LIFTING VIA SUNFLOWERS

Toniann Pitassi

U. Toronto and

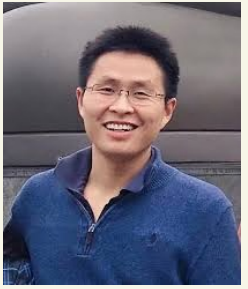
IAS

In Collaboration With :

Shachar Lovett
UCSD

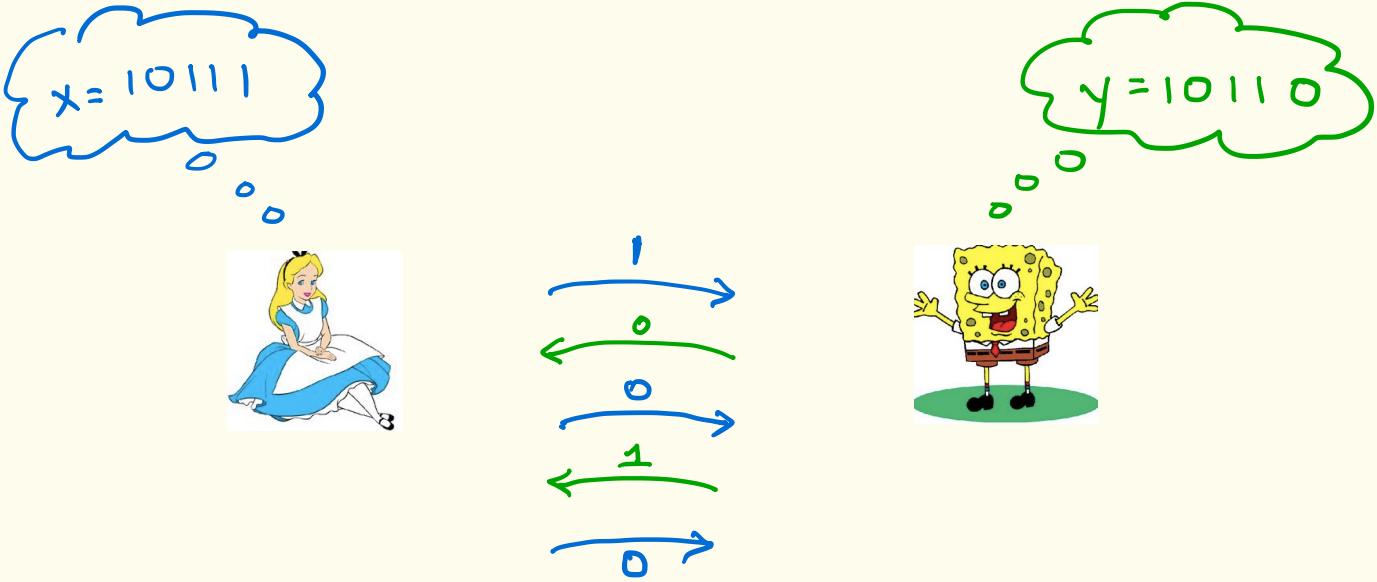
Ian Mertz
U Toronto

Raghu Meka
UCLA



Jiapeng Zhang
USC

Communication complexity (Yao '79)

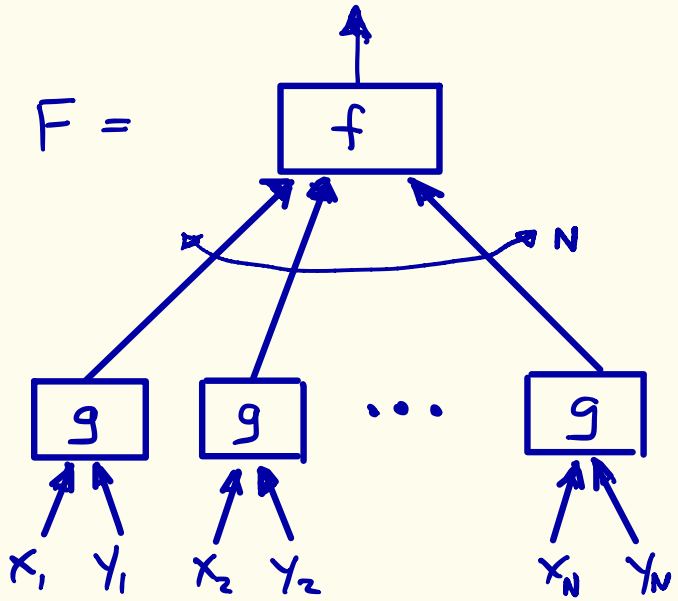


$$f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

$$cc(f) = \min_{\pi \text{ computing } f} cc(\pi)$$

QUERY TO COMMUNICATION LIFTING

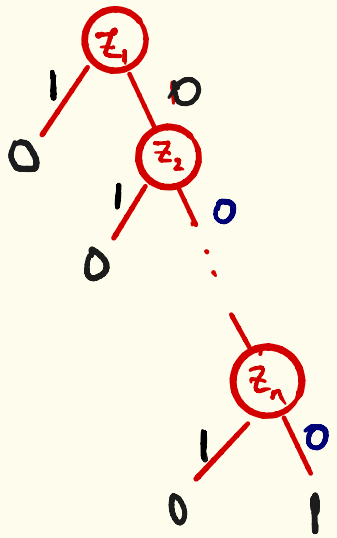
$f : \{0,1\}^N \to \{0,1\}$ $\rightsquigarrow$ $F =$

