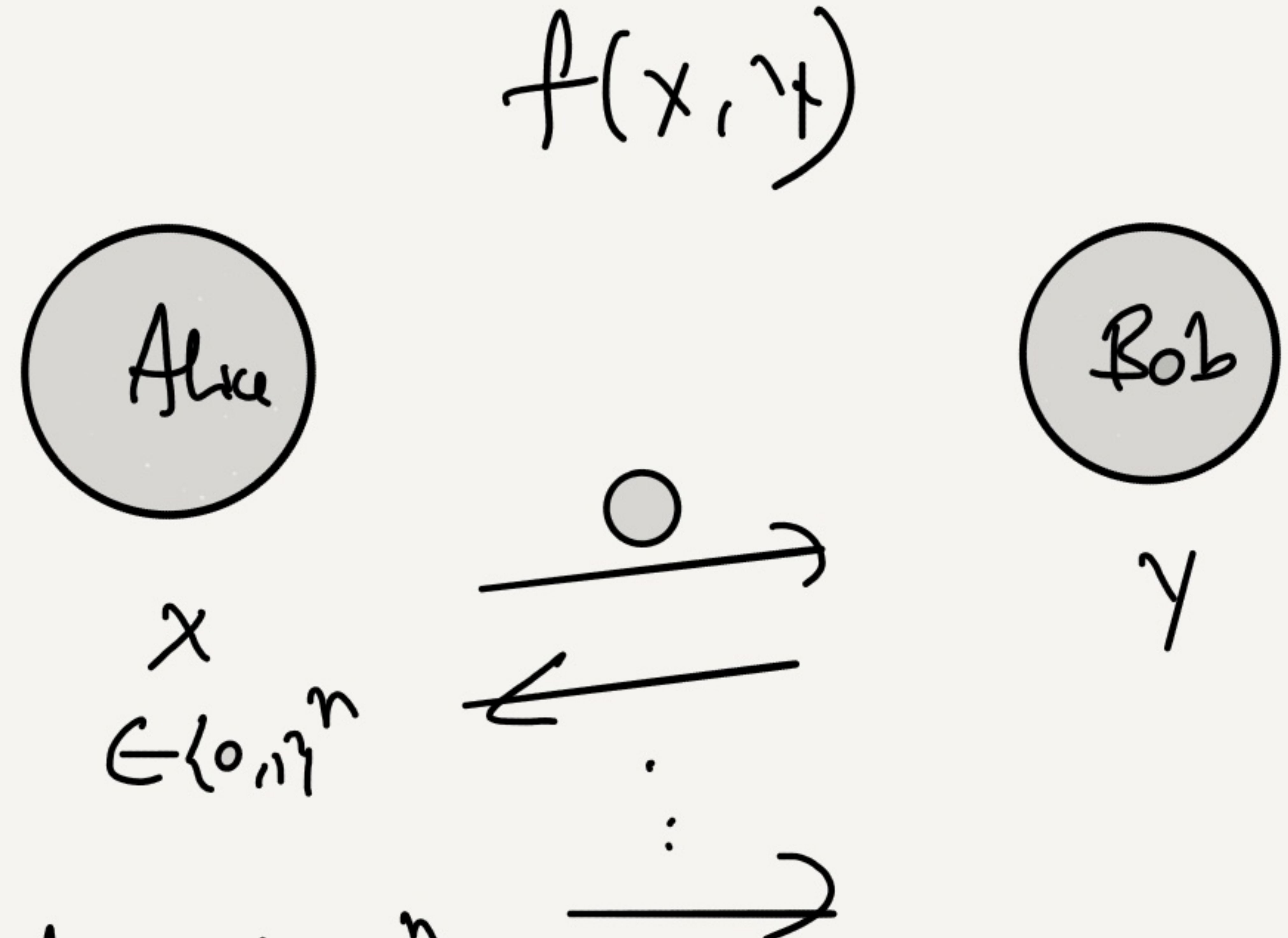
→ Corruption bound
→ Approx. rank, sign-rank, . . .

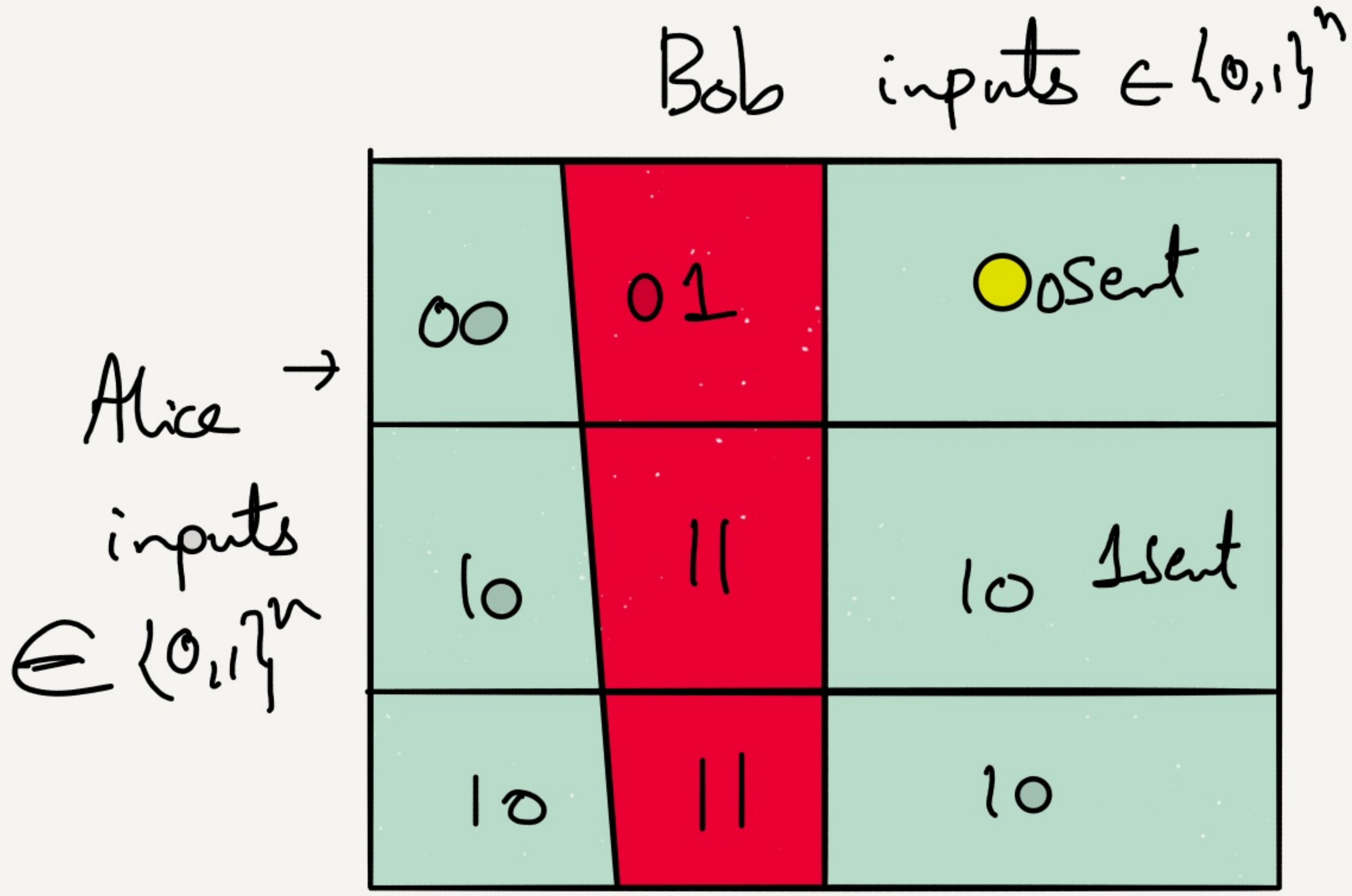
} Analytical

→ Information Cost
→ Zero-error Comm.

} Information theoretic

Protocols:


f(x, y)
Alice
Bob
x
∈{0,1}^n
y


Bob inputs ∈{0,1}^n
Alice inputs ∈{0,1}^n
00
01
0 sent
10
11
10
1 sent
10
11
10

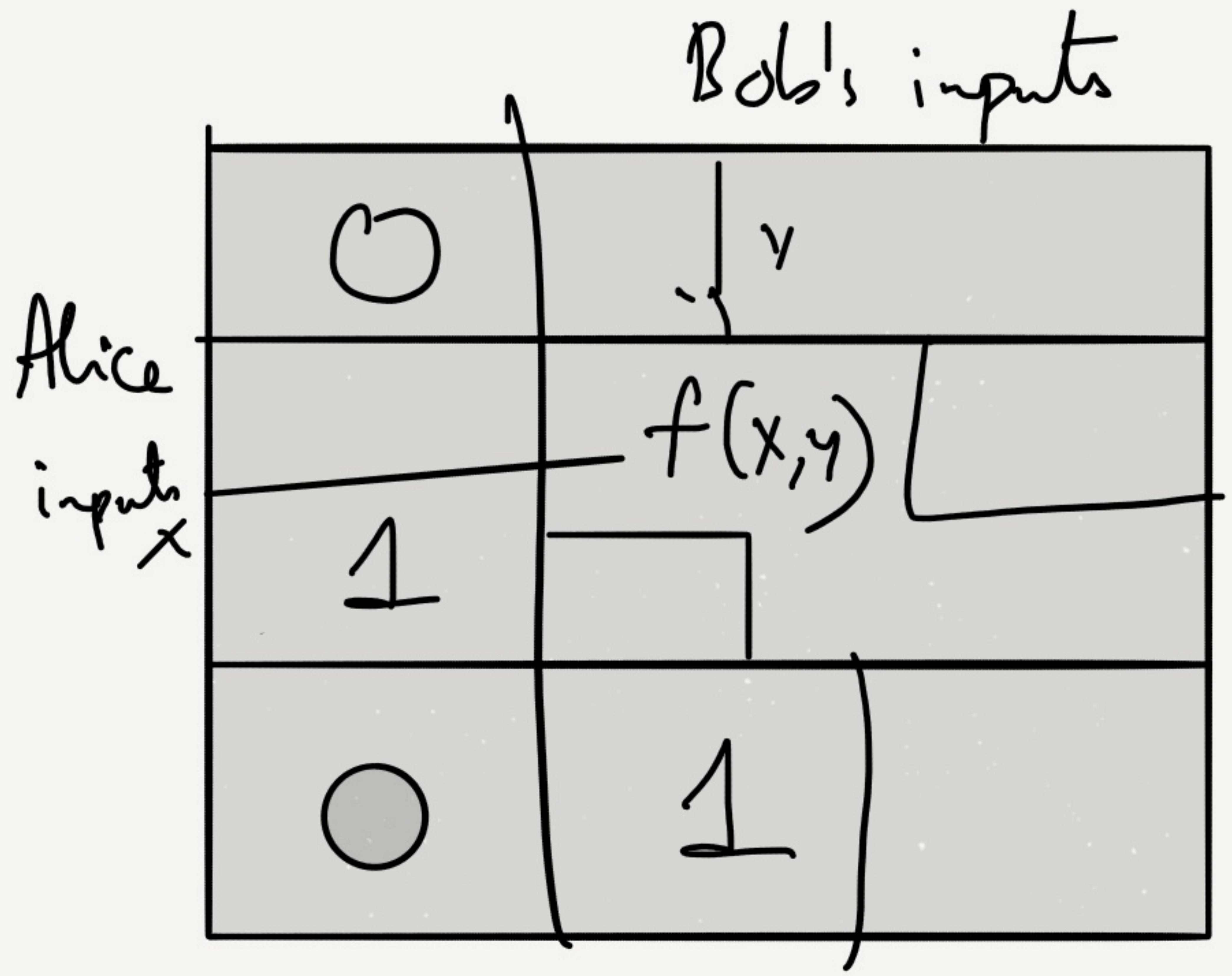
Claim: A protocol Π with $\leq C$ bits partitions the matrix into $\leq 2^C$ rectangles where Π has the same answer.

Rectangle: $A \times B$, $A \subseteq \{0,1\}^n$, $B \subseteq \{0,1\}^n$

<u>Claim:</u> If $CC(f) \le C$, then the Comm. matrix can be partitioned into $\le 2^C$ rectangles that are <u>monochromatic</u>.

