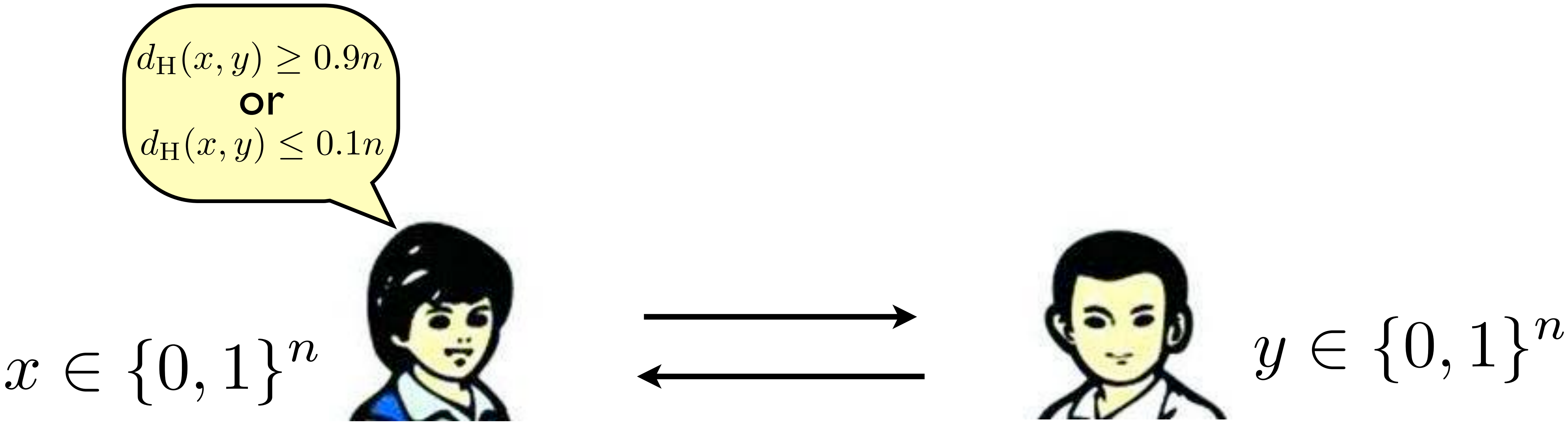
Communication Complexity

BASICS Summer School 2015

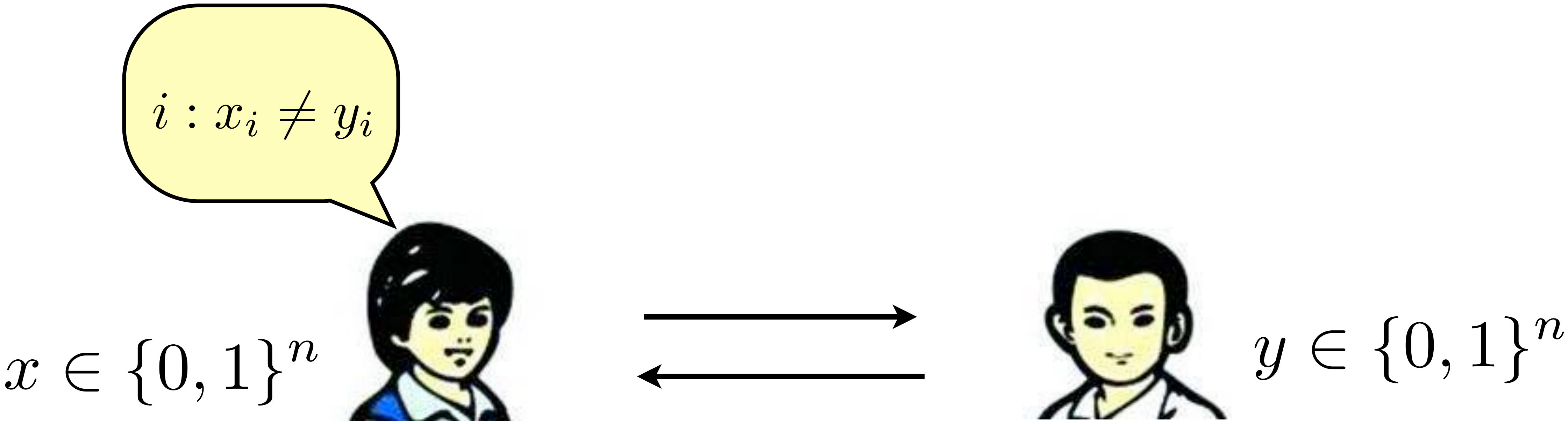
南京大学 尹一通

- Communication Complexity of Relations
- Direct Sum
- Lower Bounds for Disjointness
- Asymmetric Communication Complexity and Data Structures



distinguish between the cases:

- "yes" if the hamming distance $d_H(x,y) \geq 0.9n$
- "no" if $d_H(x,y) \leq 0.1n$
- no definition for other inputs



output an index i that $x_i \neq y_i$

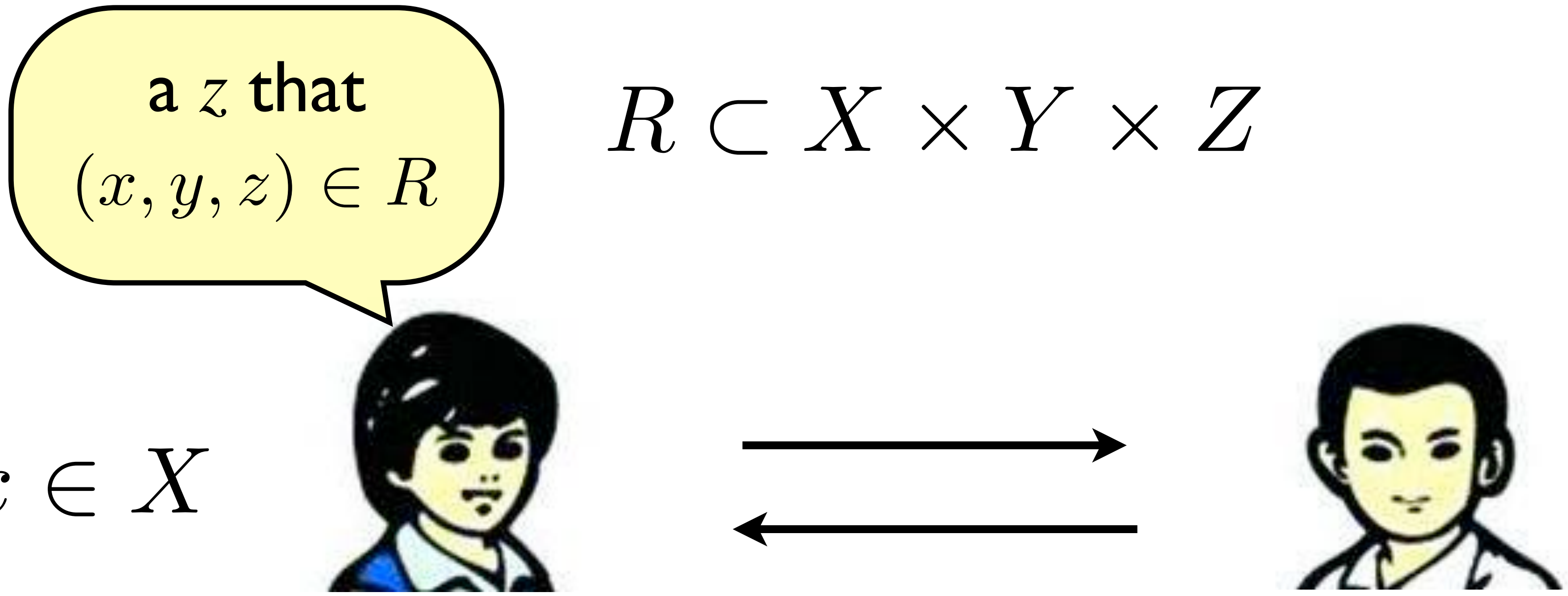
output arbitrarily if no such i exists

- some inputs may have more than one correct answers
- some inputs may be *illegal* (have 0 correct answer / all answers are correct)

Relation

$R \subset X \times Y \times Z$

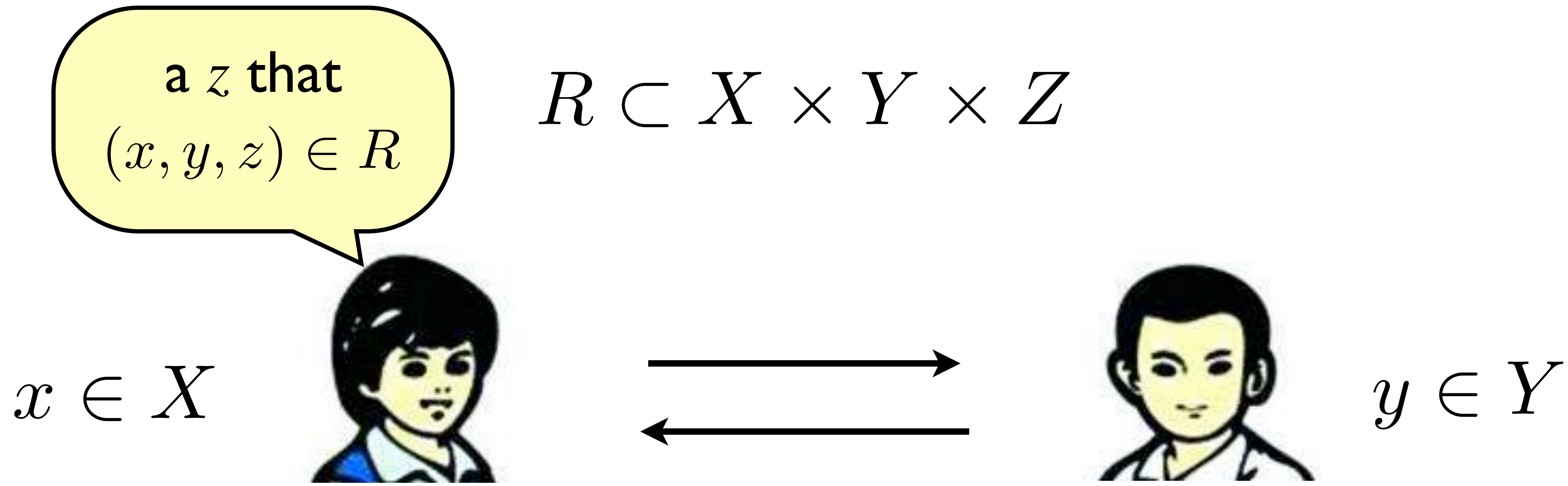
$x \in X$



$y \in Y$

deterministic, randomized, nondeterministic communication protocols are defined in the same way as before

For every *legal* input ((x,y) that ∃z, (x,y,z)∈R),
Alice outputs a z that (x,y,z)∈R
or outputs such a z with 1-δ probability
or Alice and Bob *certify* such a z that (x,y,z)∈R
by adaptive communications.



$a_1 = A(x)$ $\xrightarrow{a_1}$

$\xleftarrow{b_1}$ $b_1 = B(y, a_1)$

$a_2 = A(x, b_1)$ $\xrightarrow{a_2}$

$\xleftarrow{b_2}$ $b_2 = B(y, a_1, a_2)$

$\vdots$

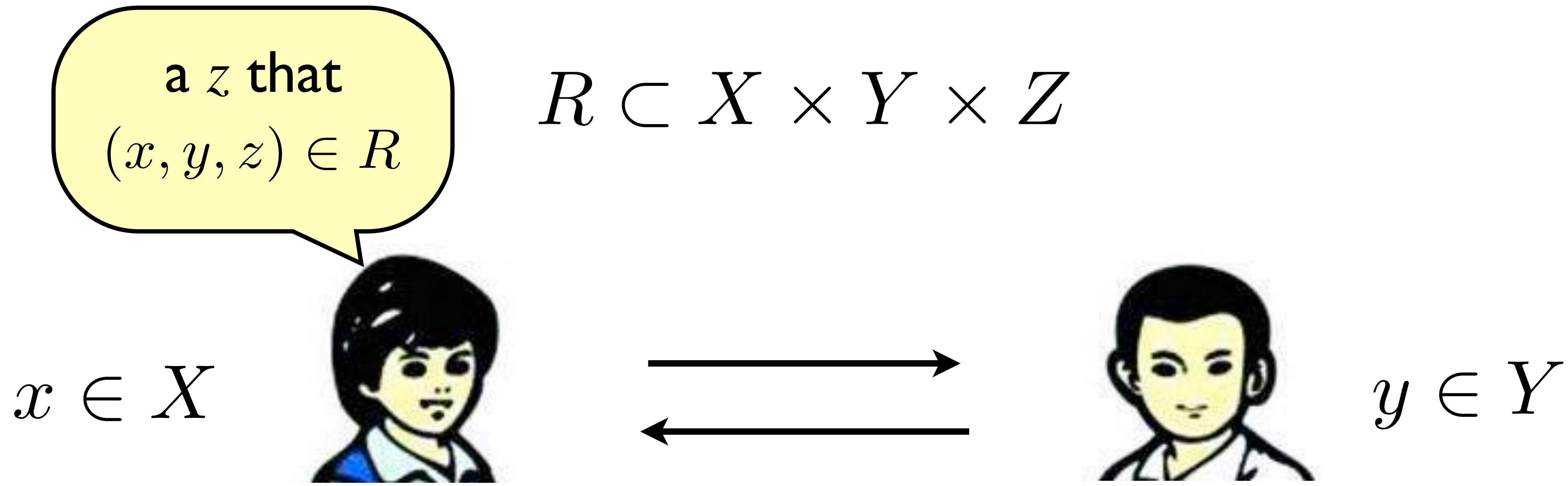
$\xleftarrow{b_i}$ $b_i = B(y, a_1, \ldots, a_i)$

$a_{i+1} = A(x, b_1, \ldots, b_i)$

$\vdots$

$z = A(x, b_1, \ldots, b_t)$ that $(x, y, z) \in R$

$R \subset X \times Y \times Z$



public random bits $r \in \{0,1\}^*$

$a_1 = A(r, x)$ $\xrightarrow{a_1}$ $b_1 = B(r, y, a_1)$

$\vdots$

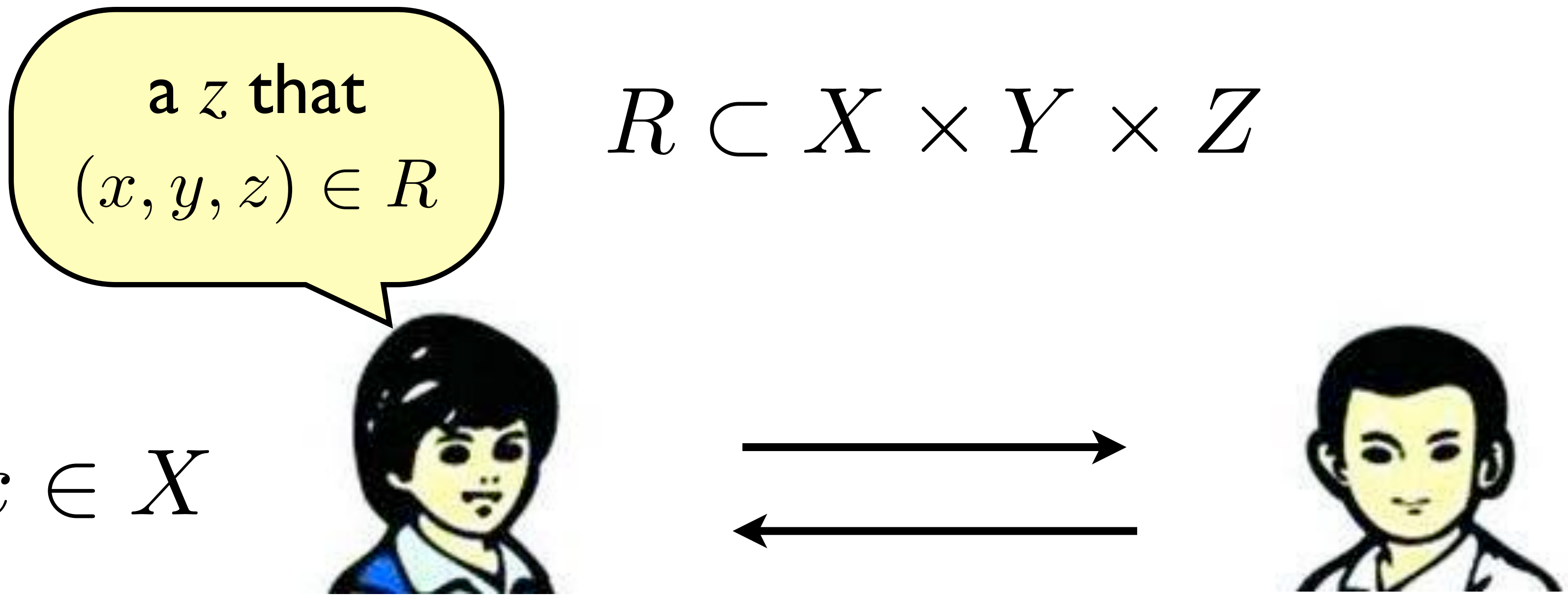
$a_{i+1} = A(r, x, b_1, \ldots, b_i)$ $\xleftarrow{b_i}$ $b_i = B(r, y, a_1, \ldots, a_i)$

$\xrightarrow{a_{i+1}}$

$\vdots$

$z = A(r, x, b_1, \ldots, b_t)$

$$\Pr_r[(x, y, z) \in R] \geq 1 - \delta$$



$R \subset X \times Y \times Z$

$x \in X$ $\qquad$ $y \in Y$

private random bits $r_A, r_B \in \{0,1\}^*$

$$a_1 = A(r_A, x) \xrightarrow{a_1} b_1 = B(r_B, y, a_1)$$

$\vdots$

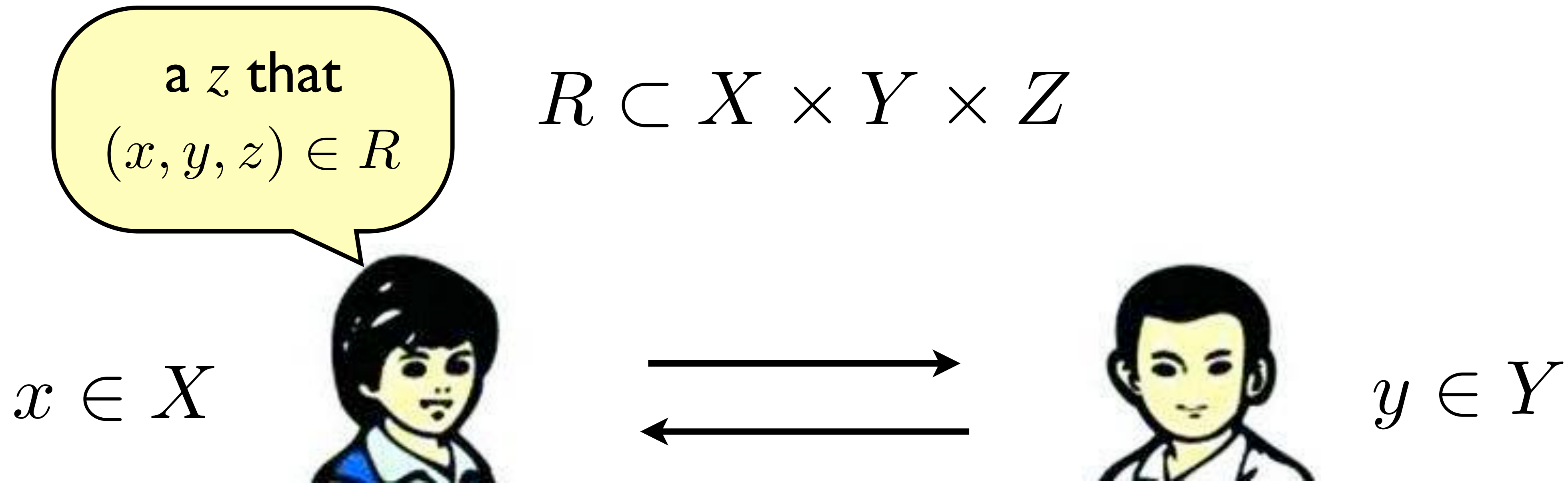
$$a_{i+1} = A(r_A, x, b_1, \ldots, b_i) \xleftarrow{b_i} b_i = B(r_B, y, a_1, \ldots, a_i)$$

$$\xrightarrow{a_{i+1}}$$

$\vdots$

$$z = A(r_A, x, b_1, \ldots, b_t)$$

$$\Pr_{r_A, r_B}[(x, y, z) \in R] \geq 1 - \delta$$



certificates: $C_A, C_B \in \{0,1\}^*$

$$a_1 = A(C_A, x) \xrightarrow{a_1} b_1 = B(C_B, y, a_1)$$

$$\vdots$$

$$a_{i+1} = A(C_A, x, b_1, \ldots, b_i) \xleftarrow{b_i} b_i = B(C_B, y, a_1, \ldots, a_i)$$

$$\xrightarrow{a_{i+1}}$$

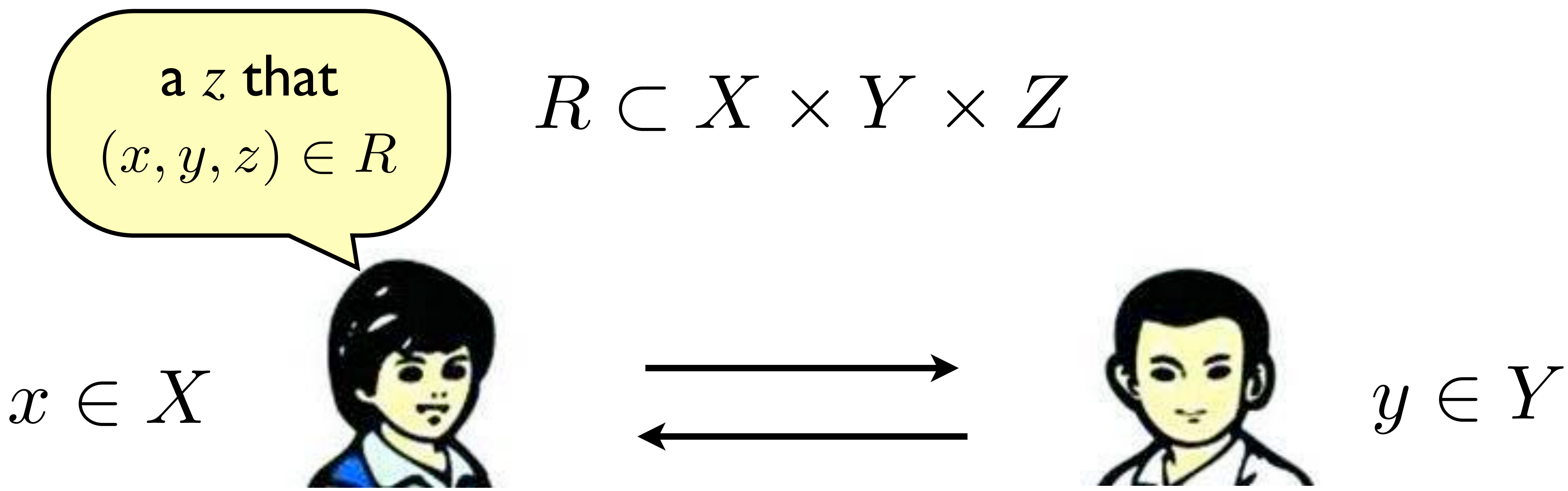
$$\vdots$$

$$z = A(C_A, x, b_1, \ldots, b_t) \in Z \cup \{\bot\}$$

$\bot$: "Can't decide."

- completeness: $\forall$ legal x,y, $\exists$certificate C_A, C_B, s.t. $(x,y,z) \in R$
- soundness: $\forall$ legal x,y, $\forall$ C_A, C_B, either $(x,y,z) \in R$ or $z = \bot$

Relation



For every *legal* input ((x,y) that $\exists z$, $(x,y,z) \in R$),
Alice outputs a z that $(x,y,z) \in R$
  or outputs such a z with $1\text{-}\delta$ probability
  or Alice and Bob *certify* such a z that $(x,y,z) \in R$
by adaptive communications.

motivated by circuit complexity:

we are interested in relations that find an i that $x_i \neq y_i$

Monochromatic Rectangles

$$R \subset \{0,1\}^3 \times \{0,1\}^3 \times \{1, 2, 3\}$$

	000	001	010	011	100	101	110	111
000	∅	{3}	{2}	{2,3}	{1}	{1,3}	{1,2}	{1,2,3}
001	{3}	∅	{2,3}	{2}	{1,3}	{1}	{1,2,3}	{1,2}
010	{2}	{2,3}	∅	{3}	{1,2}	{1,2,3}	{1}	{1,3}
011	{2,3}	{2}	{3}	∅	{1,2,3}	{1,2}	{1,3}	{1}
100	{1}	{1,3}	{1,2}	{1,2,3}	∅	{3}	{2}	{2,3}
101	{1,3}	{1}	{1,2,3}	{1,2}	{3}	∅	{2,3}	{2}
110	{1,2}	{1,2,3}	{1}	{1,3}	{2}	{2,3}	∅	{3}
111	{1,2,3}	{1,2}	{1,3}	{1}	{2,3}	{2}	{3}	∅

rectangle: $A \times B$ for some $A \subseteq X$, $B \subseteq Y$

z-*monochromatic* rectangle: $\forall (x, y) \in A \times B, (x, y, z) \in R$

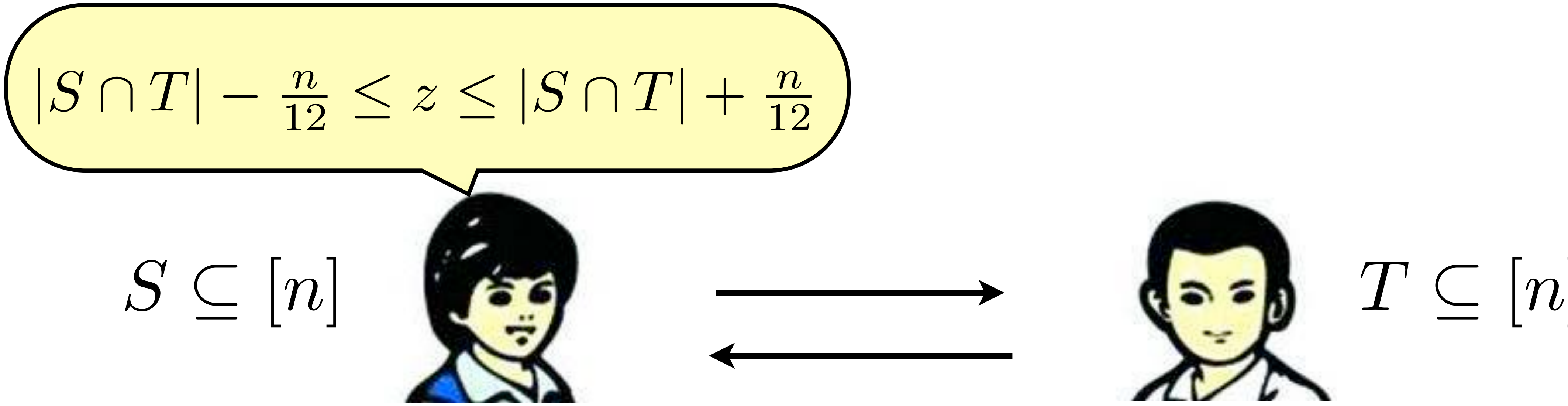
or (x,y) is *illegal*

Monochromatic Rectangles

Theorem:
Any t-bit deterministic protocol that computes the relation R induces a partition of $X \times Y$ into at most 2^t monochromatic rectangles.

R cannot be partitioned into $<M$ monochromatic rectangles

⇨ $D(R) \geq \log M$



approx-SI: approximate set intersection

approximation version of DISJ (set disjointness)

"*fooling set*":

$(S_1, \overline{S}_1), \ldots, (S_M, \overline{S}_M)$

$\forall i \neq j, \quad |S_i \cap \overline{S}_j| > \frac{n}{6}$ ⇒ D(approx-SI) ≥ log M

Why?

