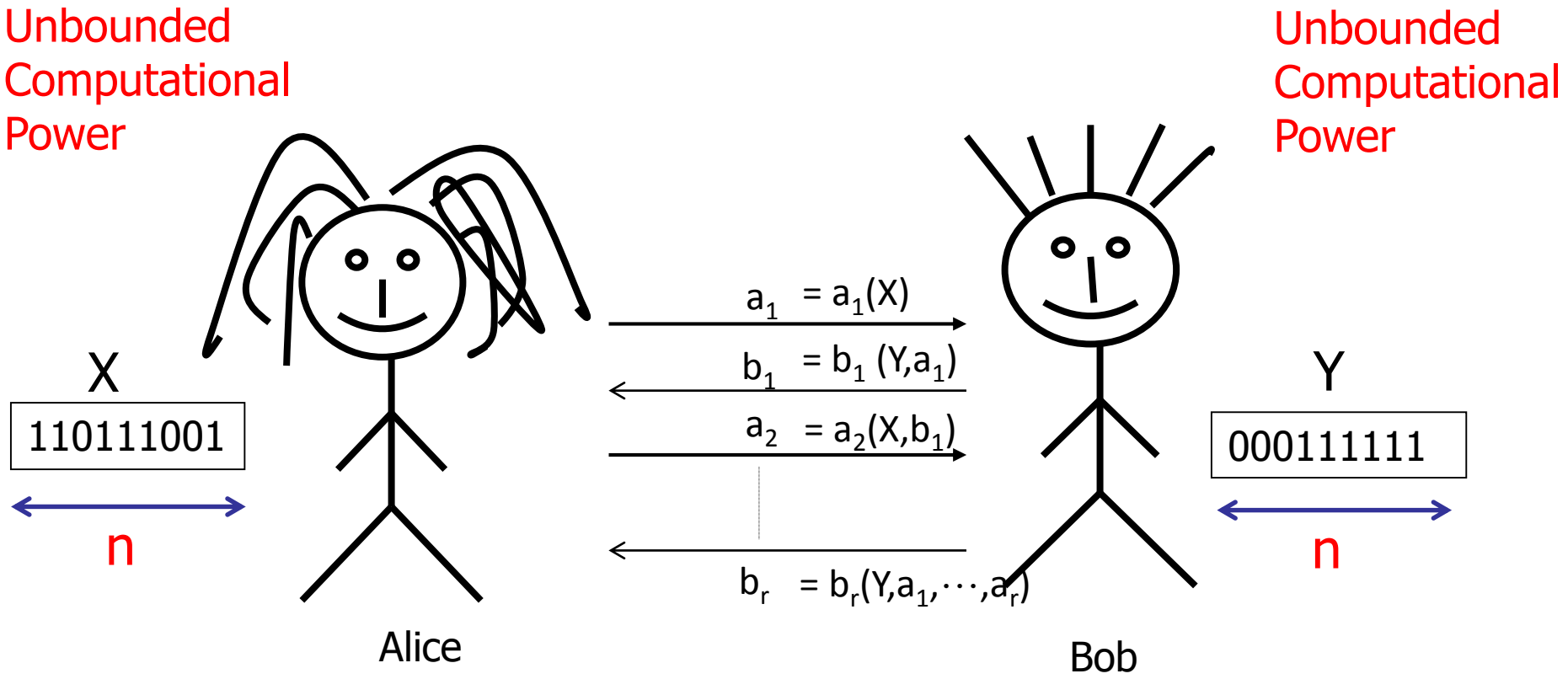
Multiparty Communication Complexity
(A biased introduction)

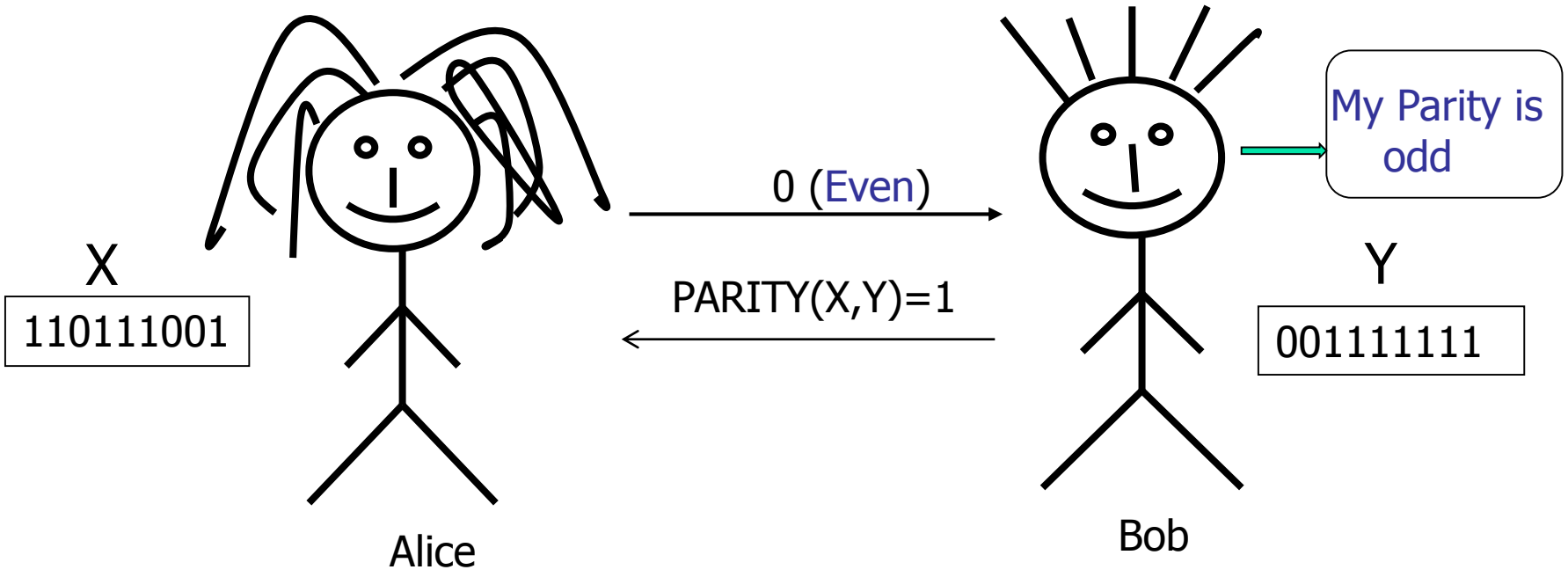
Arkadev Chattopadhyay
TIFR, Mumbai

Yao's 2-Party Model of 1979



- Alice and Bob collaborate to compute f(X,Y).
- Aim to minimize the communication cost.
- Complexity of any f is at most n+1.

Easy Functions



Compute PARITY(X,Y).

- CC(PARITY) = 2.
- CC(MAJORITY) = O(log n).