$f(x,y)$

Comm. Matrix

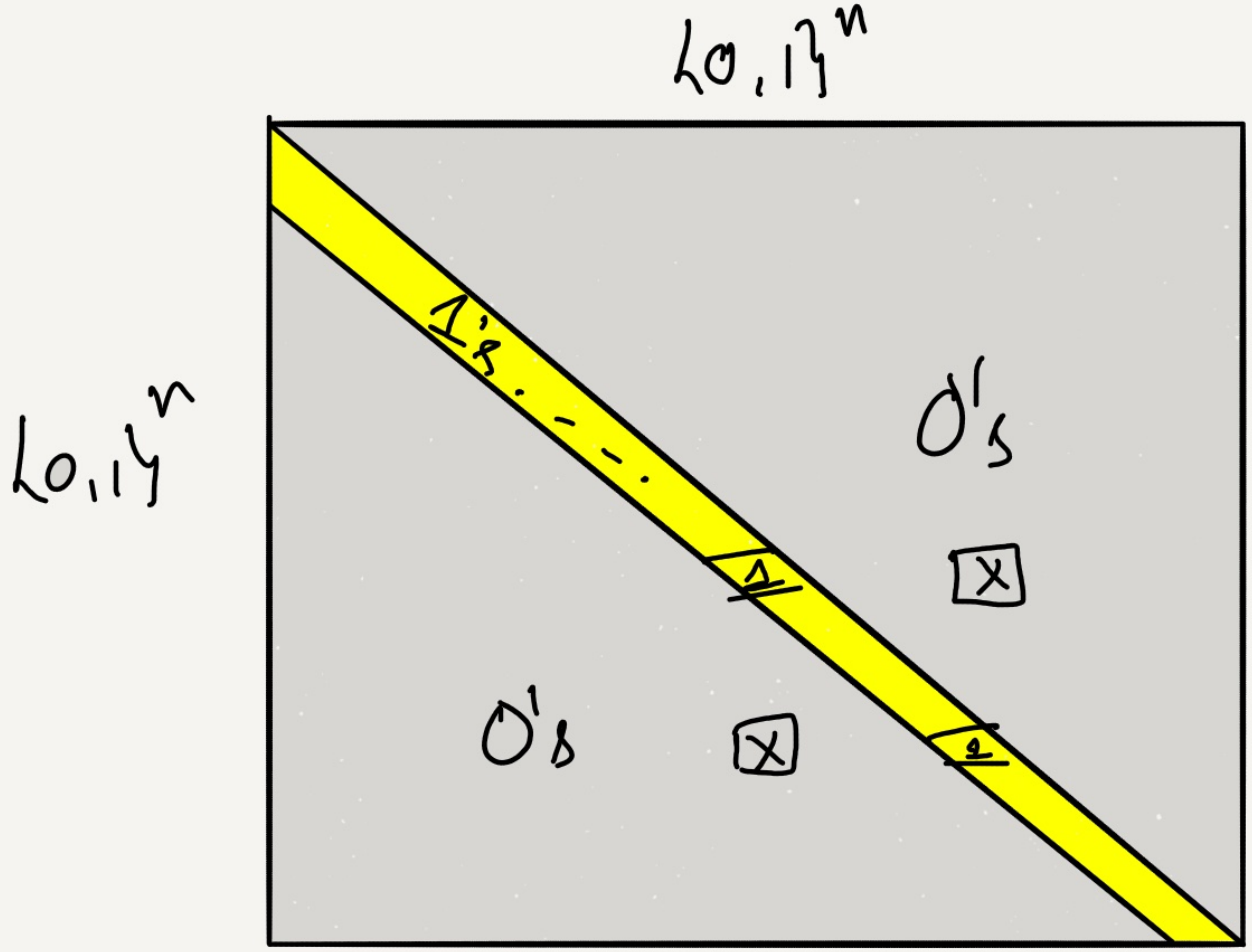


$$\mathrm{Par}(f) = \log\Big(\text{min \# monochromatic rectangles needed to partition the comm. matrix}\Big).$$

$$\boxed{\mathrm{Cov}(f) \le \mathrm{Par}(f) \le CC(f)}$$

$$\mathrm{Cov}(f) = \log\Big(\text{min \# monochromatic rectangles needed to cover all 1's (without covering 0's)}\Big).$$

Theorem: $Cov(EQ_n) = \underline{\ n\ }$.



If $< n$

$\Rightarrow < 2^n$ rectangles to cover all 1's

$\Rightarrow$ two on diagonal $\in$ same.

Theorem: $\quad Cov(DISJ_n) \geq n \cdot \left(\log\left(\frac{3}{2}\right)\right).$

(To prove optimal bound we need "Fooling-set Method").

$$\boxed{\underline{\underline{\text{Theorem:}}} \quad R_{1/3}(\mathrm{DISJ}_n) = \Omega(n).}$$

KS 89, Razborov92, $\underbrace{\text{[BCY01, BJKS04]}}_{\text{This is the proof we will see.}}$

Information Theory Primer

$$\rightarrow H(X) = \sum_{x \in \mathrm{Supp}(X)} \Pr[X=x] \cdot \log\left(\frac{1}{\Pr[X=x]}\right).$$

$$\rightarrow I(X;Y) = H(X) + H(Y) - H((X,Y)).$$

$$(\geq 0).$$

$$\rightarrow I(X;Y|Z) = \mathop{\mathbb{E}}_{z \leftarrow Z}\left[I\left(X|_{Z=z} ; Y|_{Z=z}\right)\right]$$

$X \leftarrow$ a uniformly random bit

$Y \leftarrow$ a uniformly random bit

$H(X) = H(Y) = 1$.

$I(X;Y) =$

$Z \leftarrow X \oplus Y$

$I(X;Z) = 0$, $I(Y;Z) = 0$

$I(X;Y|Z) = 1$

1. $I(X;Y) = 0$ if X, Y are independent.

$I(X;Y|Z) = 0$ if $X|_{Z=z}, Y|_{Z=z}$ are indep. $\forall z$.

2. $I(X;Y|Z) \leq I(X;Y,Y'|Z)$

3. (Chain rule)

$$I(X_1,\dots,X_n;\Pi|Y)$$
$$= \sum_{i=1}^{n} I(X_i;\Pi|Y,X_1,X_2,\dots,X_{i-1}).$$

Distributional Comm. Complexity.

Π computes f with $\frac{1}{3}$-error means

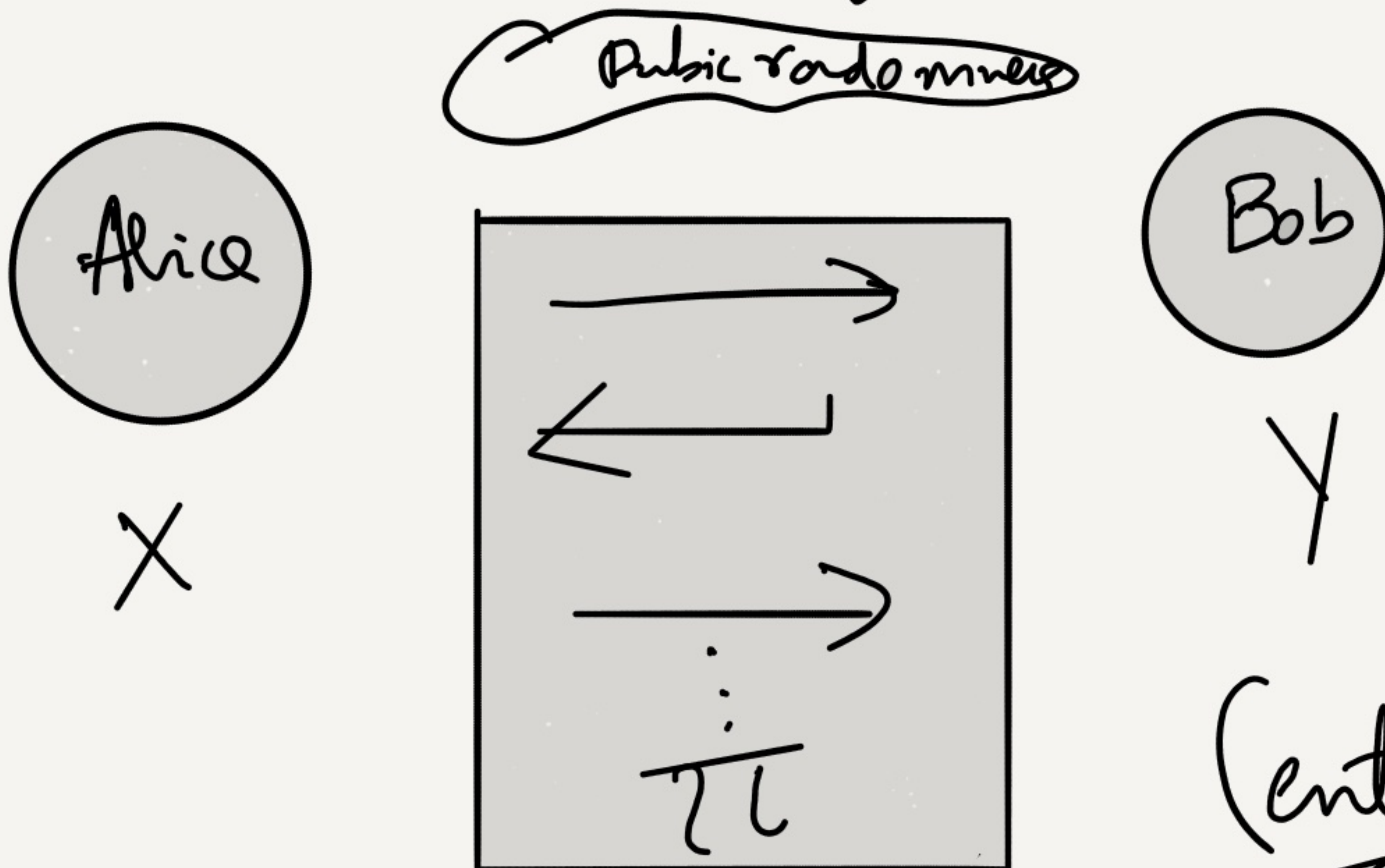
$$\forall (x,y), \quad \Pr_{\substack{\downarrow \\ \text{Public rand of } \Pi}} \left[\Pi(x,y) = f(x,y) \right] \geq \frac{2}{3}.$$

$$\Downarrow$$

Any distribution μ on (x,y), then

$$\Pr_{\substack{\downarrow \\ \text{Public rand. of } \Pi \\ (x,y) \leftarrow \mu}} \left[\Pi(x,y) = f(x,y) \right] \geq \frac{2}{3}$$

Information Cost of a protocol.



$(X,Y) \leftarrow \mu$

(entire transcript & public randomness)

$$\boxed{IC(\Pi,\mu) = I(X;\Pi \mid Y) + I(Y;\Pi \mid X)}$$

[BCR01, BJKS04] $\left(IC^{ext}(\Pi,\mu) = I((X,Y);\Pi)\right)$.