$|S \cap T| - \frac{n}{12} \le z \le |S \cap T| + \frac{n}{12}$

$S \subseteq [n]$  $\longrightarrow$ $\longleftarrow$  $T \subseteq [n]$

by the probabilistic method:

$\exists\ (S_1, \overline{S}_1), \ldots, (S_M, \overline{S}_M)$

$\forall i \neq j, \quad |S_i \cap \overline{S}_j| > \frac{n}{6}$

⇒ D(approx-SI) ≥ log $M = \Omega(n)$

sample each $S_i \subseteq [n]$ uniformly & independently:

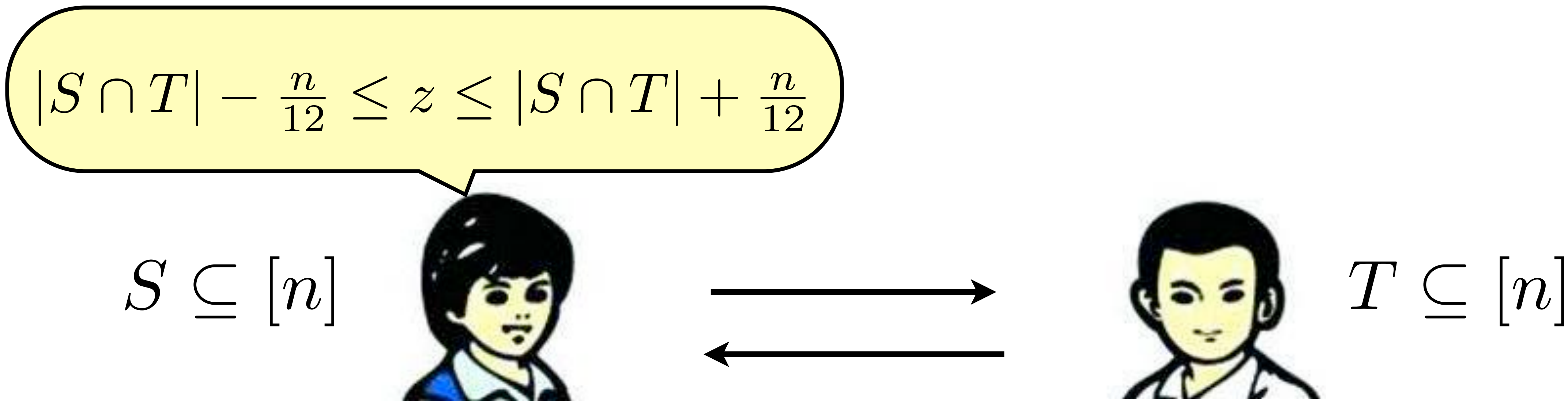
fix $\forall i \neq j$ $\qquad \forall k \in [n],\ \text{let } Z_k = \begin{cases} 1 & k \in S_i \cap \overline{S}_j \\ 0 & \text{otherwise} \end{cases}$

$$|S_i \cap \overline{S}_j| = \sum_{k \in [n]} Z_k = Z \qquad \mathbb{E}[Z] = \frac{n}{4}$$

Chernoff bound: $\Pr[|S_i \cap \overline{S}_j| \le \frac{n}{6}] = \Pr[Z \le \frac{2}{3}\mathbb{E}[Z]] \le \mathrm{e}^{-\frac{n}{18}}$

union bound: $\Pr[\exists i \neq j, |S_i \cap \overline{S}_j| \le \frac{n}{6}] < M^2 \mathrm{e}^{-\frac{n}{18}} < 1$

for some $M = \mathrm{e}^{\Omega(n)}$



randomized protocol:

k uniformly random points $X_1, \ldots, X_k \in [n]$

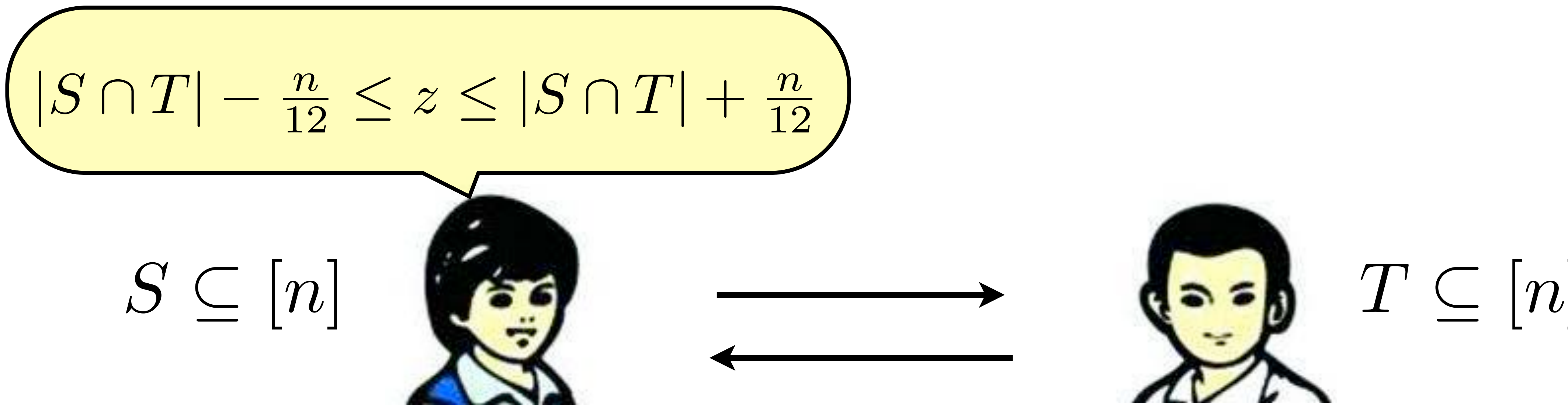
let $Z_i = \begin{cases} 1 & X_i \in S \cap T \\ 0 & \text{otherwise} \end{cases}$ and $Z = \sum_{i=1}^{k} Z_i$

output: $\frac{nZ}{k}$ cost: $k \log n$ $= O(\log n)$

error: $\mathbb{E}[Z] = \frac{k|S \cap T|}{n}$

$$\Pr\left[\left|\frac{nZ}{k} - |S \cap T|\right| > \frac{n}{12}\right] = \Pr\left[|Z - \mathbb{E}[Z]| > \frac{k}{12}\right]$$

Chernoff bound: $< 2e^{-\Omega(k)}$ $<1/3$ for $k=O(1)$



approx-SI: approximate set intersection

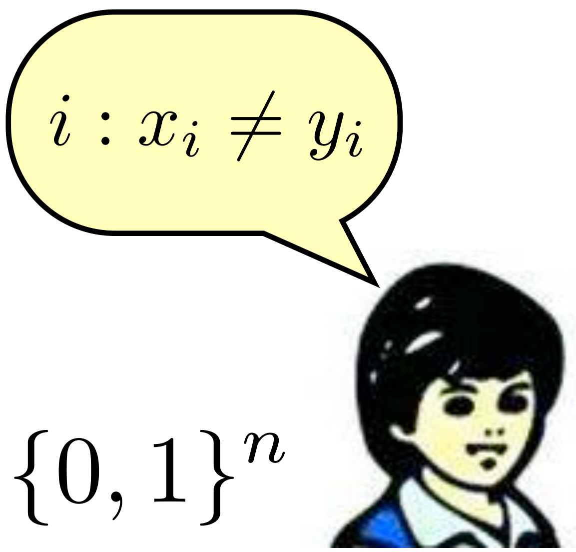
approximation version of DISJ (set disjointness)

D(approx-SI) = $\Omega(n)$

R(approx-SI) = $O(\log n)$

while R(DISJ) = $\Omega(n)$

Universal Relation



$U \subset \{0,1\}^n \times \{0,1\}^n \times \{1,\ldots,n\}$

$U = \{(x,y,i) \mid x_i \neq y_i\}$

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

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

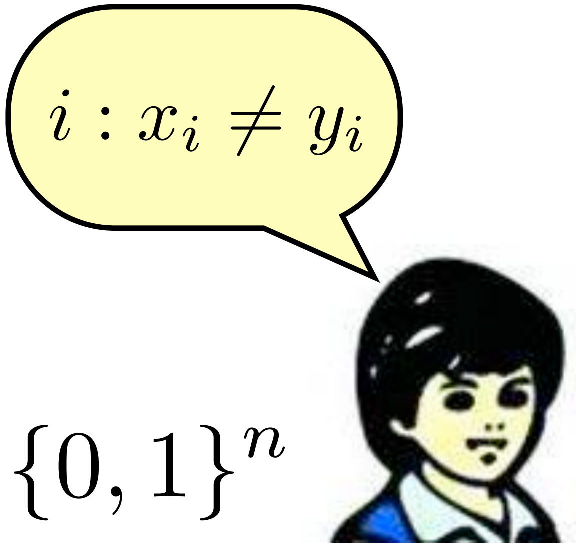
$$R \subset \{0,1\}^3 \times \{0,1\}^3 \times \{1,2,3\}$$

	000	001	010	011	100	101	110	111
000	∅	{3}	{2}	{2,3}	{1}	{1,3}	{1,2}	{1,2,3}
001	{3}	∅	{2,3}	{2}	{1,3}	{1}	{1,2,3}	{1,2}
010	{2}	{2,3}	∅	{3}	{1,2}	{1,2,3}	{1}	{1,3}
011	{2,3}	{2}	{3}	∅	{1,2,3}	{1,2}	{1,3}	{1}
100	{1}	{1,3}	{1,2}	{1,2,3}	∅	{3}	{2}	{2,3}
101	{1,3}	{1}	{1,2,3}	{1,2}	{3}	∅	{2,3}	{2}
110	{1,2}	{1,2,3}	{1}	{1,3}	{2}	{2,3}	∅	{3}
111	{1,2,3}	{1,2}	{1,3}	{1}	{2,3}	{2}	{3}	∅

Universal Relation

$$U \subset \{0,1\}^n \times \{0,1\}^n \times \{1,\ldots,n\}$$

$$U = \{(x,y,i) \mid x_i \neq y_i\}$$



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

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

$$\mathrm{D}(U) \geq \mathrm{D}(\mathrm{EQ}) - 2 \;\geq n - 2$$

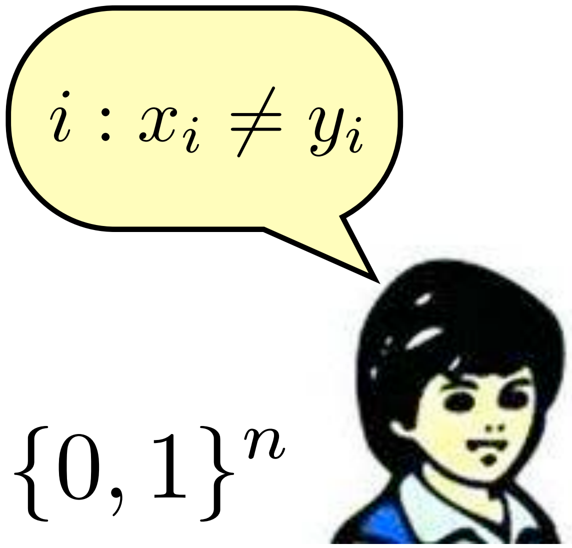
a protocol for EQ using the protocol for U:

run protocol P_U for U on the inputs of EQ;
if output of P_U is i, then Alice and Bob share x_i,y_i;
if x_i=y_i or an illegal input is detected, return "*yes*";
else return "*no*";

Universal Relation

$$U \subset \{0,1\}^n \times \{0,1\}^n \times \{1,\ldots,n\}$$
$$U = \{(x,y,i) \mid x_i \neq y_i\}$$

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



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

$$\mathrm{D}(U) \geq n - 2$$

$$\mathrm{N}(U) = O(\log n)$$

just send (i, x_i) to Bob

recall: $\mathrm{D}(f) = O(\mathrm{N}(f)^2)$

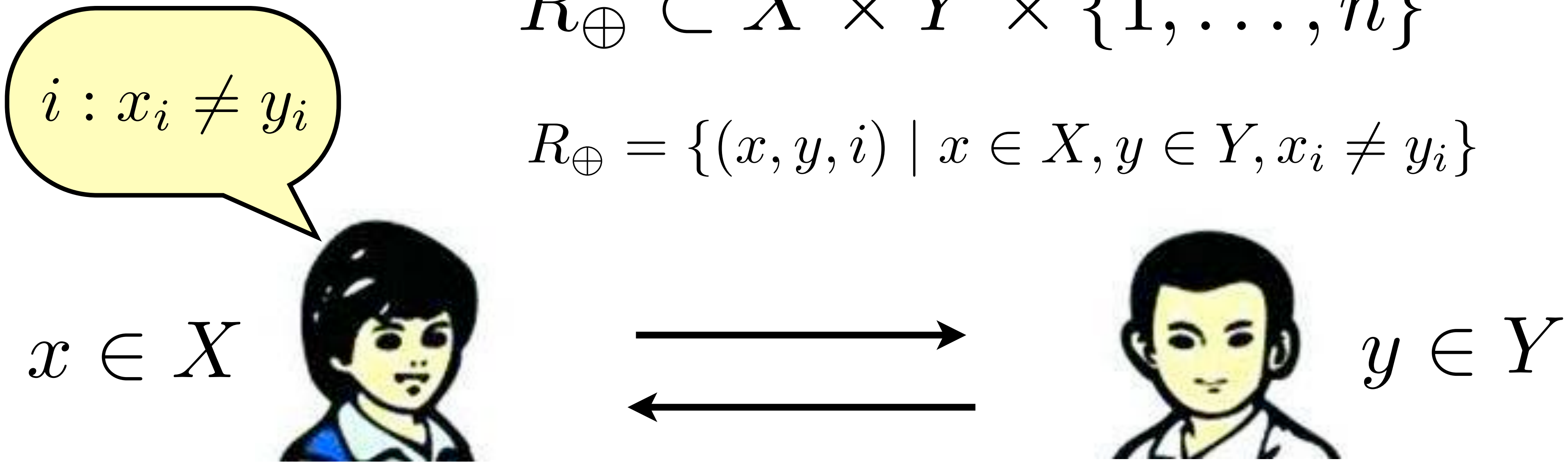
for any *total* function f

"Differences are easier to certify than their nonexistence."

with relations (or partial functions) we avoid the hard instances

$$R_\oplus \subset X \times Y \times \{1,\ldots,n\}$$

$$R_\oplus = \{(x,y,i) \mid x \in X, y \in Y, x_i \neq y_i\}$$



for any $x \in \{0,1\}^n$ its parity is $\left(\sum_i x_i\right) \bmod 2$

X: all $x \in \{0,1\}^n$ with parity 1

Y: all $y \in \{0,1\}^n$ with parity 0

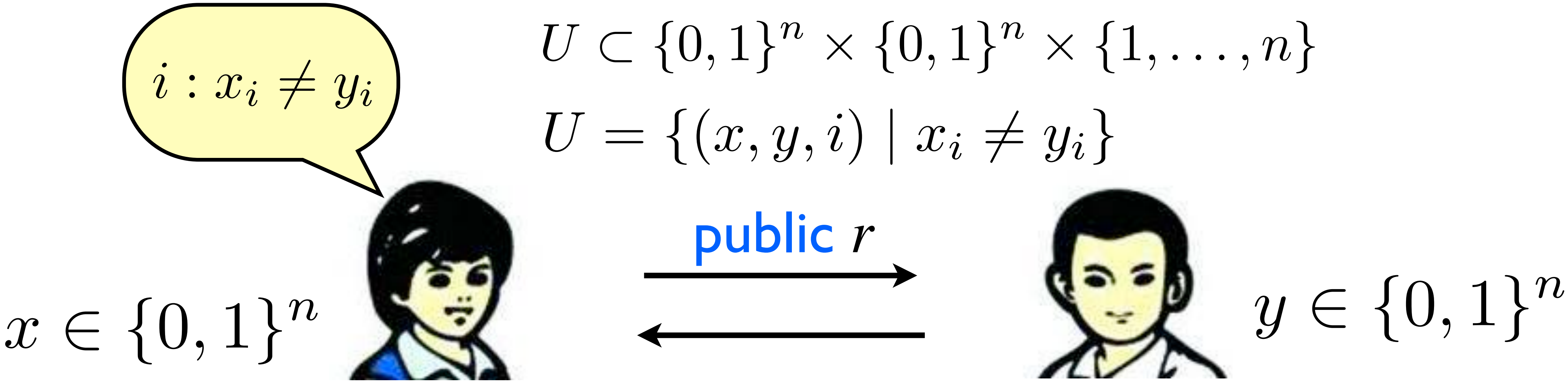
a sub-relation of U, all inputs must be legal

$$\mathrm{D}(R_\oplus) = O(\log n)$$

binary search: maintain an (i,j) such that the parity of $(x_i,\ldots,x_j)$ is different from parity of $(y_i,\ldots,y_j)$

$$U \subset \{0,1\}^n \times \{0,1\}^n \times \{1,\ldots,n\}$$

$$U = \{(x,y,i) \mid x_i \neq y_i\}$$



$$\mathsf{R}^{\mathsf{Pub}}(U) = O(\log n)$$

(O(1) bits) compare whether $\langle x, r\rangle = \langle y, r\rangle$

$\langle x, r\rangle := \left(\sum_i x_i r_i\right) \bmod 2$ is the *inner-product* over GF(2)

(*legal* input) if $x \neq y$: $<x,r> \neq <y,r>$ with probability 1/2

x,y have different parities over $\{i\text{: } r_i=1\}$

(O(log n) bits) binary search to locate $x_i \neq y_i$ (deterministically)

(O($1/n$) error) repeat for O(log n) times

$$U \subset \{0,1\}^n \times \{0,1\}^n \times \{1,\ldots,n\}$$

$$U = \{(x,y,i) \mid x_i \neq y_i\}$$

$i : x_i \neq y_i$

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

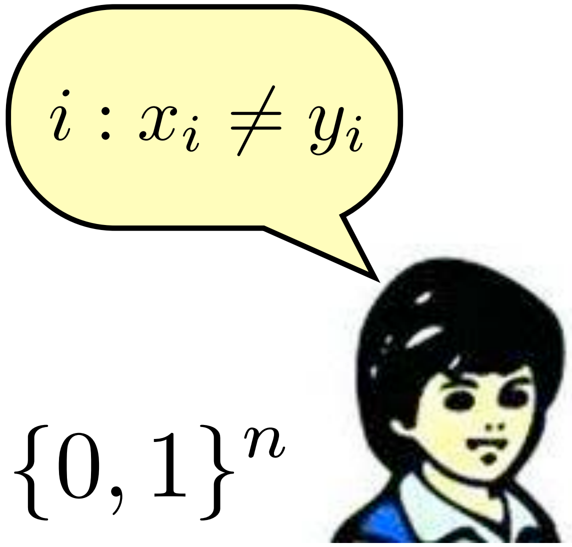
public r

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

$$\mathsf{R}^{\mathsf{Pub}}(U) = O(\log n)$$

recall:

$$\mathsf{R}(R) = O(\mathsf{R}^{\mathsf{Pub}}(R) + \log n)$$



$$U \subset \{0,1\}^n \times \{0,1\}^n \times \{1,\ldots,n\}$$

$$U = \{(x,y,i) \mid x_i \neq y_i\}$$

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

public r

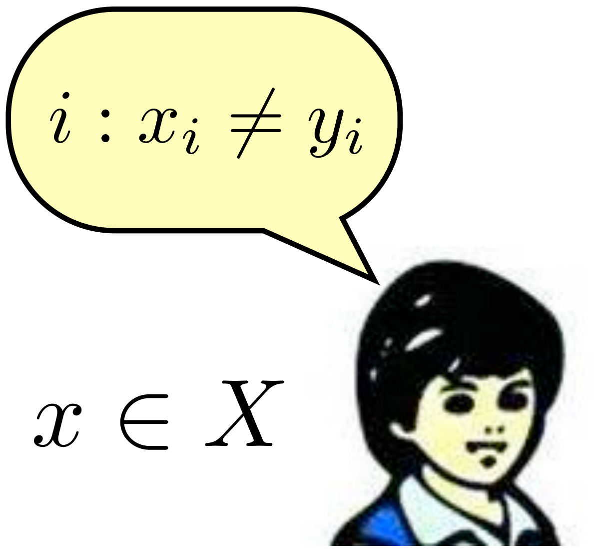
$y \in \{0,1\}^n$

$$\mathsf{R}(U) = O(\log n)$$

recall: $\mathsf{R}(R) = O(\mathsf{R}^{\mathsf{Pub}}(R) + \log n)$

$$R_\oplus \subset X \times Y \times \{1, \ldots, n\}$$

$$R_\oplus = \{(x, y, i) \mid x \in X, y \in Y, x_i \neq y_i\}$$



for any $x \in \{0,1\}^n$ its parity is $(\sum_i x_i) \bmod 2$

X : all $x \in \{0,1\}^n$ with parity 1

Y : all $y \in \{0,1\}^n$ with parity 0

a sub-relation of U, all inputs must be legal

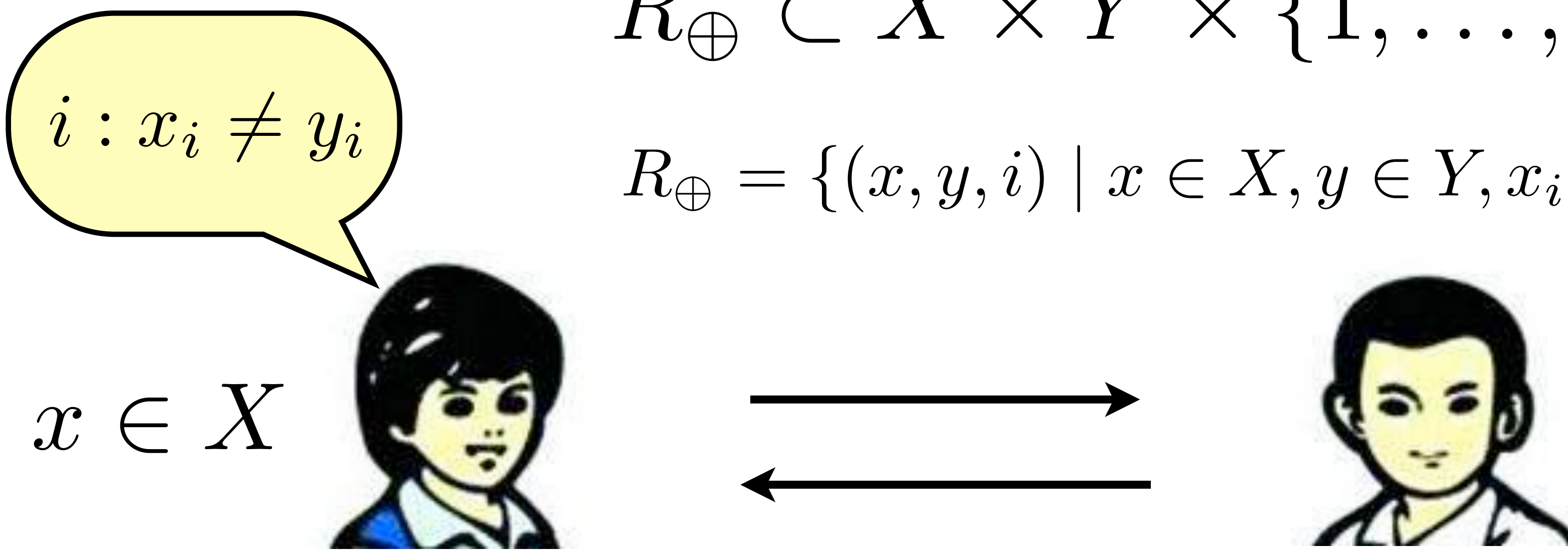
$$\mathrm{D}(R_\oplus) = O(\log n)$$

binary search: maintain an (i, j) such that the parity of $(x_i, \ldots, x_j)$ is different from parity of $(y_i, \ldots, y_j)$

$$R_\oplus \subset X \times Y \times \{1, \ldots, n\}$$

$$R_\oplus = \{(x, y, i) \mid x \in X, y \in Y, x_i \neq y_i\}$$

$x \in X$



$y \in Y$

for any $x \in \{0,1\}^n$ its parity is $(\sum_i x_i) \bmod 2$

X: all $x \in \{0,1\}^n$ with parity 1

Y: all $y \in \{0,1\}^n$ with parity 0

a sub-relation of U, all inputs must be legal

$$\mathrm{D}(R_\oplus) = \Theta(\log n)$$

Theorem: disjoint $X, Y \subseteq \{0,1\}^n$

$$R = \{(x, y, i) \mid x \in X, y \in Y, x_i \neq y_i\}$$

$$C = \{(x, y) \mid x \in X, y \in Y, d_{\mathrm{H}}(x, y) = 1\}$$

partition# of R $\geq \dfrac{|C|^2}{|X||Y|}$

R cannot be partitioned into $< \frac{|C|^2}{|X||Y|}$ monochromatic rectangles

⇨ $\mathsf{D}(R) = \Omega(2 \log |C| - \log |X| - \log |Y|)$

for $R_\oplus$ X: all $x \in \{0,1\}^n$ with parity 1

Y: all $y \in \{0,1\}^n$ with parity 0

$$|X| = |Y| = 2^{n-1} \qquad |C| = n2^{n-1}$$

⇨ $\mathsf{D}(R_\oplus) = \Omega(\log n)$

Theorem: disjoint $X, Y \subseteq \{0,1\}^n$

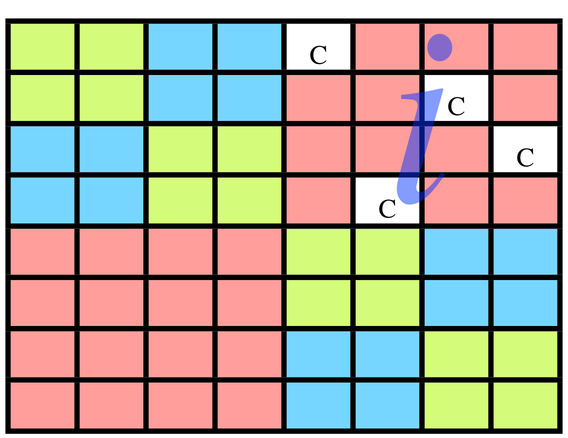
$$R = \{(x, y, i) \mid x \in X, y \in Y, x_i \neq y_i\}$$

$$C = \{(x, y) \mid x \in X, y \in Y, d_{\mathrm{H}}(x, y) = 1\}$$

partition# of $R \geq \dfrac{|C|^2}{|X||Y|}$

$R_1, R_2, \ldots, R_t$: optimal partition of R into monochromatic rectangles

let $m_i = |R_i \cap C|$ then $|X||Y| = \sum_{i=1}^{t} |R_i|$ $|C| = \sum_{i=1}^{t} m_i$



in any monochromatic rectangle:

$(x,y) \in C$ can only appear in *distinct* rows and columns

$\Rightarrow$ $|R_i| \geq m_i^2$

Theorem: disjoint $X,Y \subseteq \{0,1\}^n$

$$R = \{(x,y,i) \mid x \in X, y \in Y, x_i \neq y_i\}$$

$$C = \{(x,y) \mid x \in X, y \in Y, d_{\mathrm{H}}(x,y) = 1\}$$

partition# of R $\geq \dfrac{|C|^2}{|X||Y|}$

$R_1, R_2, \ldots, R_t$: optimal partition of R into monochromatic rectangles

let $m_i = |R_i \cap C|$ then

$$|X||Y| = \sum_{i=1}^{t} |R_i| \qquad |C| = \sum_{i=1}^{t} m_i \qquad |R_i| \geq m_i^2$$

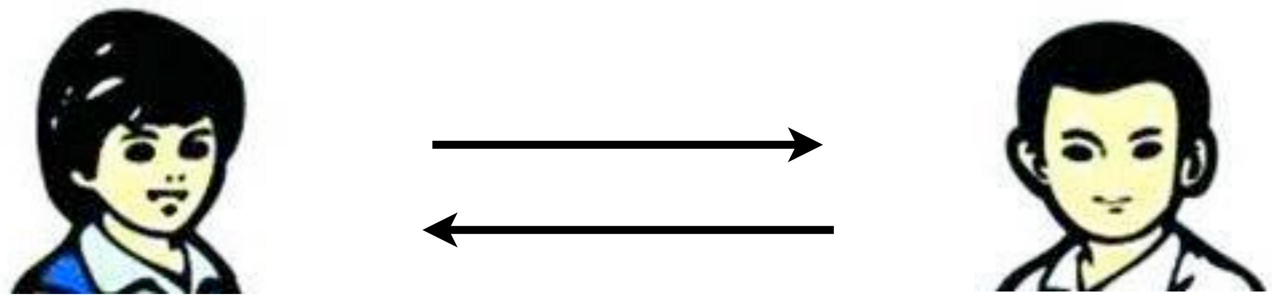
$$|C|^2 = \left(\sum_{i=1}^{t} m_i\right)^2 \leq t \sum_{i=1}^{t} m_i^2 \leq t \sum_{i=1}^{t} |R_i| = t|X||Y|$$

(Cauchy-Schwarz)

$$\Rightarrow \quad t \geq \frac{|C|^2}{|X||Y|}$$

$$\mathsf{R}_{\epsilon+\delta}(R) = \mathsf{R}^{\mathsf{Pub}}_{\epsilon}(R) + O(\log n + \log \delta^{-1})$$

transform any public-coin protocol P to P'
which uses only $O(\log n + \log(1/\delta))$ public random bits

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

public random bits $r \sim \Sigma$ (of any length)

$$Z(x,y,r) = \begin{cases} 1 & \text{if } P \text{ is wrong on inputs } x,y \text{ and random bits } r \\ 0 & \text{otherwise} \end{cases}$$

$$\forall \text{ legal } x,y, \quad \mathbb{E}_{r\sim\Sigma}[Z(x,y,r)] \le \epsilon$$

Goal: $\exists\ r_1, r_2, \ldots, r_t$ such that for uniform $i \in [n]$

$$\forall \text{ legal } x,y, \quad \mathbb{E}_{i}[Z(x,y,r_i)] \le \epsilon + \delta$$

i is new random bits, $\{r_1, r_2, \ldots, r_t\}$ is hard-wired into protocol P'

$$\mathsf{R}_{\epsilon+\delta}(R) = \mathsf{R}^{\mathsf{Pub}}_{\epsilon}(R) + O(\log n + \log \delta^{-1})$$

$$Z(x,y,r) = \begin{cases} 1 & \text{if } P \text{ is wrong on inputs } x, y \text{ and random bits } r \\ 0 & \text{otherwise} \end{cases}$$

$$\forall \text{ legal } x, y, \quad \mathbb{E}_{r\sim\Sigma}[Z(x,y,r)] \le \epsilon$$

Goal: $\exists\ r_1, r_2, \ldots, r_t$ such that for uniform $i \in [n]$

$$\forall \text{ legal } x, y, \quad \mathbb{E}_i[Z(x,y,r_i)] \le \epsilon + \delta$$

sample $r_1, r_2, \ldots, r_t$ i.i.d according to Σ

$\forall$ particular legal x,y, $\quad \mathbb{E}_i[Z(x,y,r_i)] = \frac{1}{t}\sum_{i=1}^{t} Z(x,y,r_i)$

Chernoff bound:

$$\Pr_{r_1,\ldots,r_t}[\mathbb{E}_i[Z(x,y,r_i)] > \epsilon+\delta] = \Pr_{r_1,\ldots,r_t}\left[\sum_{i=1}^{t} Z(x,y,r_i) > (\epsilon+\delta)t\right] \le \mathrm{e}^{-2\delta^2 t}$$

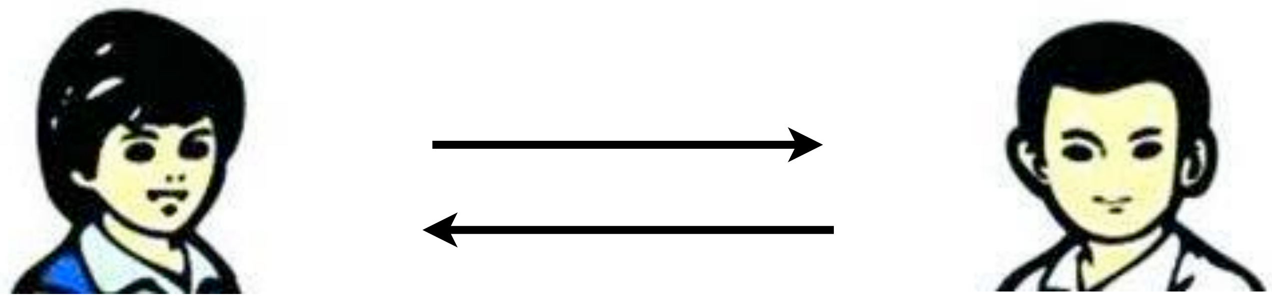
choose t=O(n/δ²) $\quad < 2^{-2n}$

union bound:

$$\Pr_{r_1,\ldots,r_t}[\exists x, y, \mathbb{E}_i[Z(x,y,r_i)] > \epsilon+\delta] < 1$$

$$\mathsf{R}_{\epsilon+\delta}(R) = \mathsf{R}^{\mathsf{Pub}}_{\epsilon}(R) + O(\log n + \log \delta^{-1})$$

transform any public-coin protocol P to P'
which uses only $O(\log n + \log \delta^{-1})$ public random bits

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

public random bits $r \sim \Sigma$ (of any length)

find such random bits $r_1, r_2, \ldots, r_t$, $t=O(n/\delta^2)$:

$\forall$ legal inputs x, y

$$\Pr_i[P \text{ is wrong on } x, y \text{ with random bits } r_i] \le \epsilon + \delta$$