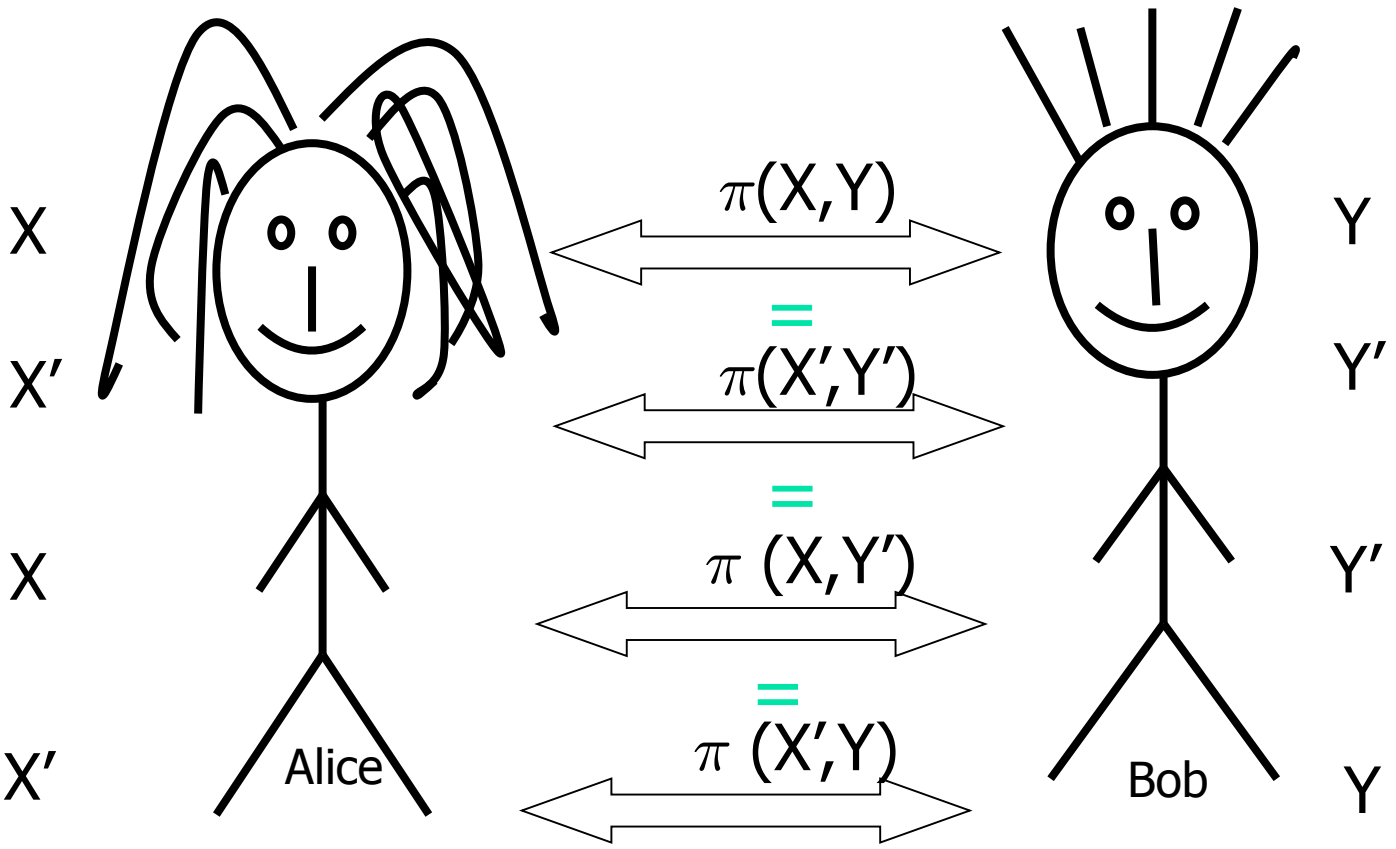
Hard Functions

How about EQ(X,Y), i.e. is X=Y?

Intuitively, this should require n bits of communication!

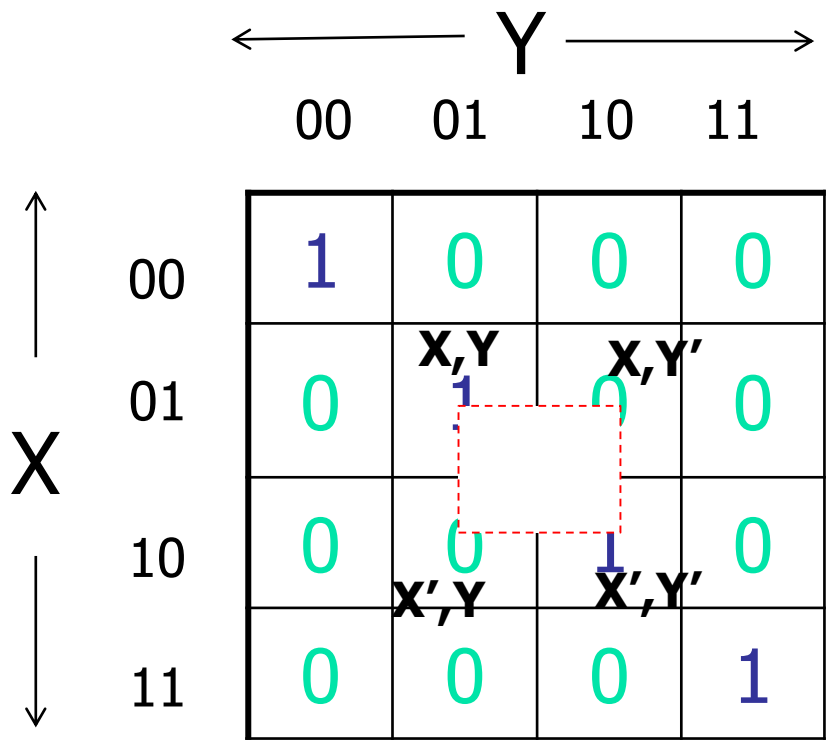
Needs an argument!

Rectangularity of Protocols



Observation. Every transcript corresponds to a rectangle of form $R_X \times C_Y$.

Diagonals are Hard to Cover



CC(Equality)
$\geq \log(2^n) + 1$
$= n + 1.$

Fact: No two 1's on diagonal share the same transcript.

Set-Disjointness

Disj(x,y) = 0 iff for some i, $x_i = y_i = 1$.

Alice	1	0	1	1	0	1	0	0	1
Bob	1	1	0	1	0	1	1	0	1

Disj(A,B)=0

CC(Disj) $\geq$ n + 1

Suppose $\pi(a,a^c) = \pi(b,b^c)$

Contradiction!

Then $\pi(a,b^c) = \pi(b,a^c) = \pi(a,a^c) = \pi(b,b^c)$

Conclusion: All 2^n inputs of form (x,x^c) have distinct transcripts.

Inner-Product

$$\mathbf{IP(x,y) \equiv \sum_i x_i \cdot y_i \pmod 2}$$

Alice	1	0	1	1	0	1	0	0	1	**x**
Bob	1	1	0	1	0	1	1	0	0	**y**

IP(X,Y)=1

$R_x \times C_y$ be 0-monochromatic.