Claim: $IC(\Pi, \mu) \leq |\Pi|$

$\#$ bits exchanged $= |\Pi|$

$$I(X; \Pi \mid Y) + I(Y; \Pi \mid X)$$

Defn: $IC_\mu(f) = \min IC(\Pi, \mu)$

overall protocols that

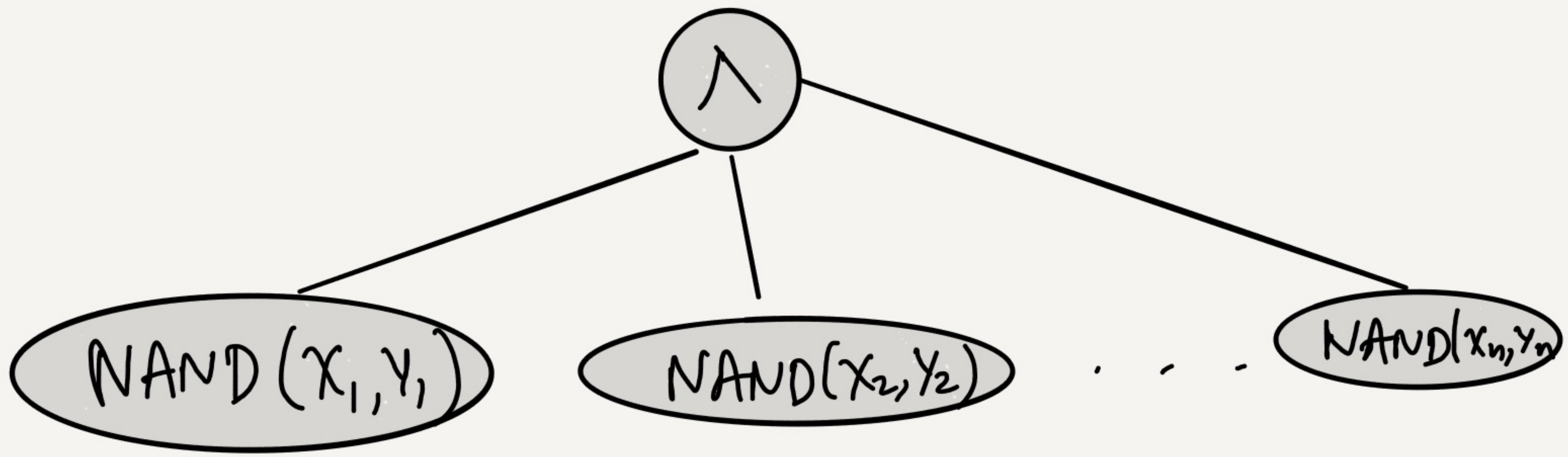
$\frac{1}{3}$-compute f.

$$IC(f) = \max_{\text{all dist } \mu} IC_\mu(f).$$

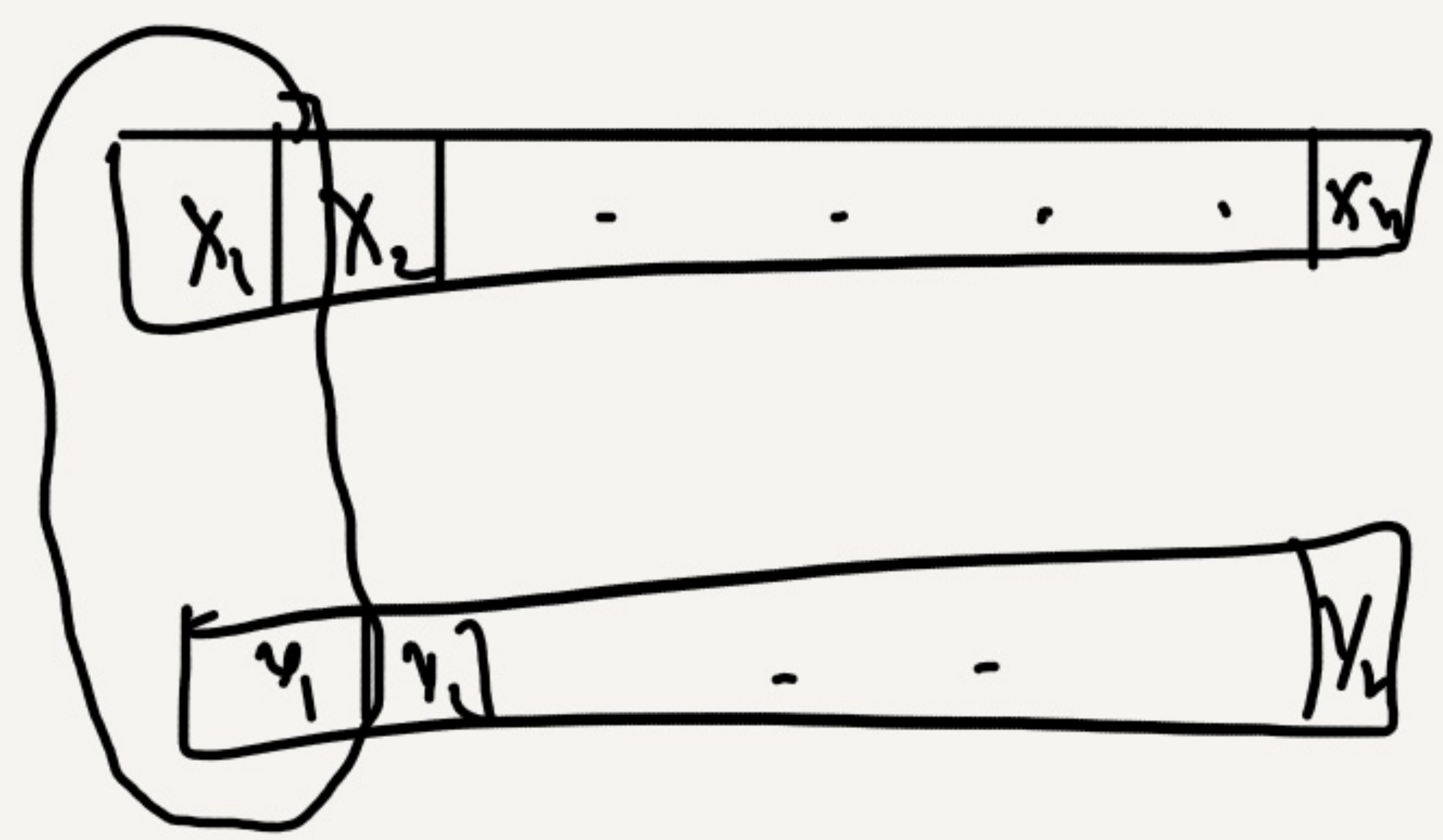
Claim: $IC(f) \leq R_{1/3}(f)$

Thm: $IC(DISJ_n) = \Omega(n).$

$DISJ_n \equiv$



Distribution:



$$\mu = \sigma^n$$

$\sigma \equiv$

$x \backslash y$	0	1
0	$\frac{1}{2}$	$\frac{1}{4}$
1	$\frac{1}{4}$	0

$$IC_{\sigma^n}(DISJ_n) = \Omega(n).$$

1. $$IC_{\sigma^n}(DISJ_n) \geq n \cdot IC_{\sigma}(NAND)$$

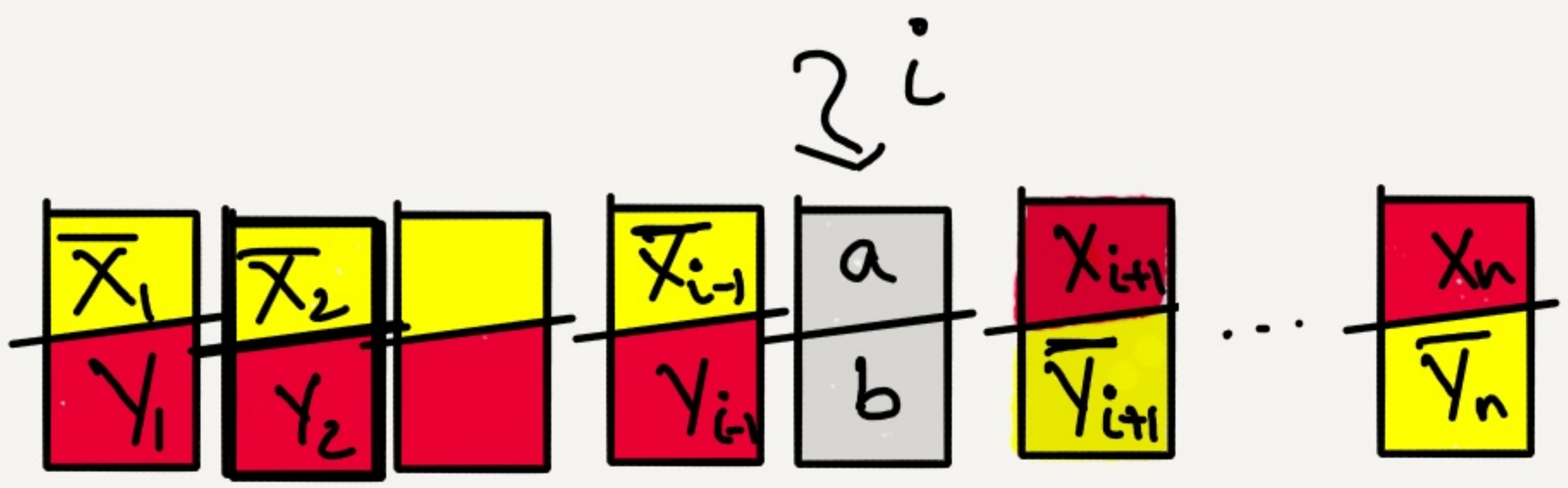
2. $$IC_{\sigma}(NAND) = \Omega(1).$$

Goal: $I_{\sigma}(\text{NAND}) \le \frac{1}{n} \cdot I_{\sigma^n}(\text{DIST}_n)$.

$\downarrow$

Π_n

Input $(a,b) \leftarrow \sigma$



(Yellow = Public; Red = private)

(This sampling from [Braverman, Rao 10])

① Pick a random $i \in_u [n]$.

② Choose $\bar{X}_1, \dots, \bar{X}_{i-1}, \bar{Y}_{i+1}, \dots, \bar{Y}_n$

③ Alice generates $X_{i+1}, X_{i+2}, \dots, X_n$ } Private randomness.
Bob generates $Y_1, Y_2, \dots, Y_{i-1}$

④ Run Π_n.

$$I(a;\pi\mid b) + I(b;\pi\mid a)$$

$$= I(a;\, i, \bar{x}, \bar{y}, \pi_n \mid b)$$

(Prop 2).

$$\le I(a;\, i, \bar{x}, y, \pi_n \mid b)$$

all n bits.

$$= I(a;\, i, \bar{x}, y \mid b) + \underbrace{I(a;\pi_n \mid i, \bar{x}, y, b)}$$

$$\parallel$$

$$0 \quad \text{(Prop 1)}$$

$$I\left(a; \Pi_n \mid i, \bar{X}, Y\right)$$

$$\leq \frac{1}{n} \sum_{j=1}^{n} I\left(X_j; \Pi_n \mid \bar{X}_1, \bar{X}_2, \ldots, \bar{X}_{j-1}, Y\right).$$

Chain rule!!

$$= \frac{1}{n} \cdot I\left(\underset{\substack{\shortparallel \\ X_1, \ldots, X_n.}}{X}; \Pi_n \mid Y\right).$$

Therefore, $$IC(\pi, \sigma) \leq \frac{1}{n} IC\left(\Pi_n, \sigma^n\right)$$

Proves Part 1.

Lecture 3

Recap:

$$\boxed{IC(\Pi,\mu) = I(X;\Pi|Y) + I(Y;\Pi|X)}$$

$$\boxed{IC_\mu(f) = \min_{\Pi:\ \frac{1}{3}\text{-Correct}} IC(\Pi,\mu)}$$

$$\boxed{IC(f) = \max_{\mu} IC_\mu(f)}$$

$$\boxed{\text{Theorem:} \quad IC(DISJ_n) = \Omega(n)}$$

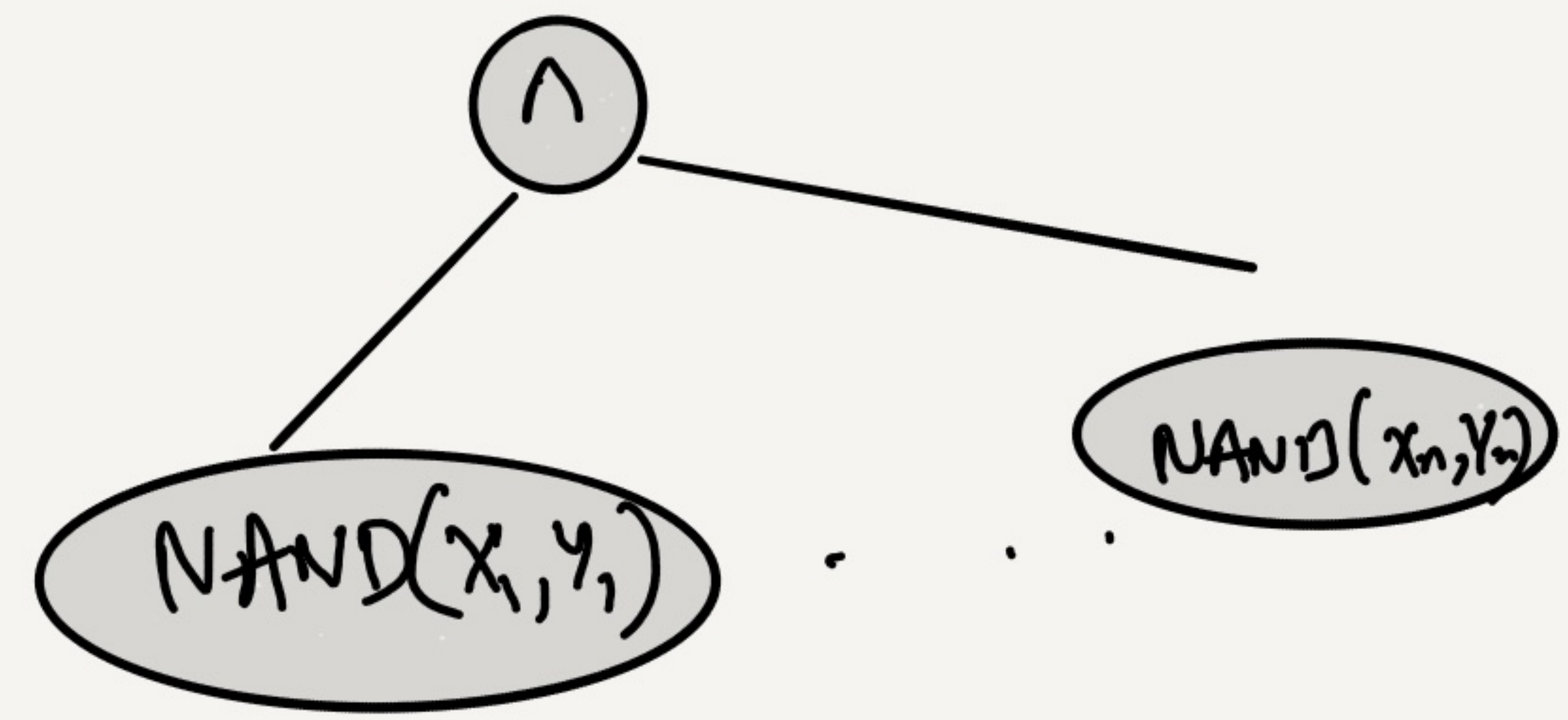
Proof: $\rightarrow$ Define $\mu = \sigma^n$.

$$\boxed{\rightarrow IC_\sigma(NAND) \leq \frac{1}{n} IC_{\sigma^n}(DISJ_n)}$$

$$\rightarrow \quad IC_\sigma(NAND) = \Omega(1).$$

Claim: $R_{1/3}(f) \geq IC(f)$

$$IC_{\sigma}(\text{NAND}) \leq \frac{1}{n} IC_{\sigma^n}(\text{DISJ}_n)$$

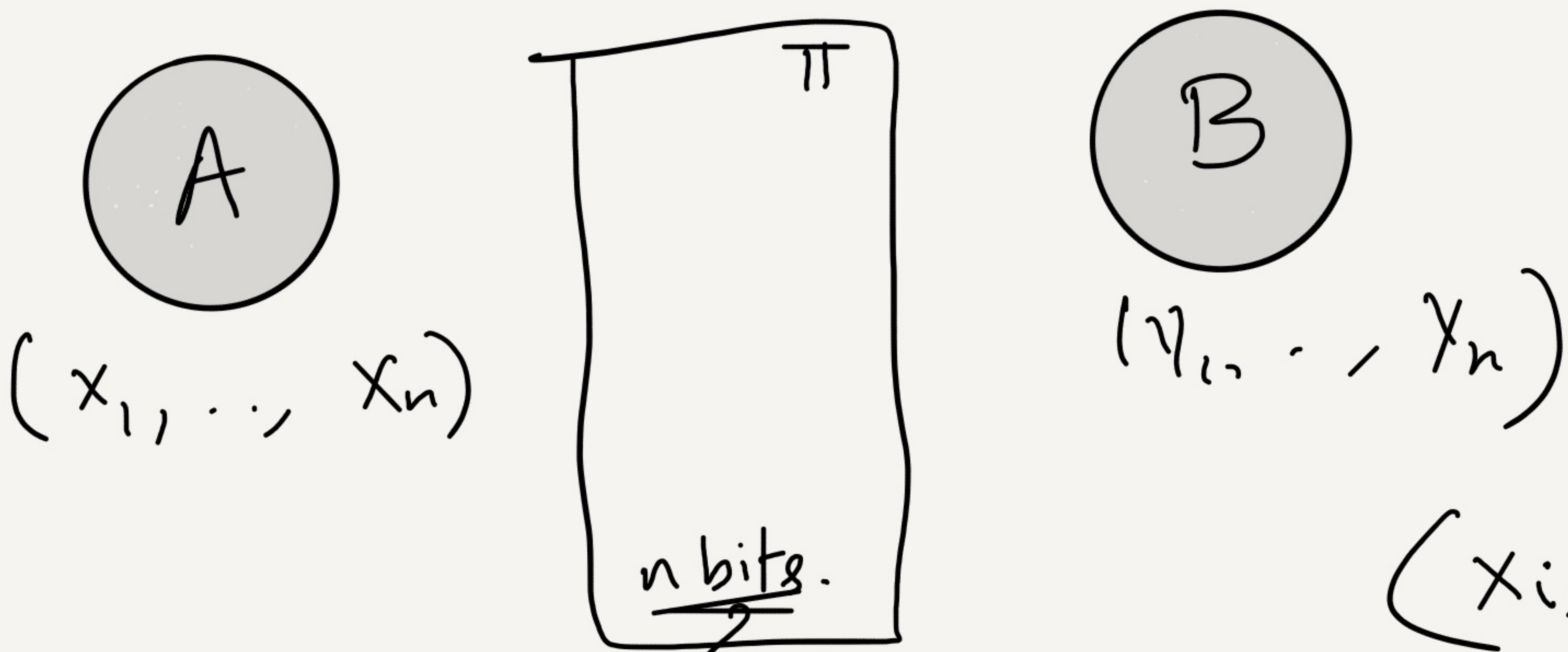


Very General:

$$IC_{\sigma}(g) \leq \frac{1}{n} IC_{\sigma^n}(g^{\otimes n})$$

$$g : A \times B \to \{0,1\}$$

$$IC_\sigma(g) \le \frac{1}{n} IC_{\sigma^n}(g^{\otimes n})$$

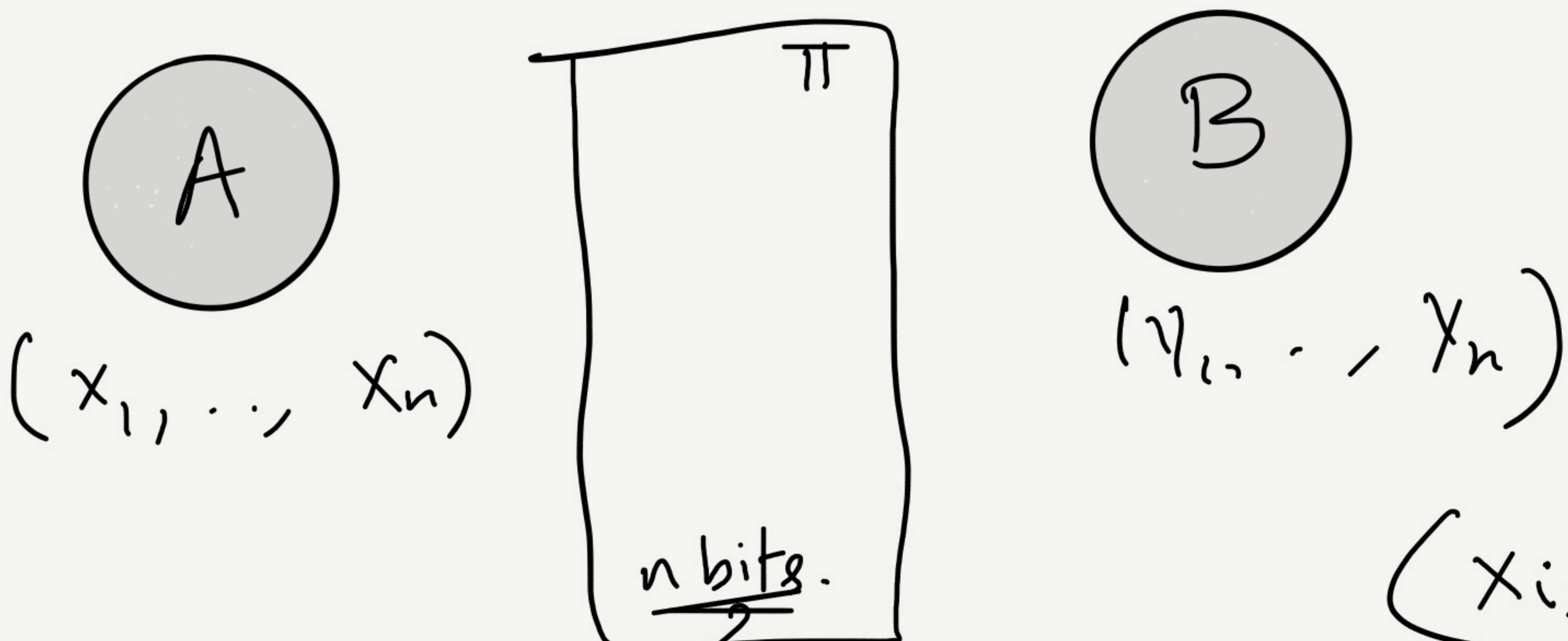


$(x_i, y_i) \leftarrow \sigma$

Π is $\frac{1}{3}$ - correct for $g^{\otimes n}$

if $\Pr[\text{correct for any } i] \ge \frac{2}{3}$.

$$IC_{\sigma}(g) \leq \frac{1}{n} IC_{\sigma^n}(g^{\otimes n})$$



$(x_i, y_i) \leftarrow \sigma$

$$\boxed{R_{1/3}(g) \overset{?}{\leq} \frac{1}{n} R_{1/3}(g^{\otimes n})}$$

Open:

$$R_{1/3}(g) \overset{?}{\leq} \frac{1}{n} R_{1/3}(g^{\otimes n})$$

(BBCR10)