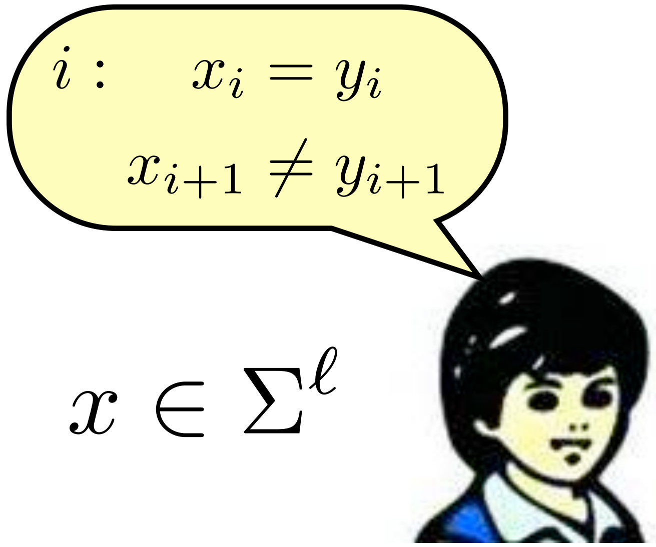
Alice and Bob know $\{r_1, r_2, \ldots, r_t\}$ without communication

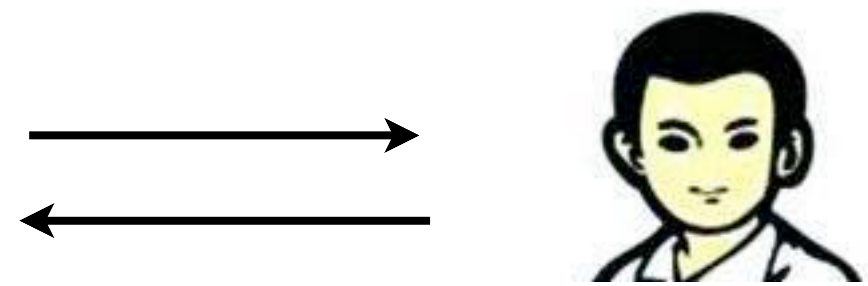
P': run $P(x,y,r_i)$ where uniform i is new public random bits

FORK Relation

$$\mathrm{FORK} \subset \Sigma^\ell \times \Sigma^\ell \times \{1, \ldots, \ell - 1\}$$

$x \in \Sigma^\ell$





$y \in \Sigma^\ell$

alphabet $\Sigma = \{1, 2, \ldots, w\}$

output: such an index i that

$x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

FORK Relation

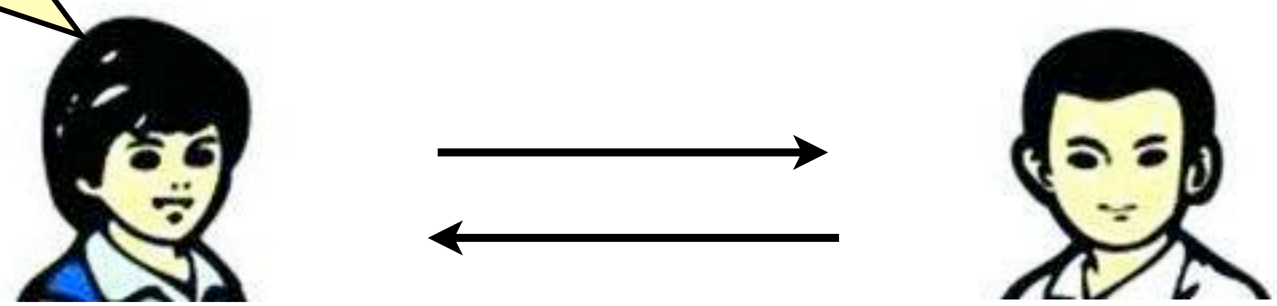
$i: \quad x_i = y_i$

$x_{i+1} \neq y_{i+1}$

$$\text{FORK} \subset \Sigma^\ell \times \Sigma^\ell \times \{0, 1, \ldots, \ell\}$$

$$\overset{1}{\overset{||}{x_0}} x_1 \cdots x_\ell \overset{1}{\overset{||}{x_{\ell+1}}}$$

$$x_1 x_2 \cdots x_\ell \in \Sigma^\ell$$



$$\overset{1}{\overset{||}{y_0}} y_1 \cdots y_\ell \overset{2}{\overset{||}{y_{\ell+1}}}$$

$$y_1 y_2 \cdots y_\ell \in \Sigma^\ell$$

alphabet $\Sigma=\{1,2, ..., w\}$

output: such an index i that

$x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

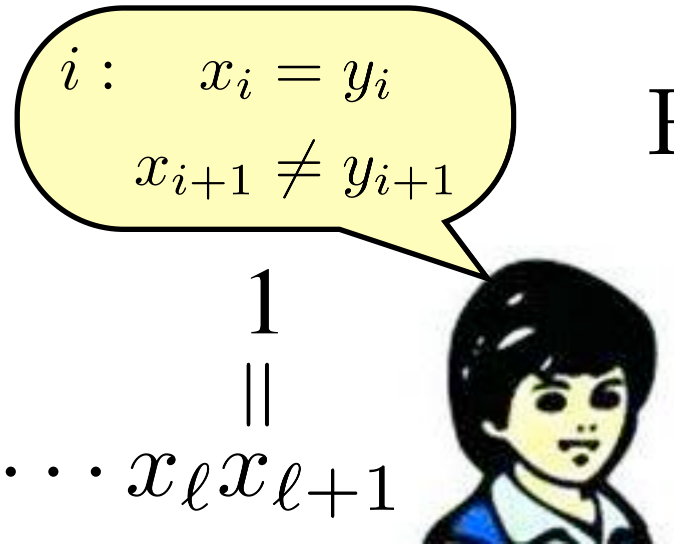
output 0 if $x=y$ and 1 if $x \neq y$ *entry-wise*

w=3	Alice:	1	2	3	1	2	1	3	1
l=6	Bob:	1	3	2	1	2	2	3	2

correct answers i= 0 4 6

FORK Relation

$$\mathrm{FORK} \subset \Sigma^\ell \times \Sigma^\ell \times \{0, 1, \ldots, \ell\}$$



$$\begin{matrix} 1 & & 1 \\ \| & & \| \\ x_0 x_1 & \cdots & x_\ell x_{\ell+1} \end{matrix}$$

$x_1 x_2 \cdots x_\ell \in \Sigma^\ell$

$\longrightarrow$

$\longleftarrow$

$$\begin{matrix} 1 & & 2 \\ \| & & \| \\ y_0 y_1 & \cdots & y_\ell y_{\ell+1} \end{matrix}$$

$y_1 y_2 \cdots y_\ell \in \Sigma^\ell$

alphabet $\Sigma=\{1,2, \ldots, w\}$

$$\mathrm{D(FORK)} = O(\log \ell \log w)$$

How?

binary search to maintain an (i, j) such that

$i < j,\ x_i = y_i$ and $x_j \neq y_j$

starting with $i=0, j=l$

by exchanging a character in Σ in each round

FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$ for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

a protocol for FORK is a $(1, l)$-protocol

Lemma: $\exists$ c-bit (α, l)-protocol for FORK

$\Rightarrow$ $\exists$ (c-1)-bit $(\alpha/2, l)$-protocol for FORK

P : successfully solves FORK for $\forall x,y \in S$ with $|S| \geq \alpha w^l$

WLOG: Alice sends the 1st bit $a \in \{0,1\}$
choose a larger $S_a = \{x \in S \mid \text{ Alice sends } a\}$

run P without Alice sending the 1st bit (under the assumption that Alice sent a) $\Rightarrow$ correct for $\forall x,y \in S_a$

FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$
for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

a protocol for FORK is a $(1, l)$-protocol

Lemma: $\exists$ c-bit (α, l)-protocol for FORK
⇒ $\exists$ (c-1)-bit $(\alpha/2, l)$-protocol for FORK

⇒ $\mathrm{D}(\mathrm{FORK}) = \Omega(\log w)$

How?

Why not bigger?

the subproblem should be nontrivial

$\alpha < 1/w$ may trivialize the problem

FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$
for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

a protocol for FORK is a $(1, l)$-protocol

Lemma: $\exists$ c-bit (α, l)-protocol for FORK
⇒ $\exists$ (c-1)-bit $(\alpha/2, l)$-protocol for FORK

Amplification Lemma: for FORK, for $\alpha > \frac{100}{w}$
$\exists$ c-bit (α, l)-protocol ⇒ $\exists$ c-bit $\left(\frac{\sqrt{\alpha}}{2}, \frac{\ell}{2}\right)$-protocol

⇒ $\mathrm{D}(\mathrm{FORK}) = \Omega(\log \ell \log w)$

a protocol for FORK is a $(1, l)$-protocol

then it must also be a $(1/w^{1/3}, l)$-protocol

Lemma: ∃ c-bit (α, l)-protocol for FORK

⇒ ∃ (c-1)-bit $(\alpha/2, l)$-protocol for FORK

⇒ $\exists (c - \Omega(\log w))$-bit $\left(\frac{4}{w^{2/3}}, \ell\right)$-protocol

Amplification Lemma: for FORK, for $\alpha > \frac{100}{w}$

∃ c-bit (α, l)-protocol ⇒ ∃ c-bit $\left(\frac{\sqrt{\alpha}}{2}, \frac{\ell}{2}\right)$-protocol

⇒ $\exists (c - \Omega(\log w))$-bit $\left(\frac{1}{w^{1/3}}, \frac{\ell}{2}\right)$-protocol

repeat for $O(\log l)$ times

$\exists (c - \Omega(\log \ell \log w))$-bit $\left(\frac{1}{w^{1/3}}, 2\right)$-protocol ⇒ $c > \Omega(\log \ell \log w)$

FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$
for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

Lemma: $\exists$ c-bit (α, l)-protocol for FORK
$\Rightarrow$ $\exists$ (c-1)-bit $(\alpha/2, l)$-protocol for FORK

Amplification Lemma: for FORK, for $\alpha > \frac{100}{w}$
$\exists$ c-bit (α, l)-protocol $\Rightarrow$ $\exists$ c-bit $\left(\frac{\sqrt{\alpha}}{2}, \frac{\ell}{2}\right)$-protocol

[Gringi, Sipser '91]
$\Rightarrow$

$$\mathrm{D(FORK)} = \Omega(\log \ell \log w)$$

FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$ for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

Amplification Lemma: for FORK, for $\alpha > \frac{100}{w}$

$\exists$ c-bit (α, l)-protocol $\Rightarrow$ $\exists$ c-bit $\left(\frac{\sqrt{\alpha}}{2}, \frac{\ell}{2}\right)$-protocol

P *P'*

P : solve inputs from $S \subseteq \Sigma^l$

P' : use protocol P to solve inputs from a denser $S' \subseteq \Sigma^{l/2}$

$x \in S' \subseteq \Sigma^{\ell/2}$

$\downarrow$

$f(x) \in S \subseteq \Sigma^\ell$

$\longrightarrow$

$\longleftarrow$

$y \in S' \subseteq \Sigma^{\ell/2}$

$\downarrow$

$g(y) \in S \subseteq \Sigma^\ell$

FORK($f(x)$, $g(y)$) answers FORK(x, y)

i that $f(x)_i = g(y)_i, f(x)_{i+1} \neq g(y)_{i+1}$ tells us j that $x_j = y_j, x_{j+1} \neq y_{j+1}$

FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$
for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

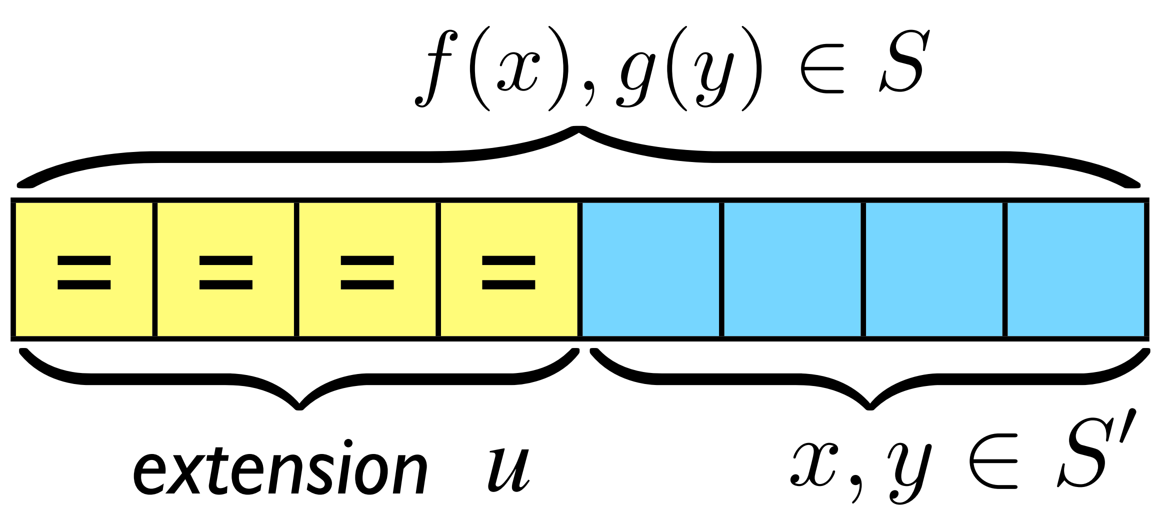
Amplification Lemma: for FORK, for $\alpha > \frac{100}{w}$

$\exists$ c-bit (α, l)-protocol $\Rightarrow$ $\exists$ c-bit $\left(\frac{\sqrt{\alpha}}{2}, \frac{\ell}{2}\right)$-protocol

P $\qquad\qquad$ P'

P : solve inputs from $S \subseteq \Sigma^l$

P' : use protocol P to solve inputs from a denser $S' \subseteq \Sigma^{l/2}$



$\exists\ u \in \Sigma^{l/2}$: *many* elements $z \in S$ is in form $z=(u,x)$

FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$
for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

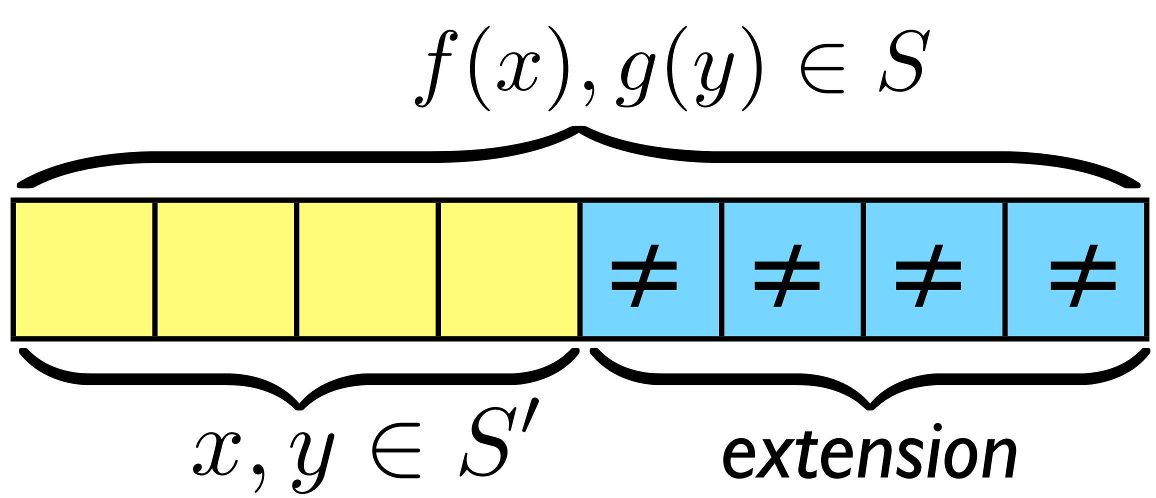
Amplification Lemma: for FORK, for $\alpha > \frac{100}{w}$

$\exists$ c-bit (α, l)-protocol ⇒ $\exists$ c-bit $\left(\frac{\sqrt{\alpha}}{2}, \frac{\ell}{2}\right)$-protocol

P *P'*

P : solve inputs from $S \subseteq \Sigma^l$

P' : use protocol P to solve inputs from a denser $S' \subseteq \Sigma^{l/2}$



$\exists$ large $S' \subseteq \Sigma^{l/2}$: any $x,y \in S'$ can be extended to $(x,F(x)),(y,G(y)) \in S$
such that $F(x), G(y)$ are entry-wise different

FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$
for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

Amplification Lemma: for FORK, for $\alpha > \frac{100}{w}$

$\exists$ c-bit (α, l)-protocol ⇒ $\exists$ c-bit $\left(\frac{\sqrt{\alpha}}{2}, \frac{\ell}{2}\right)$-protocol

$S \subseteq \Sigma^\ell$ and $|S| \geq \alpha w^\ell$ ⇒

$\exists\ u \in \Sigma^{l/2}$: *many* elements $z \in S$ is in form $z=(u,x)$

or

$\exists$ *large* $S' \subseteq \Sigma^{l/2}$: any $x,y \in S'$ can be extended to $(x, F(x)), (y, G(y)) \in S$
such that $F(x), G(y)$ are entry-wise different

"*many*" = "*large*" = $\frac{\sqrt{\alpha}}{2} w^{\frac{\ell}{2}}$

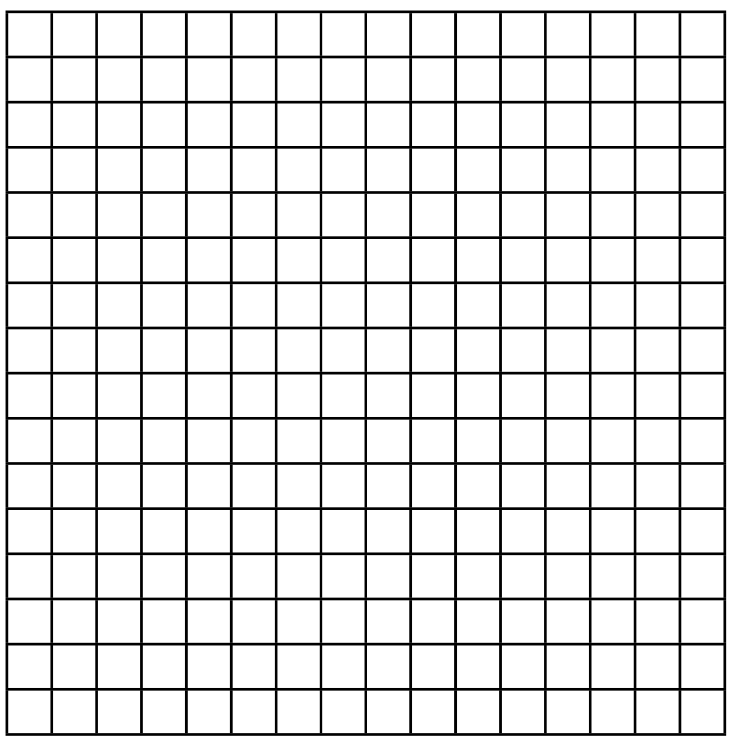
$S \subseteq \Sigma^\ell$ and $|S| \geq \alpha w^\ell$ ⇒ "*many*" = "*large*" = $\frac{\sqrt{\alpha}}{2} w^{\frac{\ell}{2}}$:

- $\exists\ u \in \Sigma^{l/2}$: *many* elements $z \in S$ is in form $z=(u,x)$
- or
- $\exists$ *large* $S' \subseteq \Sigma^{l/2}$: any $x,y \in S'$ can be extended to $(x, F(x)), (y, G(y)) \in S$ such that $F(x), G(y)$ are entry-wise different

Boolean matrix S :

$\Sigma^{\ell/2}$

$\Sigma^{\ell/2}$



$$\forall u, v \in \Sigma^{\ell/2}, \quad S(u,v) = \begin{cases} 1 & \text{if } (u,v) \in S \\ 0 & \text{otherwise} \end{cases}$$

S is *α-dense* (of 1-entries)

⇒

- $\exists$ a row u that is $\geq \sqrt{\frac{\alpha}{2}}$ *-dense*
- or
- $\exists \sqrt{\frac{\alpha}{2}}$ *-fraction* of rows $\geq \frac{\alpha}{2}$ *-dense*

"Either one row is *very dense*, or there are many rows that are *pretty dense*."

By contradiction:

all rows are $< \sqrt{\frac{\alpha}{2}}$-dense and $< \sqrt{\frac{\alpha}{2}} w^{\ell/2}$ rows are $\geq \frac{\alpha}{2}$-dense

⇒ density of S $< \frac{\alpha}{2} + \sqrt{\frac{\alpha}{2}}\sqrt{\frac{\alpha}{2}} = \alpha$ contradiction!

$S \subseteq \Sigma^\ell$ and $|S| \geq \alpha w^\ell$ ⇒ "*many*" = "*large*" = $\frac{\sqrt{\alpha}}{2} w^{\frac{\ell}{2}}$:

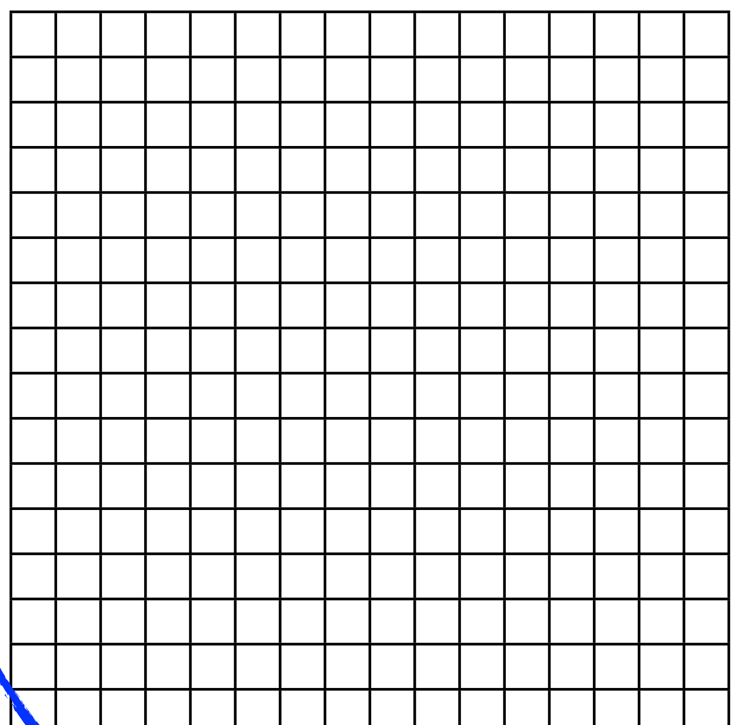
- $\exists\ u \in \Sigma^{l/2}$: *many* elements $z \in S$ is in form $z=(u,x)$

or

- $\exists$ *large* $S' \subseteq \Sigma^{l/2}$: any $x,y \in S'$ can be extended to $(x, F(x)), (y, G(y)) \in S$ such that $F(x), G(y)$ are entry-wise different

Boolean matrix S :

$\Sigma^{\ell/2}$



$\Sigma^{\ell/2}$

$$\forall u, v \in \Sigma^{\ell/2}, \quad S(u,v) = \begin{cases} 1 & \text{if } (u,v) \in S \\ 0 & \text{otherwise} \end{cases}$$

S is *α-dense* (of 1-entries)

⇒

- $\exists$ a row u that is $\geq \sqrt{\frac{\alpha}{2}}$*-dense*

or

- $\exists \sqrt{\frac{\alpha}{2}}$ *-fraction* of rows $\geq \frac{\alpha}{2}$*-dense*

⇒

- $\exists u \in \Sigma^{\ell/2}: \quad |\{(u,x) \in S\}| \geq \sqrt{\frac{\alpha}{2}} w^{\frac{\ell}{2}}$

or

- $\exists \geq \sqrt{\frac{\alpha}{2}} w^{\ell/2}$ many $x \in \Sigma^{\ell/2}: \quad |\{(x,u) \in S\}| \geq \frac{\alpha}{2} w^{\frac{\ell}{2}}$

we still need

$S \subseteq \Sigma^\ell$, $\exists \geq \sqrt{\frac{\alpha}{2}} w^{\ell/2}$ many $x \in \Sigma^{\ell/2}$: $|\{(x,u) \in S\}| \geq \frac{\alpha}{2} w^{\frac{\ell}{2}}$

⇨ $\exists\ S' \subseteq \Sigma^{l/2}$ of size $|S'| \geq \frac{\sqrt{\alpha}}{2} w^{\ell/2}$ such that:

any $x,y \in S'$ can be extended to $(x,F(x)), (y, G(y)) \in S$
such that $F(x), G(y)$ are *entry-wise* different

Goal: find nonempty subsets: $F_1, F_2, \ldots, F_{\ell/2} \subset \Sigma$

and their compliments: $\overline{F}_1, \overline{F}_2, \ldots, \overline{F}_{\ell/2} \subset \Sigma$

such that for $\geq \frac{\sqrt{\alpha}}{2} w^{\ell/2}$ many $x \in \Sigma^{l/2}$

$\exists u \in F_1 \times \cdots \times F_{\ell/2}$ such that $(x,u) \in S$ ($F(x)=u$)

and $\exists v \in \overline{F}_1 \times \cdots \times \overline{F}_{\ell/2}$ such that $(x,v) \in S$ ($G(x)=v$)

⇨ any $u \in F_1 \times \cdots \times F_{\ell/2}$ and any $v \in \overline{F}_1 \times \cdots \times \overline{F}_{\ell/2}$
must be *entry-wise* different: $\forall 1 \leq i \leq \frac{\ell}{2}, \quad u_i \neq v_i$

$S \subseteq \Sigma^\ell$, $\exists \geq \sqrt{\frac{\alpha}{2}} w^{\ell/2}$ many $x \in \Sigma^{\ell/2}$: $|\{(x,u) \in S\}| \geq \frac{\alpha}{2} w^{\frac{\ell}{2}}$

⇨ $\exists$ $S' \subseteq \Sigma^{l/2}$ of size $|S'| \geq \frac{\sqrt{\alpha}}{2} w^{\ell/2}$ such that:

any $x,y \in S'$ can be extended to $(x, F(x)), (y, G(y)) \in S$ such that $F(x), G(y)$ are *entry-wise* different

independently random: $F_1, F_2, \ldots, F_{\ell/2} \subset \Sigma$

and their compliments: $\overline{F}_1, \overline{F}_2, \ldots, \overline{F}_{\ell/2} \subset \Sigma$

each $F_i \in \binom{\Sigma}{w/2}$ is sampled uniformly and independently at random

for any "good" x that $|\{(x,u) \in S\}| \geq \frac{\alpha}{2} w^{\frac{\ell}{2}}$

$$\Pr\left[\begin{array}{l} \exists u \in F_1 \times \cdots \times F_{\ell/2} \text{ such that } (x,u) \in S \\ \text{and } \exists v \in \overline{F}_1 \times \cdots \times \overline{F}_{\ell/2} \text{ such that } (x,v) \in S \end{array}\right] > ?$$

$S \subseteq \Sigma^\ell$, $\exists \geq \sqrt{\frac{\alpha}{2}} w^{\ell/2}$ many $x \in \Sigma^{\ell/2}$: $|\{(x,u) \in S\}| \geq \frac{\alpha}{2} w^{\frac{\ell}{2}}$

⇒ $\exists$ $S' \subseteq \Sigma^{l/2}$ of size $|S'| \geq \frac{\sqrt{\alpha}}{2} w^{\ell/2}$ such that:

any $x,y \in S'$ can be extended to $(x, F(x)), (y, G(y)) \in S$
such that $F(x), G(y)$ are *entry-wise* different

independently random: $F_1, F_2, \ldots, F_{\ell/2} \subset \Sigma$
and their compliments: $\overline{F}_1, \overline{F}_2, \ldots, \overline{F}_{\ell/2} \subset \Sigma$

each $F_i \in \binom{\Sigma}{w/2}$ is sampled uniformly and independently at random

for any "good" x that $|\{(x,u) \in S\}| \geq \frac{\alpha}{2} w^{\frac{\ell}{2}}$

$\Pr\Big[$ x is "*really good*" $\Big] > ?$

$S \subseteq \Sigma^\ell$, $\exists \geq \sqrt{\frac{\alpha}{2}} w^{\ell/2}$ many $x \in \Sigma^{\ell/2}$: $|\{(x,u) \in S\}| \geq \frac{\alpha}{2} w^{\frac{\ell}{2}}$

⇨ $\exists\ S' \subseteq \Sigma^{l/2}$ of size $|S'| \geq \frac{\sqrt{\alpha}}{2} w^{\ell/2}$ such that:

any $x,y \in S'$ can be extended to $(x,F(x)), (y, G(y)) \in S$ such that $F(x), G(y)$ are *entry-wise* different

independently random: $F_1, F_2, \ldots, F_{\ell/2} \subset \Sigma$

and their compliments: $\overline{F}_1, \overline{F}_2, \ldots, \overline{F}_{\ell/2} \subset \Sigma$

each $F_i \in \binom{\Sigma}{w/2}$ is sampled uniformly and independently at random

for any "good" x that $|\{(x,u) \in S\}| \geq \frac{\alpha}{2} w^{\frac{\ell}{2}}$

Why?

$$\Pr[\forall u \in F_1 \times \cdots \times F_{\ell/2}, (x,u) \notin S] + \Pr[\forall v \in \overline{F}_1 \times \cdots \times \overline{F}_{\ell/2}, (x,v) \notin S] < 2\left(1 - \frac{\alpha}{2}\right)^{\frac{w}{2}} < 2\mathrm{e}^{-\alpha w/4}$$

x is "really good": $\exists u \in F_1 \times \cdots \times F_{\ell/2}, (x,u) \in S$ and
$\exists v \in \overline{F}_1 \times \cdots \times \overline{F}_{\ell/2}, (x,v) \in S$

$S \subseteq \Sigma^\ell$, $\exists \geq \sqrt{\frac{\alpha}{2}} w^{\ell/2}$ many $x \in \Sigma^{\ell/2}$: $|\{(x,u) \in S\}| \geq \frac{\alpha}{2} w^{\frac{\ell}{2}}$

$\Rightarrow$ $\exists$ $S' \subseteq \Sigma^{l/2}$ of size $|S'| \geq \frac{\sqrt{\alpha}}{2} w^{\ell/2}$ such that:

any $x,y \in S'$ can be extended to $(x,F(x)), (y, G(y)) \in S$ such that $F(x), G(y)$ are *entry-wise* different

independently random: $F_1, F_2, \ldots, F_{\ell/2} \subset \Sigma$

and their compliments: $\overline{F}_1, \overline{F}_2, \ldots, \overline{F}_{\ell/2} \subset \Sigma$

each $F_i \in \binom{\Sigma}{w/2}$ is sampled uniformly and independently at random

for any "good" x that $|\{(x,u) \in S\}| \geq \frac{\alpha}{2} w^{\frac{\ell}{2}}$

$$\Pr[x \text{ is really good }] > 1 - 2\mathrm{e}^{-\alpha w/4}$$

$$\mathbb{E}[\#\text{of really good } x] \geq (1 - 2\mathrm{e}^{\alpha w/4})\sqrt{\frac{\alpha}{2}} \geq \frac{\sqrt{\alpha}}{2}$$ (for $\alpha > \frac{100}{w}$)

x is "really good": $\exists u \in F_1 \times \cdots \times F_{\ell/2}, (x,u) \in S$ and