$$|R_x| = 2^{\alpha \cdot n}, \quad |C_y| = 2^{\beta \cdot n}$$

$$\alpha+\beta \leq 1$$

$x^1, \cdots, x^{\alpha n}$ **Lin. Ind.**

$y^1, \cdots, y^{\beta n}$ **Lin. Ind.**

$\Leftarrow$ $x^i \cdot y^j = 0$

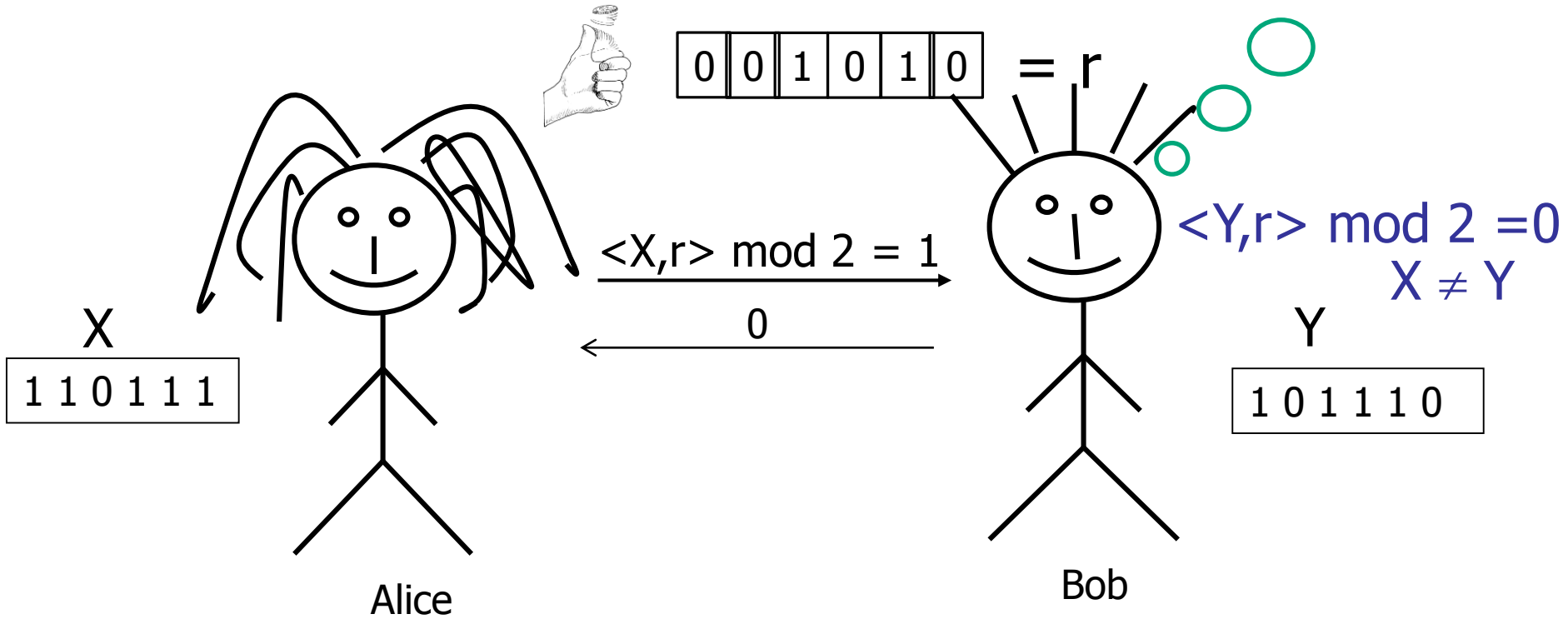
Concl: Size of monochromatic rectangle is at most 2^n.

$$CC(IP) \geq n - o(n)$$

Can randomization help?

One central theme of theory of computation.

The Power of Randomness



Compute
EQUALITY(X,Y).

- $R_{1/2}$ (EQ) = 2.

Randomized protocols can be much more powerful than deterministic ones.

Limits of Random Protocols

Set-Disjointness:

Disj(x,y) = 0 iff for some i, $x_i = y_i = 1$.

Alice	1	0	1	1	0	1	0	0	1
Bob	1	1	0	1	0	1	1	0	1

Disj(A,B)=0

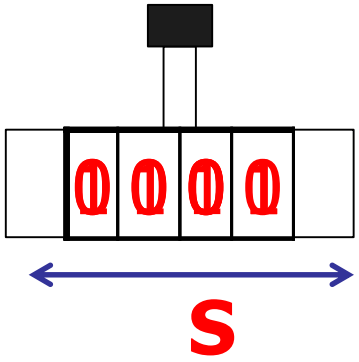
R(Set-Disj) = Ω(n).

(**Kalyanasundaram-Schnitger'87, Razborov'90**).

Celebrated Result

Streaming Computation

1	2	4	8	1	5	7	4	3



D[1,⋯,m]

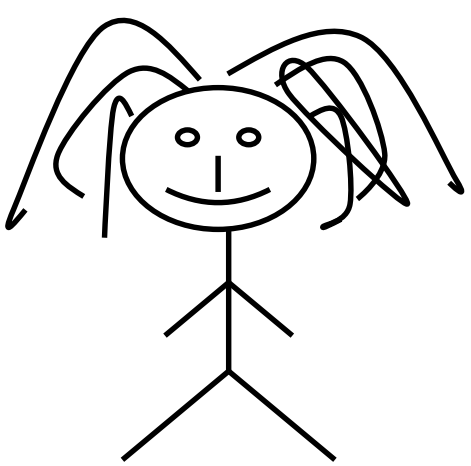
D[i] ∈ {1,⋯, n}

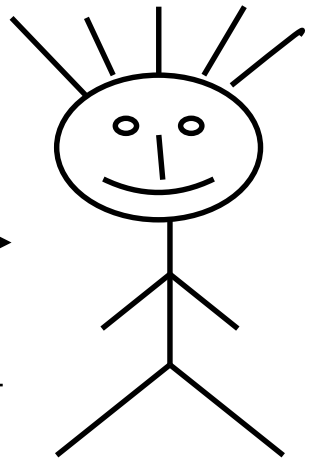
Goal: Answer questions about the frequency distribution on {1,⋯,n}.

Problem: How much space **S** is needed to approximate the maximal frequency?

Application to Streaming

How much space needed to compute max frequency?





S bits

0

X

110100

Y

001111

Alice

Bob

A_x

1	2	4

3	4	5	6

B_y

$|A_x \cup B_y|_\infty = 2$

Concl: $|M|_\infty^S$ needs $\Omega(N)$ space

Many More Applications…

Data Structures.

Circuit complexity.

Pseudo-randomness.

Combinatorial Optimization.

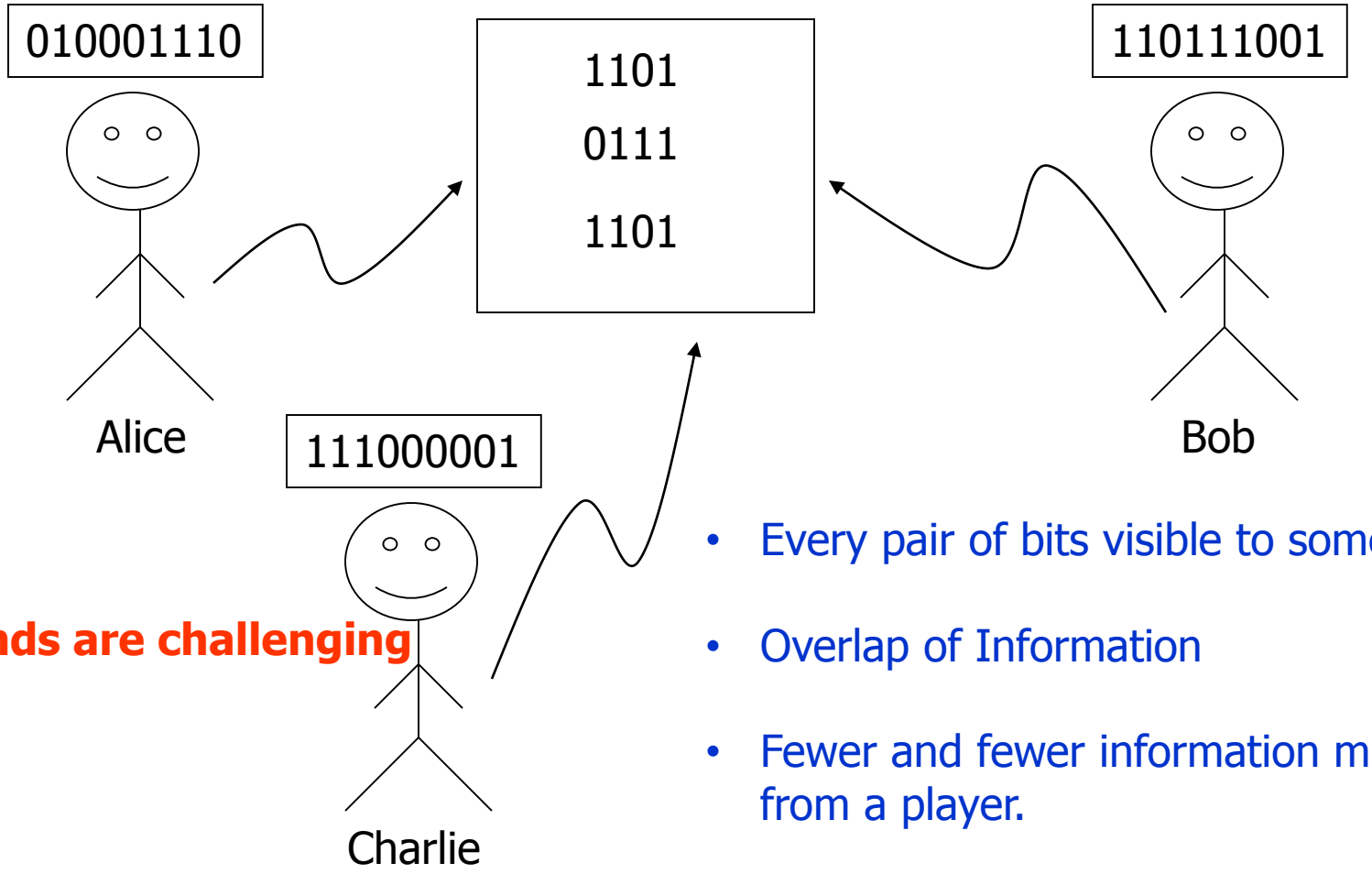
Property Testing.