$$\leq \frac{1}{\sqrt{n}} R_{1/3}(g^{\otimes n})$$

$$(\log R_{1/3}(g)).$$

$$IC(g) \leq \frac{1}{n} IC(g^{\otimes n})$$

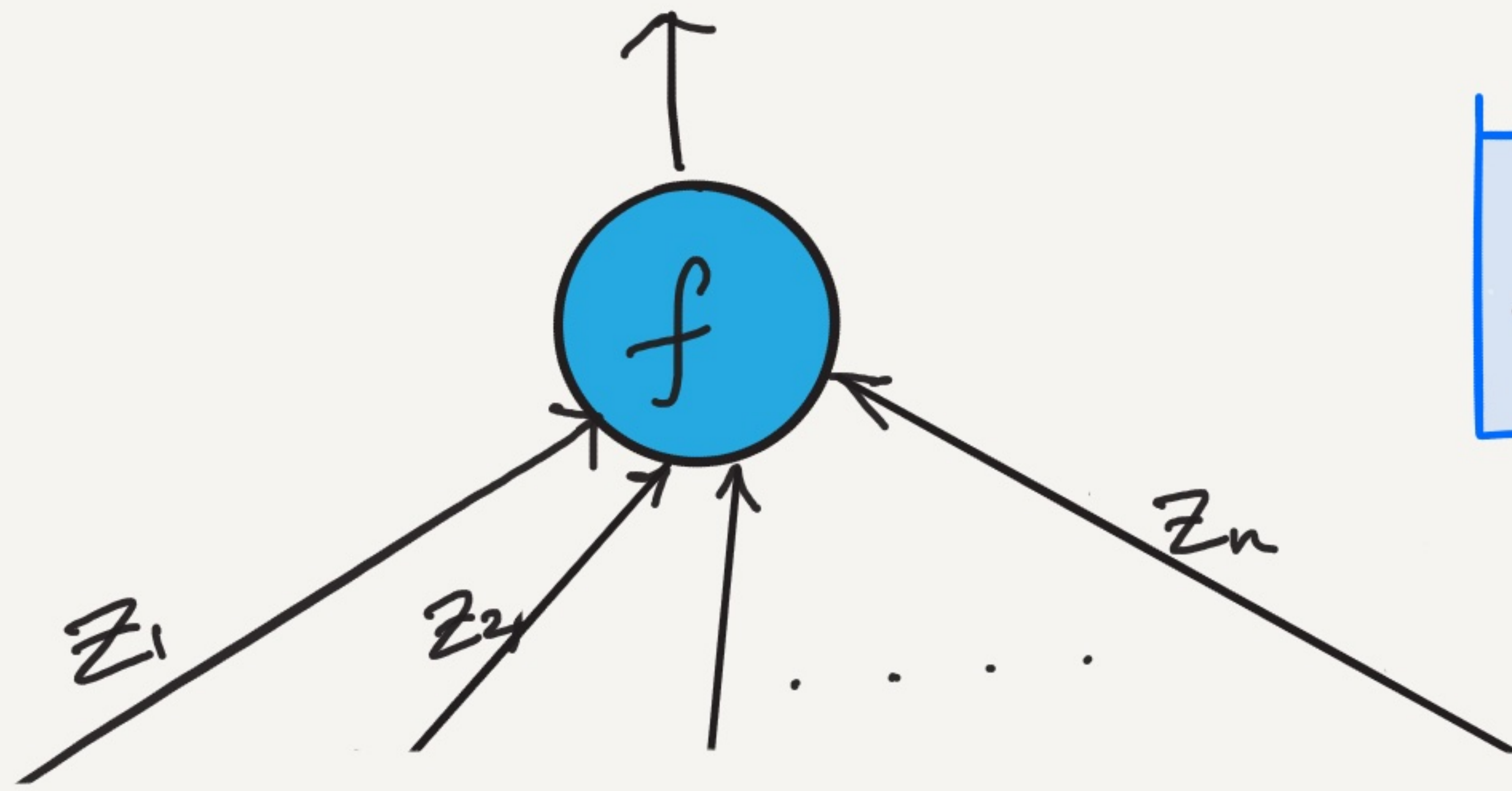
Open: $$R_{1/3}(g) \overset{?}{\le} \frac{1}{n} R_{1/3}(g^{\otimes n})$$

(Barak, Braverman, Chen, Rao 10)