$\exists v \in \overline{F}_1 \times \cdots \times \overline{F}_{\ell/2}, (x,v) \in S$

FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$
for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

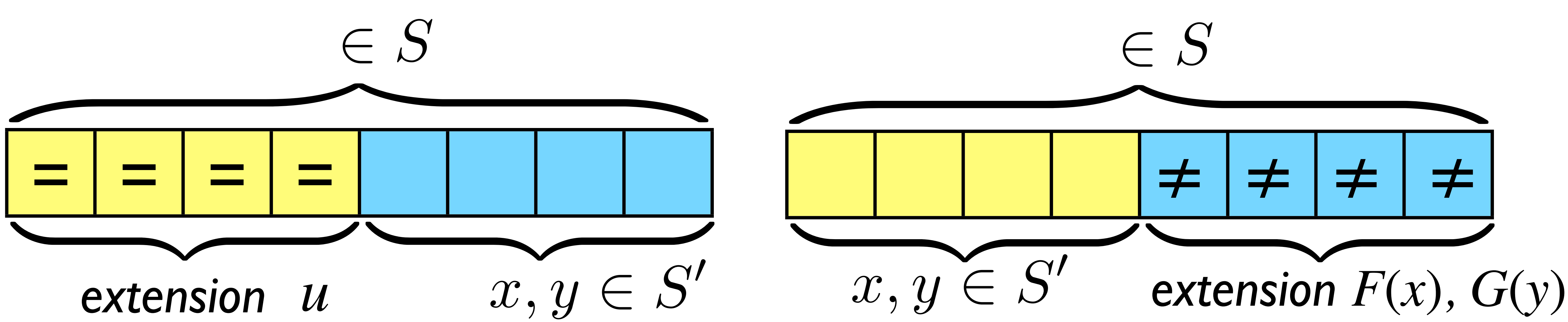
Amplification Lemma: for FORK, for $\alpha > \frac{100}{w}$

$\exists$ c-bit (α, l)-protocol $\Longrightarrow$ $\exists$ c-bit $\left(\frac{\sqrt{\alpha}}{2}, \frac{\ell}{2}\right)$-protocol

P P'

P : solve inputs from $S \subseteq \Sigma^l$

P' : use protocol P to solve inputs from a denser $S' \subseteq \Sigma^{l/2}$



FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$ for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

Amplification Lemma: for FORK, for $\alpha > \frac{100}{w}$

$\exists$ c-bit (α, l)-protocol $\Rightarrow$ $\exists$ c-bit $\left(\frac{\sqrt{\alpha}}{2}, \frac{\ell}{2}\right)$-protocol

P $\quad$ P'

P : solve inputs from $S \subseteq \Sigma^l$

P' : use protocol P to solve inputs from a denser $S' \subseteq \Sigma^{l/2}$

either: $x \in S' \subseteq \Sigma^{\ell/2}$ $\downarrow$ $(u, x) \in S$

$y \in S' \subseteq \Sigma^{\ell/2}$ $\downarrow$ $(u, y) \in S$

or: $x \in S' \subseteq \Sigma^{\ell/2}$ $\downarrow$ $(x, F(x)) \in S$

$y \in S' \subseteq \Sigma^{\ell/2}$ $\downarrow$ $(y, G(y)) \in S$

$F(x)$, $G(y)$ are *entry-wise* different

FORK: $|\Sigma|=w$, for $\forall x, y \in \Sigma^l$, find i that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$

(α, l)-protocol: successfully solves FORK for $\forall x,y \in S$ for an $S \subseteq \Sigma^l$ of size at least $|S| \geq \alpha w^l$

Lemma: $\exists$ c-bit (α, l)-protocol for FORK

⇒ $\exists$ (c-1)-bit $(\alpha/2, l)$-protocol for FORK

Amplification Lemma: for FORK, for $\alpha > \frac{100}{w}$

$\exists$ c-bit (α, l)-protocol ⇒ $\exists$ c-bit $\left(\frac{\sqrt{\alpha}}{2}, \frac{\ell}{2}\right)$-protocol

[Gringi, Spser '91]

⇒ $\mathrm{D(FORK)} = \Omega(\log \ell \log w)$

Direct Sum

- Direct product: The probability of success of performing k independent tasks decreases in k.
    - Yao's XOR lemma, the parallel repetition theorem of Ran Raz ...
- Direct sum: The amount of resources needed to perform k independent tasks grows with k.
    - direct sum problems in CC

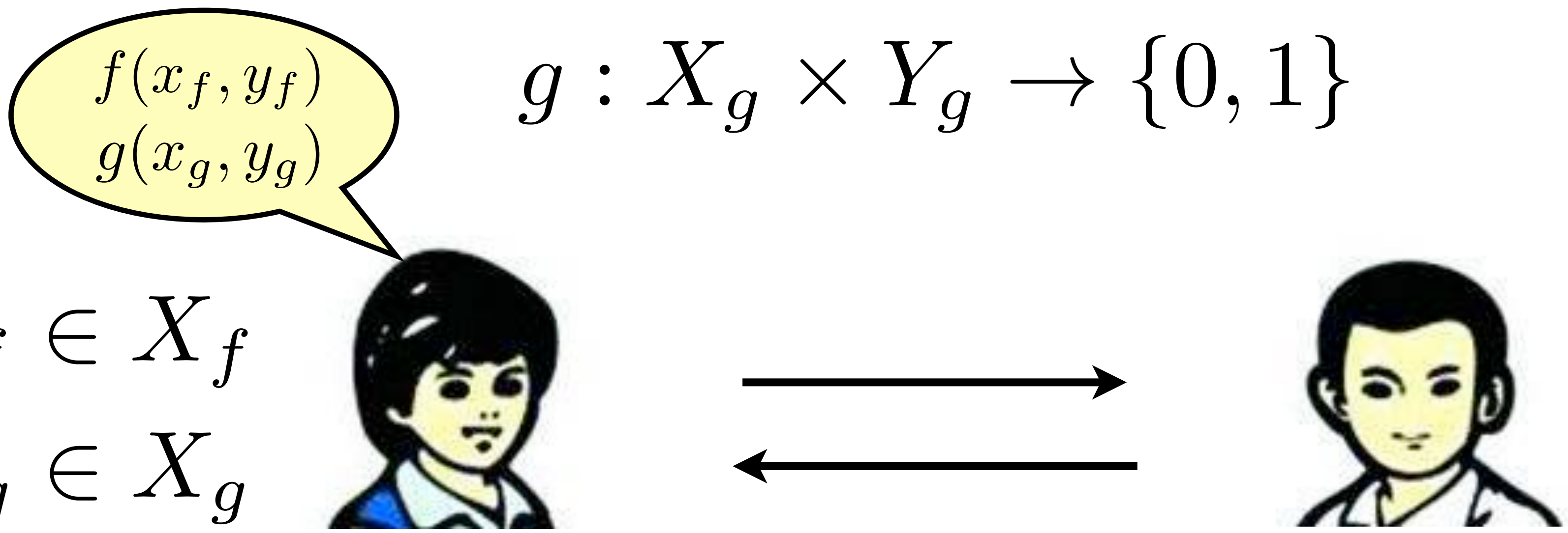
Direct Sum Settings

$$f : X_f \times Y_f \to \{0,1\}$$

$$g : X_g \times Y_g \to \{0,1\}$$

$x_f \in X_f$

$x_g \in X_g$



$y_f \in Y_f$

$y_g \in Y_g$

$$F : X_F \times Y_F \to \{0,1\}^2 \quad \text{with} \quad \begin{cases} X_F = X_f \times X_g \\ Y_F = Y_f \times Y_g \end{cases}$$

$$F((x_f, x_g), (y_f, y_g)) = (f(x_f, y_f), g(x_g, y_g))$$

subproblems are *independent*:

inputs are arbitrary over $\forall((x_f, x_g), (y_f, y_g)) \in (X_f \times X_g) \times (Y_f \times Y_g)$

μ_f over $X_f \times Y_f$ $\quad$ μ_g over $X_g \times Y_g$ $\Rightarrow$ $\mu_F = \mu_f \times \mu_g$

Direct Sum Settings

$$f : X_f \times Y_f \to \{0,1\}$$

$$g : X_g \times Y_g \to \{0,1\}$$

$x_f \in X_f$

$x_g \in X_g$

$y_f \in Y_f$

$y_g \in Y_g$

$$F : X_F \times Y_F \to \{0,1\}^2 \quad \text{with} \begin{cases} X_F = X_f \times X_g \\ Y_F = Y_f \times Y_g \end{cases}$$

$$F((x_f, x_g), (y_f, y_g)) = (f(x_f, y_f), g(x_g, y_g))$$

communication complexity: $\mathsf{CC}(f,g) \triangleq \mathsf{CC}(F)$

for deterministic, randomized, nondeterministic protocols...

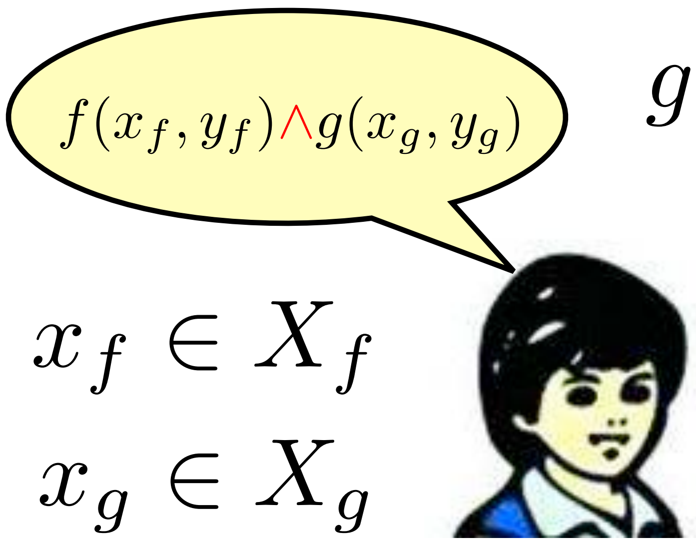
Direct Sum Settings

$$f : X_f \times Y_f \to \{0,1\}$$

$$g : X_g \times Y_g \to \{0,1\}$$

$x_f \in X_f$

$x_g \in X_g$



$\longrightarrow$

$\longleftarrow$

$y_f \in Y_f$

$y_g \in Y_g$

$$F : X_F \times Y_F \to \{0,1\} \quad \text{with} \begin{cases} X_F = X_f \times X_g \\ Y_F = Y_f \times Y_g \end{cases}$$

$$F((x_f, x_g), (y_f, y_g)) = f(x_f, y_f) \wedge g(x_g, y_g)$$

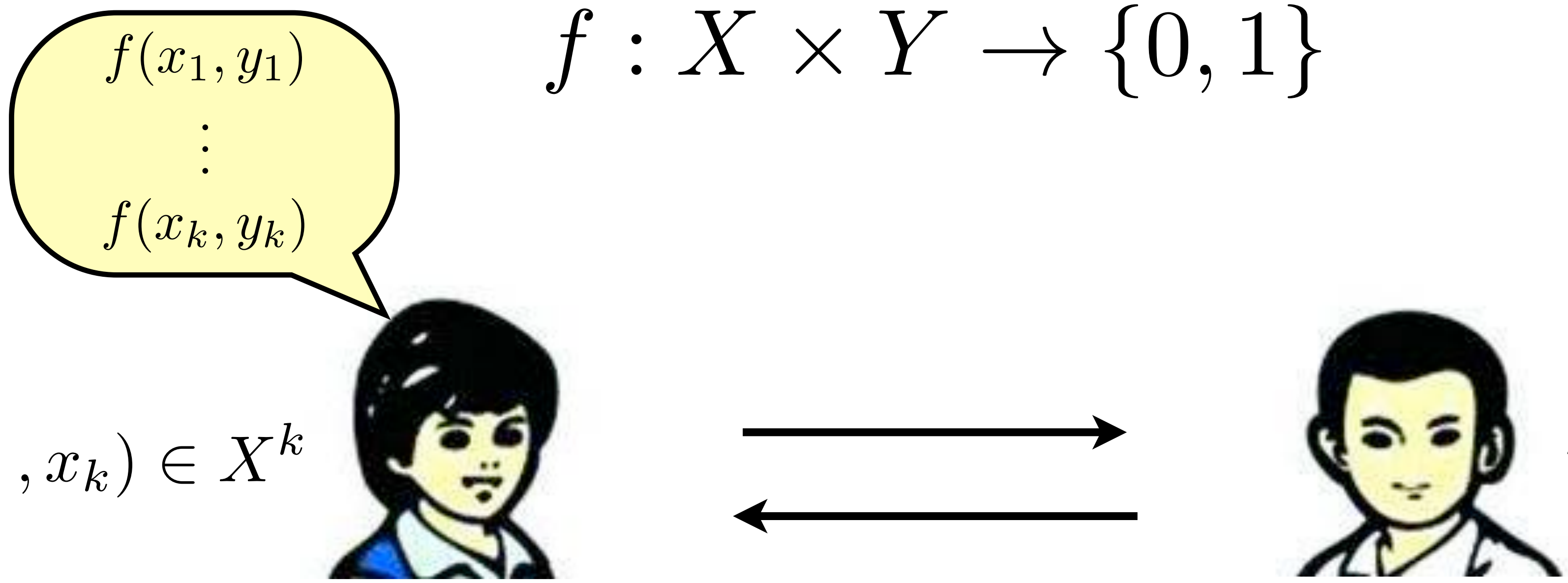
communication complexity: $\mathrm{CC}(f \wedge g) \triangleq \mathrm{CC}(F)$

for deterministic, randomized, nondeterministic protocols...

Direct Sum Settings

$$f : X \times Y \to \{0,1\}$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$



$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

$$f^k : X^k \times Y^k \to \{0,1\}^k$$

$$f^k(\vec{x}, \vec{y}) = (f(x_1, y_1), \ldots, f(x_k, y_k))$$

communication complexity: $\mathsf{CC}(f^k)$

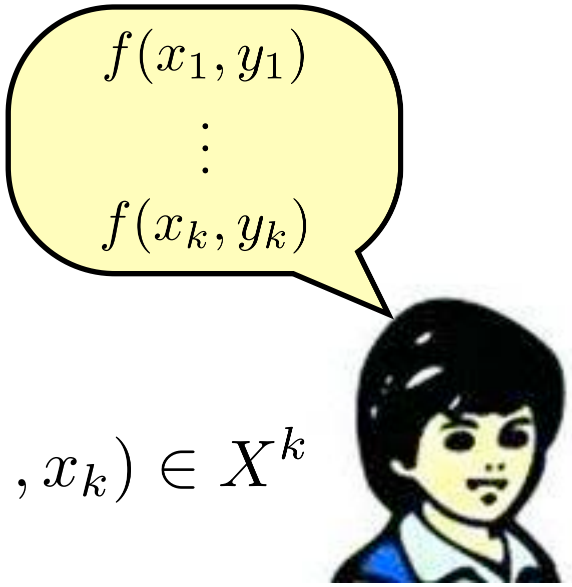
Direct Sum Problems

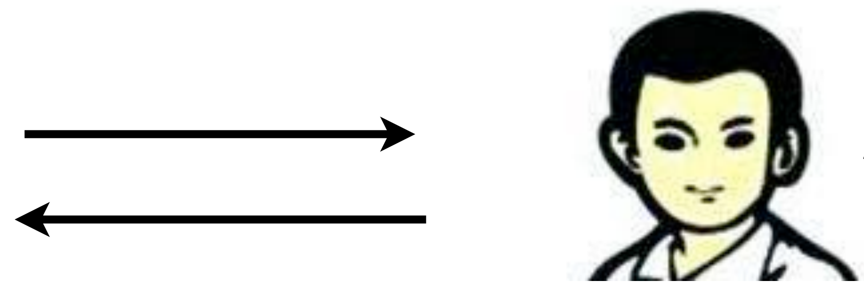
- Question I: Can $\mathsf{CC}(f^k) \ll k \cdot \mathsf{CC}(f)$?
- Question II: Can $\mathsf{CC}(\wedge^k f) \ll k \cdot \mathsf{CC}(f)$?
- "Can we solve several problems simultaneously in a way that is substantially better than to solve each of the problems separately?"
- Answer(?) to QI: possibly "no" for all functions.
- Contemporary tool: Information Complexity

Randomized Protocols

$$f : X \times Y \to \{0,1\}$$
$$f^k : X^k \times Y^k \to \{0,1\}^k$$

$\vec{x} = (x_1, \dots, x_k) \in X^k$





$\vec{y} = (y_1, \dots, y_k) \in Y^k$

- *Individually* correct: each **output**(x_i,y_i) is correct with probability > 2/3.
- *Simultaneously* correct: all **output**(x_i,y_i) are correct simultaneously with probability > 2/3.

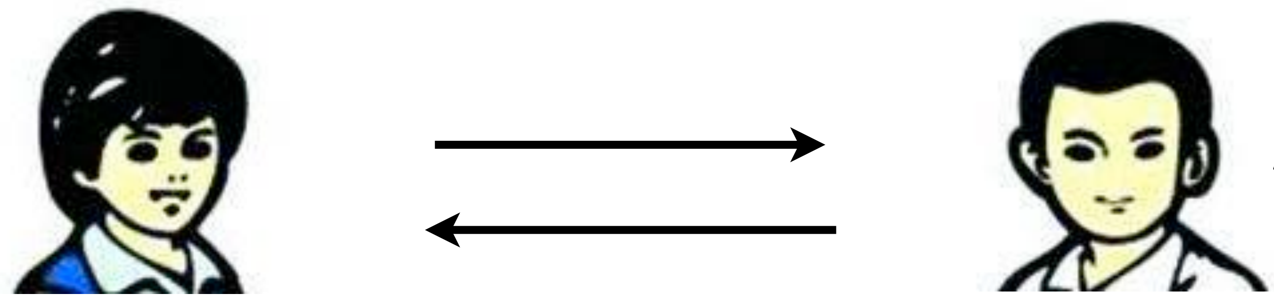
direct product (conjecture): The probability of simultaneous success is < $(2/3)^{\Omega(k)}$ with any communication cost « $O(k \cdot \mathrm{CC}(f))$.

examples: parallel repetition theorem, Yao XOR lemma

$$\mathrm{EQ} : X \times Y \to \{0,1\}$$

$$X = Y = \{0,1\}^n$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$



$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

$\mathrm{EQ}^k(\vec{x}, \vec{y}) = \vec{z}$ where z_i indicates whether x_i=y_i

$$\mathsf{R}^{\mathsf{Pub}}(\mathrm{EQ}) = O(1)$$

by checking whether $\langle x, r \rangle = \langle y, r \rangle$

where r is a shared random Boolean vector

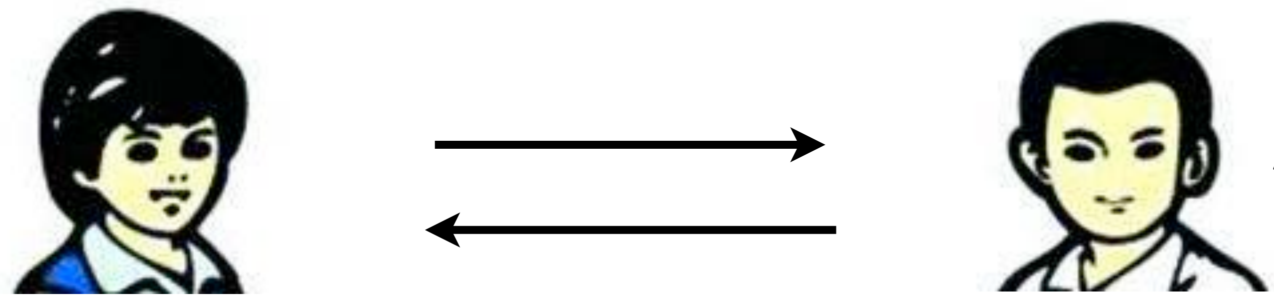
and $\langle x, r \rangle := \left(\sum_i x(i) r(i) \right) \bmod 2$

is the inner-product over $\mathrm{GF}(2)$

$$\mathrm{EQ} : X \times Y \to \{0,1\}$$

$$X = Y = \{0,1\}^n$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$



$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

$\mathrm{EQ}^k(\vec{x}, \vec{y}) = \vec{z}$ where z_i indicates whether x_i=y_i

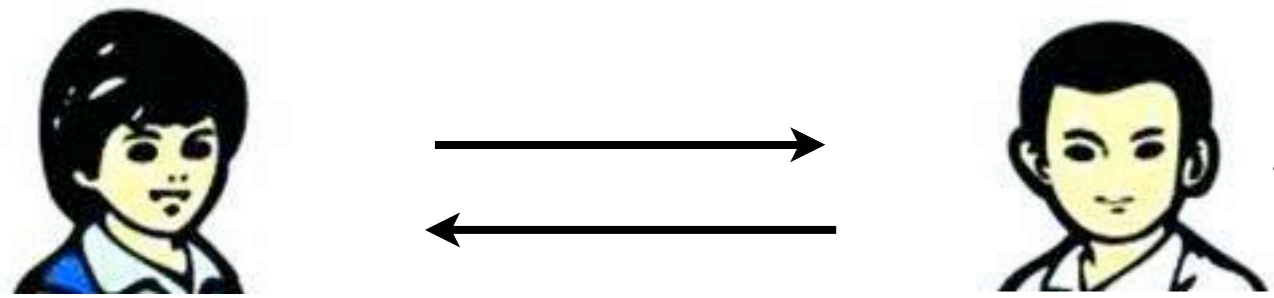
$$\mathsf{R}^{\mathsf{Pub}}(\mathrm{EQ}) = O(1)$$

recall:

Theorem: $\mathsf{R}(f) = O(\mathsf{R}^{\mathsf{Pub}}(f) + \log n)$

$$\mathrm{EQ} : X \times Y \to \{0,1\}$$
$$X = Y = \{0,1\}^n$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$



$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

$\mathrm{EQ}^k(\vec{x}, \vec{y}) = \vec{z}$ where z_i indicates whether $x_i = y_i$

$$\mathsf{R}^{\mathsf{Pub}}(\mathrm{EQ}) = O(1)$$

$$\mathsf{R}(f) = O(\mathsf{R}^{\mathsf{Pub}}(f) + \log n)$$

repeat the protocol on every instance (x_i, y_i) for $O(\log k)$ times

each instance: $1/3k$ error

$\Pr[\mathtt{output}(x_i, y_i) = 1 \mid x_i \neq y_i] \leq \frac{1}{3k}$

union bound

all k instances: $1/3$ error

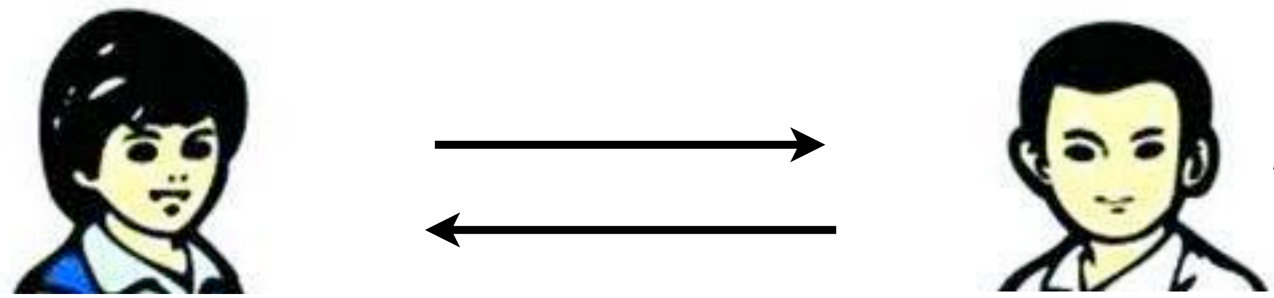
$\Pr[\exists i, \mathtt{output}(x_i, y_i) = 1 \mid \vec{x} \neq \vec{y}] \leq \frac{1}{3}$

$$\mathsf{R}^{\mathsf{Pub}}(\mathrm{EQ}^k) = O(k \log k)$$
$$\mathsf{R}(\mathrm{EQ}^k) = O(k \log k + \log n)$$

$$\mathrm{EQ} : X \times Y \to \{0,1\}$$

$$X = Y = \{0,1\}^n$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$



$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

$\mathrm{EQ}^k(\vec{x}, \vec{y}) = \vec{z}$ where z_i indicates whether $x_i = y_i$

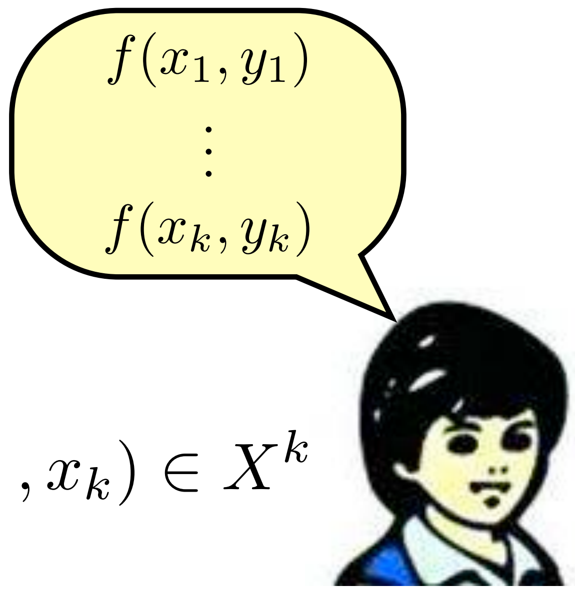
$$\mathsf{R}(\mathrm{EQ}^k) = O(k \log k + \log n)$$

recall: **Theorem**: $\mathsf{R}(\mathrm{EQ}) = \Theta(\log n)$

consider $k = \log n$:

$$\mathsf{R}(\mathrm{EQ}^k) = O(\log n \log\log n) \ll k \cdot \mathsf{R}(\mathrm{EQ}) = \Theta((\log n)^2)$$

Randomized Protocols



$f : X \times Y \to \{0,1\}$ $\quad X = Y = \{0,1\}^n$

$f^k : X^k \times Y^k \to \{0,1\}^k$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$

$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

Observations:

individually correct: $\mathsf{R}(f^k) \le k \cdot \mathsf{R}(f)$

simultaneously correct: $\mathsf{R}(f^k) = O(k \log k \cdot \mathsf{R}(f))$

individual: apply the protocol independently on k instances

simultaneous: repeat $\mathrm{O}(\log k)$ times for every instance

individual error $\le 1/3k$, then apply union bound

Randomized Protocols

$f(x_1, y_1)$

$\vdots$

$f(x_k, y_k)$

$f : X \times Y \to \{0,1\}$ $\qquad$ $X = Y = \{0,1\}^n$

$f^k : X^k \times Y^k \to \{0,1\}^k$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$

$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

Observations:

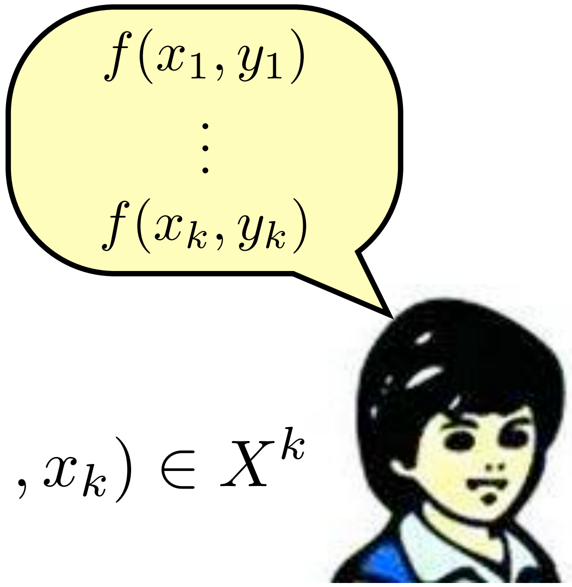
individually correct: $\mathsf{R}^{\mathsf{Pub}}(f^k) \le k \cdot \mathsf{R}^{\mathsf{Pub}}(f)$

simultaneously correct: $\mathsf{R}^{\mathsf{Pub}}(f^k) = O(k \log k \cdot \mathsf{R}^{\mathsf{Pub}}(f))$

recall:

Theorem: $\mathsf{R}(f) = O(\mathsf{R}^{\mathsf{Pub}}(f) + \log n)$

Randomized Protocols



$$f : X \times Y \to \{0,1\} \qquad X = Y = \{0,1\}^n$$

$$f^k : X^k \times Y^k \to \{0,1\}^k$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$

$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

$$\mathsf{R}(f^k) = O\left(\mathsf{R}^{\mathsf{Pub}}(f^k) + \log kn\right)$$

(*simultaneous correctness*) $\leq O\left(k \log k \cdot \mathsf{R}^{\mathsf{Pub}}(f) + \log n\right)$

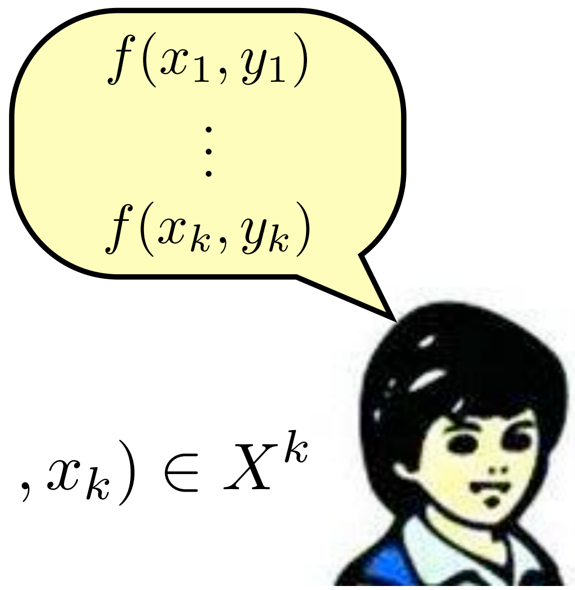
when $\mathsf{R}^{\mathsf{Pub}}(f) \ll \log n$ and $\mathsf{R}(f) = \Omega(\log n)$

this gives an acceleration over $k \cdot \mathsf{R}(f)$ for small k

Randomized Protocols

$$f : X \times Y \to \{0,1\} \qquad X = Y = \{0,1\}^n$$

$$f^k : X^k \times Y^k \to \{0,1\}^k$$



$\vec{x} = (x_1, \ldots, x_k) \in X^k$

$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

Observations:

individually correct: $\mathsf{R}^{\mathsf{Pub}}(f^k) \leq k \cdot \mathsf{R}^{\mathsf{Pub}}(f)$

simultaneously correct: $\mathsf{R}^{\mathsf{Pub}}(f^k) = O(k \log k \cdot \mathsf{R}^{\mathsf{Pub}}(f))$

List-Non-Equality problem:

$$\mathrm{LNE}_{k,n}(\vec{x},\vec{y}) = \bigwedge_i x_i \neq y_i \qquad X = Y = \{0,1\}^n$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$  ⇄  $\vec{y} = (y_1, \ldots, y_k) \in Y^k$

$$\mathrm{R}^{\mathrm{Pub}}(\mathrm{LNE}_{k,n}) = ? \qquad \mathrm{R}(\mathrm{LNE}_{k,n}) = ?$$

1st trial: run the inner-product protocol on every (x_i,y_i)

each $x_i \neq y_i$ is missed with probability $1/3$

$$\Pr[\text{ miss one of } x_i \neq y_i] = 1 - (2/3)^k$$

2nd trial: run the protocol on every (x_i,y_i) for $\Theta(\log k)$ times

every $x_i \neq y_i$ is missed with probability $<1/3k$

cost = $O(k \log k)$

3ird trial: make every $x_i \neq y_i$ missed with probability $<1/3k$

and every (x_i,y_i) repeated for $O(1)$ times on average!