(Swiss-Army Knife of Computer Scientists)

Multiparty Communication

Number-on-Forehead Model

Chandra-Furst-Lipton'83

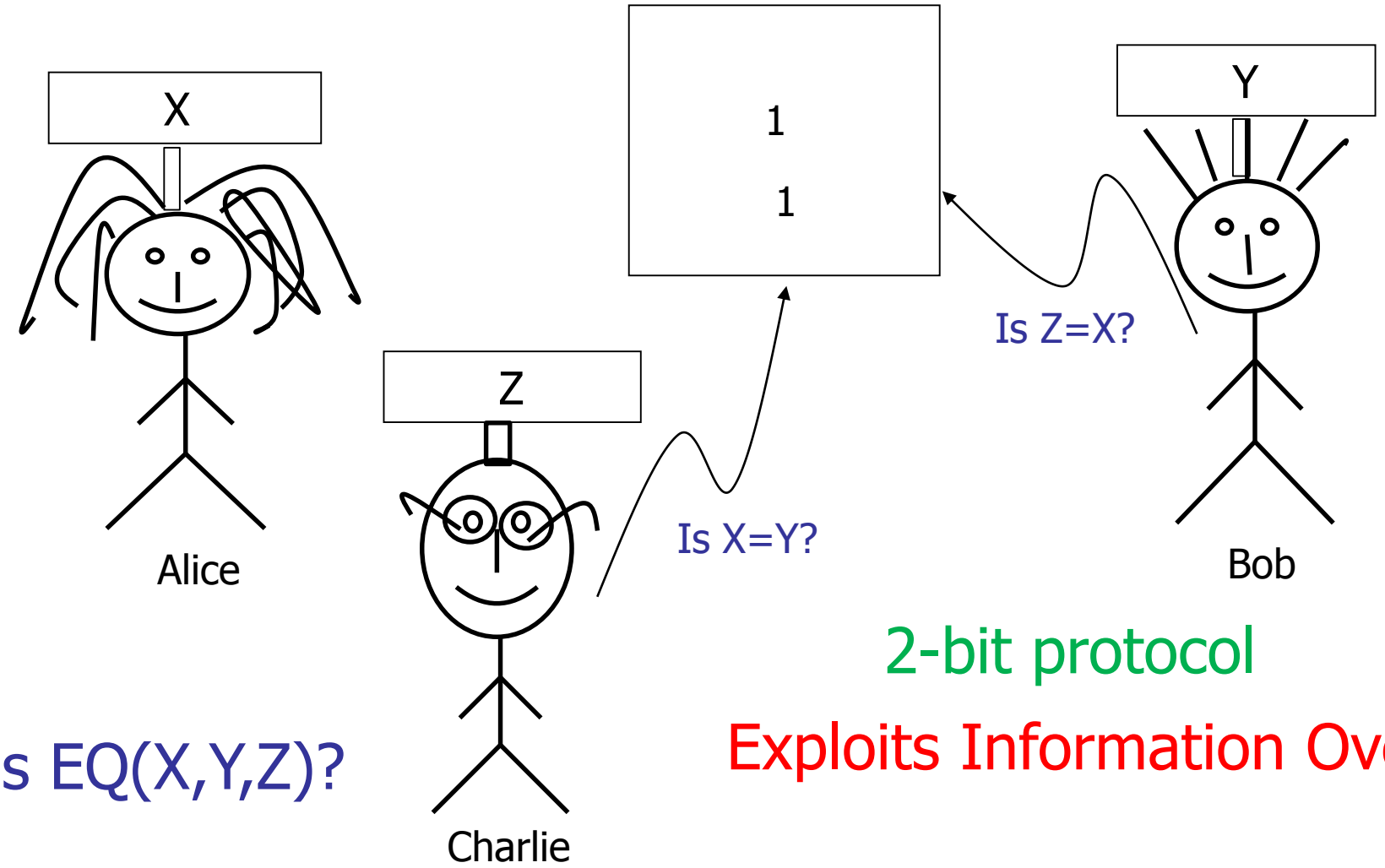


Lower bounds are challenging

- Every pair of bits visible to someone.
- Overlap of Information
- Fewer and fewer information missing from a player.

Foreheads Make a Difference

EQUALITY is hard for 2 parties!



Is EQ(X,Y,Z)?

2-bit protocol

Exploits Information Overlap

NOF Lower Bounds Benefits

- Circuit Lower Bounds
- Branching Program Lower Bounds
- Pseudo-random generators
- Lower bounds on length of proofs
- Data-structure lower bounds
- More to be discovered….