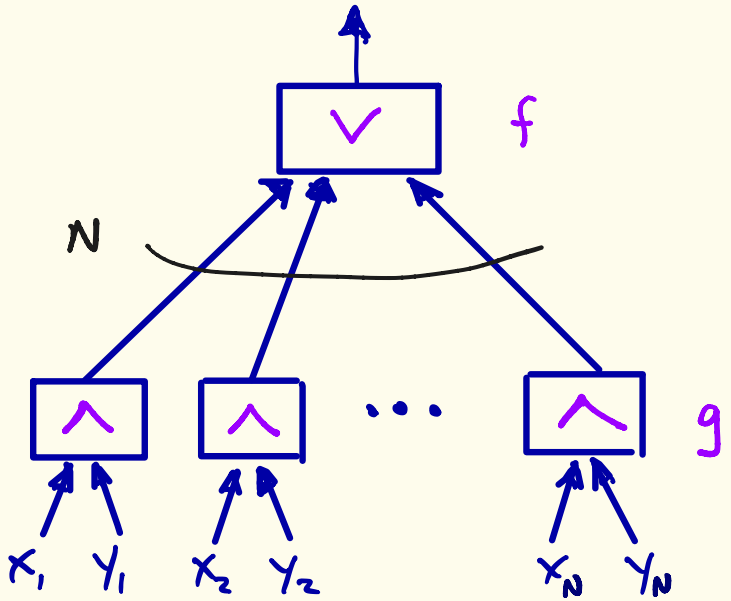


Lifting Theorem

Query complexity of f $\approx$ Communication Complexity of $F = f \circ g^N$

EXAMPLE: SET DISJOINTNESS





$DT(f) = \Theta(N)$

$CC(f \circ g^N) = \Theta(N)$

SOME LIFTING THEOREMS

	CC Model	Query Model
Raz-Mckenzie '99	Determinstic CC	Dec Tree
Razborov '03	Quantum CC	approx Degree
Sherstov '07	discrepancy, sign rank	Threshold degree
gLMWZ '15	Nondet CC	approx Junta degree
LRS '15	semidefinite Rank	SOS degree
KMR '16	NonNeg Rank	Junta degree
P-Robere '17	algebraic Tiling	Nullstellensatz degree
göös-P-Watson '17	Randomized CC	Randomized dec trees

Lifting Makes Lower Bounds Easy!

2 Steps

- Prove Query Lower bound
- Apply Lifting to get CC lower boun

Applications of Lifting

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

Using Communication Complexity to Prove Formula Size Lower Bounds

THEOREM [KW]

FORMULA-SIZE(f) is equal to the communication complexity of KW_f^{cc}

THEOREM (monotone version) f monotone

Monotone-FORMULA-SIZE(f) is equal to the cc of monotone-KW_f^{cc} (find i such that $x_i > y_i$)

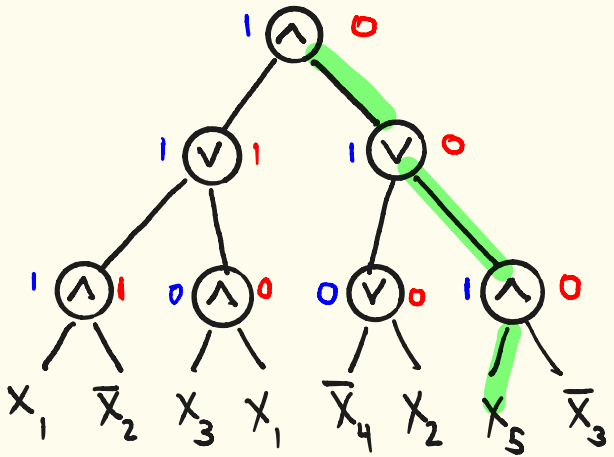
* Also a dag-like version of cc $\approx$ circuit size