$$IC(g) \le \frac{1}{n} IC(g^{\otimes n})$$

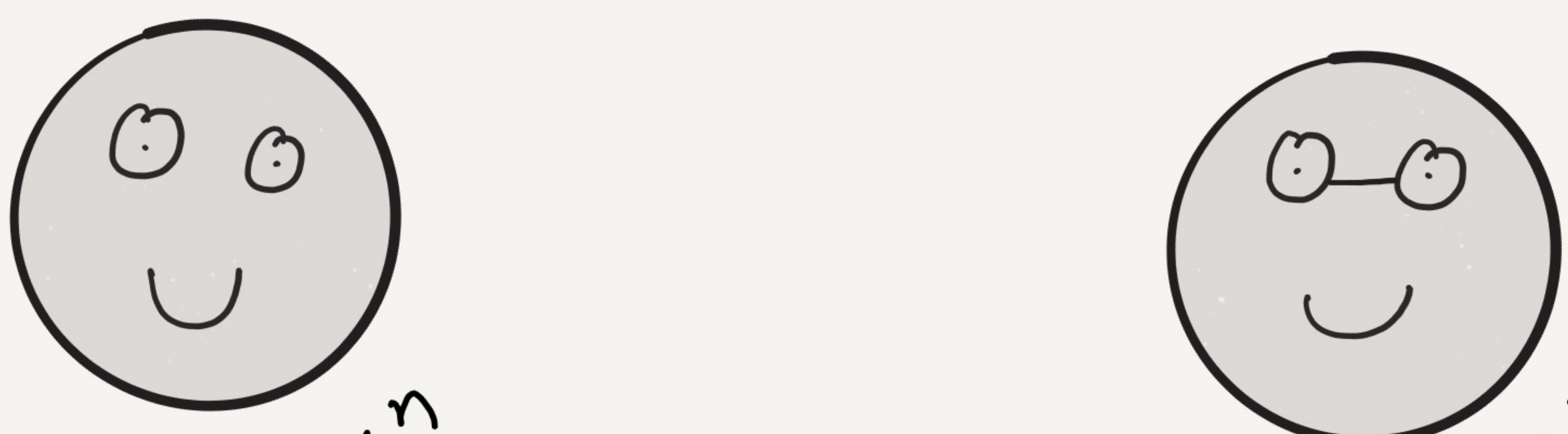
If $$R_{1/3}(g) \not\le O(IC(g))$$

LIFTING THEOREMS



$f : \{0,1\}^n \longrightarrow \mathbb{R}$

$g : A \times B \longrightarrow \{0,1\}$

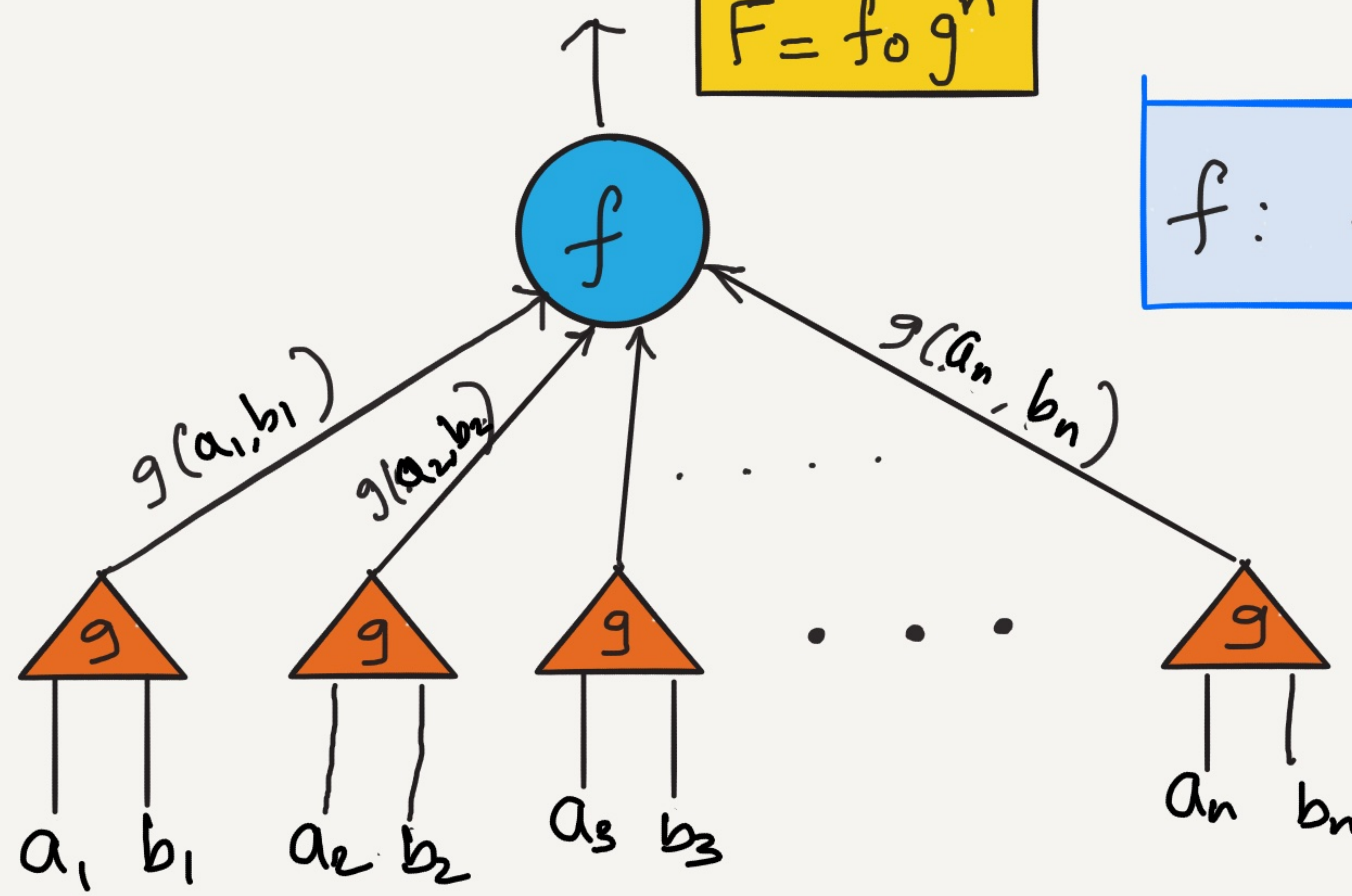


$a \in A^n$ $b \in B^n$

LIFTING THEOREMS

$F = f \circ g^n$

$f : \{0,1\}^n \longrightarrow \mathbb{R}$

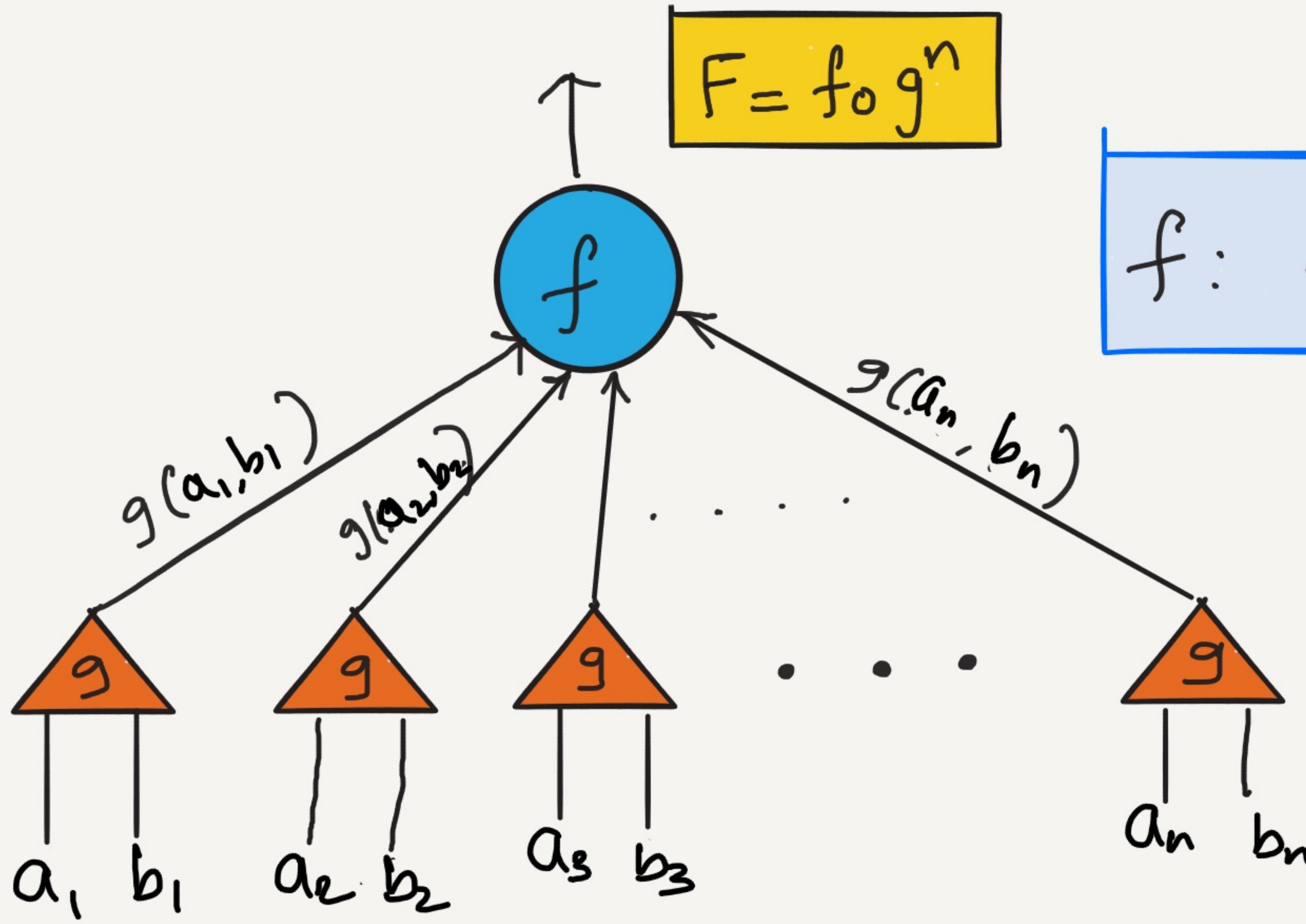


$g : A \times B \longrightarrow \{0,1\}$

$DISJ_n$: $f =$ AND; $g =$ NAND

EQ: $f =$ AND; $g =$ EQ

LIFTING THEOREMS



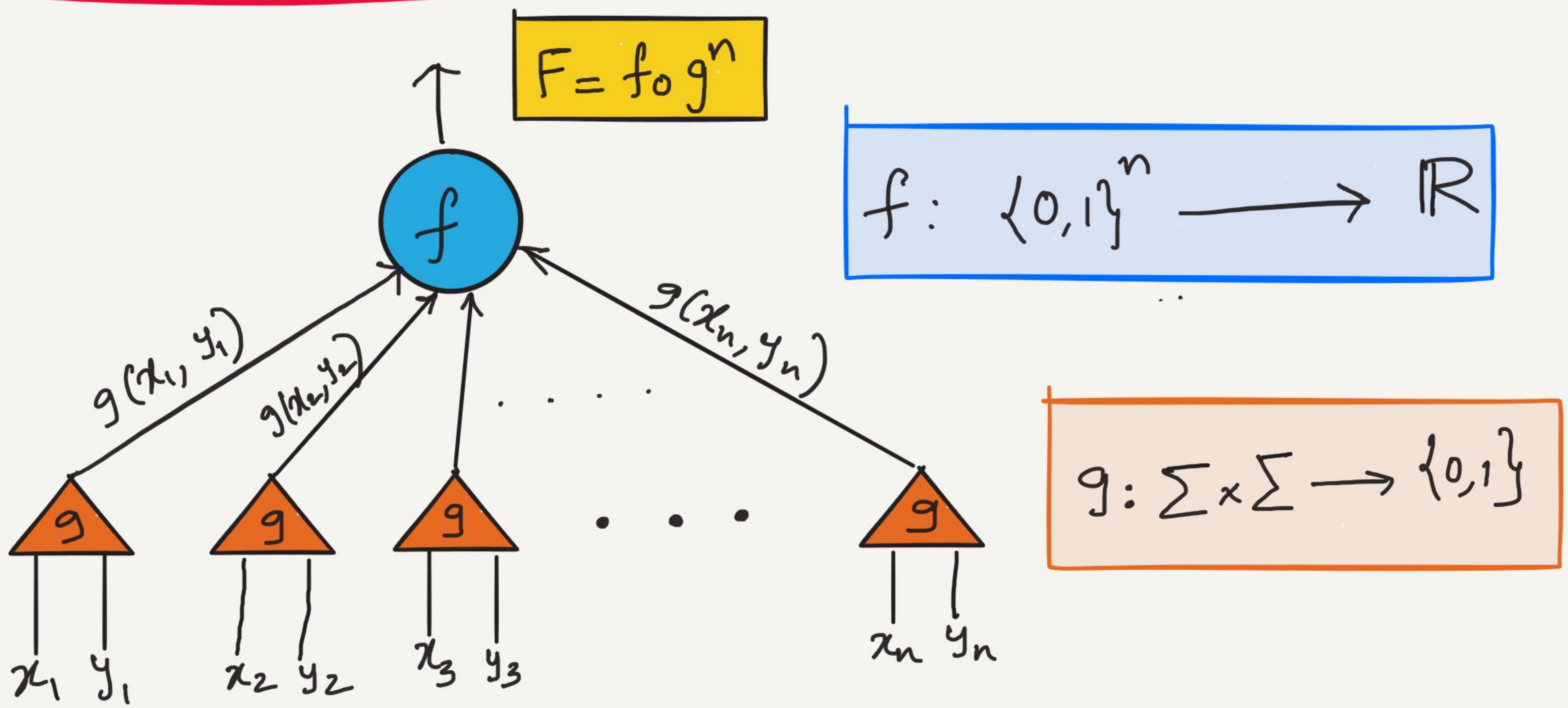
$f : \{0,1\}^n \longrightarrow \mathbb{R}$

$g : A \times B \longrightarrow \{0,1\}$

MAIN CHALLENGE: (FOR A SUITABLE g)

COMM. COMP. (F) $\approx$ SOME-MEASURE (f)?

LIFTING THEOREMS



MAIN CHALLENGE: (FOR A SUITABLE g)

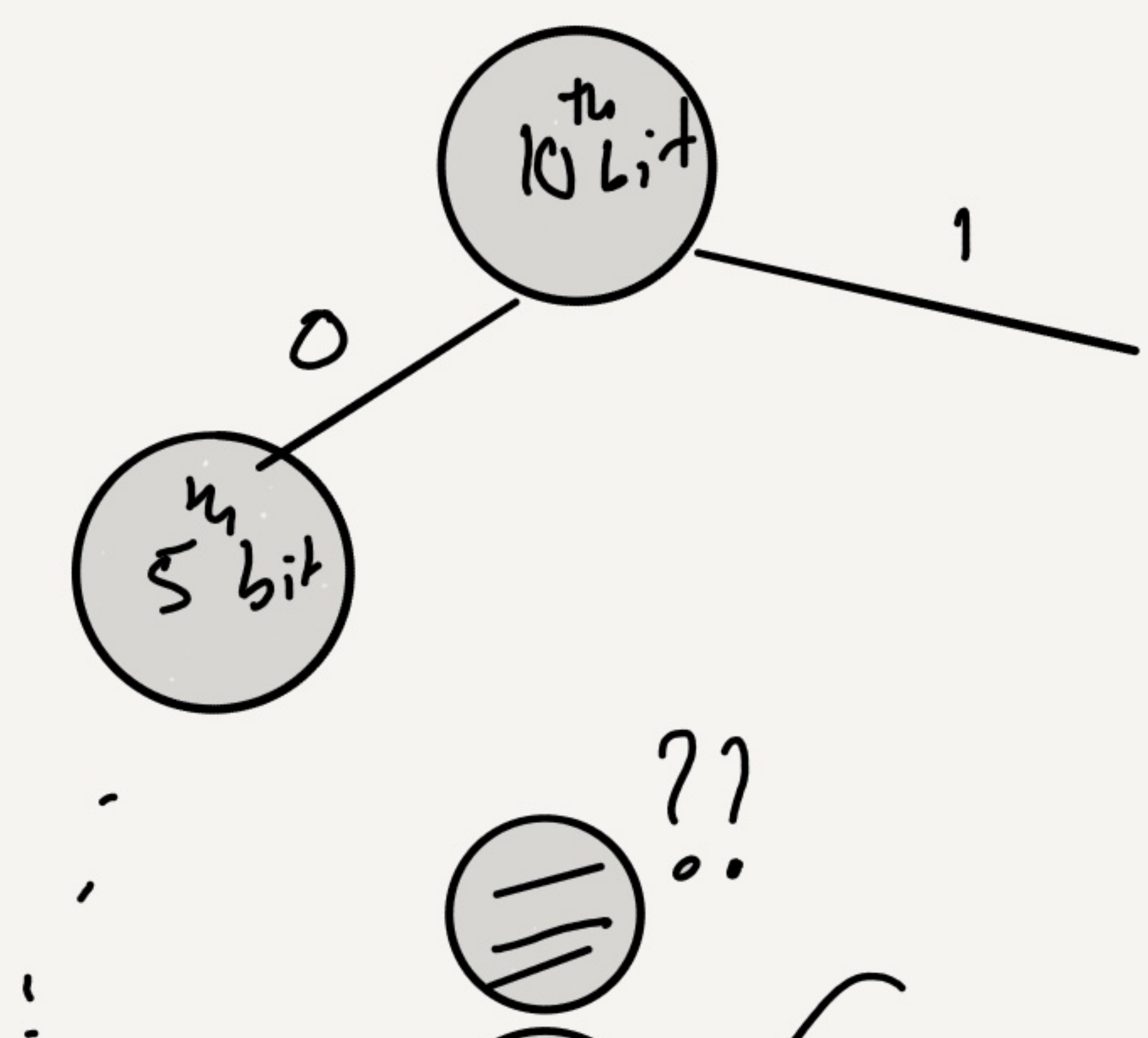
COMM. COMP.$(F) \approx$ SOME-MEASURE(f)?

Example:

Det. Comm. Com of $f \circ g^n$ $\longrightarrow$ "Measure" of f.

$g: \{0,1\}^k \times \{0,1\}^k \longrightarrow \{0,1\}$.

f



$$CC(f \circ g^n) \overset{=\,??}{\leq} \Big(DT(f)\Big) \cdot k$$

Converse:?? $CC(F) \geq \Omega(DT(f) \cdot k)$

(for some g).

$$R_{1/3}(F) \overset{?}{\geq} \Omega(RDT(f) \cdot k)$$

PREVIOUS WORK

FOR SUITABLE g, Σ

	MEASURE OF $f \circ g^n$	MEASURE OF f
RAZ-McKENZIE '97	DET. CC	DECISION TREE
RAZBOROV '03	QUANTUM CC*	APPROX-DEGREE*
SHERSTOV '07, ...	DISCREPANCY SIGN-RANK UNBOUNDED-ERROR	THRESHOLD DEGREE
GLMWZ15 (Goos et al...)	NON-DET. CC PARTITION, ...	...
LRS15	SEMIDEFINITE RANK	SOS-DEGREE

PREVIOUS WORK

FOR SUITABLE g, Σ

	MEASURE OF $f \circ g^n$	MEASURE OF f
Kothari, M, Raghavendra 17	Non-negative rank	"non-negative degree"
Goos, Pitassi, Watson 17	Randomized CC	RDT

⋮

Many nice applications . . .

GAME THEORY

In Game Theory, No Clear Path to Equilibrium

13

John Nash's notion of equilibrium is ubiquitous in economic theory, but a new study shows that it is often impossible to reach efficiently.

All games have a Nash equilibrium. But will players be able to reach it?

—

Eric Nyquist for Quanta Magazine

Today ...

Lifting for Covering number (GLMWZ15)

$$\mathrm{Cov}(F) \geq \text{Measure} \cdot k$$

??

<u>Fix:</u>

$$g : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}$$

$$g(a,b) = \langle a,b \rangle \bmod 2.$$

$$k = 10 \log n.$$

What measure of f??

$$\mathrm{Cert}_z(f) = \min_{|I|} \{ z' : z'_I = z_I \Rightarrow f(z') = 1 \}. \qquad z \in \{0,1\}^n$$

$$\mathrm{Cert}(f) = \max_{z : f(z)=1} \mathrm{Cert}_z(f)$$

eg: $\mathrm{Cert}(\mathrm{AND}) = n$

$\mathrm{Cert}(\mathrm{OR}) = 1$

$$\boxed{\textbf{Thm:}\quad \mathrm{Cov}(f \circ g^n) = \Theta\big(\mathrm{cert}(f) \cdot k\big).\qquad \text{(GLMWZ)}}$$