Constant-Depth Circuits

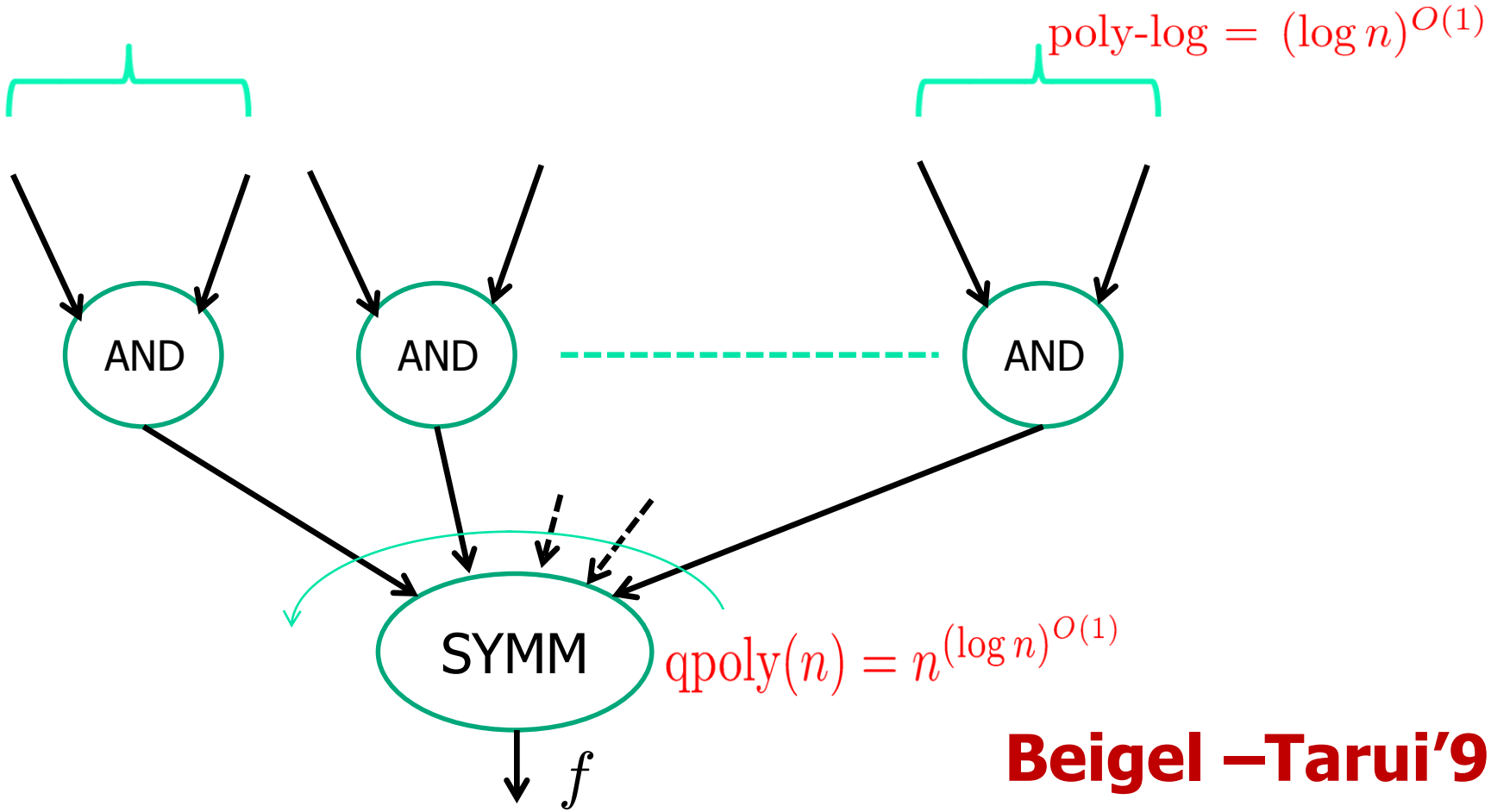
Conjecture (Smolensky'87): MAJ needs exponential size circuits of constant depth having AND/OR/MOD_m gates.

ACC^0 $\equiv$ {fns having poly-size ckts with AND/OR/MOD gates}.

Open: Is NP $\subseteq$ ACC^0 ?

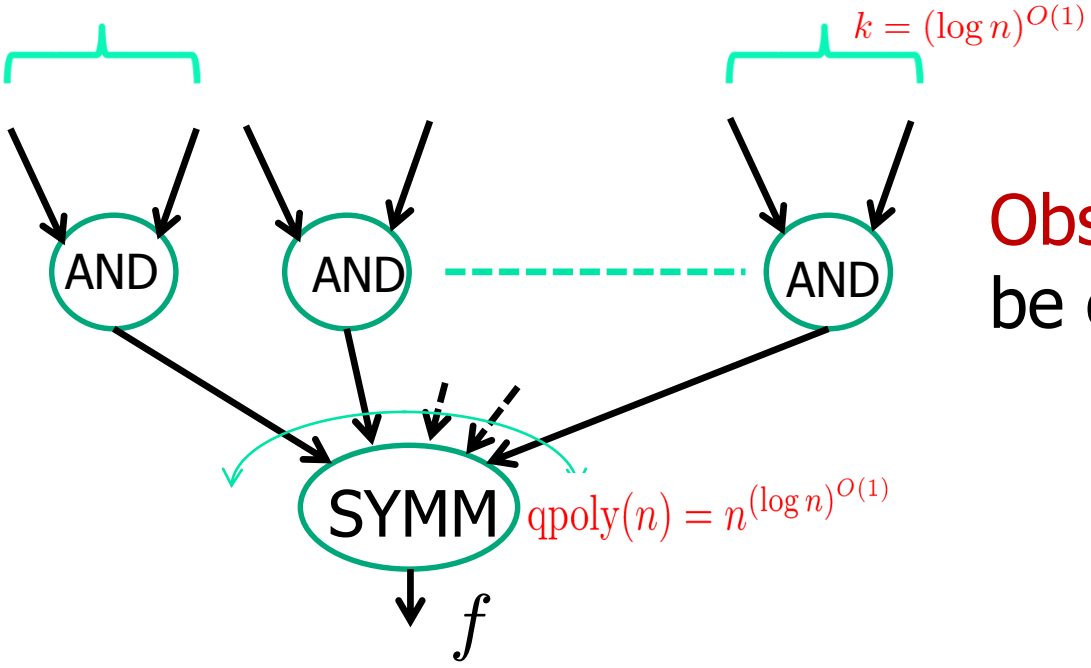
Bounded Depth Circuits

f computed by constant-depth circuits with AND/OR/MOD gates efficiently,



Beigel –Tarui'91

Protocols for Depth 2



Observ: Each AND gate can be computed by one player.

Question: k+1-party NOF complexity of f ?

Protocol: $k \cdot (\log n)^{O(1)}$

- Players 1,⋯,k send the number of AND gates they see firing 1, communicating only poly-log bits each.
- Player k+1 announces the answer.

NOF Attack on ACC

Theorem: Every $f \in ACC^0$ has poly-log(n) simultaneous k-party communication complexity for some k = poly-log(n), under every input partition.

Corollary of Beigel-Tarui'91

Major Goal: Find f that is hard for large number of players.

A Conjecture

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

$(f \circ q)(X_1, X_2, \cdots, X_k) =$ $f(q(C_1), q(C_2), \ldots, q(C_n))$

Question: Complexity of (MAJ ∘ MAJ)?

Observation:

$$\text{Let } D_k^{\text{sim}}(\text{MAJ} \circ \text{MAJ}) = (\log n)^{\omega(1)}$$

$\Rightarrow$ MAJ ∘ MAJ $\notin$ ACC^0

a la Beigel-Tarui'91

$\Rightarrow$ MAJ $\notin$ ACC^0

	0	1	0	1	1	0	0
X_1	0	1	1	1	1	1	1
X_2	1	1	0	1	1	0	1
X_3	0	1	1	1	1	0	0
	.	.	.	.	.	.	.
	.	.	.	.	.	.	.
X_k	1	1	1	1	1	1	0

Proposed by Babai-Kimmel-Lokam'95 $\longleftarrow n \longrightarrow$

Examples of Composition

k=2

	Popular Names	Deterministic	Randomized
PARITY ∘ AND	≡ **IP**	$\Theta(n)$.	$\Theta(n)$.
	Complexity ?	**Folklore**	**Chor-Goldreich'85**
			Discrepancy
NOR ∘ AND	≡ **Set-Disj**	$\Theta(n)$.	$\Theta(n)$.
	Complexity ?	**Folklore**	**KS'87, Razborov'90 BJKS'02**
			Very influential

Remark 1: Argument for Set-Disj spawned many new techniques.

Remark 2: Has many diverse applications.

NOF Lower Bounds

Popular Names	$k \geq 3$ Deterministic/Randomized	
PARITY $\circ$ AND $\equiv$ **GIP**	$\Omega(n/4^k)$.	**Babai-Nisan-Szegedy'89** Seminal Paper
NOR $\circ$ AND $\equiv$ **Set-Disj**	$\Omega((\log n)/k)$.	**Tesson'05**
	$\Omega\left(\frac{n}{2^k 2^{2k}}\right)^{\frac{1}{k+1}}$	**Lee-Shraibman'08, C-Ada'08**

Apology: SKIPPED other attempts

Improvement **Beame-Huynh-Ngoc'09**

$$\Omega\left(\frac{n}{4^k}\right)^{1/4}$$ **Sherstov'12**

Deterministic

$$\Omega\left(\frac{n}{4^k}\right)$$ **Rao-Yehudayoff'14**

$\leftarrow$

$$\Omega\left(\frac{\sqrt{n}}{k2^k}\right)$$ **Sherstov'13**

NOF Lower Bounds

Popular Names

$k \geq 3$

Deterministic/Randomized

PARITY $\circ$ AND $\equiv$ **GIP**

$\Omega(n/4^k)$.