KARCHMER-WIGDERSON GAME KW_f^{cc}

Alice gets $x \in f^{-1}(1)$ Bob gets $y \in f^{-1}(0)$

FIND i SUCH THAT $x_i \neq y_i$

$x = 10011$



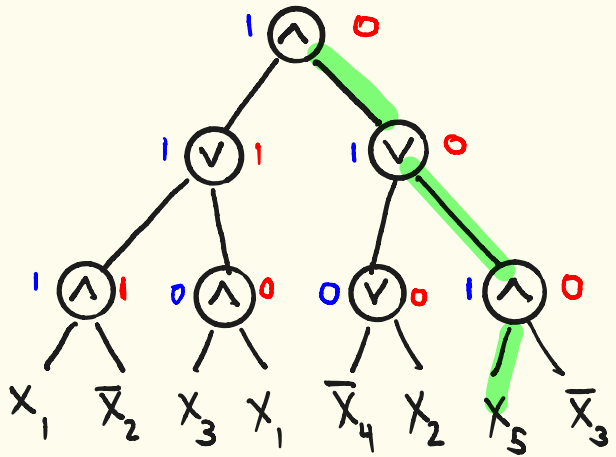
$y = 10010$

Monotone KARCHMER-WIGDERSON GAME KW_f^{cc}

Alice gets $x \in f^{-1}(1)$ Bob gets $y \in f^{-1}(0)$

FIND i SUCH THAT $x_i > y_i$

$x = 10011$

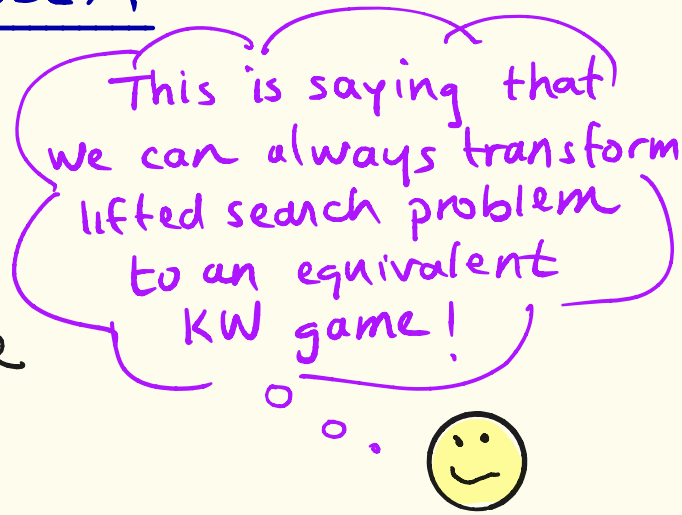


$y = 10010$

LIFTED SEARCH PROBLEM

Search($\mathcal{C} \circ g^n$):

Alice gets x
Bob gets y
Find a falsified clause



Theorem [göös-P]

For any unsatisfiable boolean formula $\mathcal{C}$ there is a Boolean function $F_{\mathcal{C}}$ such that monotone KW game for $F_{\mathcal{C}}$ equals Search($\mathcal{C} \circ g^n$)

Examples

1. C = Tseitin formula

   $Search(C \circ g^N)$ ≡ KW game for Clique / Monotone kCSP

2. C = Pebbling($\not\Delta$)

   $Search(C \circ g^N)$ ≡ KW game for STCONN, GEN

TODAY: SIMPLER PROOF USING SUNFLOWERS

f: N-bit boolean function / search problem

g: index gadget $\mathrm{IND}(x, y) = y_x$ $\quad |y| = N^{10}$ $\quad |x| = 10 \log N$

Theorem 1 (Deterministic Lifting) [RM, GPW]

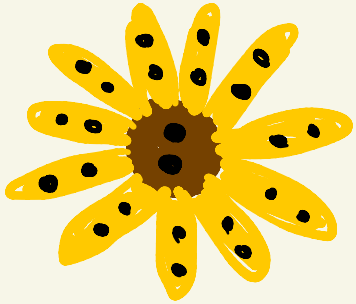
$$DT(f) \cdot \Theta(\log N) = CC(f \circ g^N)$$

Theorem 2 (DAG-Lifting)

$$\mathrm{width}(f) \cdot \Theta \log(N) = \log\left(\text{DAG-cc}(f \circ g^N)\right)$$

* We improve gadget size to $|y| = N^{11+\varepsilon}$

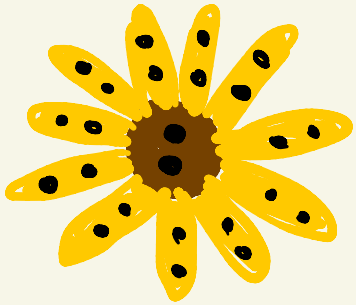
SUNFLOWER LEMMA



$K=4$, $p=11$

Let $\mathcal{X}$ be a k-uniform set system.
If $|\mathcal{X}| > r^k$ then $\mathcal{X}$ contains a sunflower with p petals.

SUNFLOWER LEMMA



$K=4$, $p=11$

Let $\mathcal{X}$ be a k-uniform set system over $\mathcal{U}$.
If $|\mathcal{X}| > r^k$ then $\mathcal{X}$ contains a sunflower with p petals.

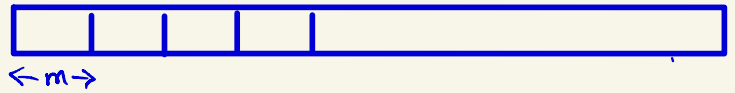
Old: True for $r \sim pk$

Conjecture: True for $r \sim p$

NEW: True for $r \sim p\log(pk)$ [ALWZ '19]

$|\mathcal{X}|$ large $\Rightarrow$  $\in \mathcal{X}$

WLOG $\mathcal{U} = [mN]$

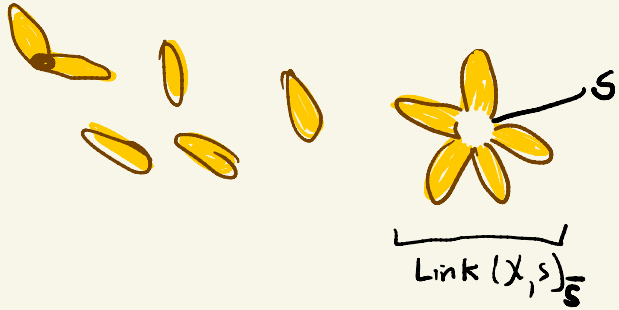


each $x \in \mathcal{X}$ contains at most one element per block

$\mathcal{X}$ is **r-spread** iff

$\forall I \subseteq [N] \quad \forall s \subseteq [m]^I$

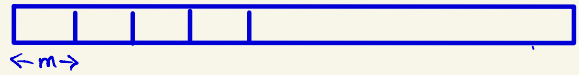
$$|\mathrm{Link}(\mathcal{X}, s)_{\bar{s}}| \leq |\mathcal{X}| / r^{|I|}$$