List-Non-Equality problem:

$$\mathrm{LNE}_{k,n}(\vec{x},\vec{y}) = \bigwedge_i x_i \neq y_i \qquad X = Y = \{0,1\}^n$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$

$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

> for i=1 to k
> repeat the IP protocol on (x_i,y_i) until detecting $x_i \neq y_i$;
> break and return 0 at any time if overall repetitions $> Ck$;
> return 1;

communication complexity: $O(Ck)$

$\exists i, x_i = y_i$ ⇨ always correct

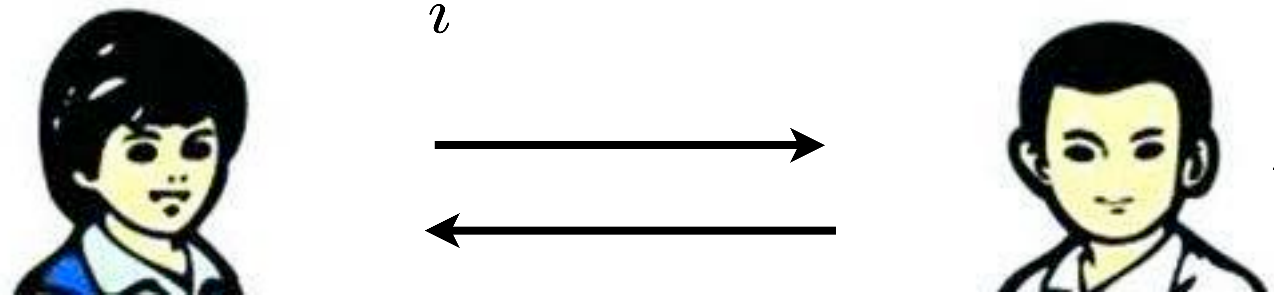
$\forall i, x_i \neq y_i$ ⇨ $(C\text{-}1)k$ failures in Ck independent trials
each trial succeeds with prob. $\geq 1/2$

Chernoff: C=3, exponentially small probability

List-Non-Equality problem:

$$\mathrm{LNE}_{k,n}(\vec{x},\vec{y}) = \bigwedge_i x_i \neq y_i \qquad X = Y = \{0,1\}^n$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$



$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

> for i=1 to k
>   repeat the IP protocol on (x_i,y_i) until detecting $x_i \neq y_i$;
>   break and return 0 at any time if overall repetitions $> 3k$;
> return 1;

communication complexity: $\mathrm{O}(k)$

$\exists i, x_i = y_i$ ⇒ always correct

$\forall i, x_i \neq y_i$ ⇒ incorrect with $\exp(-\Omega(k))$ prob.

⇒ $\mathrm{R}^{\mathrm{Pub}}(\mathrm{LNE}_{k,n}) = O(k)$ ⇒ $\mathrm{R}(\mathrm{LNE}_{k,n}) = O(k + \log n)$

List-Non-Equality problem:

$$\mathrm{LNE}_{k,n}(\vec{x},\vec{y}) = \bigwedge_i x_i \neq y_i \qquad X = Y = \{0,1\}^n$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$

$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

Las Vegas:

> for i=1 to k
>
> repeat for ≤ t times the IP protocol on (x_i, y_i) until detecting $x_i \neq y_i$;
>
> if a (x_i, y_i) has been repeated for t times
>
> Alice sends Bob x_i to see whether $x_i = y_i$
>
> and if so break and return 0;
>
> return 1;

always correct if terminates

the first $x_i = y_i$ ⇨ costs O(t+n) bits

each $x_i \neq y_i$ ⇨ expectedly costs $O\left(\sum_{j=1}^{t} j2^{-j} + n2^{-t}\right)$ =O(1)

when t=n

List-Non-Equality problem:

$$\mathrm{LNE}_{k,n}(\vec{x},\vec{y}) = \bigwedge_i x_i \neq y_i \qquad X = Y = \{0,1\}^n$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$

$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

Las Vegas:

for i=1 to k
    repeat for ≤ t times the IP protocol on (x_i,y_i) until detecting $x_i \neq y_i$;
    if a (x_i,y_i) has been repeated for n times
        Alice sends Bob x_i to see whether $x_i=y_i$
        and if so break and return 0;
return 1;

always correct if terminates

communication cost in expectation: $O(k+n)$

$$\mathrm{R}_0^{\mathrm{Pub}}(\mathrm{LNE}_{k,n}) = O(k+n) \Rightarrow \mathrm{R}_0(\mathrm{LNE}_{k,n}) = O(k+n)$$

List-Non-Equality problem:

$$\mathrm{LNE}_{k,n}(\vec{x},\vec{y}) = \bigwedge_i x_i \neq y_i \qquad X = Y = \{0,1\}^n$$

$\vec{x} = (x_1, \ldots, x_k) \in X^k$

$\vec{y} = (y_1, \ldots, y_k) \in Y^k$

$$\mathrm{LNE}_{k,n} = \wedge^k \overline{\mathrm{EQ}}_n$$

Monte Carlo: $\mathsf{R}(\mathrm{LNE}_{k,n}) = O(k + \log n)$

Las Vegas: $\mathsf{R}_0(\mathrm{LNE}_{k,n}) = O(k + n)$

while: $\mathsf{R}(\overline{\mathrm{EQ}}) = \Theta(\log n)$

$\mathsf{R}_0(\overline{\mathrm{EQ}}) = \Theta(\log n)$

Nondeterministic Protocols

$\mathsf{N}_1(f)$: complexity of optimally certifying positive instances of f

μ is a probability distribution over 1s of f:

μ is a distribution over $\{(x,y) \mid f(x,y) = 1\}$

Definition The *rectangle size bound* of f is

$$B_*(f) := \max_{\mu \text{ over 1s}} \min_{R} \frac{1}{\mu(R)}$$

where R ranges over all 1-monochromatic rectangles.

Theorem

$$\log_2 B_*(f) \leq \mathsf{N}_1(f) \leq \log_2 B_*(f) + \log_2 n$$

$$B_*(f) := \max_{\mu \text{ over 1s}} \min_{R\text{: 1-rect.}} \frac{1}{\mu(R)}$$

Theorem

$$\log_2 B_*(f) \le \mathsf{N}_1(f) \le \log_2 B_*(f) + \log_2 n$$

$$\mathsf{N}_1(f) = \log_2 \mathsf{C}_1(f)$$

$\mathsf{C}_1(f)$: #of monochromatic rectangles to *cover* 1s of f

optimal cover: $\mathcal{C} = \{R_1, R_2, \ldots, R_{\mathsf{C}_1(f)}\}$

for *any* distribution μ over 1s of f:

$$1 \le \sum_{R\in\mathcal{C}} \mu(R) \le \mathsf{C}_1(f) \max_{R\in\mathcal{C}} \mu(R) \Rightarrow \min_{R\in\mathcal{C}} \frac{1}{\mu(R)} \le \mathsf{C}_1(f)$$

$$B_*(f) \le \mathsf{C}_1(f)$$

the other direction:

build up a rectangle cover greedily by always taking the largest rectangle in a uniform μ over *remaining* 1s $\Rightarrow$ $\mathsf{C}_1(f) \le O(nB_*(f))$

$$B_*(f) := \max_{\mu \text{ over 1s}} \min_{R:\text{ 1-rect.}} \frac{1}{\mu(R)}$$

Theorem

$$\log_2 B_*(f) \le \mathsf{N}_1(f) \le \log_2 B_*(f) + \log_2 n$$

$$B_*(f \wedge g) \ge B_*(f) \cdot B_*(g)$$

$$\mathsf{N}_1(\wedge^k f) \ge \log B_*(\wedge^k f) \ge k \log B_*(f)$$

$$\ge k(\mathsf{N}_1(f) - \log n)$$

by symmetry: $\mathsf{N}_0(\vee^k f) \ge k(\mathsf{N}_0(f) - \log n)$

⇨ $\mathsf{N}(f^k) \ge \max(\mathsf{N}_1(\wedge^k f), \mathsf{N}_0(\vee^k f))$

$$\ge k(\mathsf{N}(f) - \log n)$$

$\mathsf{N}(f)$: complexity of optimal nondeterministic protocol for f

$$B_*(f) := \max_{\mu \text{ over 1s}} \min_{R\text{: 1-rect.}} \frac{1}{\mu(R)}$$

$$\boxed{B_*(f \wedge g) \geq B_*(f) \cdot B_*(g)}$$

suppose optimums are achieved by:

$$B_*(f) = \min_R \frac{1}{\mu_f(R)}, B_*(g) = \min_R \frac{1}{\mu_g(R)}$$

⇨ $B_*(f) \leq \frac{1}{\mu_f(R)}, B_*(g) \leq \frac{1}{\mu_g(R)}$ for all 1-rectangles R

Goal: find a distribution μ over 1s of $f \wedge g$ such that

∀1-rectangles R in $f \wedge g$,

$$\mu(R) \leq \mu_f(R_f)\mu(R_g)$$

for some 1-rectangles R_f in f and R_g in g

⇨ $B_*(f \wedge g) \geq \frac{1}{\mu(R)} \geq \frac{1}{\mu(R_f)\mu(R_g)} \geq B_*(f) \cdot B_*(g)$

given μ_f over 1s of f, and μ_g over 1s of g

Goal: find a distribution μ over 1s of $f \wedge g$ such that

$\forall$ 1-rectangles R in $f \wedge g$, $\mu(R) \leq \mu_f(R_f)\mu(R_g)$

for some 1-rectangles R_f in f and R_g in g

define μ over inputs of $f \wedge g$ as:

$$\mu((x_f, x_g), (y_f, y_g)) = \mu_f(x_f, y_f)\mu_g(x_g, y_g)$$

⇨ μ is a distribution over 1s of $f \wedge g$

$\forall$ 1-rectangle R in $f \wedge g$, projections $\begin{cases} R_f = \{(x_f, y_f) \mid ((x_f, *), (y_f, *)) \in R\} \\ R_g = \{(x_g, y_g) \mid ((*, x_g), (*, y_g)) \in R\} \end{cases}$

are 1-rectangles in f and g (because of $\wedge$)

$$R_f \times R_g = \{((x_f, x_g), (y_f, y_g)) \mid ((x_f, y_f) \in R_f, (x_g, y_g) \in R_g\}$$

is a 1-rectangle in $f \wedge g$ and $R \subseteq R_f \times R_g$

⇨ $\mu(R) \leq \mu(R_f \times R_g) \leq \mu(R_f) \cdot \mu(R_g)$

$$B_*(f) := \max_{\mu \text{ over 1s}} \min_{R\text{: 1-rect.}} \frac{1}{\mu(R)}$$

$$B_*(f \wedge g) \geq B_*(f) \cdot B_*(g)$$

key property in the proof:

given μ_f over 1s of f, and μ_g over 1s of g

find a distribution μ over 1s of $f \wedge g$ such that

$\forall$ 1-rectangles R in $f \wedge g$, $\mu(R) \leq \mu_f(R_f)\mu(R_g)$

for some 1-rectangles R_f in f and R_g in g

consequence:

$$\mathsf{N}(f^k) \geq k(\mathsf{N}(f) - \log n)$$

Deterministic Protocols

$\mathsf{D}(f)$: complexity of optimal deterministic protocol for f

$$\mathsf{CC}^{\mathsf{D}}(f^k) \quad \text{vs.} \quad k \cdot \mathsf{CC}^{\mathsf{D}}(f)$$

Theorem: $\mathsf{D}(f) \leq O(\mathsf{N}(f)^2)$

$$\Rightarrow \quad \mathsf{D}(f^k) \geq \mathsf{N}(f^k) \geq k(\mathsf{N}(f) - \log n)$$
$$\geq \Omega\left(k\left(\sqrt{\mathsf{D}(f)} - \log n\right)\right)$$

$$\text{rank}(f \wedge g) = \text{rank}(f)\text{rank}(g)$$

communication matrix:

$$M_{f \wedge g} = M_f \otimes M_g$$

Kronecker product

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & \cdots & a_{mn}\mathbf{B} \end{bmatrix}$$

$$\mathbf{A} \otimes \mathbf{B}((i,k),(j,l)) = a_{ij}b_{kl}$$

$$\text{rank}(\mathbf{A} \otimes \mathbf{B}) = \text{rank}(\mathbf{A})\text{rank}(\mathbf{B})$$

$$\text{rank}(f \wedge g) = \text{rank}(f)\text{rank}(g)$$

$\mathrm{LNE}_{k,n}(\vec{x},\vec{y}) = \bigwedge_i x_i \neq y_i$ so $\mathrm{LNE}_{k,n} = \wedge^k \overline{\mathrm{EQ}}$

⇨ $\text{rank}(\mathrm{LNE}_{k,n}) = \text{rank}(\overline{\mathrm{EQ}})^k = (2^n)^k$

⇨ $\mathrm{D}(\mathrm{LNE}_{k,n}) \geq \log \text{rank}(\mathrm{LNE}_{k,n}) = kn$ $=n^2$

recall:

$\mathrm{R}(\mathrm{LNE}_{k,n}) = O(k + \log n)$ (1-sided error with false negative)

$\mathrm{R}_0(\mathrm{LNE}_{k,n}) = O(k + n)$ $=O(n)$

$\mathrm{N}_1(\mathrm{LNE}_{k,n}) \leq \mathrm{R}(\mathrm{LNE}_{k,n}) = O(k + \log n)$

$\mathrm{N}_0(\mathrm{LNE}_{k,n}) \leq O(\log k + n)$ (Alice sends (i, x_i) with $x_i=y_i$ to Bob)

when $k=n$ $\quad \mathrm{N}(\mathrm{LNE}_{k,n}) = O(n)$

$$\mathsf{rank}(f \wedge g) = \mathsf{rank}(f)\mathsf{rank}(g)$$

there is a function (LNE) such that

$$\mathsf{D}(f) = \Omega(\mathsf{N}_0(f)\mathsf{N}_1(f))$$

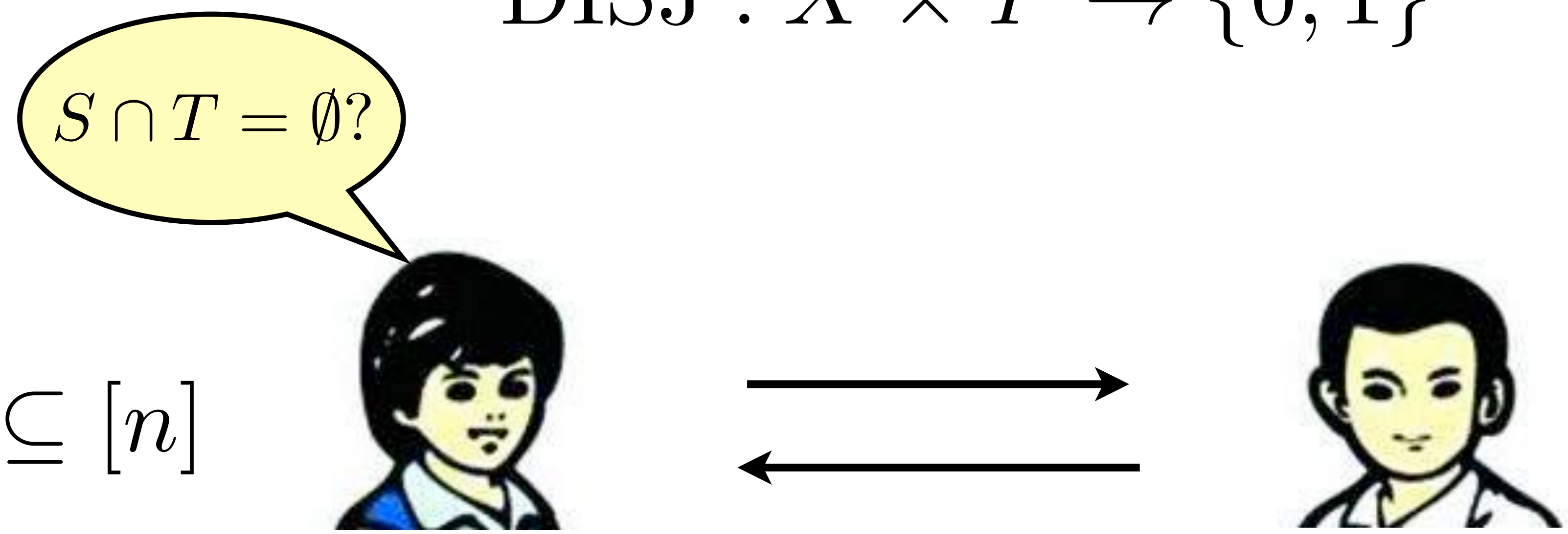
$$\mathsf{D}(f) = \Omega(\mathsf{R}_0(f)^2)$$

(both achieve largest possible gaps)

Disjointness

$$\mathrm{DISJ} : X \times Y \to \{0, 1\}$$

$S \subseteq [n]$



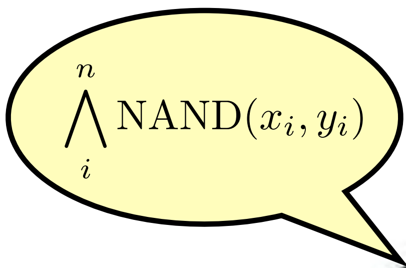
$T \subseteq [n]$

$$X = Y = 2^{[n]}$$

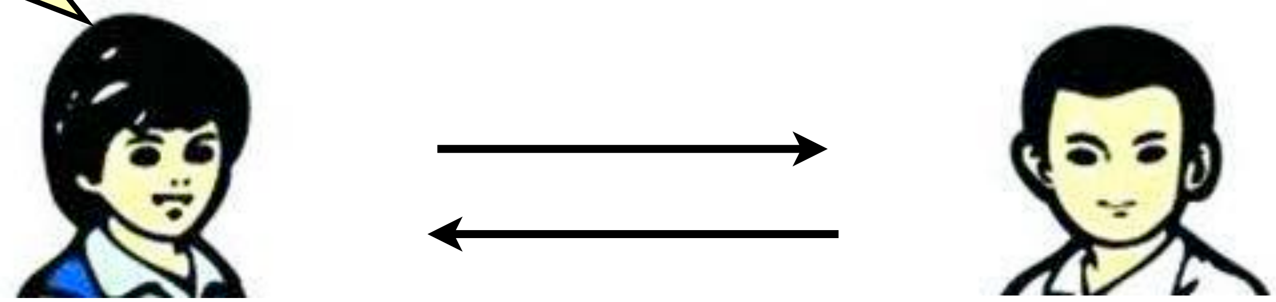
$$\mathrm{DISJ}(S, T) = \begin{cases} 1 & \text{if } S \cap T = \emptyset \\ 0 & \text{otherwise} \end{cases}$$

Disjointness

$$\mathrm{DISJ} : X \times Y \to \{0,1\}$$



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



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

$$X = Y = \{0,1\}^n$$

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

$$\mathrm{DISJ}(x,y) = \bigwedge_{i=1}^{n} \bar{x}_i \vee \bar{y}_i = \bigwedge_{i}^{n} \mathrm{NAND}(x_i, y_i)$$

$\mathsf{D}(\mathrm{DISJ}) = \Omega(n)$ by fooling set

Theorem: [Kalyanasundaram, Schnitger'92] [Razborov'92] [Bar-Yossef, Jayram, Kumar, Sivakumar'02]

$$\mathsf{R}(\mathrm{DISJ}) = \Omega(n)$$

Theorem: [Babai, Frankl, Simon'02]

The deterministic communication complexity on distributional inputs:

$$\mathsf{D}_\mu(\mathrm{DISJ}) = O(\sqrt{n} \log n)$$

for all product distributions μ.

$\mathsf{D}(\mathrm{DISJ}) = \Omega(n)$ by fooling set

Theorem: [Kalyanasundaram, Schnitger'92] [Razborov'92] [Bar-Yossef, Jayram, Kumar, Sivakumar'02]

$$\mathsf{R}(\mathrm{DISJ}) = \Omega(n)$$

idea:

$$\mathsf{R}(\mathrm{DISJ}) = \mathsf{R}(\wedge^n \mathrm{NAND})$$
$$\geq \Omega(n)\mathsf{R}(\mathrm{NAND})?$$

[Bar-Yossef, Jayram, Kumar, Sivakumar'02]

$$\mathsf{R}(\mathrm{DISJ}) \geq \mathsf{IC}_\mu(\mathrm{DISJ}) = \mathsf{IC}_\mu(\wedge^n \mathrm{NAND})$$
$$\geq \Omega(n)\mathsf{IC}_\mu(\mathrm{NAND})$$

Information Theory

entropy:

$$H(X) = \sum_x P(x) \log \frac{1}{P(x)}$$

conditional entropy:

$$H(X \mid Y) = \sum_y P(y) H(X \mid Y = y)$$

mutual information:

$$I(X;Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X)$$

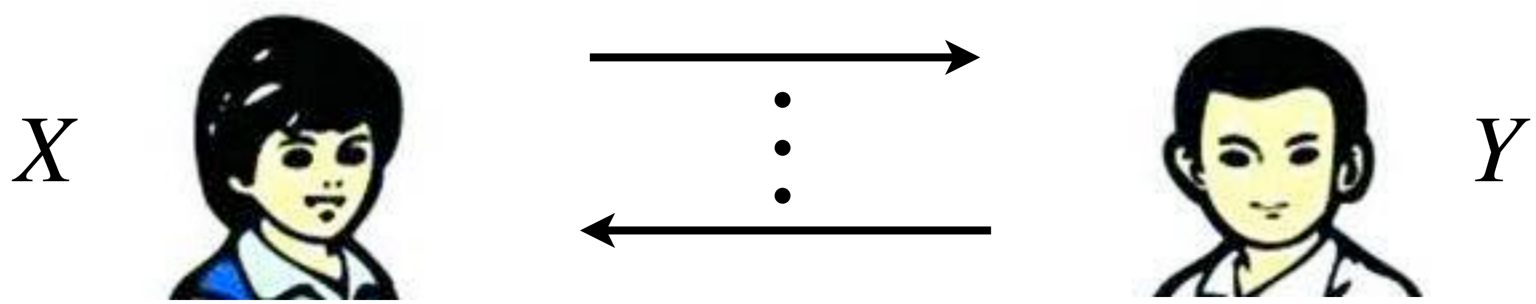
conditional mutual information:

$$I(X;Y \mid Z) = H(X \mid Z) - H(X \mid YZ)$$

$$= I(X;YZ) - I(X;Z)$$

private-coin randomized protocol π :

(X,Y) is sampled according to μ



communication transcript $\Pi = \Pi(X, Y, r_{\mathrm{A}}, r_{\mathrm{B}})$

mutual info: $I(XY;\Pi) = H(XY) - H(XY \mid \Pi)$

the amount of info. about inputs one can get
by seeing the contents of communications

Definition

The (*external*) information cost of a protocol π is

$$\mathsf{IC}_\mu(\pi) = \mathsf{IC}_\mu^{\mathsf{ext}}(\pi) = I(XY;\Pi)$$

Definition: The information complexity of f is

$$\mathsf{IC}_\mu(f) = \inf_\pi \mathsf{IC}_\mu(\pi)$$

where π ranges over all private-coin randomized protocols for f with bounded-error on *all* inputs

$\mathsf{IC}_\mu(f)$ optimizes over the same protocols as $\mathsf{R}(f)$

input distribution μ is only used to generate Π

X ranges over s values $\Rightarrow$ $0 \leq H(X) \leq \log s$

subadditivity:

$$H(X,Y) \leq H(X) + H(Y)$$

equality is achieved if and only if X, Y are independent

$$H(X,Y \mid Z) \leq H(X \mid Z) + H(Y \mid Z)$$

equality is achieved if and only if X, Y are conditionally independent given Z

data processing inequality:

if X, Z are conditionally independent given Y

$$I(X;Y \mid Z) \leq I(X;Y)$$

$$\mathsf{IC}_\mu(f) = \inf_\pi I(XY;\Pi)$$

where π ranges over all private-coin randomized protocols for f with bounded-error on *all* inputs

$$\forall \mu, \mathsf{R}(f) \geq \mathsf{IC}_\mu(f)$$

π : optimal private-coin protocol for f

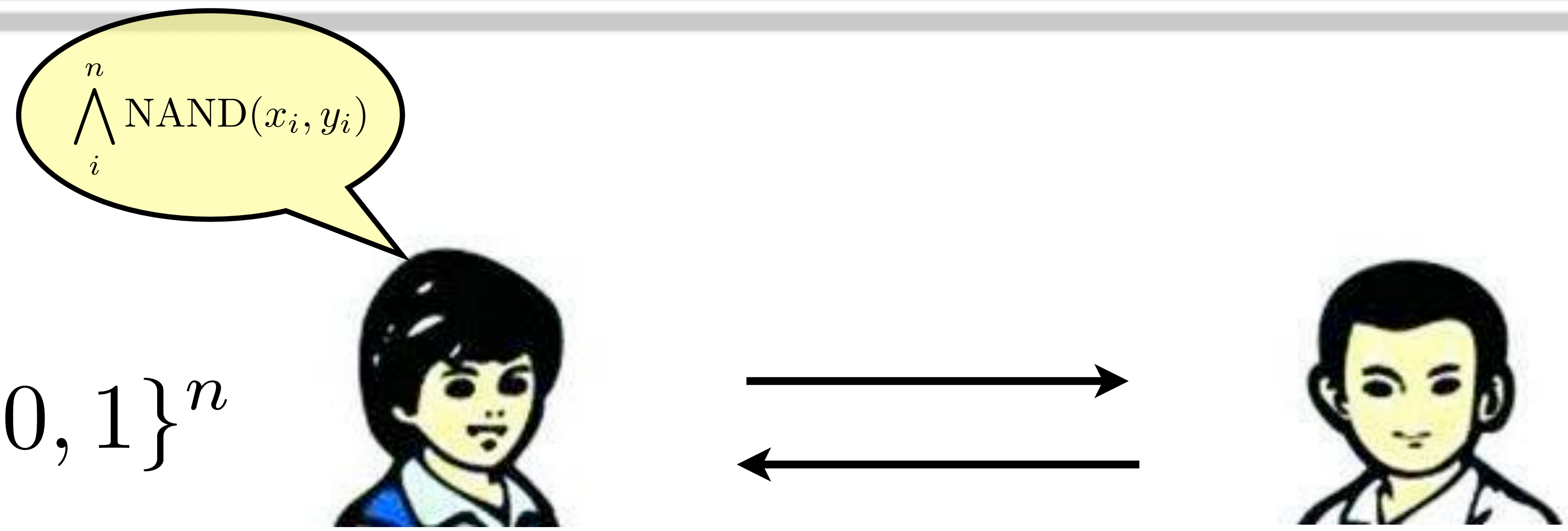
$$\mathsf{R}(f) = \mathsf{CC}(\pi) \geq H(\Pi) \geq I(XY;\Pi) \geq \mathsf{IC}_\mu(f)$$

X ranges over s values ⇨ $0 \leq H(X) \leq \log s$

$$Z = (Z_1, \ldots, Z_n) \text{ are mutually independent}$$

$$\Rightarrow \quad I(Z;\Pi) \geq I(Z_1;\Pi) + \cdots I(Z_n;\Pi)$$

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



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

each (X_i,Y_i) is distributed *independently* according to μ :

$$\Pr[(x_i, y_i) = (0,0)] = \frac{1}{2}$$

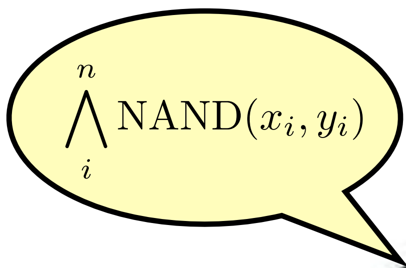
$$\Pr[(x_i, y_i) = (0,1)] = \Pr[(x_i, y_i) = (1,0)] = \frac{1}{4}$$

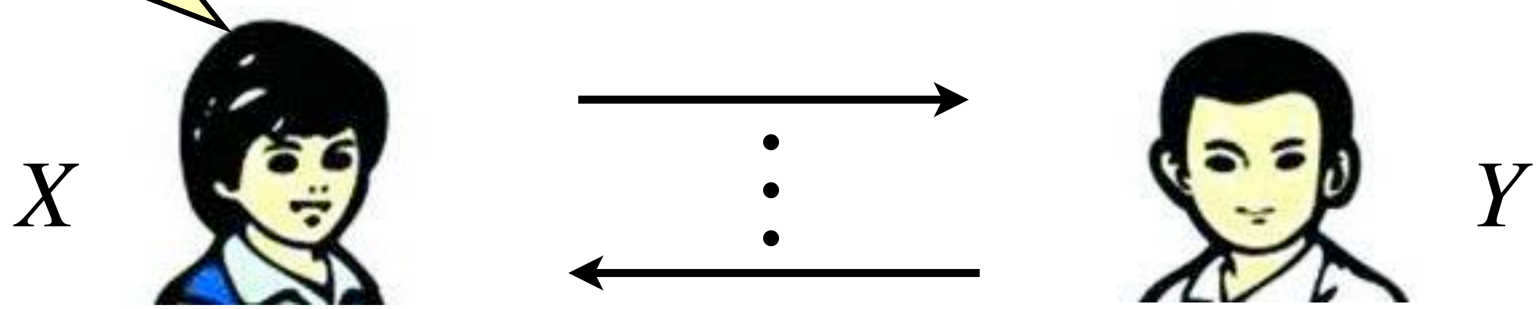
(X,Y) follows the product distribution μ^n

$$I(XY;\Pi) \geq \sum_{i=1}^{n} I(X_iY_i;\Pi)$$

π : optimal private-coin protocol for DISJ

comm. transcript $\Pi = \Pi(X, Y, r_A, r_B)$





each (X_i,Y_i) is distributed *independently* according to μ :

$$\Pr[(x_i, y_i) = (0,0)] = \tfrac{1}{2}$$

$$\Pr[(x_i, y_i) = (0,1)] = \Pr[(x_i, y_i) = (1,0)] = \tfrac{1}{4}$$

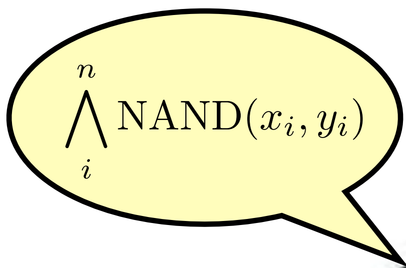
(X,Y) follows the product distribution μ^n

all possible inputs have $\mathrm{DISJ}(X,Y)=1$ (Is this a problem?)