Babai-Nisan-Szegedy'89

Seminal Paper

Remark 1: There is no separate, easier argument for deterministic case.

Remark 2: All strong bounds on (interactive) k-complexity use variations of the BNS argument.

Remark 3: All known bounds decay exponentially in k, are trivial for k= ω(log n).

Remark 4: By contrast, for k=2 several methods are known.

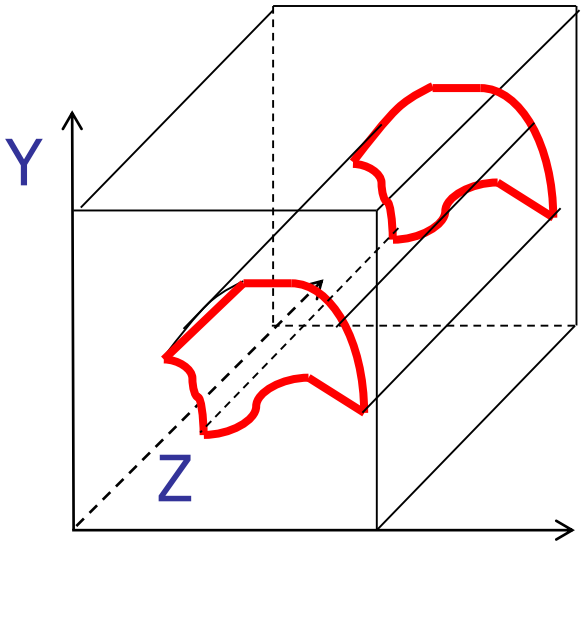
Discrepancy	**Corruption**	**Fourier-analytic**	**Information Theory**
Chor-Goldreich'85	**Razborov'89**	**Raz'95**	**BJKS'02 and many more**

Surprising Upper Bounds

	Popular Names	$k \geq 3$
		Deterministic
SYM ∘ AND	**{GIP, Disj,…}**	$O(n/2^k + k \cdot \log n)$.
		Grolmusz'91, Pudlak
		Almost- Simultaneous
SYM ∘ g	{GIP, MAJ ∘ MAJ, Disj…}	$O(k.(\log n)^2)$, $k \geq \log n + 2$.
g: compressible		**Babai-Gal-Kimmel-Lokam'**
		Simultaneous
SYM ∘ ANY		$O(k.(\log n)^2)$, $k \geq \log n + 4$.
		Ada-C-Fawzi-Nguyen'12
		Simultaneous
$SYM \circ ANY_s$		poly-log(n), $k \geq 2\log n$
$s \approx \log \log n$		**C-Saks'14**
		Almost- Simultaneous

Cylinder Intersections

Rectangles , i.e. $C_1(X) \times C_2(Y) \times C_3(Z)$, are **very** special.



$c_Z \equiv C_Z(X,Y)$

$c_Y \equiv C_Y(X,Z)$

$c_X \equiv C_X(Y,Z)$

$C = c_X \cap c_Y \cap c_Z$ is a cylinder intersection.

Fact: A c-bit deterministic protocol partitions inputs into at most 2^c monochromatic cylinder intersections.

The Discrepancy Method

Discrepancy: For a probability distr μ,

$disc_\mu(f,C)$ = | μ-wt of $f^{-1}(1)$ in C − μ-wt of $f^{-1}(-1)$ in C |

$disc_\mu(f)$ = $\max_C disc_\mu(f,C)$.

$\Pi \equiv C_1 \cup C_2 \cup \cdots \cup C_t$

Adv in C_i = $disc_\mu(f,C_i)$

Total Adv = 2ϵ

Union bound

Discrepancy Method: $R_k^\epsilon(f) \geq D_k^{\mu,\epsilon}(f) \geq \log\left(\frac{2\epsilon}{\mathrm{disc}_\mu(f)}\right)$

Yao's method

Question: How do we compute discrepancy?

An inductive Cauchy-Schwarz argument.

Cauchy-Schwarz Magic

$$\mathrm{disc}(f,C)^{2\times 2} = \left|\mathbb{E}_{X,Y,Z}\left[f(X,Y,Z)C_Z(X,Y)C_Y(X,Z)C_X(Y,Z)\right]\right|^{2\times 2}$$

$$\leq \left|\mathbb{E}_{X,Y}\left[\left|C_Z(X,Y)\right| \cdot \left|\mathbb{E}_Z\left[f(X,Y,Z)C_Y(X,Z)C_X(Y,Z)\right]\right|\right]\right|^{2\times 2}$$

0/1 valued

Cauchy-Schwarz

$$\leq \mathbb{E}_{X,Y}\left[\left(\mathbb{E}_Z\left[f(X,Y,Z)C_Y(X,Z)C_X(Y,Z)\right]\right)^2\right]^2$$

$$\leq \mathbb{E}_{Z^0,Z^1,X,Y}\left[f(X,Y,Z^0)f(X,Y,Z^1)C_Y^{Z^0}(X)C_Y^{Z^1}(X)C_X^{Z^0}(Y)C_X^{Z^1}(Y)\right]$$

$f^{Z^0,Z^1}(X,Y)$ $\quad R_a^{Z^0,Z^1}(X)$ $\quad R_b^{Z^0,Z^1}(Y)$

$$\mathrm{disc}\left(f^{Z^0,Z^1}, R^{Z^0,Z^1}\right)^2$$

$$\leq \mathbb{E}_Z \left|\left[\quad\right]\right|$$

$$\leq \mathbb{E}_{Y^0,Y^1}\left|\mathbb{E}_X\left[f^{Z^0,Z^1,Y^0,Y^1}(X)R_b^{Z^0,Z^1,Y^0,Y^1}\right]\right|$$

ind of X

$$\mathrm{disc}(f,C)^{2^2} \leq \mathbb{E}_{Z^0,Z^1,Y^0,Y^1}\left|\mathbb{E}_X\left[f^{Z^0,Z^1,Y^0,Y^1}(X)\right]\right|$$

$$= \mathbb{E}_{Z^0,Z^1,Y^0,Y^1}\left|\mathbb{E}_X\left[\prod_{u\in\{0,1\}^2} f\left(X,Y^{u_1},Z^{u_2}\right)\right]\right|$$

The BNS-Chung Criterion

Theorem (Raz'00):

$$\left(\mathrm{disc}_{\mu}(f)\right)^{2^k} \leq \mathop{\mathbb{E}}_{Y^{1,0},Y^{1,1},\ldots,Y^{k,0},Y^{k,1}} \left| \mathbb{E}_X \left[\prod_{u\in\{0,1\}^k} f\left(X, Y^{1,u_1}, \ldots, Y^{k,u_k}\right) \right] \right|$$

Cube Measure/Gower's norm

$$\mathcal{E}_{\mu,k}(f)$$

Application to GIP

$$\left(\mathrm{disc}\left(\mathrm{GIP}_{k+1}\right)\right)^{2^k} \leq \mathop{\mathbb{E}}_{\ldots,Y^{j,0},Y^{j,1},\ldots} \left|\mathbb{E}_X\left[(-1)^{\sum_{i=1}^{n} X_i \overbrace{(Y_i^{10}+Y_i^{11})\cdots(Y_i^{k0}+Y_i^{k1})}^{c_i}}\right]\right|$$

Observation:

$$\Pr_{\ldots,Y^{j,0},Y^{j,1},\ldots}\left[\forall i : c_i = 0\right] \leq \left(1-\tfrac{1}{2^k}\right)^n \leq \exp\left(-n/2^k\right)$$

Conclusion: $\mathrm{disc}\left(\mathrm{GIP}_{k+1}\right) \leq \exp\left(-n/4^k\right)$

↓ Discrepancy Method:

$$R_\epsilon\left(\mathrm{GIP}_{k+1}\right) = \Omega\left(\tfrac{n}{4^k}\right)$$

Limitations of Discrepancy

L^- = set of non-disjoint inputs
L^+ = set of disjoint inputs.