$|X|$ large $\Rightarrow$  $\in X$

$x \subset [m]^N$

WLOG $\mathcal{U} = [mN]$

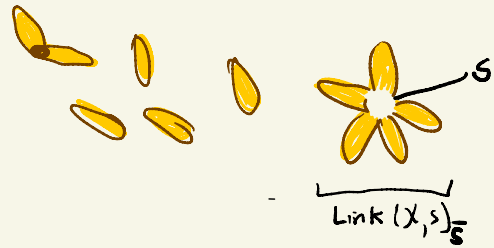


each $x \in X$ contains at most one element per block

X is **r-spread** iff

$\forall I \subseteq [N] \quad \forall s \subseteq [m]^I$

$|\text{Link}(X, s)_s| \leq |X| / r^{|I|}$



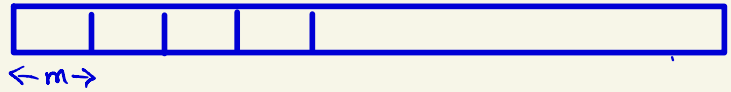
Equivalently X is **log r - dense**: $\forall I \subseteq [N] \quad H_\infty(X_I) \geq \log r \cdot |I|$

where $H_\infty(X) = \min_{x \in X} \log\left(\frac{1}{\Pr[X = x]}\right)$

$r = m^{.9}$: minentropy of $X_I \geq .9\,|I| \log m$ (little info known about X_I)

$|X|$ large $\Rightarrow$  $\in X$

WLOG $\mathcal{U} = [mN]$

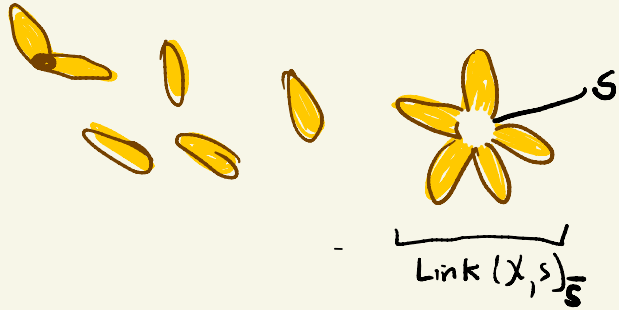


each $x \in X$ contains at most one element per block

X is r-spread iff

$\forall I \subseteq [N] \quad \forall s \subseteq [m]^I$

$|\,\mathrm{Link}(X,s)_{\bar{s}}\,| \leq |X|/r^{|I|}$



Lemma X r-spread $\Rightarrow$ X contains $p = r/N$ disjoint sets

Robust Sunflowers (Rossman)

Let $\mathcal{X}$ be a set system over $\mathcal{U}$

$\mathcal{X}$ is $(\frac{1}{2}, \varepsilon)$-satisfying if:

$$\Pr_{Y \subseteq_{\frac{1}{2}} \mathcal{U}} [\forall x \in \mathcal{X} \; x \not\subseteq Y] \leq \varepsilon$$

$X_{DNF} = x_1 x_7 x_9 \vee x_3 x_4 x_8 \vee x_2 x_6 x_8$

Y: random vector in $\{0,1\}^{|\mathcal{U}|}$, $\Pr[Y_i = 1] = \frac{1}{2}$

Then $\Pr_Y [X_{DNF}(Y) \neq 1] \leq \varepsilon$

Robust Sunflowers

Let $\mathcal{X}$ be a set system over $\mathcal{U}$

$\mathcal{X}$ is $(\frac{1}{2}, \varepsilon)$-satisfying if:

$$\Pr_{Y \subseteq_{\frac{1}{2}} \mathcal{U}} [\forall x \in \mathcal{X} \; x \not\subseteq Y] \leq \varepsilon$$

$X_{DNF} = x_1 x_7 x_9 \vee x_3 x_4 x_8 \vee x_2 x_6 x_8$

Y: random vector in $\{0,1\}^{|\mathcal{U}|}$, $\Pr[Y_i = 1] = \frac{1}{2}$

Then $\Pr_Y [X_{DNF}(Y) \neq 1] \leq \varepsilon$

Theorem [ALWS] Let $\mathcal{X}$ be r-spread, $r = c \log(\frac{M}{\varepsilon})$. Then

$$\Pr [X_{DNF}(Y) \neq 1] \leq \varepsilon$$

↖ true even for nonmonotone DNF

Robust Sunflowers

Let $\mathcal{X}$ be a set system over $\mathcal{U}$

$\mathcal{X}$ is $(\frac{1}{2}, \varepsilon)$-satisfying if:

$$\Pr_{Y \subseteq_{\frac{1}{2}} \mathcal{U}} [\forall x \in \mathcal{X} \; x \not\subseteq Y] \leq \varepsilon$$