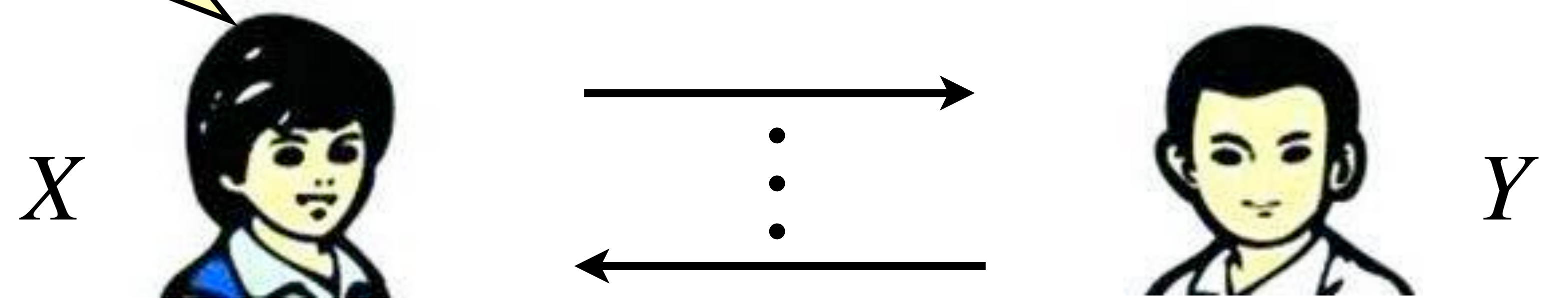
subadditivity *data processing*

$$I(XY;\Pi) \geq \sum_{i=1}^{n} I(X_iY_i;\Pi) \geq \sum_{i=1}^{n} I(X_iY_i;\Pi \mid \mathbf{D})$$

π : optimal private-coin protocol for DISJ



comm. transcript $\Pi=\Pi(X, Y, r_A, r_B)$



each (X_i,Y_i) is distributed *independently* according to μ :

sample uniform "switches" $D_i \in \{0,1\}$
$\mathbf{D} = (D_1, \ldots, D_n)$

if $D_i=0$ ⇨ $\begin{cases} X_i \in \{0,1\} \text{ uniformly random} \\ Y_i = 0 \end{cases}$

if $D_i=1$ ⇨ $\begin{cases} X_i = 0 \\ Y_i \in \{0,1\} \text{ uniformly random} \end{cases}$

X_i,Y_i are conditionally independent given D_i!

$$I(X_iY_i;\Pi \mid \mathbf{D}) \geq \mathsf{IC}_\mu(\mathrm{NAND} \mid D_i)$$

sample uniform "switches" $D_i \in \{0,1\}$

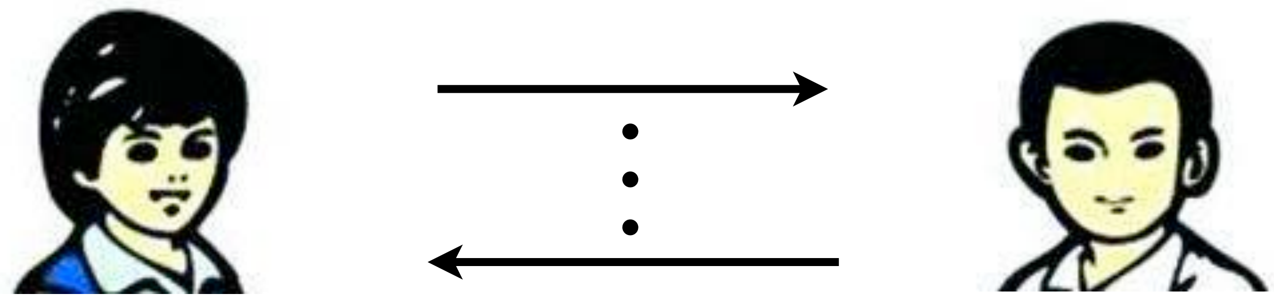
$\mathbf{D} = (D_1, \ldots, D_n)$

if $D_i=0$ ⇨ $\begin{cases} X_i \in \{0,1\} \text{ uniformly random} \\ Y_i = 0 \end{cases}$

if $D_i=1$ ⇨ $\begin{cases} X_i = 0 \\ Y_i \in \{0,1\} \text{ uniformly random} \end{cases}$

A NAND(A,B) B

X_2 ⋮ X_n Y_2 ⋮ Y_n



for i=1 :

$$I(X_iY_i;\Pi \mid \mathbf{D}) = \mathbb{E}_{d_2,\ldots d_n}[I(X_iY_i;\Pi \mid D_1, D_2=d_2,\ldots,D_n=d_n)]$$

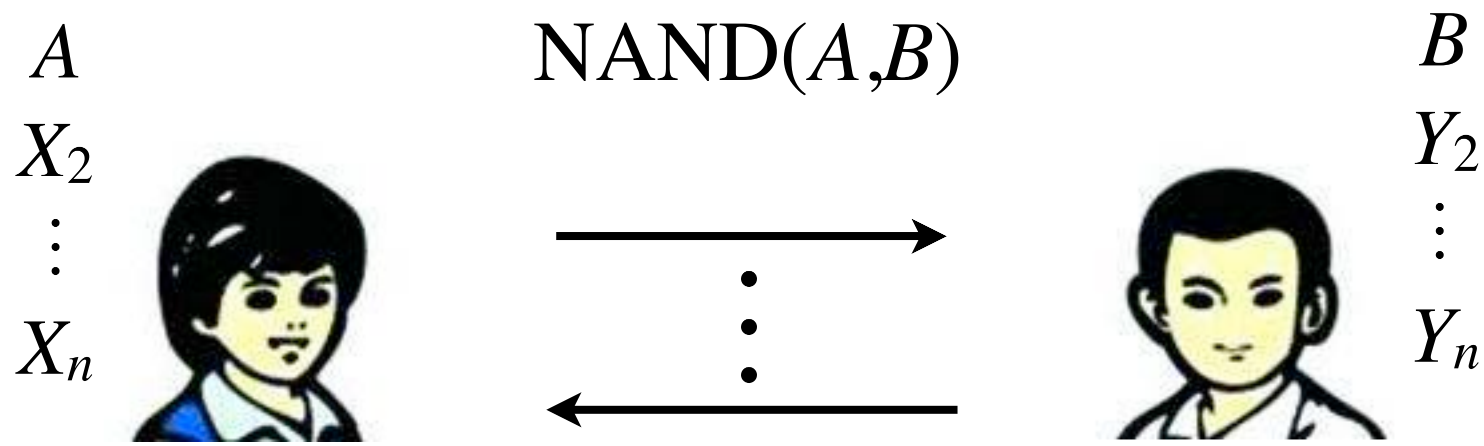
fix any particular $D_2 = d_2, \ldots, D_n = d_n$ X_i,Y_i are independent for i>1

Alice and Bob can sample X_i,Y_i with *private* coins

so that NAND(A,B) is solved by $\Pi(AX_2 \ldots X_n, BY_2 \ldots Y_n)$

⇨ $I(X_1Y_1;\Pi \mid D_1, D_2=d_2,\ldots,D_n=d_n) \geq \mathsf{IC}_\mu(\mathrm{NAND} \mid D_1)$

$$I(X_iY_i;\Pi \mid \mathbf{D}) \geq \mathsf{IC}_\mu(\mathrm{NAND} \mid D_i)$$



for i=1 :

$$I(X_iY_i;\Pi \mid D) = \mathbb{E}_{d_2,\ldots d_n}[I(X_iY_i;\Pi \mid D_1, D_2 = d_2, \ldots, D_n = d_n)]$$

fix any particular $D_2 = d_2, \ldots, D_n = d_n$ X_i,Y_i are independent for i>1

Alice and Bob can sample X_i,Y_i with *private* coins

so that NAND(A,B) is solved by $\Pi(AX_2 \ldots X_n, BY_2 \ldots Y_n)$

this gives a private-coin protocol θ for NAND

with bounded error on all inputs such that

$$I(AB;\Theta \mid D_1) = I(X_1Y_1;\Pi \mid D_1, D_2 = d_2, \ldots, D_n = d_n)$$

$$\Rightarrow \quad I(X_iY_i;\Pi \mid D_1, D_2 = d_2, \ldots, D_n = d_n) \geq \mathsf{IC}_\mu(\mathrm{NAND} \mid D_1)$$

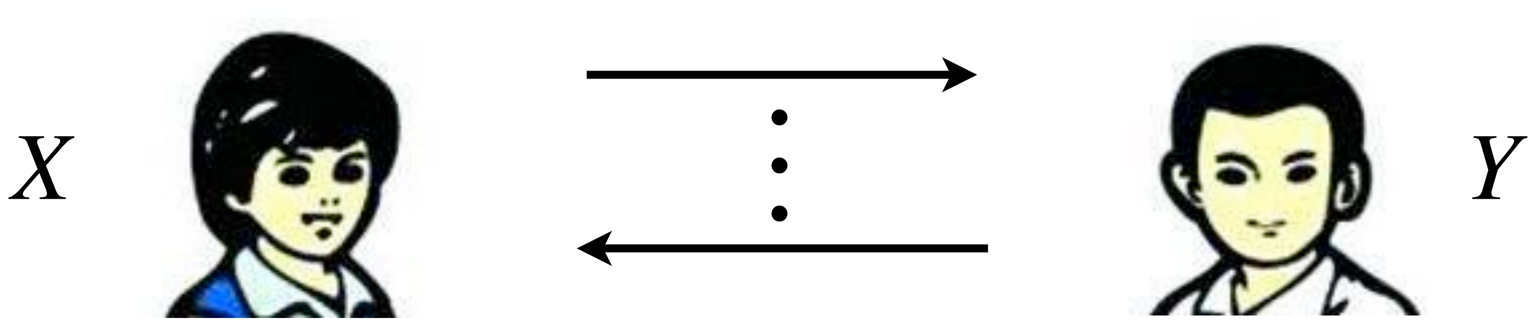
$$\mathsf{R}(f) \geq \mathsf{IC}_\mu(f)$$

$$I(XY;\Pi) \geq \sum_{i=1}^{n} I(X_iY_i;\Pi) \geq \sum_{i=1}^{n} I(X_iY_i;\Pi \mid \mathbf{D})$$

$$I(X_iY_i;\Pi \mid \mathbf{D}) \geq \mathsf{IC}_\mu(\mathrm{NAND} \mid D_i)$$

$\mathsf{R}(\mathrm{DISJ}) \geq \mathsf{IC}_\mu(\mathrm{DISJ}) = I(XY;\Pi) \geq n \cdot \mathsf{IC}_\mu(\mathrm{NAND} \mid D_i)$

(X,Y) is sampled according to μ



comm. transcript $\Pi = \Pi(X, Y, r_A, r_B)$

$$\mathsf{R}(\mathrm{DISJ}) \geq n \cdot \mathsf{IC}_{\mu}(\mathrm{NAND} \mid D)$$

Goal:

$$\boxed{\mathsf{IC}_{\mu}(\mathrm{NAND} \mid D) = \Omega(1)}$$

NAND(A,B) $\Pi = \Pi(A, B, r_{\mathrm{A}}, r_{\mathrm{B}})$

A  $\longrightarrow$ ⋮ $\longleftarrow$  B

sample uniform "switches" $D \in \{0,1\}$

if D=0 ⇒ $\begin{cases} A \in \{0,1\} \text{ uniformly random} \\ B = 0 \end{cases}$

if D=1 ⇒ $\begin{cases} A = 0 \\ B \in \{0,1\} \text{ uniformly random} \end{cases}$

$$\mathsf{IC}_{\mu}(\mathrm{NAND} \mid D) = I(AB; \Pi \mid D)$$

$$= \tfrac{1}{2} I(AB; \Pi \mid D = 0) + \tfrac{1}{2} I(AB; \Pi \mid D = 1)$$

$$= \tfrac{1}{2} I(A; \Pi(A, 0)) + \tfrac{1}{2} I(B; \Pi(0, B)) \quad \geq ?$$

$$\frac{1}{2}I(A;\Pi(A,0)) + \frac{1}{2}I(B;\Pi(0,B))$$

treat random variables $\Pi(0,0), \Pi(0,1), \Pi(1,0)$ as vectors $\pi_{0,0}, \pi_{0,1}, \pi_{1,0}$ where $\pi_{a,b}(x) = \Pr[\Pi(a,b) = x]$

Definition: Hellinger Distance between two probability distributions $P=\{p_x\}$, $Q=\{q_x\}$:

$$h(P,Q) = \frac{1}{\sqrt{2}}\left\|\sqrt{P} - \sqrt{Q}\right\|_2 = \sqrt{\frac{1}{2}\sum_x(\sqrt{p_x} - \sqrt{q_x})^2}$$

1. relation to *mutual information*:

$$I(A;\Pi(A,0)) \geq h^2(\Pi(0,0),\Pi(1,0))$$
$$I(B;\Pi(0,B)) \geq h^2(\Pi(0,0),\Pi(0,1))$$

2. relation to *total variation distance*:

$$\frac{1}{2}\|P - Q\|_1 \leq \sqrt{2}h(P,Q)$$

3. cut-and-paste:

$$h(\Pi(a,b),\Pi(c,d)) = h(\Pi(a,d),\Pi(c,b))$$

Definition: Hellinger Distance between two probability distributions $P=\{p_x\}, Q=\{q_x\}$:

$$h(P,Q) = \frac{1}{\sqrt{2}} \left\| \sqrt{P} - \sqrt{Q} \right\|_2 = \sqrt{\frac{1}{2} \sum_x (\sqrt{p_x} - \sqrt{q_x})^2}$$

1. relation to *mutual information*:

$$I(A;\Pi(A,0)) \geq h^2(\Pi(0,0),\Pi(1,0))$$
$$I(B;\Pi(0,B)) \geq h^2(\Pi(0,0),\Pi(0,1))$$

Kullback-Leibler divergence: $D_{\mathrm{KL}}(P\|Q) = \sum_x p_x \log \frac{p_x}{q_x}$

Jensen-Shannon distance: $r = \frac{1}{2}(P+Q)$

$$\mathsf{JS}(P,Q) = \frac{1}{2}(D_{\mathrm{KL}}(P\|r) + D_{\mathrm{KL}}(Q\|r))$$

- $\mathsf{JS}(P,Q) \geq h^2(P,Q)$
- Π, B are random variables: B is a bit

$$I(B;\Pi) = \mathsf{JS}(\Pi \mid B=0, \Pi \mid B=1)$$

Definition: Hellinger Distance between two probability distributions $P=\{p_x\}$, $Q=\{q_x\}$:

$$h(P,Q)=\frac{1}{\sqrt{2}}\left\|\sqrt{P}-\sqrt{Q}\right\|_2=\sqrt{\frac{1}{2}\sum_x(\sqrt{p_x}-\sqrt{q_x})^2}$$

1. relation to *mutual information*:

$$I(A;\Pi(A,0))\geq h^2(\Pi(0,0),\Pi(1,0))$$
$$I(B;\Pi(0,B))\geq h^2(\Pi(0,0),\Pi(0,1))$$

2. relation to *total variation distance*:

$$\tfrac{1}{2}\|P-Q\|_1\leq\sqrt{2}h(P,Q)$$

3. cut-and-paste:

$$h(\Pi(a,b),\Pi(c,d))=h(\Pi(a,d),\Pi(c,b))$$

Definition: Hellinger Distance between two probability distributions $P=\{p_x\}$, $Q=\{q_x\}$:

$$h(P,Q) = \frac{1}{\sqrt{2}}\left\|\sqrt{P}-\sqrt{Q}\right\|_2 = \sqrt{\frac{1}{2}\sum_x(\sqrt{p_x}-\sqrt{q_x})^2} = 1-\sum_x\sqrt{p_x q_x}$$

3. cut-and-paste:

$$h(\Pi(x,y),\Pi(a,b)) = h(\Pi(x,b),\Pi(a,y))$$

it is enough to prove: $\forall$particular transcript τ

$$\Pr[\Pi(a,b)=\tau]\Pr[\Pi(c,d)=\tau] = \Pr[\Pi(a,d)=\tau]\Pr[\Pi(c,b)=\tau]$$

$\forall$particular transcript τ, $\exists$a “rectangle” $R_\tau = S_\tau \times T_\tau$

where S_τ,T_τ contain (input, random bits) pairs for Alice & Bob

$$\Pr[\Pi(a,b)=\tau] = \Pr[((a,R_A),(b,R_B))\in R_\tau]$$

$$= \Pr[(a,R_A)\in S_\tau,(b,R_B)\in T_\tau]$$

$$= \Pr[(a,R_A)\in S_\tau]\Pr[(b,R_B)\in T_\tau]$$ (private coins)

Definition: Hellinger Distance between two probability distributions $P=\{p_x\}$, $Q=\{q_x\}$:

$$h(P,Q) = \frac{1}{\sqrt{2}} \left\| \sqrt{P} - \sqrt{Q} \right\|_2 = \sqrt{\frac{1}{2}\sum_x (\sqrt{p_x} - \sqrt{q_x})^2}$$

1. relation to *mutual information*:

$$I(A;\Pi(A,0)) \geq h^2(\Pi(0,0),\Pi(1,0))$$
$$I(B;\Pi(0,B)) \geq h^2(\Pi(0,0),\Pi(0,1))$$

2. relation to *total variation distance*:

$$\tfrac{1}{2}\|P-Q\|_1 \leq \sqrt{2}h(P,Q)$$

3. cut-and-paste:

$$h(\Pi(a,b),\Pi(c,d)) = h(\Pi(a,d),\Pi(c,b))$$

$$\tfrac{1}{2}I(A;\Pi(A,0)) + \tfrac{1}{2}I(B;\Pi(0,B))$$

Definition: Hellinger Distance between two probability distributions $P=\{p_x\}$, $Q=\{q_x\}$:

$$h(P,Q) = \frac{1}{\sqrt{2}} \left\| \sqrt{P} - \sqrt{Q} \right\|_2 = \sqrt{\frac{1}{2} \sum_x (\sqrt{p_x} - \sqrt{q_x})^2}$$

$$\tfrac{1}{2} I(A; \Pi(A,0)) + \tfrac{1}{2} I(B; \Pi(0,B))$$

(MI bound) $\geq \frac{1}{2} \left(h^2(\Pi_{0,0}, \Pi_{1,0}) + h^2(\Pi_{0,0}, \Pi_{0,1}) \right)$

(Cauchy-Schwarz) $\geq \frac{1}{4} \left(h(\Pi_{0,0}, \Pi_{1,0}) + h(\Pi_{0,0}, \Pi_{0,1}) \right)^2$

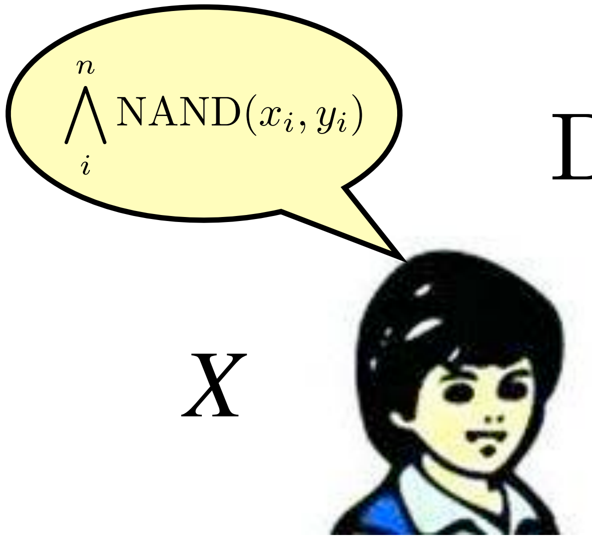
(triangle inequality) $\geq \frac{1}{4} h^2(\Pi(1,0), \Pi(0,1))$

(cut&paste) $\geq \frac{1}{4} h^2(\Pi(0,0), \Pi(1,1))$

(TV bound) $\geq \frac{1}{32} \| \Pi(0,0) - \Pi(1,1) \|_1^2 \geq \Omega(\epsilon^2)$

(soundness of the protocol)

Disjointness



$$\mathrm{DISJ}_n = \wedge^n \mathrm{NAND}$$

transcript Π

X → ← Y

(X_1,Y_1), ..., (X_2,Y_2) i.i.d. according to μ

(X_i,Y_i) conditionally independent given D_i

if D_i=0 ⇒ $\begin{cases} X_i \in \{0,1\} \text{ uniformly random} \\ Y_i = 0 \end{cases}$ if D_i=1 ⇒ $\begin{cases} X_i = 0 \\ Y_i \in \{0,1\} \text{ uniformly random} \end{cases}$

$$\mathsf{R}(\mathrm{DISJ}) \geq \mathsf{IC}_\mu(\mathrm{DISJ}) = I(XY;\Pi) \geq \sum_{i=1}^{n} I(X_iY_i;\Pi \mid \mathbf{D})$$

$$= n \cdot I(AB;\Pi \mid D)$$ for NAND with input $(A,B)\sim\mu$

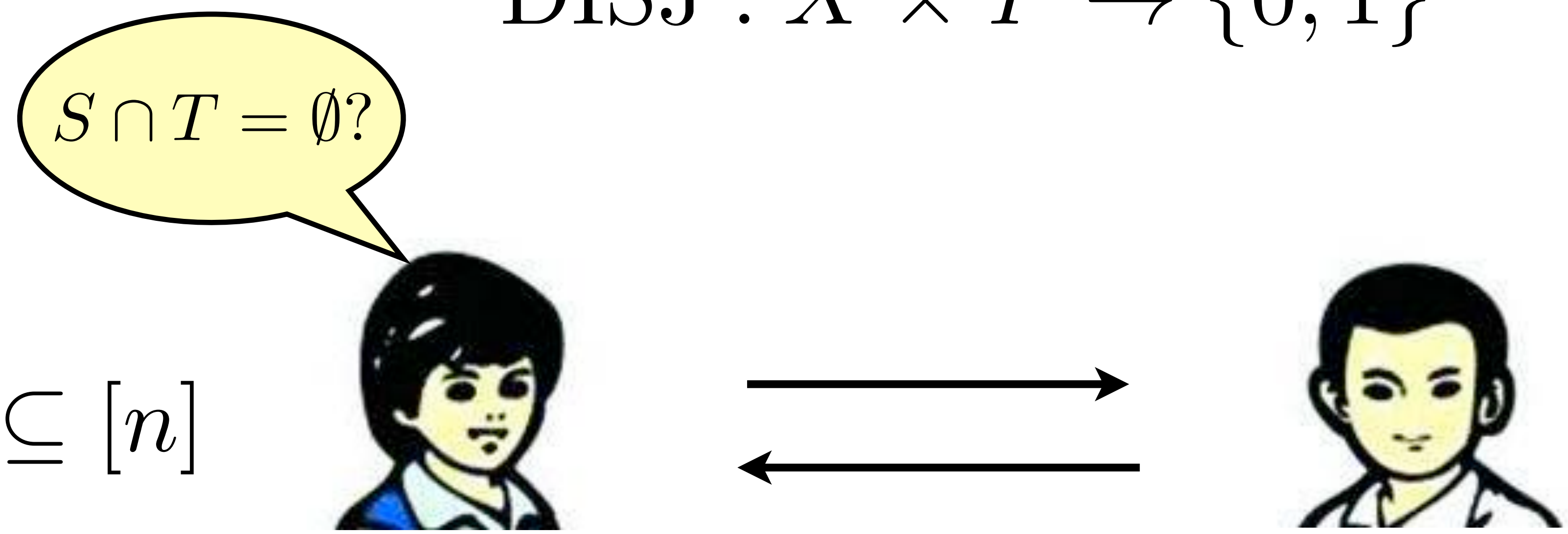
$$= \frac{n}{2}\left(I(A;\Pi(A,0)) + I(B;\Pi(0,B))\right)$$

$$\geq \Omega(\epsilon^2 n)$$

Disjointness

$$\text{DISJ} : X \times Y \to \{0,1\}$$

$S \subseteq [n]$



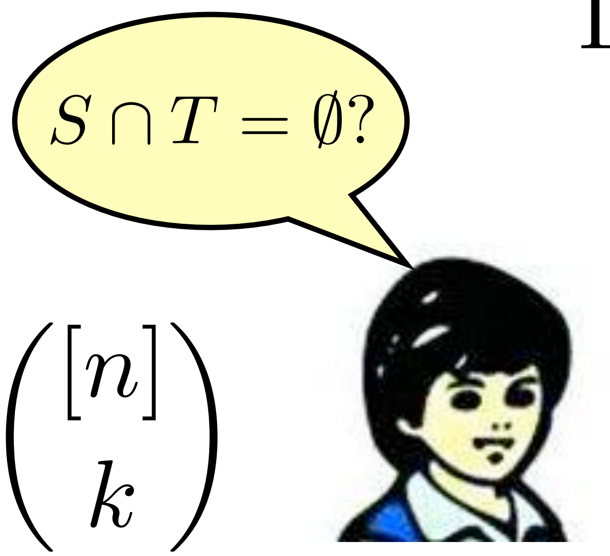
$T \subseteq [n]$

$$X = Y = 2^{[n]}$$

$$\text{DISJ}(S,T) = \begin{cases} 1 & \text{if } S \cap T = \emptyset \\ 0 & \text{otherwise} \end{cases}$$

Disjointness of k-Sets

$$\mathrm{DISJ}_k^n : X \times Y \to \{0,1\}$$



$S \in \binom{[n]}{k}$

$T \in \binom{[n]}{k}$

$$X = Y = \binom{[n]}{k}$$

$$\mathrm{DISJ}_k^n(S,T) = \begin{cases} 1 & \text{if } S \cap T = \emptyset \\ 0 & \text{otherwise} \end{cases}$$

Disjointness of k-Sets

Theorem [Håstad, Wigderson' 07]:

$$\mathsf{R}^{\mathsf{Pub}}(\mathrm{DISJ}_k^n) = O(k)$$

Theorem [Håstad, Wigderson' 07]:

$$\mathsf{R}^{\mathsf{Pub}}(\mathrm{DISJ}_k^n) = O(f(k))$$

"*fixed parameter tractable*"

Theorem [Håstad, Wigderson' 07]:

$$\mathsf{R}^{\mathsf{Pub}}(\mathrm{DISJ}_k^n) = O(f(k))$$

$\exists i, S \subseteq Z_i \wedge T \subseteq \overline{Z}_i?$

$t = f(k)$

$f(k)=O(2^{2k})$

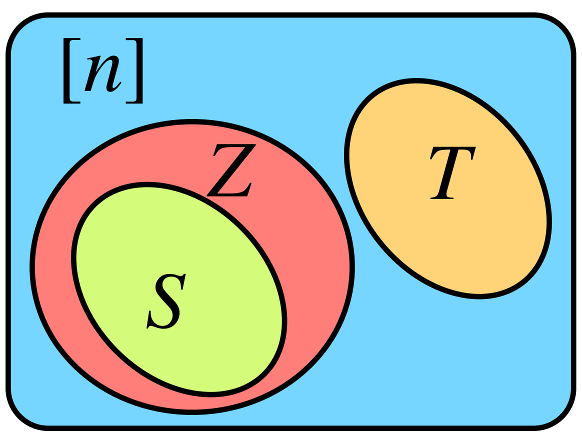
$S \in \binom{[n]}{k}$

$T \subseteq \overline{Z}_i?$ ←

$T \in \binom{[n]}{k}$

public randomness:

uniform independent $Z_1, Z_2, \ldots, Z_t \subseteq [n]$



Observation:

S, T are disjoint if and only if:

$\exists\, Z \subseteq [n]$ such that $S \subseteq Z \wedge T \subseteq \overline{Z}$

S, T intersects ⇨ always correct

S, T disjoint ⇨ $\Pr[S \subseteq Z \wedge T \subseteq \overline{Z}] = 2^{-2k}$

⇨ $\Pr[\forall i, S \not\subseteq Z_i \vee T \not\subseteq \overline{Z}_i] = (1-2^{-2k})^{f(k)}$ <1/3

One phase:

$S \subseteq [n]$

$|S| = s$

$T \subseteq [n]$

$|T| = t$

public randomness:

uniform independent $Z_1, Z_2, \ldots \subseteq [n]$

Assume: $s \leq t$; Alice and Bob both know s and t

> Alice sends the smallest $i \leq 2^{2t}$ that $S \subseteq Z_i$ to Bob;
> if no such Z_i exists then stop and output "*not disjoint*";
> if $|T \cap Z_i| \leq 3t/4$ then $T \leftarrow T \cap Z_i$ and Bob updates $|T|$ to Alice;
> else stop and output "*not disjoint*";

- communication cost in one phase: $O(s+t)$
- the disjointness(non-disjointness) between S, T does not change;
- if S, T are disjoint, new $(s'+t') \leq 7(s+t)/8$ with probability $1\text{-}\exp(-\Omega(t))$.

repeat phases until $s+t=O(1)$, then solve it in $O(2^{2(s+t)})=O(1)$

- overall communication cost: $O\left(\sum_{i\geq 1} k\left(\frac{7}{8}\right)^i\right) = O(k)$
- accumulative error: $\sum_{i\geq 1} \exp(-\Omega(k(\frac{7}{8})^i)) = \exp(-\Omega(1))$

Disjointness of k-Sets

Theorem [Håstad, Wigderson' 07]:

$$\mathsf{R}^{\mathsf{Pub}}(\mathrm{DISJ}_k^n) = O(k)$$

Theorem [Håstad, Wigderson' 07]:

$$\mathsf{R}(\mathrm{DISJ}_k^n) = O(k + \log\log n)$$

Direct Sum

$f : X \times Y \to \{0,1\}$ distribution μ over $X \times Y$

$\mathsf{CC}_\mu(f)$: complexity of optimal protocols (using both public and private coins) for f with bounded error on μ

$\mathsf{CC}_{\mu^k}(f^k)$: bounded *per-instance* error

direct-sum: $\mathsf{CC}_{\mu^k}(f^k) > \Omega(k) \cdot \mathsf{CC}_\mu(f)$?