C_i = set of inputs that have an all-one ith column

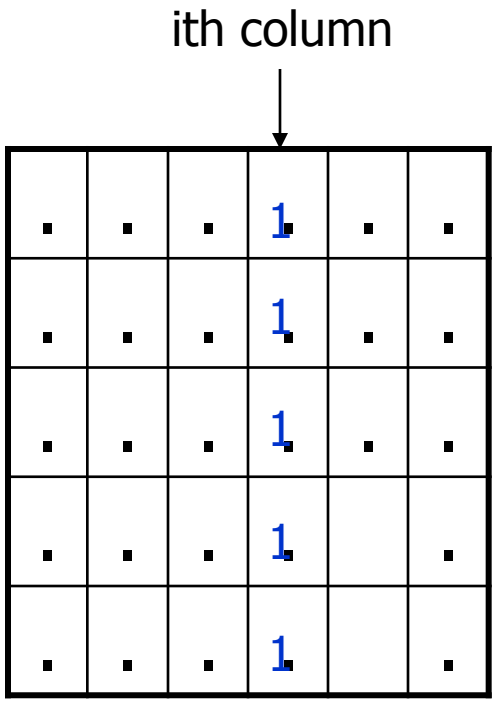
Fact: $L^- = C_1 \cup \cdots \cup C_n$.

Fact: Each C_i is a rectangle.

Conclusion 1: L^- has a small *cover*.

Conclusion 2: For every distribution μ,

$$\mathrm{disc}_\mu(\mathrm{DISJ}) \geq \frac{1}{2n} - \frac{1}{2n^2}.$$



Corollary: Impossible to get $\omega(\log n)$ bounds for DISJ by direct DM.

Generalized Discrepancy

Lemma (Generalized Discrepancy): Denote $X = Y_1 \times \cdots \times Y_k$. Let $f: X \to \{1,-1\}$ and $g: X \to \{1,-1\}$ be such that $\mathrm{Corr}_\mu(f,g) \geq \delta$, for some distribution μ.

$$R_k^\epsilon(f) \geq \log\left(\frac{\delta+2\epsilon-1}{disc_{k,\mu}(g)}\right)$$

disc(g) << disc(f)

Remark: The classical discrepancy method follows by putting g=f and hence δ=1.

Klauck'01 applied to f = MAJ $\circ$ AND.

Composed Functions

Question: Given f, how to find g?

Answer: No general technique known.

For $f \circ q$, Sherstov'08 and Shi-Zhu'08 gave techniques for 2-party.

Polynomial Representation

Let V $\equiv$ {f | f:{0,1}^{n} $\rightarrow \mathbb{R}$}.

Observation: V is a vector space of dimension 2^n.

Defn: For each $S \subseteq$ {1,$\cdots$,n},

$$\chi_S = (-1)^{\sum_{i \in S} x_i}.$$

Fact: The set M $\equiv \{\chi_S \mid S \subseteq$[{1,$\cdots$,n} forms a basis of V, called the Fourier basis.

Definition: Let f= $\sum_S c_S \chi_S$. The degree of f is the cardinality of a maximal S such that $c_S \neq 0$.

Approximation of Functions

Fundamental: How closely can f:{0, 1}$^n \to \mathbb{R}$ be approximated by low degree functions?

Definition: The δ-approximate degree of f, deg$_\delta(f)$, is the minimum integer d such that there exists $\phi \in$ span($\{\chi_S : |S| \leq$ d$\}$) and

$$\max_{x \in \{0,1\}^n} \left| f(x) - \phi(x) \right| \leq \delta$$

Degree of Functions

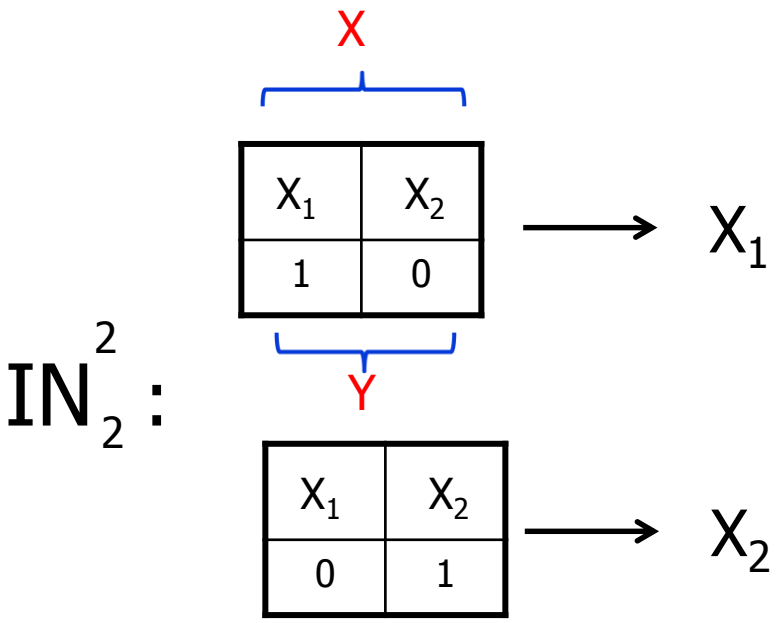
- AND(X) = $X_1 X_2 \cdots X_n$
- OR(X) = $1 - (1-X_1)(1-X_2)\cdots(1-X_n)$
- PARITY(X)
- MAJORITY(X)

Exact degree Θ(n)

Approx degree?

Fact (Nisan-Szegedy'92): $\mathrm{Deg}_{1/3}(\mathrm{OR}) = \Theta(\sqrt{n})$

Pattern Matrix Method



Let f have high approximation degree d.

Let q:$\{0,1\}^s \times \{0,1\}^s \to \{0,1\}$ have IN as a sub-(partial)function.

For $f \circ q$, Sherstov'08 applied Generalized-Discrepancy :

$$R_2^{\epsilon}(f \circ g) = \Omega(d)$$

Pattern Tensor Method

$$\mathrm{IN}_k^t : \underbrace{X}_{\{0,1\}^{t^k}} \times \underbrace{Y_1 \times \cdots \times Y_k}_{[k] \quad\quad [k]} \to \underbrace{\{0,1\}}_{X[y_1,\ldots,y_k]}$$

Indices into tensor

f : $\{0,1\}^m \to \{0,1\}$, approximation degree d.

q: $\{0,1\}^{sk} \to \{0,1\}$, contains IN_k^t.

Lee-Shraibman'08 and C-Ada'08 applied Generalized-Discrepancy :

$$R_k^{\epsilon}(f \circ q) = \Omega\left(\frac{d}{2^k}\right) \longrightarrow \Omega\left(\frac{n}{2^k 2^{2k}}\right)^{\frac{1}{k+1}}$$

provided $t \approx \frac{2^{2^k} km}{d}$

doubly exp in k

constant k, $n^{\Omega(1)}$

Block-Composition

Introduced by Shi-Zhu'08 for 2-party.