$X_{DNF} = x_1 x_7 x_9 \vee x_3 x_4 x_8 \vee x_2 x_6 x_8$

Y: random vector in $\{0,1\}^{|\mathcal{U}|}$, $\Pr[Y_i = 1] = \frac{1}{2}$

Then $\Pr_Y [X_{DNF}(Y) \neq 1] \leq \varepsilon$

Theorem [ALWS] Let $\mathcal{X}$ be r-spread, $r \geq c \log(\frac{N}{\varepsilon})$. Then:

$$\Pr_Y [X_{DNF}(Y) \neq 1] \leq \varepsilon$$

Parameters: $\mathcal{X} \subseteq [m]^N$, $m = N^{10}$, $r = m^{.9}$, $\varepsilon = 2^{-N^4}$

(exponential improvement when ε very small)

BACK TO LIFTING THEOREM

f: N-bit boolean function / search problem

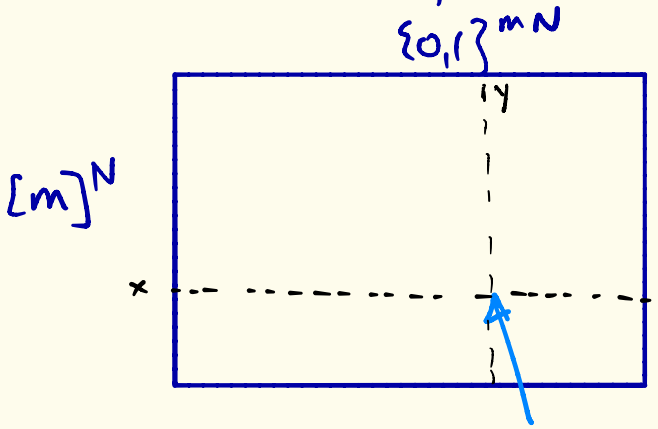
g: index gadget $\quad g(x,y) = y_x$

$|y| = N^{10} = m$, $|x| = 10 \log N$

Theorem 1 (Deterministic Lifting) [Raz, McKenzie, Göös, P, Watson]

$$DT(f) \cdot \Theta(\log N) = CC(f \circ g^N)$$

Let Π be a CC protocol for $f \circ IND^N$



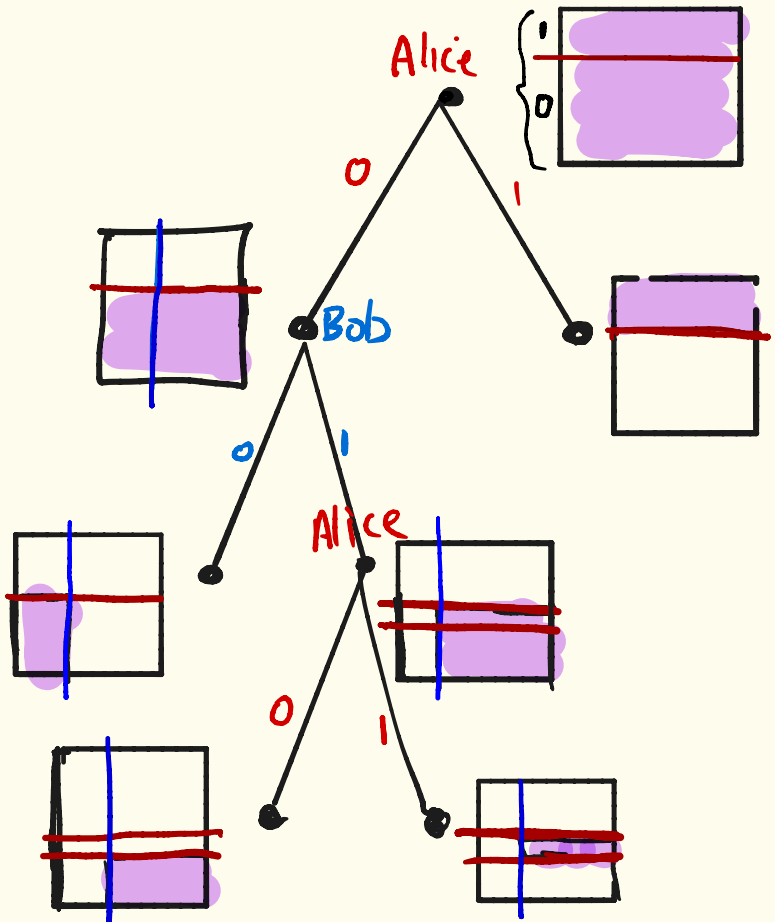
Communication matrix M

(x, y)-entry labelled by

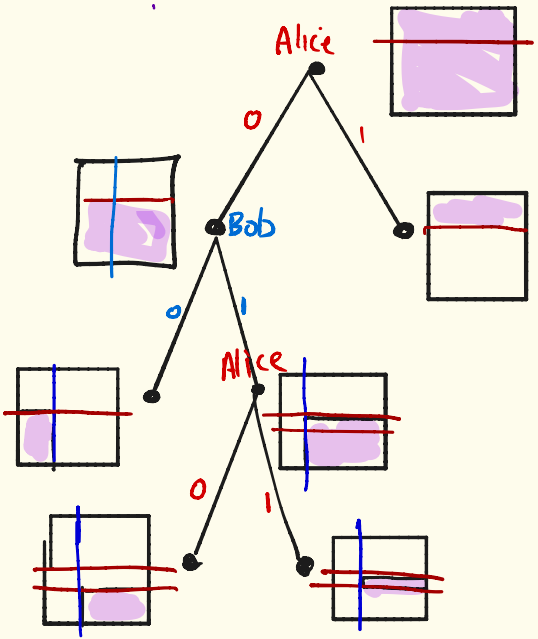
$z = IND(x_1, y_1), \ldots IND(x_N y_N)$