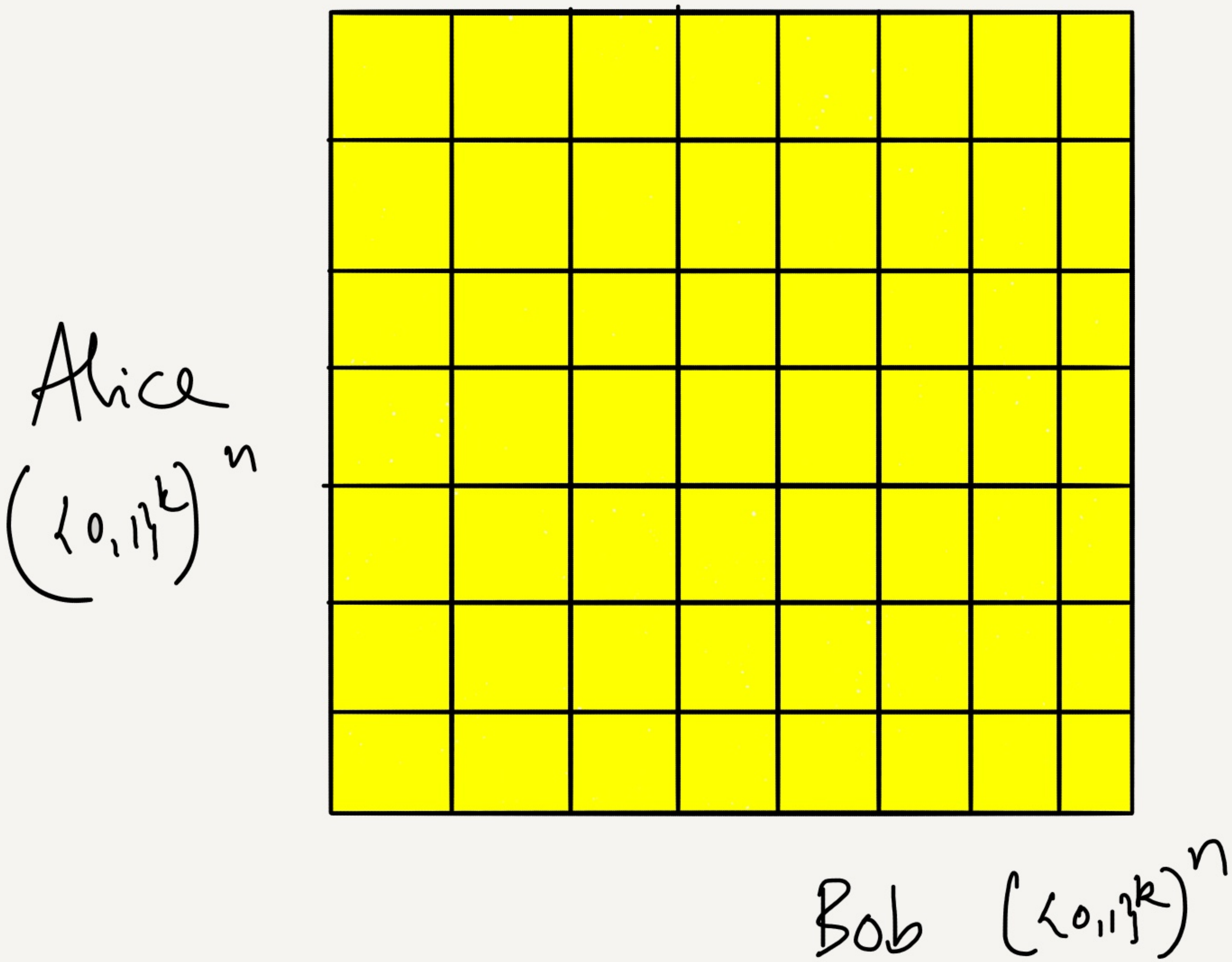
Proof:

$$\mathrm{Cov}(f \circ g^n) \leq C.$$

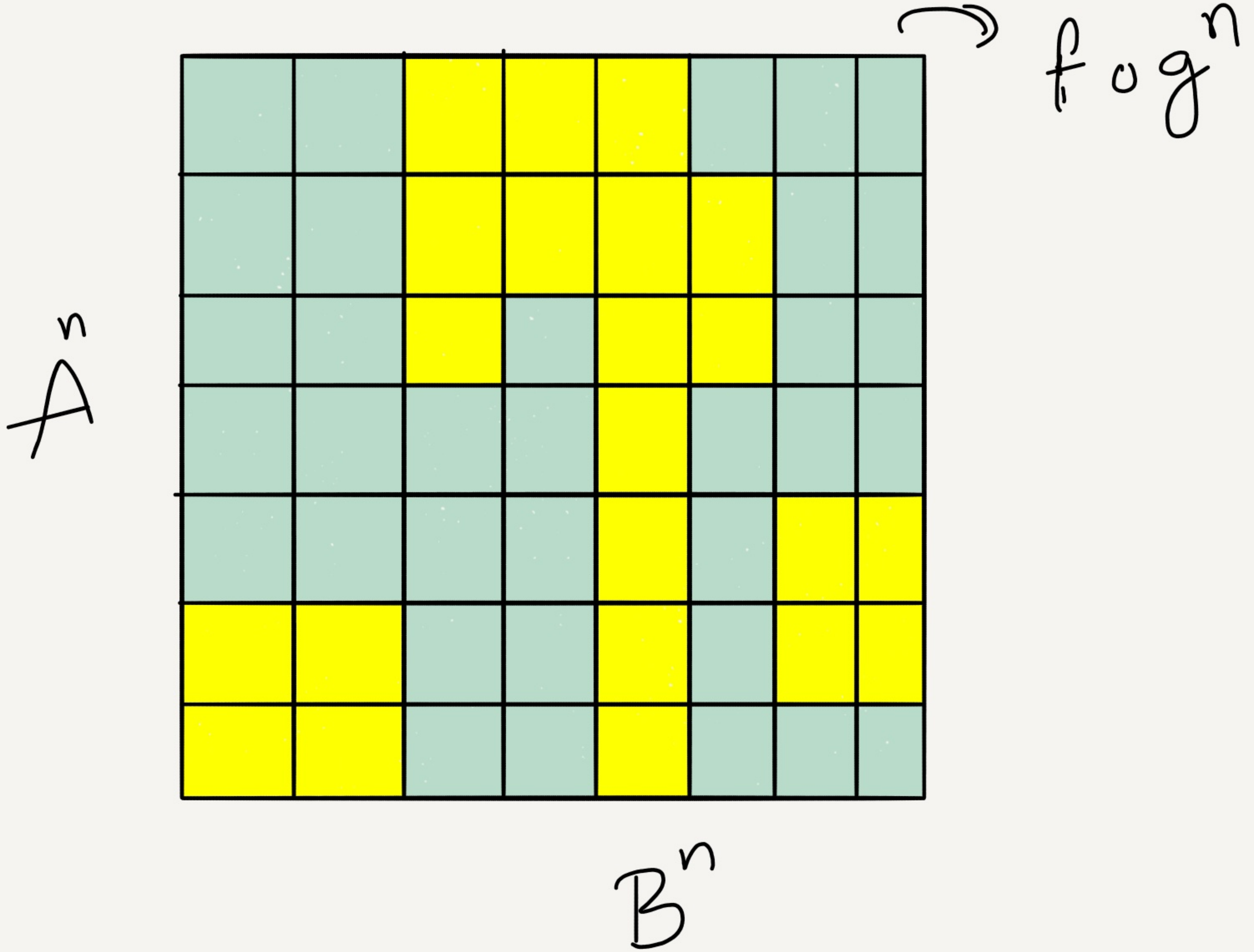
$$\Downarrow$$

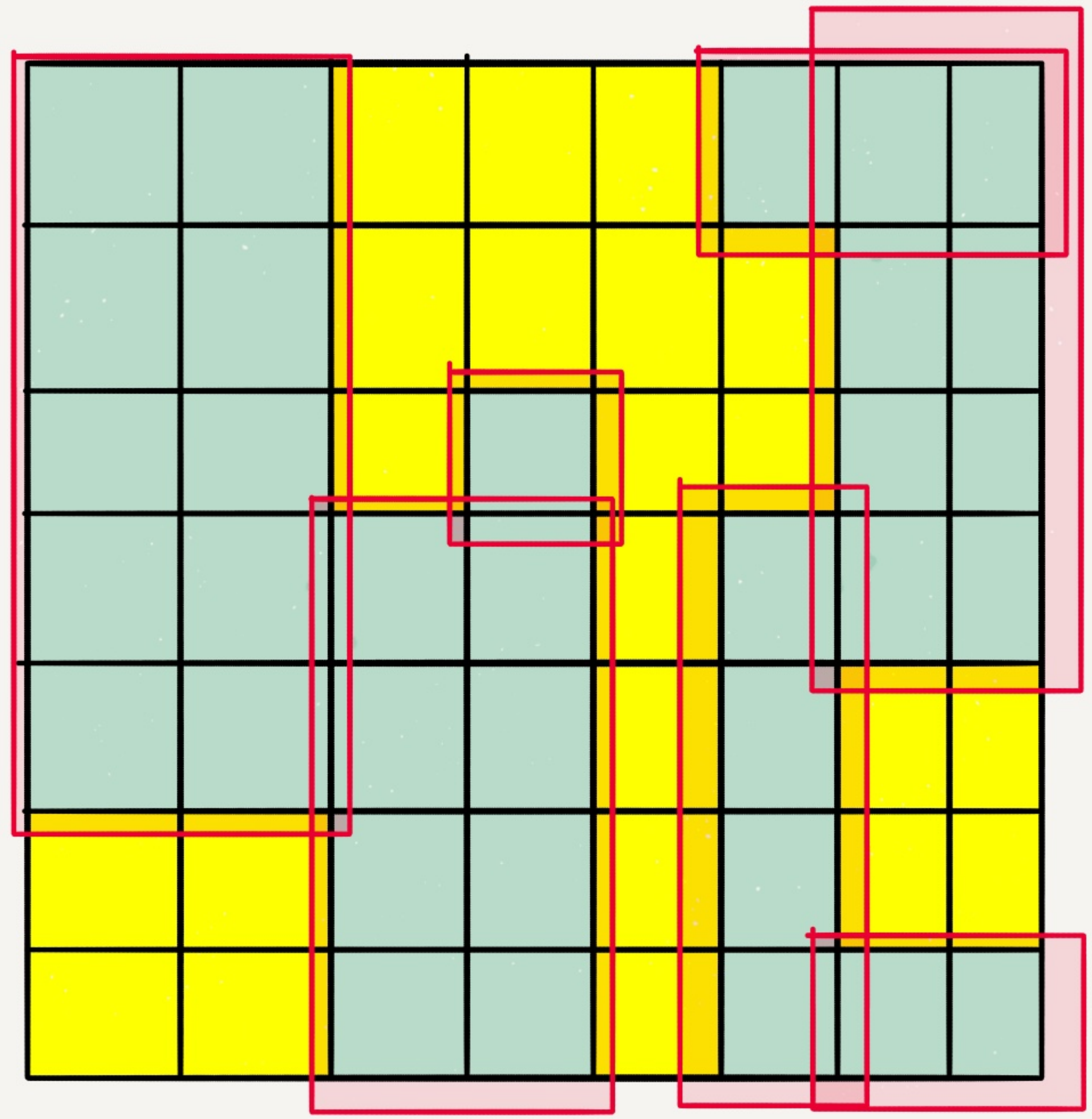
$$\mathrm{Cert}_z(f) \leq O\left(\frac{C}{k}\right).$$

fix an input z for f $\quad (f(z) = 1)$.