$f : \{0,1\}^m \to \{0,1\}$, approximation degree d. } same property as before

$q : \{0,1\}^s \times \{0,1\}^s \to \{0,1\}$. } spectral (analytic) property

$f \circ q$: Generalized-Discrepancy gives strong 2-party bounds.

How to extend to $k \geq 3$ parties?

Discrepancy Amplification

$q : \{0,1\}^{(k+1)\times t} \to \{0,1\}$.

ν : q is ν-balanced.

Defn: q is (γ,ν)-amplifiable if for all $S \subseteq [m]$:

$$\mathrm{disc}_{\nu^{|S|}}\left(\chi_S \circ q\right) \leq \gamma^{|S|}$$

Multiparty Block Composition

$f : \{0,1\}^m \to \{0,1\}$, approximation degree d. } same property as before

$q : \{0,1\}^{(k+1)\times s} \to \{0,1\}$. } **q is ν-balanced and (γ,ν)-amplifiable**

Theorem(C'08): If $\gamma \leq \frac{d}{8em}$,

$$R_k^{\epsilon}(f \circ q) = \Omega(d)$$

Proof

- Approximation-Orthogonality
- Simple Fourier Analysis

Approximation-Orthogonality

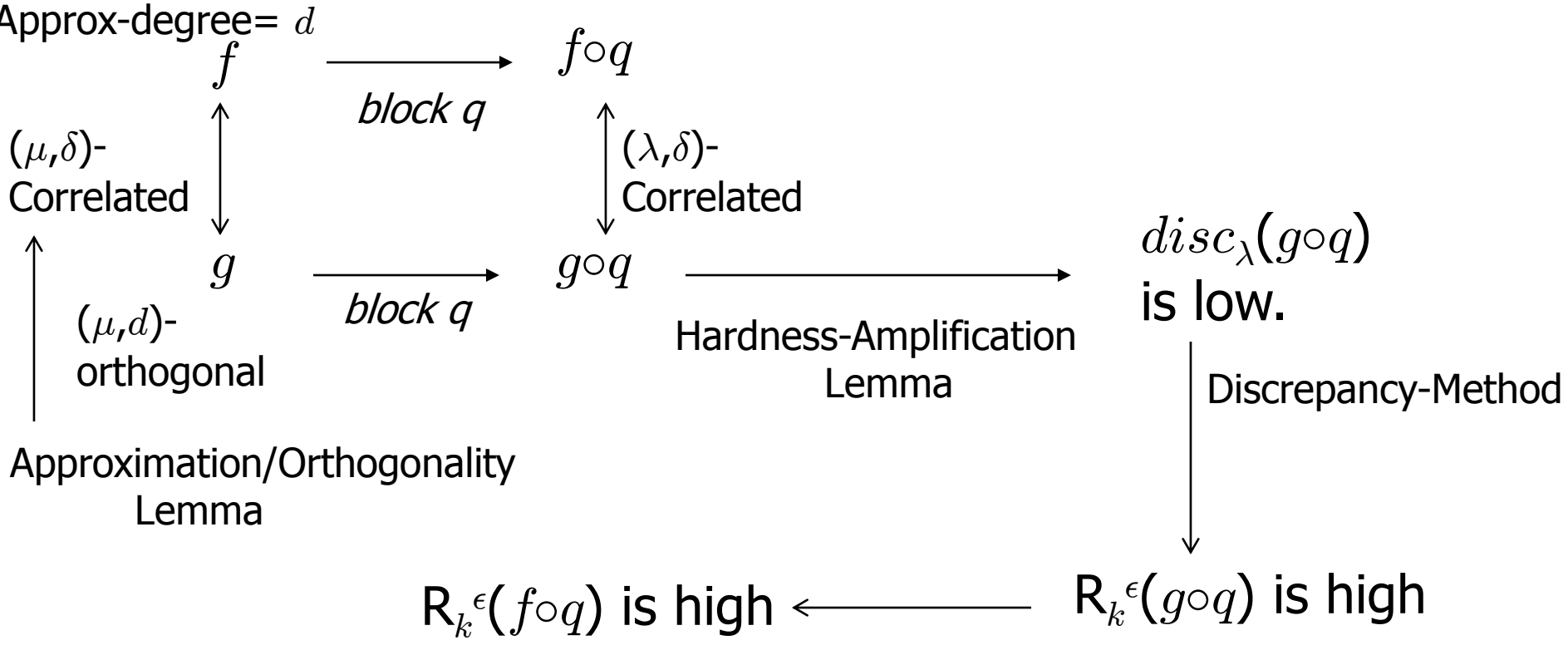
Lemma (Sherstov08, Shi-Zhu08): Let f:{0,1}$^m \to$ {-1, 1} have deg$_\delta(f)$ = d $\geq$ 1. Then, there exists a g:{0,1}$^m \to$ {-1,1} and a distribution μ such that

$$\mathrm{Corr}_\mu(f,g) = \mathbb{E}_{x\sim\mu} f(x)g(x) > \delta$$

and g is (μ,d)-orthogonal, i.e.

$$\mathrm{Corr}_\mu(g,\chi_S) = 0, \forall |S| < d.$$

Block Communication Strategy



Fact (NS'92): $\mathrm{Deg}_{1/3}(\mathrm{OR}) = \Omega(\sqrt{m})$.

The Inner Function

Question: How do we find such nice q?

Try bounding $\mathcal{E}_{\nu,k}(q)^{1/2^k}$

Theorem (C'08):

$$\mathrm{disc}_{\nu^{|S|},k+1}(\chi_S \circ q) \leq \left(\mathcal{E}_{\nu,k}(q)\right)^{|S|/2^k}$$

Theorem (C'08):

$$\mathcal{E}_{\mathcal{U},k}\left(\mathrm{IN}_k^t\right) \leq \frac{k}{t}$$

Two-Party Communication

Multiparty Block Composition

$f : \{0,1\}^m \to \{0,1\}$, approximation degree d. } same property as before

$g : \{0,1\}^{k \times s} \to \{0,1\}$. } small cube-measure $\mathcal{E}_{\mu,k}(g) \leq \gamma$

g is μ-balanced

Theorem(C'08): If $\gamma \leq \left(\frac{d}{8em}\right)^{2^k}$,

$$R_k^{\epsilon}(f \circ g) = \Omega(d)$$

Disjointness as Inner Function

NOR : $\{0,1\}^m \to \{0,1\}$, approximation degree d = $\sqrt{m}$.

UDISJ_s : $\{0,1\}^{(k+1)\times s} \to \{0,1\}$.

$\mu_{k,s}$: uniform distrbn on k × s matrices with exactly one all-1 column

$\mathcal{U}_s$: uniform distrbn on $\{0,1\}^s$

$\lambda_{k,s} : \mathcal{U}_s \times \mu_{k,s}$

NON-Prod distrbn $\mu_{k,s}$

$\mathcal{U}_s$	x_1	x_2	.	x_i	.	x_s
	0	.	.	1	.	.
	.	.	.	1	.	0
	.	0	.	1	0	.
	.	.	0	1	.	.

Theorem(Sherstov'12):

$$R_k^{\epsilon}(\text{NOR} \circ \text{UDISJ}) = \Omega\left(\frac{n}{4^k}\right)^{1/4}$$

$$n = sm$$

Recent Breakthrough

Theorem(Sherstov'13): Using more analytic technique:

$$R_k^{\epsilon}\left(\mathrm{NOR} \circ \mathrm{UDISJ}\right) = \Omega\left(\frac{\sqrt{n}}{k2^k}\right)$$

Rao-Yehudayoff'14: Simplify above. Show further

$$D_k^{\epsilon}\left(\mathrm{NOR} \circ \mathrm{UDISJ}\right) = \Omega\left(\frac{n}{4^k}\right)$$

Tight!

Conclusion

Did not cover MANY developments.

Several open directions to pursue.

Thanks!