$\in \{0,1\}^N$

Protocol Π is a tree, partitions M into subrectangles



Protocol Π is a tree, partitions M into subrectangles



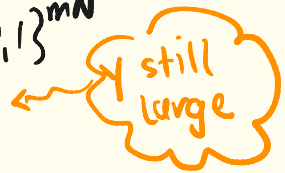
- each vertex v of tree labelled with a subrectangle $R_v = X_v \times Y_v$

given Π for $f \circ \text{IND}^N$ → construct decision tree T for f of depth $\sim \text{height}(\Pi) / \log N$

Simulation

Invariant : $X \times Y \subseteq [m]^N \times \{0,1\}^{mN}$
X is $.9 \log m$-dense
Y large : $|Y| \geq 2^{mN - n^2}$

- Initially (at root of π), $X = [m]^N$, $Y = \{0,1\}^{mN}$
- When Bob sends a bit, go to larger side
- When Alice sends a bit, go to larger side



If X no longer $.9 \log m$ dense :

- Find maximal subset $I \subseteq [N]$ and value $\alpha \in [m]^I$ that is too likely.
- Query variables $z_I = \{z_i, i \in I\}$ in T

Simulation

Invariant: $X \times Y \subseteq [m]^N \times \{0,1\}^{mN}$
X is $.9 \log m$-dense
Y large : $|Y| \geq 2^{mN - N^2}$

- Initially (at root of π), $X = [m]^N$, $Y = \{0,1\}^{mN}$
- When Bob sends a bit, go to larger side
- When Alice sends a bit, go to larger side

Y still large

If X no longer $.9 \log m$ dense:

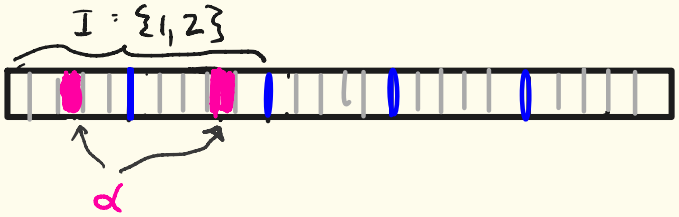
- Find maximal subset $I \subseteq [N]$ and value $\alpha \in [m]^I$ that is too likely.
- Query variables $z_I = \{x_i, i \in I\}$ in T. Say $z_I = \beta$
- This induces a refinement of $X \times Y$:

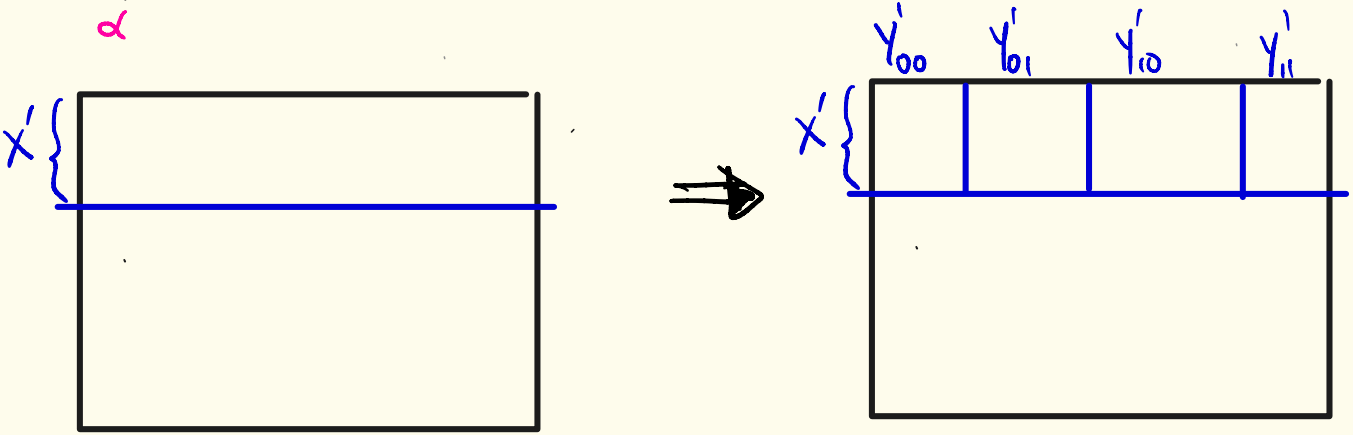
$$X' = \{x \in X \mid x_I = \alpha\}$$
$$Y'_\beta = \{y \in Y \mid \mathrm{IND}(\alpha, y_I) = \beta\}$$