Theorem (Barak, Braverman, Chen, Rao 2010)

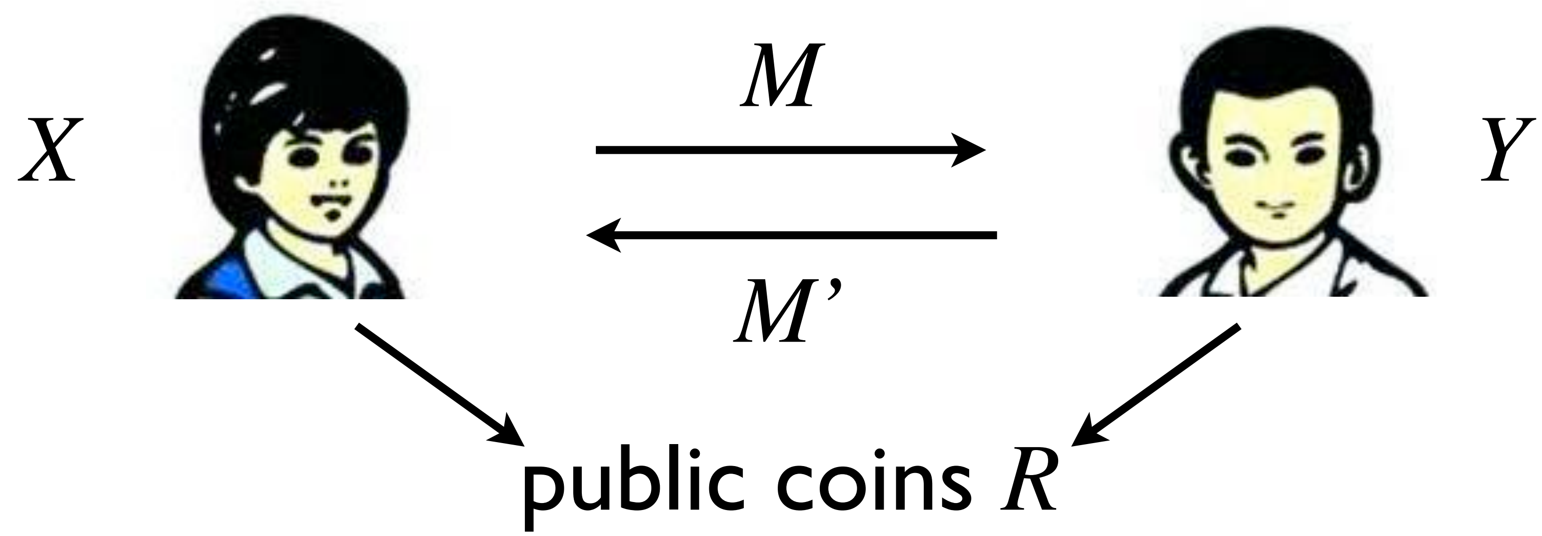
$$\mathsf{CC}_{\mu^k}(f^k) = \widetilde{\Omega}(\sqrt{k} \cdot \mathsf{CC}_\mu(f))$$

and if μ is a product measure

$$\mathsf{CC}_{\mu^k}(f^k) = \widetilde{\Omega}(k \cdot \mathsf{CC}_\mu(f))$$

Compression of Protocols

(X,Y) is sampled according to μ



If there is a N that $|N| \ll |M|$ and N allows Bob to output an N' identically distributed as M'

then N contains the same amount of information as M.

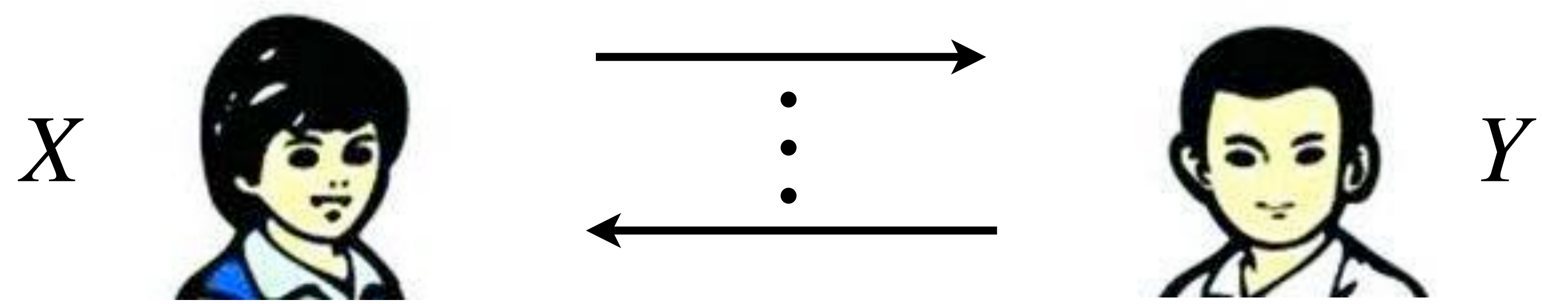
To compress ~~messages~~ protocols to the size of information entropy?

entropy of a message might be $o(1)$

Information Complexity

protocol π :

(X,Y) is sampled according to μ



comm. transcript $\Pi = \Pi(X, Y, R_{\text{pub}}, R_A, R_B)$

(including public coins)

Definition (Chakrabarti, Shi, Wirth, Yao 2001)

The (*internal*) information cost of a protocol π is

$$\mathsf{IC}_\mu(\pi) = I(\Pi; X \mid Y) + I(\Pi; Y \mid X)$$

Information Theory

entropy:

$$H(X) = \sum_{x} P(x) \log \frac{1}{P(x)}$$

conditional entropy:

$$H(X \mid Y) = \sum_{y} P(y) H(X \mid Y = y)$$

mutual information:

$$I(X;Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X)$$

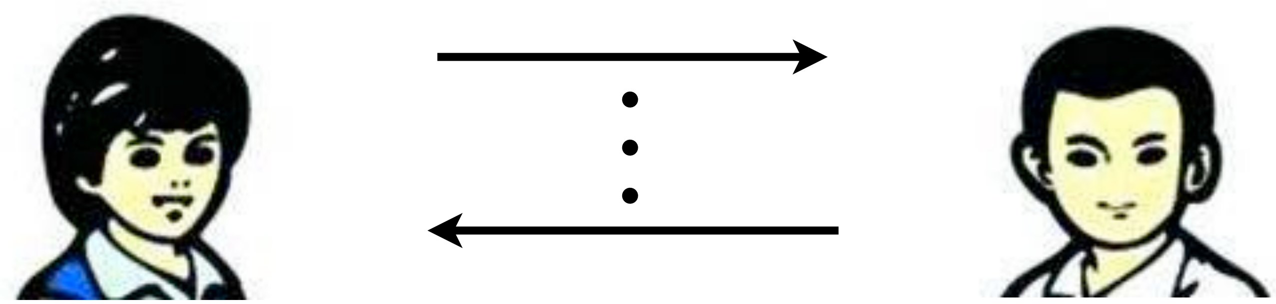
conditional mutual information:

$$\begin{aligned} I(X;Y \mid Z) &= H(X \mid Z) - H(X \mid YZ) \\ &= I(X;YZ) - I(X;Z) \end{aligned}$$

Information Complexity

protocol π :

(X,Y) is sampled according to μ

X  Y

comm. transcript $\Pi = \Pi(X, Y, R_{\text{pub}}, R_A, R_B)$

(including public coins)

Definition (Chakrabarti, Shi, Wirth, Yao 2001)

The (*internal*) information cost of a protocol π is

$$\mathsf{IC}_\mu(\pi) = I(\Pi; X \mid Y) + I(\Pi; Y \mid X)$$

Information Complexity

Definition (Chakrabarti, Shi, Wirth, Yao 2001)

The (*internal*) information cost of a protocol π is

$$\mathsf{IC}_\mu(\pi) = I(\Pi; X \mid Y) + I(\Pi; Y \mid X)$$

how much *additional* info Alice and Bob can learn about each other's inputs by observing the transcript Π

external information cost: $\mathsf{IC}^{\text{ext}}_\mu(\pi) = I(\Pi; XY)$

Definition: The information complexity of f is

$$\mathsf{IC}_\mu(f) = \inf_\pi \mathsf{IC}_\mu(\pi)$$

where π ranges over all bounded-error (on μ) protocols for f

Information Complexity

Definition (Chakrabarti, Shi, Wirth, Yao 2001)

The (*internal*) information cost of a protocol π is

$$\mathsf{IC}_\mu(\pi) = I(\Pi; X \mid Y) + I(\Pi; Y \mid X)$$

Definition: The information complexity of f is

$$\mathsf{IC}_\mu(f) = \inf_\pi \mathsf{IC}_\mu(\pi)$$

where π ranges over all bounded-error (on μ) protocols for f

$\mathsf{CC}_\mu(\pi) \geq \mathsf{IC}_\mu(\pi)$ for any distribution μ and protocol π

Can we transform any π to a τ with $\mathsf{CC}_\mu(\tau) = O(\mathsf{IC}_\mu(\pi))$?

Theorem (Raz 1998, BBCR 2010)

$$\mathsf{IC}_{\mu^k}(f^k) = k \cdot \mathsf{IC}_{\mu}(f)$$

⇨ $\forall$ protocol π for f^k with bounded (per-instance) error on μ^k

$\exists$ protocol θ for f with bounded error on μ such that

$$\mathsf{IC}_{\mu}(\theta) \leq \frac{\mathsf{IC}_{\mu^k}(\pi)}{k}$$

program of Barak-Braverman-Chen-Rao:

$$\mathsf{CC}_{\mu^k}(f^k) = \mathsf{CC}_{\mu^k}(\pi) \geq \mathsf{IC}_{\mu^k}(\pi) \geq k \cdot \mathsf{IC}_{\mu}(\theta)$$

⇨ $$\geq \Omega(k \cdot \mathsf{CC}_{\mu}(\tau)) \geq \Omega(k \cdot \mathsf{CC}_{\mu}(f))$$

Make a wish: protocol θ can be *compressed* to protocol τ with

$$\mathsf{CC}_{\mu}(\tau) = O(\mathsf{IC}_{\mu}(\theta))$$

$\forall$ protocol π for f^k with bounded (per-instance) error on μ^k

$\exists$ protocol θ for f with bounded error on μ such that

$$\mathsf{IC}_\mu(\theta) \leq \frac{\mathsf{IC}_{\mu^k}(\pi)}{k}$$

Theorem (BBCR 2010)

if $\forall$ protocol θ with $\mathsf{IC}_\mu(\theta)=I$ and $\mathsf{CC}_\mu(\theta)=C$, $\exists$ protocol τ with $\mathsf{CC}_\mu(\tau) \leq g(I,C)$ that *simulates* θ, then

$$g\left(\frac{1}{k}\mathsf{CC}_{\mu^k}(f^k), \mathsf{CC}_{\mu^k}(f^k)\right) \geq \mathsf{CC}_\mu(f)$$

Definition: a protocol π is said to *δ-simulate* protocol θ over inputs $(X,Y)\sim\mu$ if there exists a mapping ϕ such that $\| \phi(\Pi)-\Theta \|_1<\delta$ for $\Pi = \Pi(X,Y)$, $\Theta = \Theta(X,Y)$.

$\forall$ protocol π for f^k with bounded (per-instance) error on μ^k

$\exists$ protocol θ for f with bounded error on μ such that

$$\mathsf{IC}_{\mu}(\theta) \leq \frac{\mathsf{IC}_{\mu^k}(\pi)}{k} \quad \text{and} \quad \mathsf{CC}_{\mu}(\theta) \leq \mathsf{CC}_{\mu^k}(\pi)$$

Theorem (BBCR 2010)

if $\forall$ protocol θ with $\mathsf{IC}_\mu(\theta)=I$ and $\mathsf{CC}_\mu(\theta)=C$, $\exists$ protocol τ with $\mathsf{CC}_\mu(\tau)\leq g(I,C)$ that *simulates* θ, then

$$g\left(\frac{1}{k}\mathsf{CC}_{\mu^k}(f^k), \mathsf{CC}_{\mu^k}(f^k)\right) \geq \mathsf{CC}_{\mu}(f)$$

$$\mathsf{CC}_{\mu^k}(f^k) = \mathsf{CC}_{\mu^k}(\pi) \geq \mathsf{IC}_{\mu^k}(\pi) \geq k \cdot \mathsf{IC}_{\mu}(\theta) \Rightarrow \mathsf{IC}_{\mu}(\theta) \leq \frac{1}{k}\mathsf{CC}_{\mu^k}(f^k)$$

$$\mathsf{CC}_{\mu}(\theta) \leq \mathsf{CC}_{\mu^k}(\pi) = \mathsf{CC}_{\mu^k}(f^k)$$

$\Rightarrow$ $\exists$ protocol τ with $\mathsf{CC}_{\mu}(\tau) \leq g\left(\frac{1}{k}\mathsf{CC}_{\mu^k}(f^k), \mathsf{CC}_{\mu^k}(f^k)\right)$

Theorem (BBCR 2010)

if ∀ protocol θ with $\mathsf{IC}_\mu(\theta)=I$ and $\mathsf{CC}_\mu(\theta)=C$, ∃ protocol τ with $\mathsf{CC}_\mu(\tau)\leq g(I,C)$ that *simulates* θ, then

$$g\left(\frac{1}{k}\mathsf{CC}_{\mu^k}(f^k), \mathsf{CC}_{\mu^k}(f^k)\right) \geq \mathsf{CC}_\mu(f)$$

Theorem (BBCR 2010)

Any protocol with IC I and CC C can be simulated by another protocol with CC $\leq g(I,C) = \widetilde{O}(\sqrt{I \cdot C})$.

Theorem (BBCR 2010)

$$\mathsf{CC}_{\mu^k}(f^k) = \widetilde{\Omega}(\sqrt{k} \cdot \mathsf{CC}_\mu(f))$$

Theorem (Raz 1998, BBCR 2010)

$$\mathsf{IC}_{\mu^k}(f^k) = k \cdot \mathsf{IC}_\mu(f)$$

$\leq$ direction: easy by independent repetitions

$\geq$ direction: given protocol π for f^k with (per-instance) error on μ^k

construct protocol θ for f with bounded error on μ: $\mathsf{IC}_\mu(\theta) \leq \frac{\mathsf{IC}_{\mu^k}(\pi)}{k}$

sampled by public coin $\left\{ X_1, \vdots, X_{i\text{-}1} \right.$

X

sampled by private coin $\left\{ X_{i+1}, \vdots, X_k \right.$

$(X, Y) \sim \mu$

$\rightleftarrows$

$\left. Y_1, \vdots, Y_{i\text{-}1} \right\}$ sampled by private coin

Y

$\left. Y_{i+1}, \vdots, Y_k \right\}$ sampled by public coin

$i \in [k]$ is random

sampled via public coins

to ensure: $(\vec{X}, \vec{Y}) \sim \mu^k$

θ: run π on $(\vec{X}, \vec{Y})$

Theorem (Raz 1998, BBCR 2010)

$$\mathsf{IC}_{\mu^k}(f^k) = k \cdot \mathsf{IC}_{\mu}(f)$$

sampled by public coin: $X_1, \ldots, X_{i\text{-}1}$

X

sampled by private coin: $X_{i+1}, \ldots, X_k$

$(X, Y) \sim \mu$

$i \in [k]$ is random sampled via public coins

$Y_1, \ldots, Y_{i\text{-}1}$: sampled by private coin

Y

$Y_{i+1}, \ldots, Y_k$: sampled by public coin

to ensure: $(\vec{X}, \vec{Y}) \sim \mu^k$

θ: run π on $(\vec{X}, \vec{Y})$

$$I(\Theta; X \mid Y) = \sum_{i=1}^{k} \frac{1}{k} I(\Pi; X \mid Y, X_{<i}, Y_{>i}) = \frac{1}{k} \sum_{i=1}^{k} I(\Pi; X_i \mid X_{<i}, Y_{\geq i})$$

(X_i and $Y_{<i}$ are conditionally independent given $X_{<i}Y_{\geq i}$)

$$\leq \frac{1}{k} \sum_{i=1}^{k} I(\Pi; X_i \mid X_{<i}, \mathbf{Y}) = \frac{1}{k} I(\Pi; \mathbf{X} \mid \mathbf{Y})$$

(chain rule)

Theorem (Raz 1998, BBCR 2010)

$$\mathsf{IC}_{\mu^k}(f^k) = k \cdot \mathsf{IC}_\mu(f)$$

$\leq$ direction: easy by independent repetitions

$\geq$ direction: given protocol π for f^k with (per-instance) error on μ^k

construct protocol θ for f with bounded error on μ: $\mathsf{IC}_\mu(\theta) \leq \frac{\mathsf{IC}_{\mu^k}(\pi)}{k}$

$$I(\Theta; X \mid Y) \leq \frac{1}{k} I(\Pi; \mathbf{X} \mid \mathbf{Y}) \qquad I(\Theta; Y \mid X) \leq \frac{1}{k} I(\Pi; \mathbf{Y} \mid \mathbf{X})$$

$$\begin{aligned}\mathsf{IC}_\mu(\theta) &= I(\Theta; X \mid Y) + I(\Theta; Y \mid X) \\ &\leq \frac{1}{k}(I(\Pi; \mathbf{X} \mid \mathbf{Y}) + I(\Pi; \mathbf{Y} \mid \mathbf{X})) \\ &= \frac{\mathsf{IC}_{\mu^k}(\pi)}{k}\end{aligned}$$

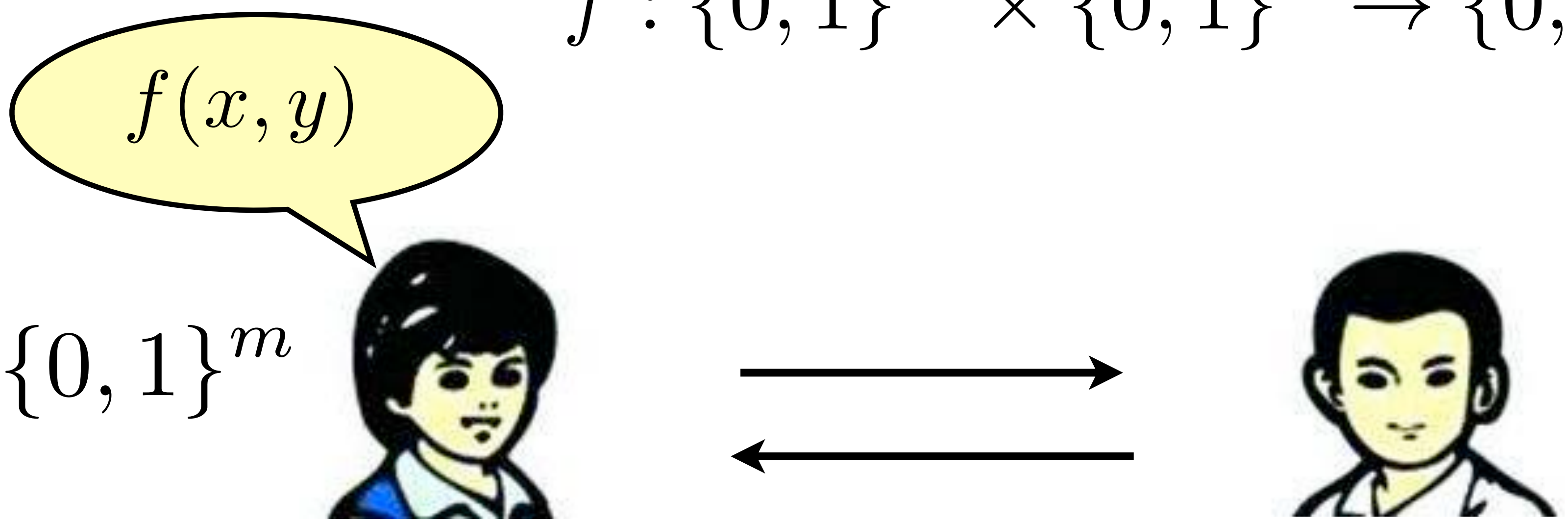
Theorem (Braverman, Rao 2011)
"Information = Amortized Communication"

$$\lim_{k\to\infty} \frac{\mathsf{CC}_{\mu^k}(f^k)}{k} = \mathsf{IC}_\mu(f)$$

Asymmetric Communications

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

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



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

$$\mathsf{D}(f) \leq \min\{m,n\}$$

when $m \ll n$ it is always very cheap to send x to Bob

we want something like this:

> "To successfully solve f, either Alice has to send a total of at least a bits or Bob has to send a total of b bits."

Asymmetric Communications

$f(x,y)$

$f : X \times Y \to \{0,1\}$

$x \in X$ 

a bits total →

← b bits total

 $y \in Y$

[a,b]-protocol: Alice sends a total of ≤a bits
Bob sends a total of ≤b bits

while communications are still interactive and adaptive

Data Structures

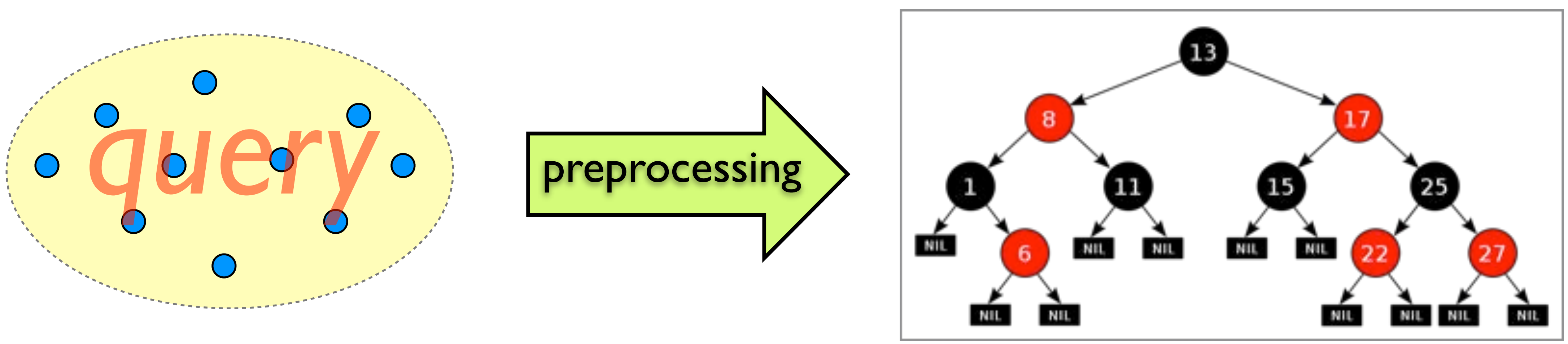
query x

access

database

$$\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in Y$$

data structure



Nearest Neighbor Search
(*NNS*)

metric space (X,dist)

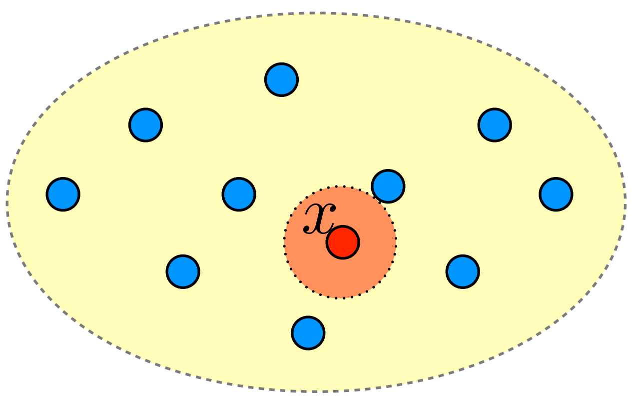
query $x \in X$

access

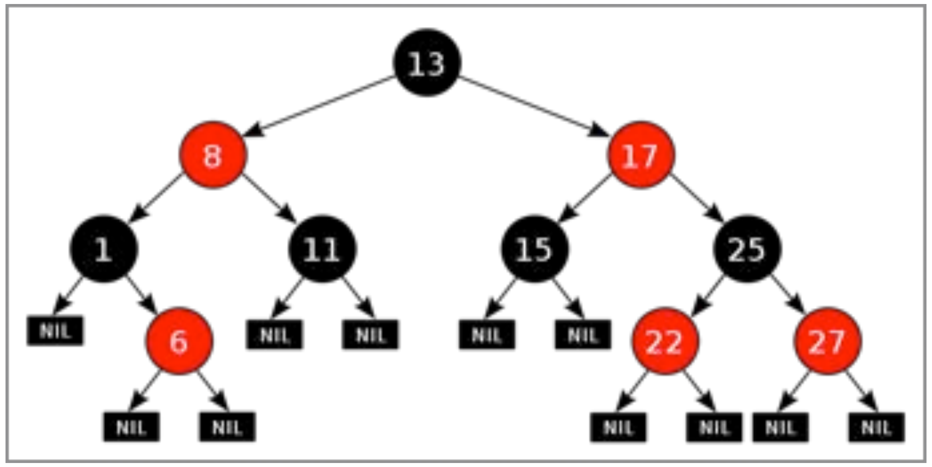
database

$\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in X^n$

data structure



preprocessing



output: the data point y_i that is closest to the query x

applications: *database, pattern matching, machine learning, ...*

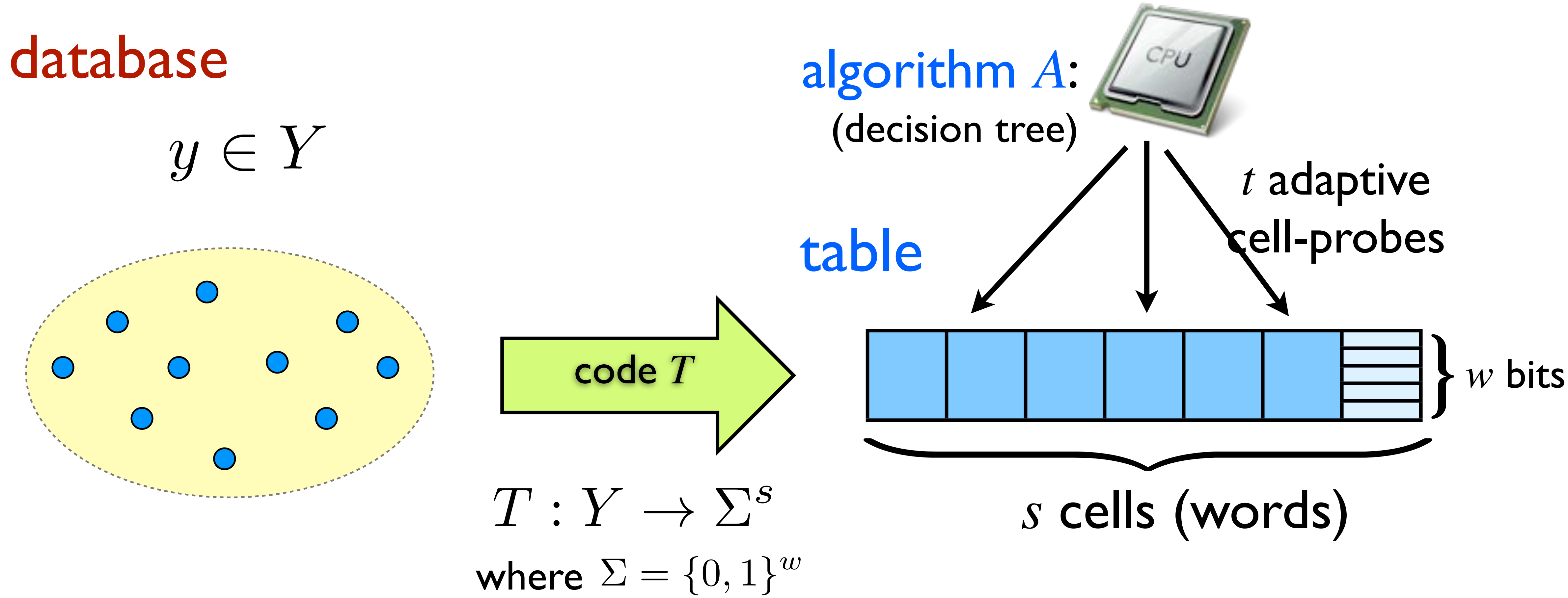
Curse of dimensionality!