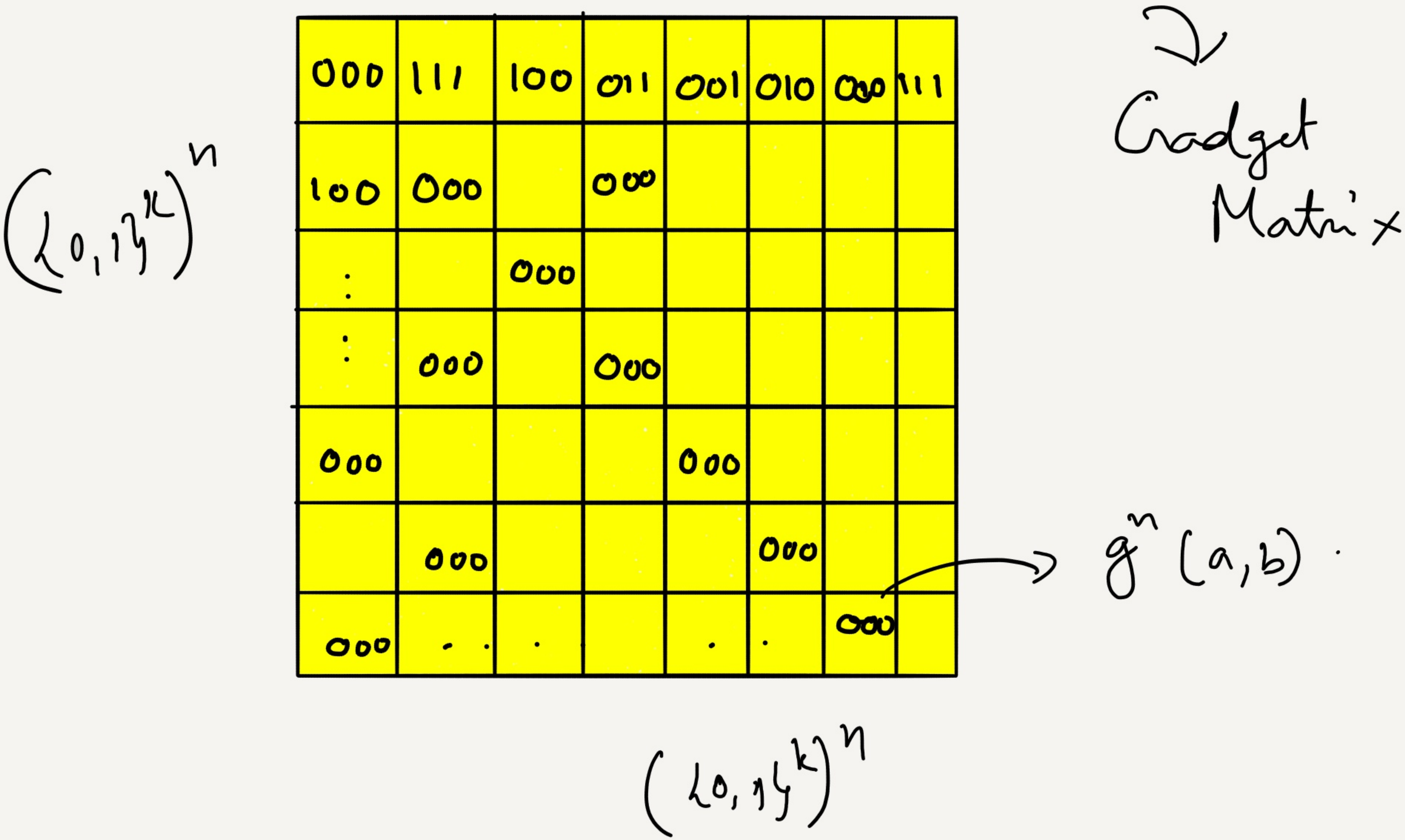


Alice
$(\{0,1\}^k)^n$
Bob $(\{0,1\}^k)^n$


$f \circ g^n$
A^n
B^n

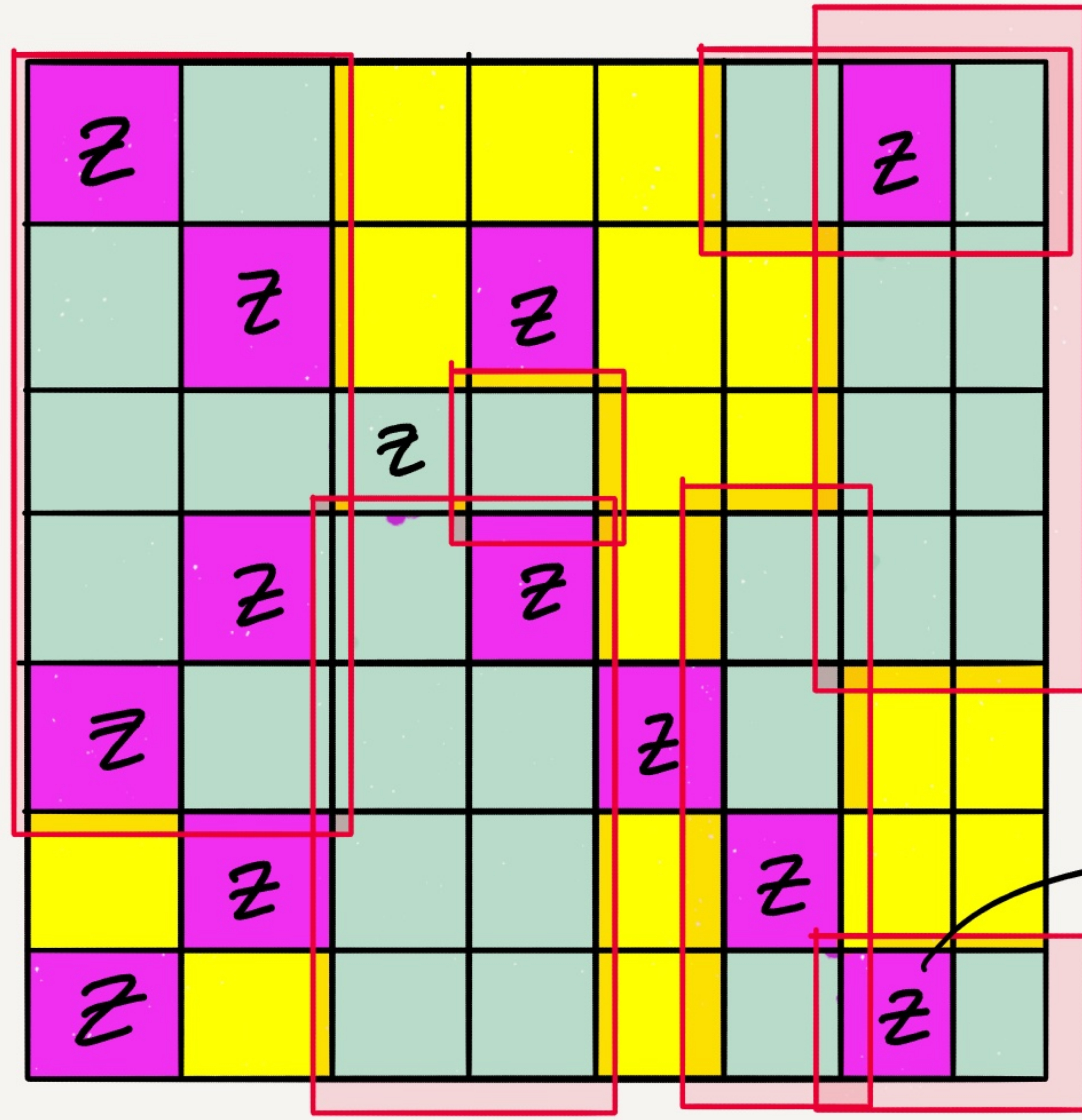


$\leq 2^C$ rectangles to cover all 1's in the comm. matrix.


Gadget Matrix
$(\{0,1\}^k)^n$
$(\{0,1\}^k)^n$
$g^n(a,b)$
000
111
100
011
001
010
000
111

z	111	100	011	001	010	z	111
100	z		z				
⋮		z					
⋮	z		z				
z				z			
	z				z		
z	. .	.		.	.	z	

$$g^n(a,b) = z.$$



Monochromatic pieces in covering

$\leq 2^C$

Z appeared.

Pick rectangle that covers most purple squares.

Pick a rectangle R (from covering)

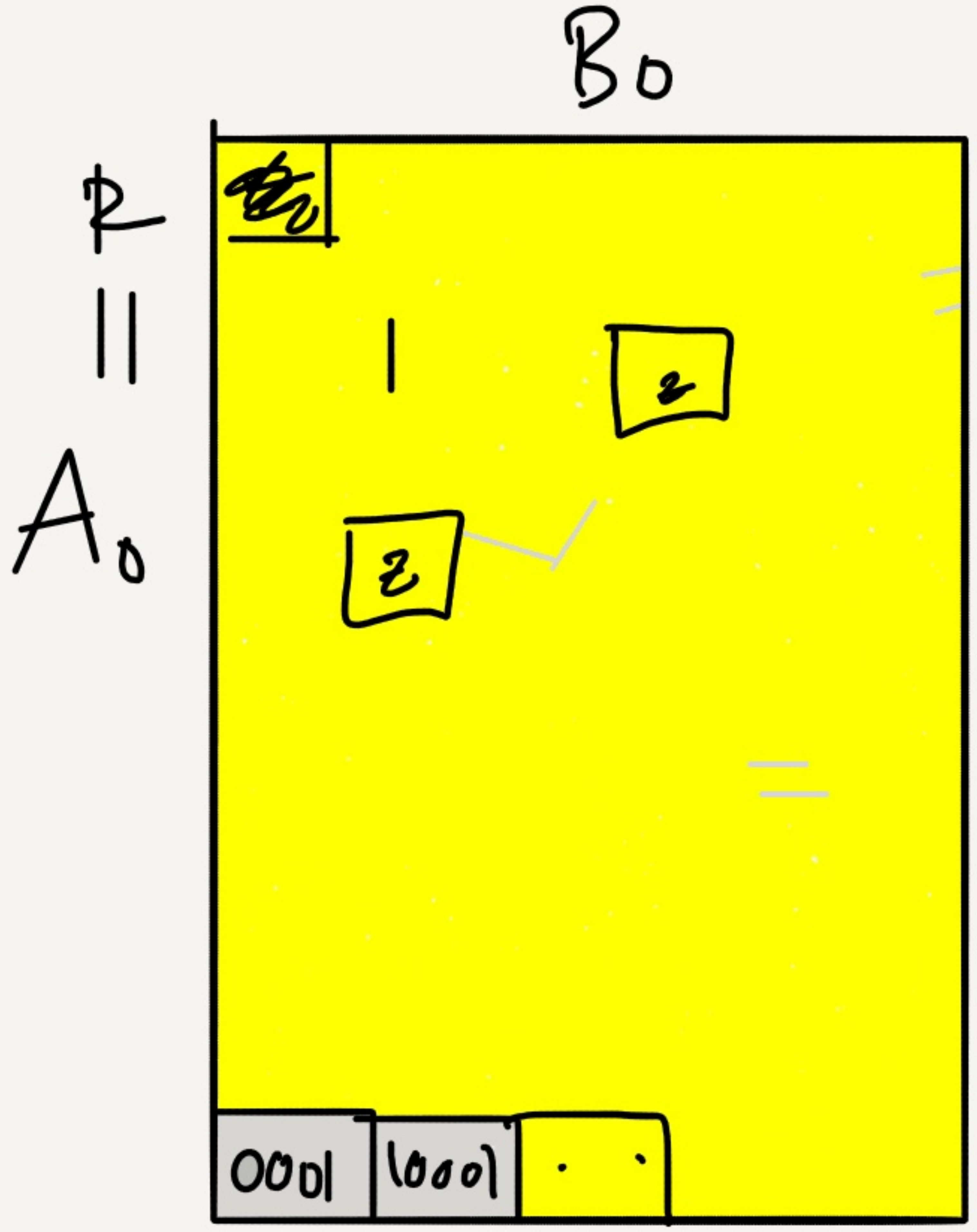
$$\left| R \cap (\text{Purple squares}) \right| \geq 2^{-C} \cdot \left| \text{Purple Squares} \right| .$$

$$g^n = G$$

$$G^{-1}(z) = \{ (a,b) : G(a,b) = z \} .$$

Pick a rectangle R (from covering)

$$|R \cap G^{-1}(z)| \geq 2^{-C} \cdot |G^{-1}(z)|.$$



$$R = A_0 \times B_0$$

$$\subseteq (\{0,1\}^k)^n \quad (\{0,1\}^k)^n.$$

$\rightarrow$ all $\{0,1\}^n$ strings appear inside.

Claim 1: $A_0, \quad B_0 \subseteq (\{0,1\}^k)^n$

$$|R \cap G^{-1}(z)| \geq 2^{-C} \cdot |G^{-1}(z)|.$$

$\left(g^n(A_0, B_0) \text{ Contain a "sub-cube".} \right)$

$\exists$ a set I, $\quad |I| \leq O\left(\frac{C}{k}\right)$ s.t

$$\{z' : z'_I = z_I\} \subseteq g^n(A_0, B_0).$$

$(k \gg \log n)$

Claim 0: $A_0, B_0 \subseteq (\{0,1\}^k)^n$

$$|A_0|, |B_0| \geq 2^{nk-C}$$

$$|I| \leq O\left(\frac{C}{k}\right)$$

$\exists$ a set I, some partial assignment α.

$$\{z' : z'_I = \alpha\} \subseteq g^n(A_0, B_0).$$

$g : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}.$ $\quad k > 10\log n.$

Question :: $A_0, \quad B_0 \subseteq \left(\{0,1\}^k\right)^n$

$$|A_0|, |B_0| \geq 2^{nk - C}$$

$$|I| \leq O\left(\frac{C}{k}\right)$$

$\exists$ a set I, some partial assignment α.

$$\{z' : z'_I = \alpha\} \subseteq g^n(A_0, B_0).$$

$$g : \{0,1\}^k \times \{0,1\}^k \longrightarrow \{0,1\}. \qquad k = 100$$