Need to show invariant holds $\forall \beta \in \{0,1\}^{|I|}$

REFINEMENT (after querying Z_I)

X no longer .9 dense:



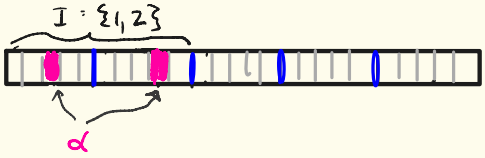


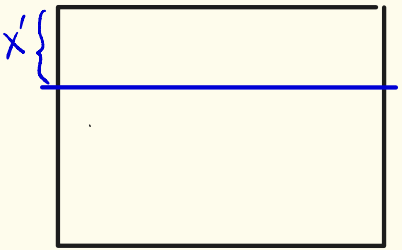
$X' = \{x \in X \mid x_I = \alpha\}$

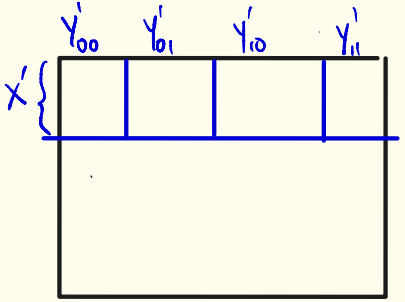
$Y'_B = \{y \in Y \mid IND^I(\alpha, y_I) = \beta\}$

REFINEMENT (after querying Z_I)

X no longer .9 dense:







$X' = \{x \in X \mid x_I = \alpha\}$

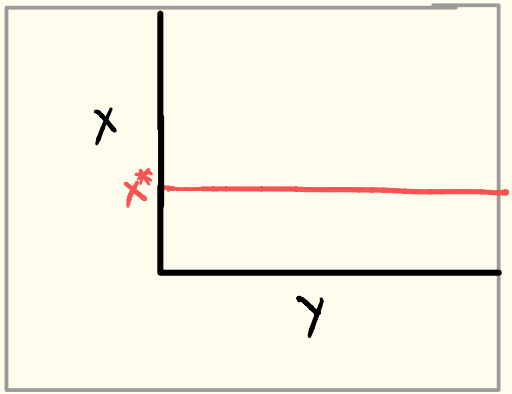
$Y'_\beta = \{y \in Y \mid IND^I(\alpha, Y_I) = \beta\}$

X' is $.9 \log m$-dense on the unfixed coordinates $[N] - I$

★ Need to show Y'_β is large

(otherwise decision tree T can err)

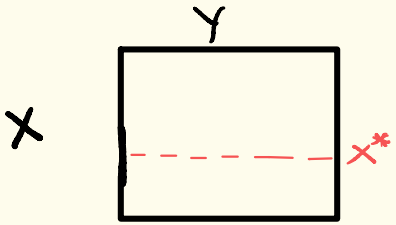
FULL RANGE LEMMA (via )



Let $X \subseteq [m]^N$ be $.9 \log m$-dense
$Y \subseteq \{0,1\}^{mN}$ be large

Then $\exists x^* \in X$ $\forall \beta \in \{0,1\}^N$ $\exists y^* \in Y$
$IND^N(x^*, y^*) = \beta$

FULL RANGE LEMMA (via )



X .9 log$m$ dense, Y large ($|Y| \geq 2^{mN-N^2}$) $\Rightarrow$

$\exists x^* \in X \; \forall \beta \in \{0,1\}^N \; \exists y_\beta \in Y : IND^N(x^*, y_\beta) = \beta$

Proof Assume $\forall x \; \exists \beta_x$ st $\forall y \in Y \quad IND^N(x,y) \neq \beta_x$

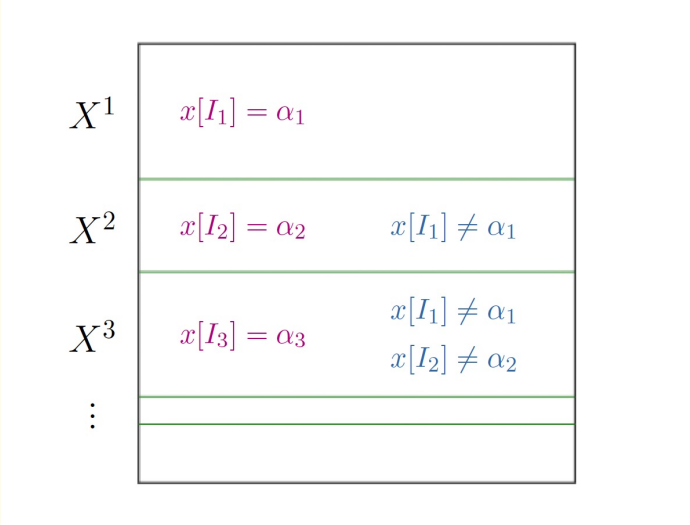
We can assume wlog that $\beta_x = 1^N$

By Robust sunflower lemma, at most $2^{-N^{\Omega}}$ fraction of all $y \in \{0,1\}^{mN}$ are bad.