Cell-Probe Model

(Yao 1981)

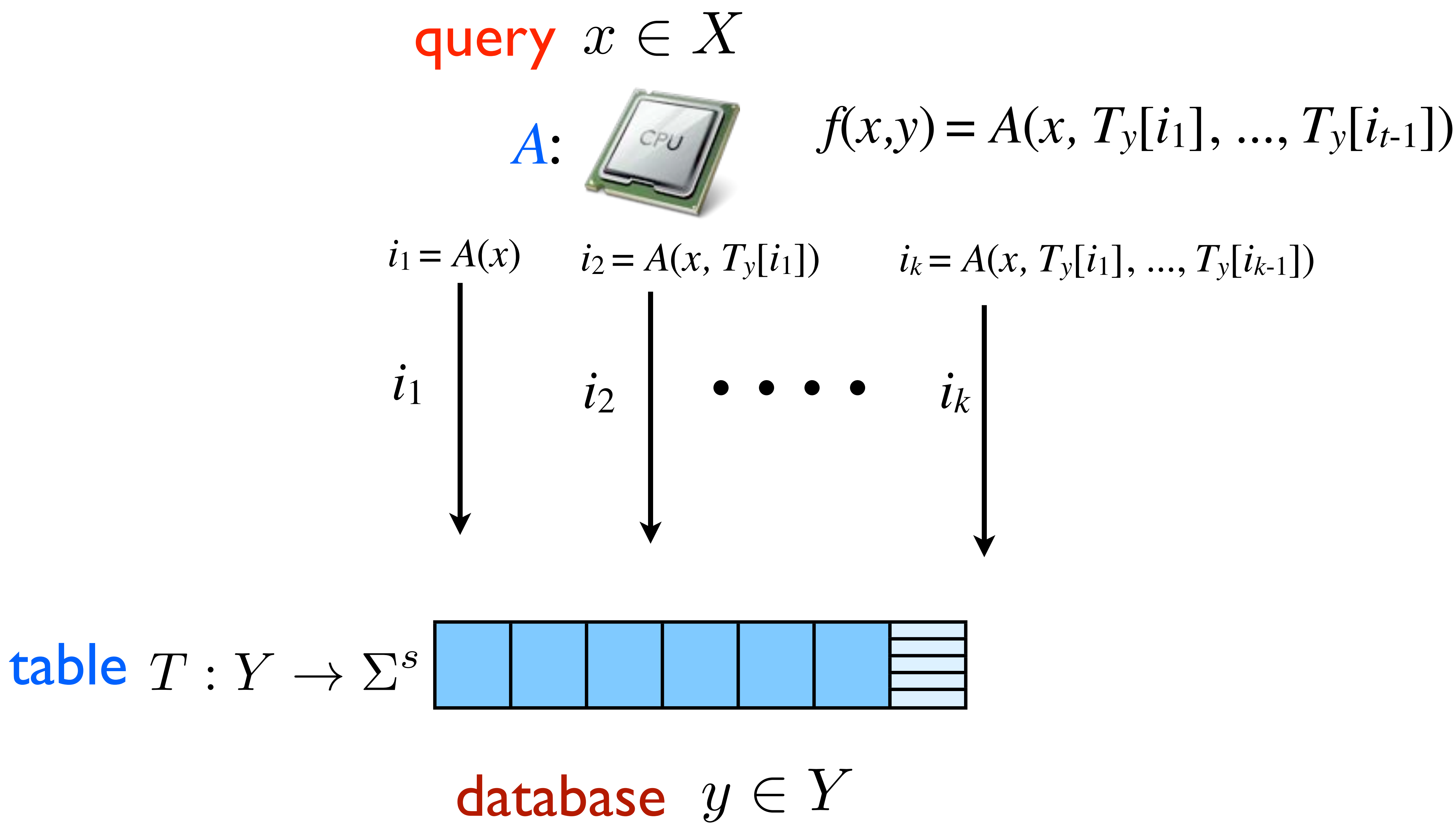
$f : X \times Y \to \{0,1\}$

query $x \in X$



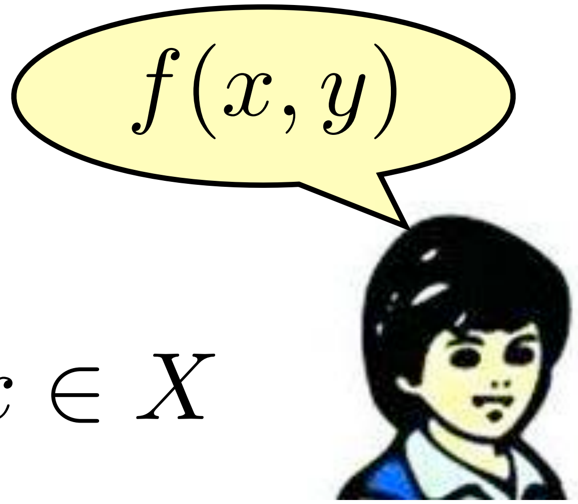
protocol (**cell-probing scheme**): the pair (A, T)

Cell-Probe Model



(s,w,t)-cell-probing scheme

$$f : X \times Y \times \to \{0,1\}$$



$x \in X$ $\rightleftarrows$ $y \in Y$

$a_1 = A(x)$ $\xrightarrow{a_1}$

$\xleftarrow{b_1}$ $b_1 = B(y, a_1)$

$a_2 = A(x, b_1)$ $\xrightarrow{a_2}$

$\xleftarrow{b_2}$ $b_2 = B(y, a_1, a_2)$

$\vdots$

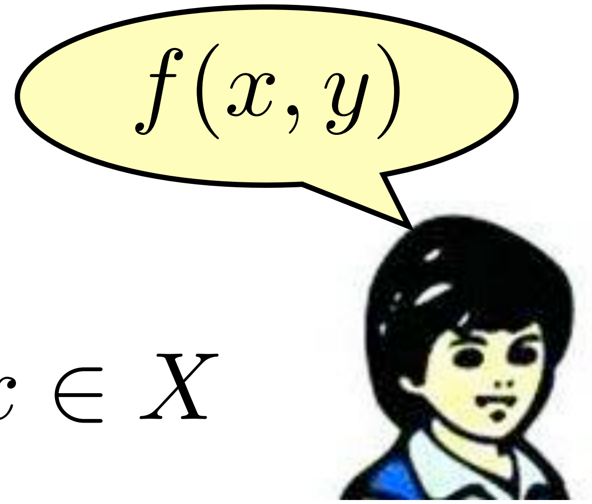
$\xleftarrow{b_i}$ $b_i = B(y, a_1, \ldots, a_i)$

$a_{i+1} = A(x, b_1, \ldots, b_i)$

$\vdots$

$$f(x,y) = A(x, b_1, \ldots, b_t)$$

$$f : X \times Y \times \to \{0,1\}$$



oblivious

$x \in X$ $\quad$ $\rightleftarrows$ $\quad$ $y \in Y$

$a_1 = A(x)$ $\xrightarrow{a_1}$

$\xleftarrow{b_1}$ $b_1 = B(y, a_1)$

$a_2 = A(x, b_1)$ $\xrightarrow{a_2}$

$\xleftarrow{b_2}$ $b_2 = B(y, a_2)$

$\vdots$

$\xleftarrow{b_i}$ $b_i = B(y, a_i)$

$a_{i+1} = A(x, b_1, \ldots, b_i)$

$\vdots$

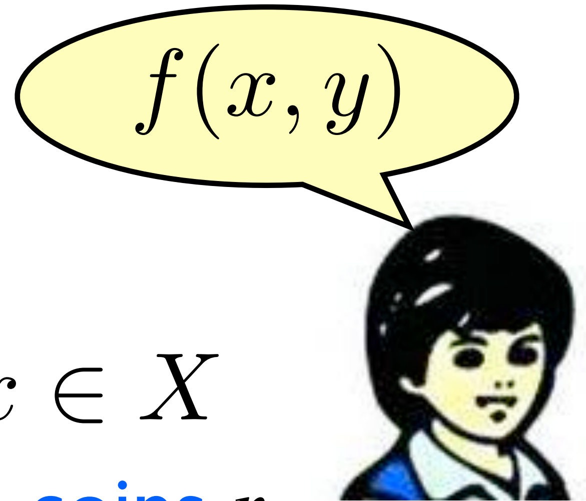
say $a_i \in [s]$, $\quad b_i \in \Sigma$

$B : Y \times [S] \to \Sigma$

$f(x,y) = A(x, b_1, \ldots, b_t)$

equivalent: $B : Y \to \Sigma^s$

$f : X \times Y \times \to \{0,1\}$



oblivious

$x \in X$

random coins r

$y \in Y$

$a_1 = A(r, x)$ $\xrightarrow{a_1}$

$\xleftarrow{b_1}$ $b_1 = B(y, a_1)$

$a_2 = A(r, x, b_1)$ $\xrightarrow{a_2}$

$\xleftarrow{b_2}$ $b_2 = B(y, a_2)$

$\vdots$

$\xleftarrow{b_i}$ $b_i = B(y, a_i)$

$a_{i+1} = A(r, x, b_1, \ldots, b_i)$

$\vdots$

say $a_i \in [s]$, $b_i \in \Sigma$

$B : Y \times [S] \to \Sigma$

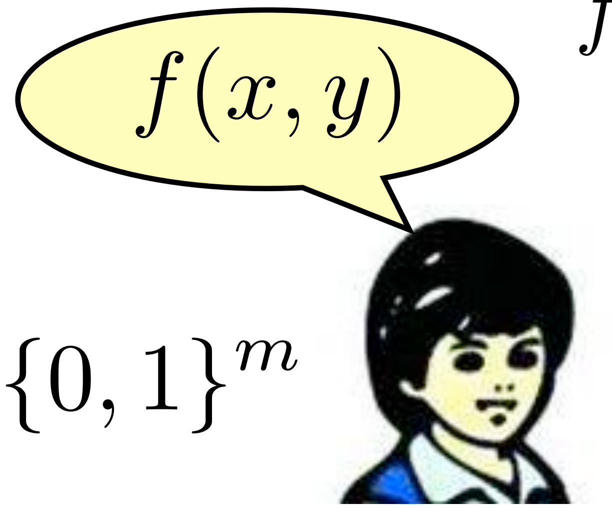
equivalent: $B : Y \to \Sigma^s$

$f(x,y) = A(r, x, b_1, \ldots, b_t)$

with large probability

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

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



every round:

$\log(s)$ bits →

← w bits

t rounds

oblivious

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

$T : Y \to \Sigma^s$

where $\Sigma = \{0,1\}^w$

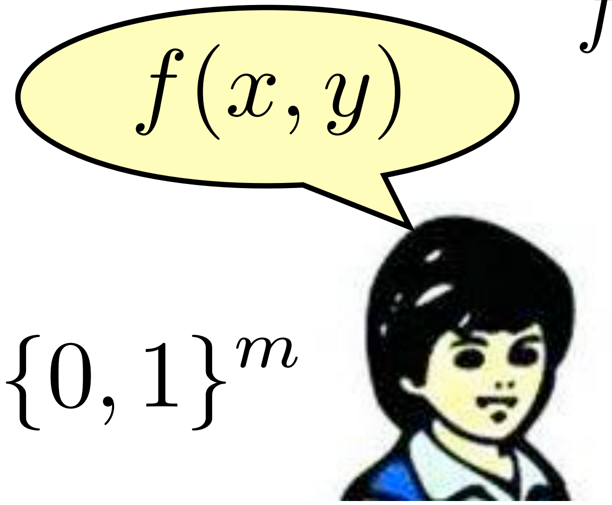
(s,w,t)-cell-probing scheme

tradeoff between time complexity t and space complexity s, w in optimal protocol

$$t \geq g(s,w,m,n)?$$

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

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



every round:

$\log(s)$ bits →

← w bits

t rounds

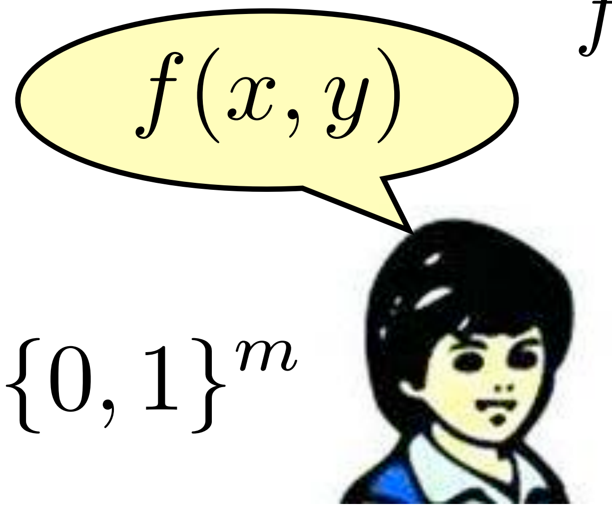
adaptive

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

trivial solution for adaptive Bob:

$$t \le \frac{m}{\log s} \qquad t \le \frac{n}{w}$$

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



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

every round:

$\log(s)$ bits →

← w bits

t rounds

oblivious

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

$T : Y \to \Sigma^s$

where $\Sigma = \{0,1\}^w$

trivial solution for adaptive Bob:

$$t \leq \frac{m}{\log s} \qquad t \leq \frac{n}{w}$$

trivial solution for oblivious Bob (cell-probe model):

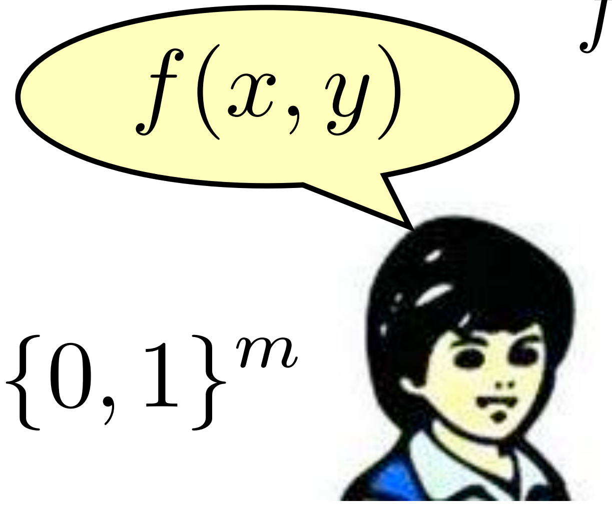
$$t \leq \frac{n}{w}$$

(retrieve entire database)

$sw \leq 2^m$ for any nontrivial t

(store answers for all queries)

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



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

every round:

$\log(s)$ bits →

← w bits

t rounds

oblivious

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

$T : Y \to \Sigma^s$

where $\Sigma = \{0,1\}^w$

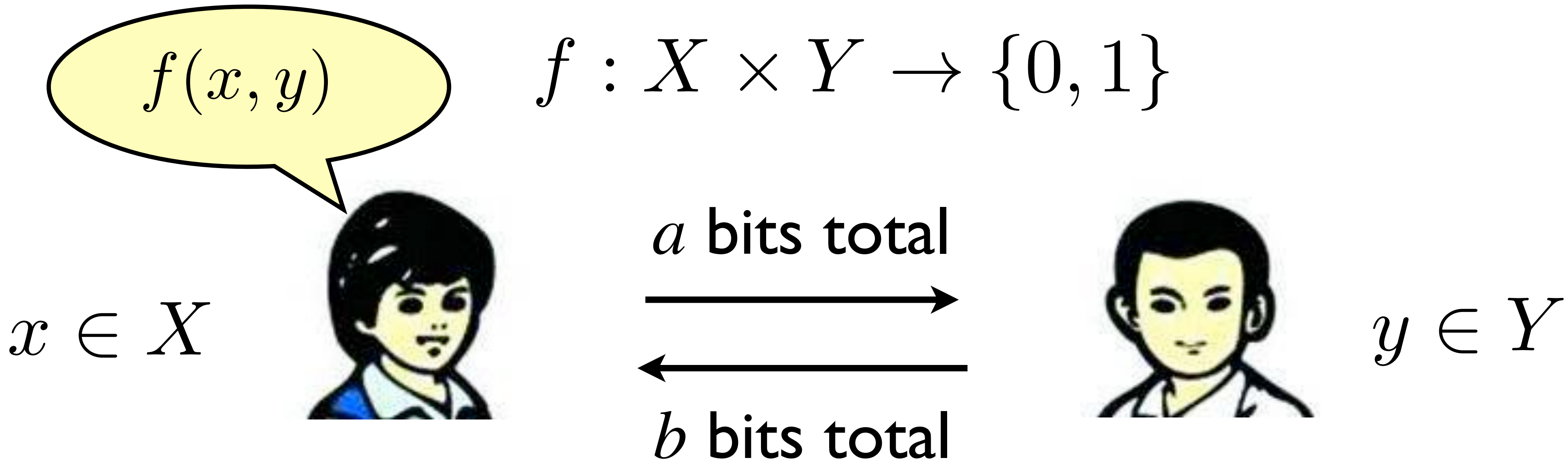
trivial solution for oblivious Bob (cell-probe model):

$t \leq \frac{n}{w}$ (retrieve entire database)

$sw \leq 2^m$ for any nontrivial t (store answers for all queries)

> **Theorem** (Miltersen 1999)
>
> there exists such $f:\{0,1\}^m \times \{0,1\}^n \to \{0,1\}$ that any deterministic cell-probing scheme solving f must have:
>
> either $t > \frac{n}{w} - \log m - O(1)$ or $sw > (1-o(1))2^m$

Asymmetric Communications



[a,b]-protocol: Alice sends a total of ≤a bits
Bob sends a total of ≤b bits

(s,w,t)-cell-probing scheme ⇒ [$t \log s$, wt]-protocol

The *Richness* Lemma

$$f : X \times Y \to \{0, 1\}$$

α-dense: density of 1s $\geq \alpha$

(u,v)-rich: $\geq v$ columns contain $\geq u$ 1s

$[a,b]$-protocol: Alice sends a total of $\leq a$ bits
Bob sends a total of $\leq b$ bits

(s,w,t)-cell-probing scheme ⇒ $[t \log s, wt]$-protocol

Richness lemma (Miltersen, Nisan, Safra, Wigderson, 1995)

f is α-dense
f has $[a,b]$-protocol
⇒ f has 1-rectangle of size:

$$\frac{\alpha|X|}{2^{O(a)}} \times \frac{\alpha|Y|}{2^{O(a+b)}}$$

The *Richness* Lemma

$$f : X \times Y \to \{0, 1\}$$

α-dense: density of 1s $\geq \alpha$

(u,v)-rich: $\geq v$ columns contain $\geq u$ 1s

$[a,b]$-protocol: Alice sends a total of $\leq a$ bits
Bob sends a total of $\leq b$ bits

(s,w,t)-cell-probing scheme ⇒ $[t \log s, wt]$-protocol

Richness lemma (Miltersen, Nisan, Safra, Wigderson, 1995)

f is α-dense
f has (s,w,t)-cell-probing scheme
⇒ f has 1-rectangle of size:

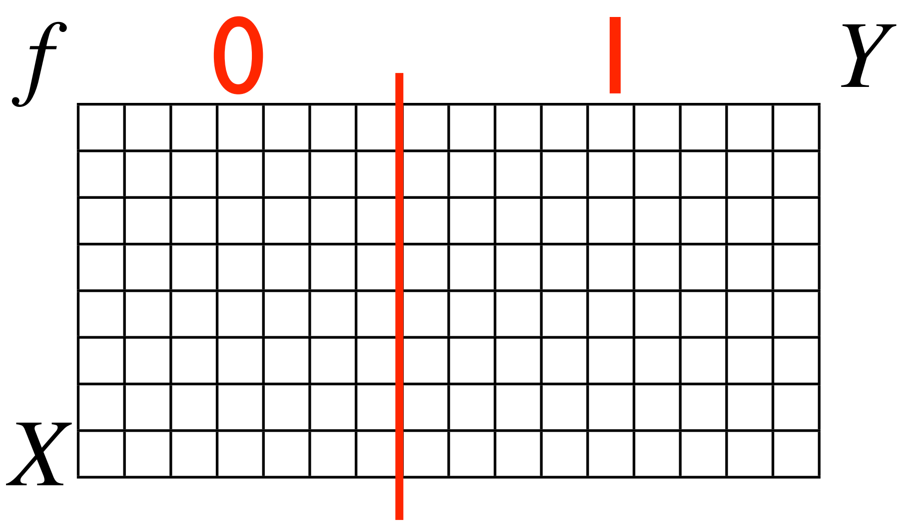
$$\frac{\alpha|X|}{2^{O(t \log s)}} \times \frac{\alpha|Y|}{2^{O(t(w+\log s))}}$$

(u,v)-rich: $\geq v$ columns contain $\geq u$ 1s

Richness lemma (Miltersen, Nisan, Safra, Wigderson, 1995)

f is (u,v)-rich
f has $[a,b]$-protocol
$\Rightarrow$ f has 1-rectangle of size:

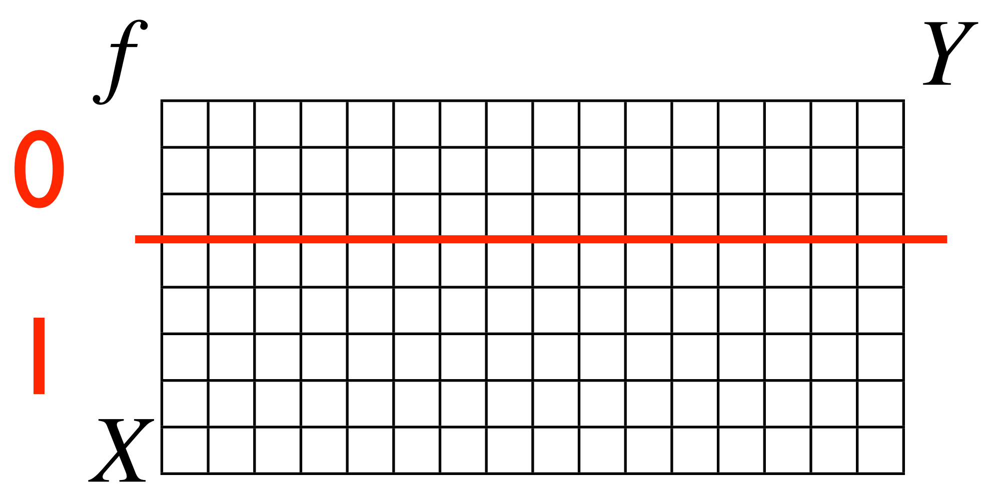
$$\frac{u}{2^{O(a)}} \times \frac{v}{2^{O(a+b)}}$$



if Bob sends the first bit:

f is partitioned to 2 subproblems each solved by a $[a, b\text{-}1]$-protocol

one of them must be $(u,v/2)$-rich



if Alice sends the first bit:

f is partitioned to 2 subproblems each solved by a $[a\text{-}1, b]$-protocol

one of them must be $(u/2,v/2)$-rich

(u,v)-rich: $\geq v$ columns contain $\geq u$ 1s

Richness lemma (Miltersen, Nisan, Safra, Wigderson, 1995)

f is (u,v)-rich
f has $[a,b]$-protocol

$\Rightarrow$ f has 1-rectangle of size:

$$\frac{u}{2^{O(a)}} \times \frac{v}{2^{O(a+b)}}$$

$\Downarrow$

Richness lemma (Miltersen, Nisan, Safra, Wigderson, 1995)

f is α-dense
f has (s,w,t)-cell-probing scheme

$\Rightarrow$ f has 1-rectangle of size:

$$\frac{\alpha|X|}{2^{O(t \log s)}} \times \frac{\alpha|Y|}{2^{O(t(w+\log s))}}$$

Approximate Near Neighbor
(ANN)

Hamming space $X = \{0,1\}^d$

query $x \in X$

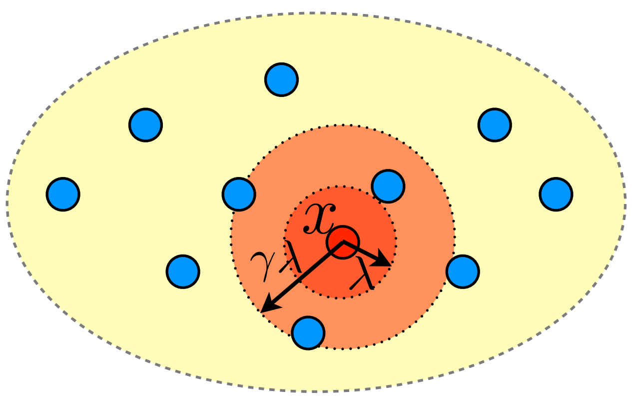
access

database

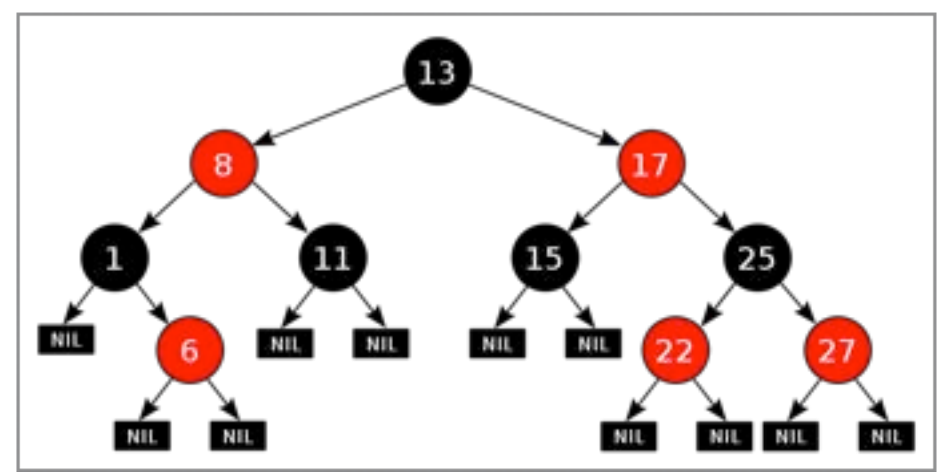
$\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in X^n$

data structure

radius λ



preprocessing



approx ratio $\gamma > 1$

***λ*-NN:** determine whether $\exists y_i$ that is λ-close to x

(*λ*, *γ*)-ANN: answer "yes" if $\exists y_i$ that is λ-close to x

"no" if all y_i are $\gamma\lambda$-far from x

arbitrary if otherwise

Lower Bounds for Hamming NNS

Hamming space $X = \{0,1\}^d$ database $\boldsymbol{y} \in X^n$

time: t cell-probes; space: s cells, each of w bits

	deterministic	randomized
exact	$t = \Omega\left(\frac{d}{\log s}\right)$ [Miltersen *et al.* STOC'95] $t = \Omega\left(\frac{d}{\log \frac{sw}{n}}\right)$ [Pătraşcu, Thorup, STOC'06] $t = \Omega\left(\frac{d}{\log \frac{sw}{nd}}\right)$ ours	$t = \Omega\left(\frac{d}{\log s}\right)$ [Barkol, Rabani, STOC'00] $t = \Omega\left(\frac{d}{\log \frac{sw}{n}}\right)$ [Pătraşcu, Thorup, STOC'06]
approx	$t = \Omega\left(\frac{d}{\log s}\right)$ [Liu, 2004] $t = \Omega\left(\frac{d}{\log \frac{sw}{n}}\right)$ [Pătraşcu, Thorup, STOC'06] $t = \Omega\left(\frac{d}{\log \frac{sw}{nd}}\right)$ ours	$t = \Omega\left(\frac{\log\log d}{\log\log\log d}\right)$ tight for $s = \mathrm{poly}(n)$ [Chakrabarti, Regev, FOCS'04] $t = \Omega\left(\frac{\log n}{\log \frac{sw}{n}}\right)$ [Panigrahy, Talwar, Wieder, FOCS'08] [Panigrahy, Talwar, Wieder, FOCS'10]

(u,v)-rich: $\geq v$ columns contain $\geq u$ 1s

Richness lemma (Miltersen, Nisan, Safra, Wigderson, 1995)

f is (u,v)-rich

f has $[a,b]$-protocol

$\Rightarrow$ f has 1-rectangle of size:

$$\frac{u}{2^{O(a)}} \times \frac{v}{2^{O(a+b)}}$$

$\Downarrow$

Richness lemma (Miltersen, Nisan, Safra, Wigderson, 1995)

f is α-dense

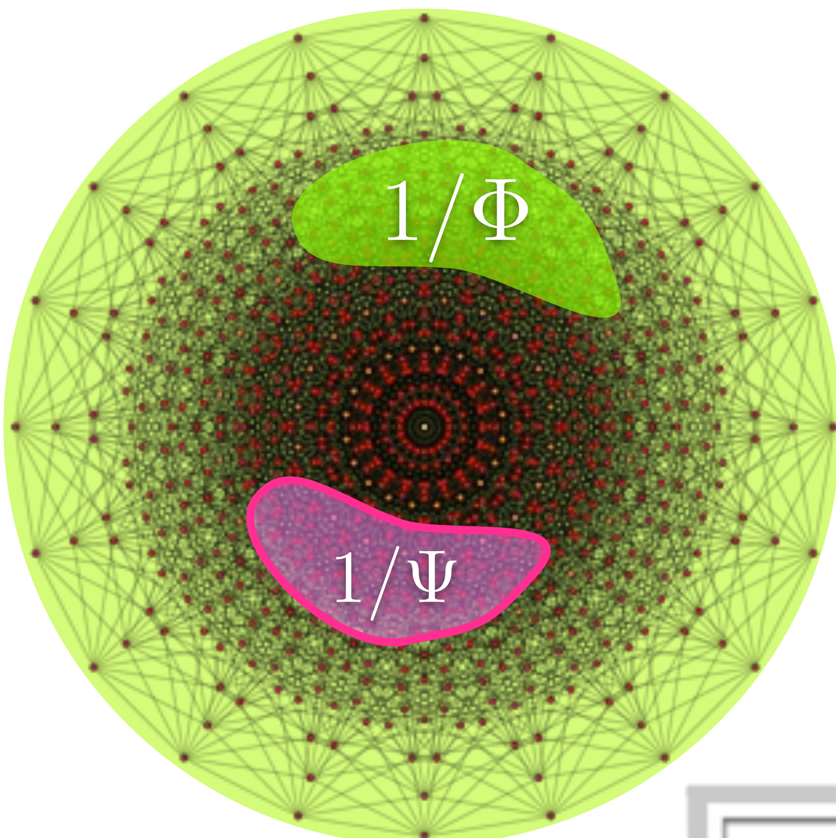
f has (s,w,t)-cell-probing scheme

$\Rightarrow$ f has 1-rectangle of size:

$$\frac{\alpha|X|}{2^{O(t\log s)}} \times \frac{\alpha|Y|}{2^{O(t(w+\log s))}}$$

Metric Expansion

metric space $X = \{0,1\}^d$



Definition (metric expansion)

Metric space X is (λ,Φ,Ψ)-expanding if any $1/\Phi$-fraction of X expands to all but at most $1/\Psi$-fraction of X in λ distance.

Harper's Inequality

Hamming space is $(\Theta(d), 2^{\Omega(d)}, 2^{\Omega(d)})$-expanding

(extremal expansion achieved by Hamming balls)

there is no 1-rectangle of size $2^{c_1 d} \times 2^{c_2 n d}$ for $c_3 d$-NN

for some constant $c_1, c_2, c_3 \in (0,1)$ $\quad c_3 \approx \frac{1}{2} + \sqrt{\frac{2\ln(2n)}{d}}$

$$\lambda\text{-NN}: \{0,1\}^d \times \{0,1\}^{n\times d} \to \{0,1\}$$

there is no 1-rectangle of size $2^{c_1 d} \times 2^{c_2 nd}$ for $c_3 d$-NN

Richness lemma (Miltersen, Nisan, Safra, Wigderson, 1995)

f is α-dense

f has (s,w,t)-cell-probing scheme

⇒ f has 1-rectangle of size: $\frac{\alpha|X|}{2^{O(t\log s)}} \times \frac{\alpha|Y|}{2^{O(t(w+\log s))}}$

⇒ for λ-NN: either $t = \Omega\left(\frac{d}{\log s}\right)$ or $wt = \Omega(nd)$

Cell-Sampling Richness lemma

f is α-dense

f has (s,w,t)-cell-probing scheme

⇒ $\forall t \le \Delta \le s$, f has 1-rectangle of size: $\frac{\alpha|X|}{2^{O(t\log\frac{s}{\Delta})}} \times \frac{\alpha|Y|}{2^{O(w\Delta + \Delta\log\frac{s}{\Delta})}}$

⇒ for λ-NN: choose some $\Delta = \Theta\left(\frac{nd}{w}\right)$, then $t = \Omega\left(\frac{d}{\log\frac{sw}{nd}}\right)$

Lower Bounds for Hamming NNS

Hamming space $X = \{0,1\}^d$ database $\boldsymbol{y} \in X^n$

time: t cell-probes; space: s cells, each of w bits

	deterministic	randomized
exact	$t = \Omega\left(\frac{d}{\log s}\right)$ [Miltersen *et al.* STOC'95] $t = \Omega\left(\frac{d}{\log \frac{sw}{n}}\right)$ [Pătraşcu, Thorup, STOC'06] $t = \Omega\left(\frac{d}{\log \frac{sw}{nd}}\right)$ ours	$t = \Omega\left(\frac{d}{\log s}\right)$ [Barkol, Rabani, STOC'00] $t = \Omega\left(\frac{d}{\log \frac{sw}{n}}\right)$ [Pătraşcu, Thorup, STOC'06]
approx	$t = \Omega\left(\frac{d}{\log s}\right)$ [Liu, 2004] $t = \Omega\left(\frac{d}{\log \frac{sw}{n}}\right)$ [Pătraşcu, Thorup, STOC'06] $t = \Omega\left(\frac{d}{\log \frac{sw}{nd}}\right)$ ours	$t = \Omega\left(\frac{\log\log d}{\log\log\log d}\right)$ tight for $s = \mathrm{poly}(n)$ [Chakrabarti, Regev, FOCS'04] $t = \Omega\left(\frac{\log n}{\log \frac{sw}{n}}\right)$ [Panigrahy, Talwar, Wieder, FOCS'08] [Panigrahy, Talwar, Wieder, FOCS'10]

Thank you!