This contradicts that Y is large. #

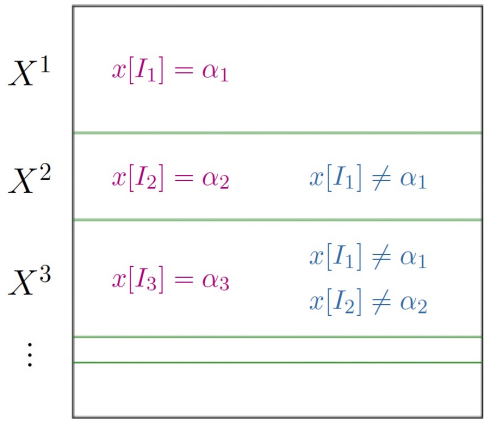
Extending Full Range Lemma to show all y^i_β are large

(Not hard)

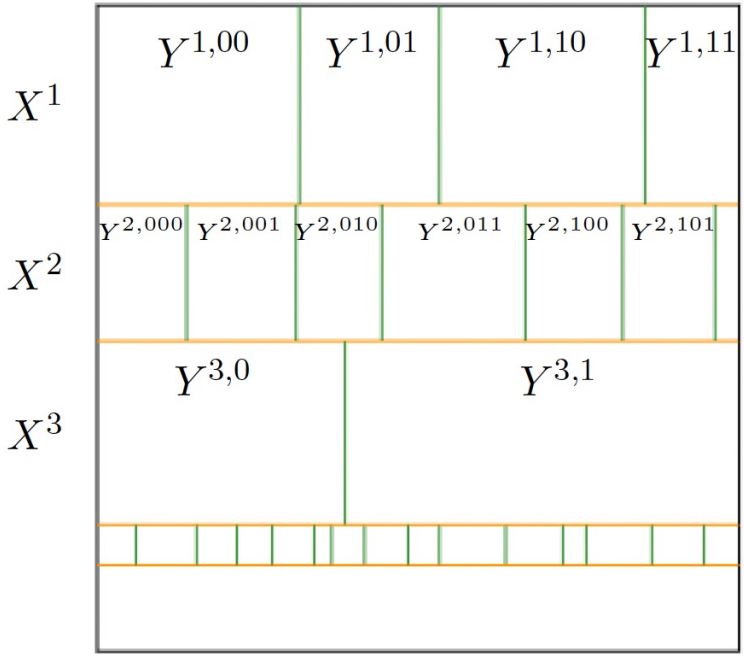


Partition all of X

Extending Full Range Lemma

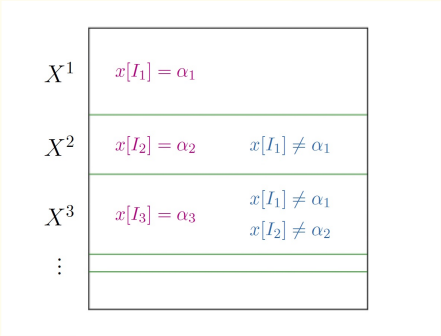


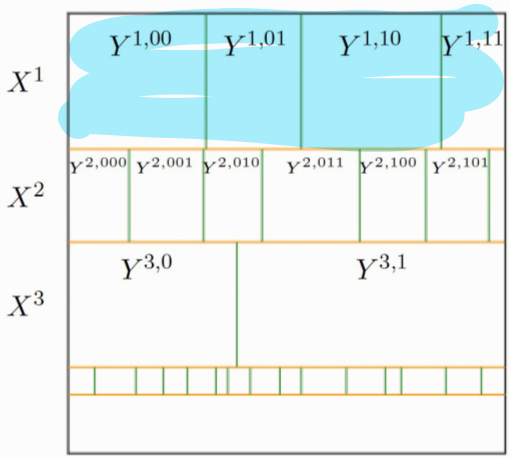
Partition all of X



Refinement of Y

Extending Full Range Lemma





$j = 1$

Theorem

$\exists j \quad \forall \beta \in \{0,1\}^{I_j}$

$Y^j_\beta = \{ y \in Y \mid IND(\alpha_j, Y_{I_j}) = \beta \}$ is large

Proof Sketch

- Assume for contradiction $\forall j \; \exists \beta_j$

$$Y_\beta^j = \{ y \in Y \mid IND(\alpha_j, Y_{I_j}) = \beta_j \} \text{ is small}$$

- $Y_{BAD} = \{ y \in Y \mid \exists j \; IND(\alpha_j, Y_{I_j}) = \beta_j \}$
- $|Y_{BAD}| < |Y|/2$ since Y is large
- Apply Full Range Lemma to $Y - Y_{BAD}$ and X to get contradiction

OPEN PROBLEMS

- Nonmonotone Lower Bounds (KRW conjecture)
- Constant-sized gadgets ?

OPEN PROBLEMS

- Nonmonotone Lower Bounds
  (KRW conjecture)

- Constant-sized gadgets ?

Conjecture $\exists c\ \forall m$ suff large:

X over $[m]^N$, Y over $\{0,1\}^{mN}$,

each entropy deficiency $\leq \Delta$.

then $\exists I \subseteq [N]$, $|I| \leq c\Delta$, $\alpha \in \{0,1\}^I$ s.t.

$\forall z \in \{0,1\}^N$ with $z_I = \alpha$ $\quad \Pr_{X,Y}[IND^N(X,Y) = z] > 0$

$IND^N(X,Y)$ contains subcube of codimension $c\Delta$