

LIFTING VIA SUNFLOWERS

Toniann Pitassi

U. Toronto and

IAS



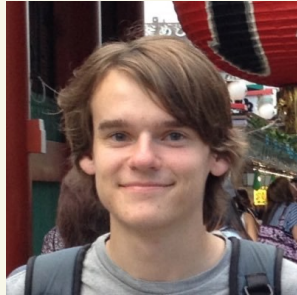
In collaboration With :



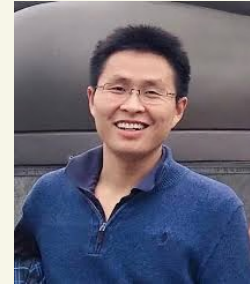
Shochar Lovett
UCSD



Raghu Meka
UCLA



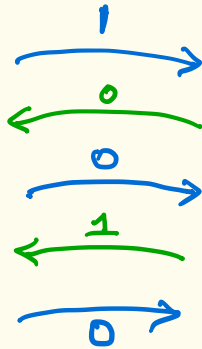
Ian Mertz
U Toronto



Jiaipeng Zhang
USC

Communication Complexity (Yao '79)

$x = 10111$



$y = 10110$



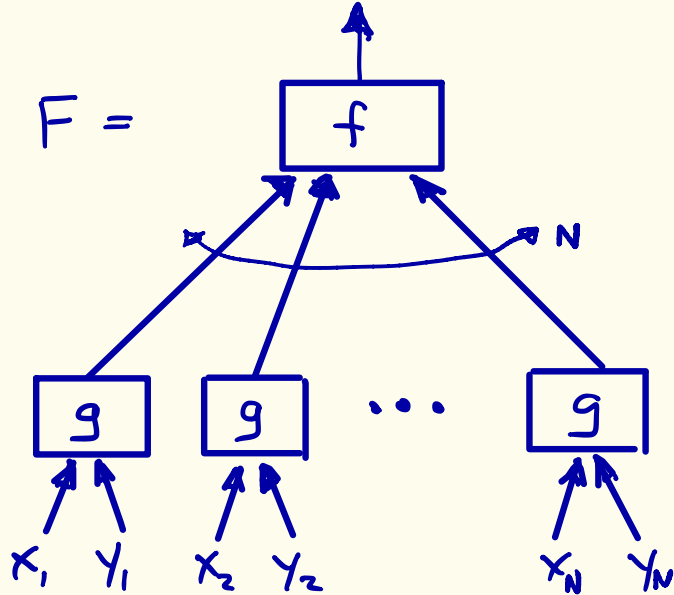
$$f: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$$

$$CC(f) = \min_{\Pi \text{ computing } f} CC(\Pi)$$

QUERY TO COMMUNICATION LIFTING

$$f: \{0,1\}^N \rightarrow \{0,1\}$$

$\rightsquigarrow F =$



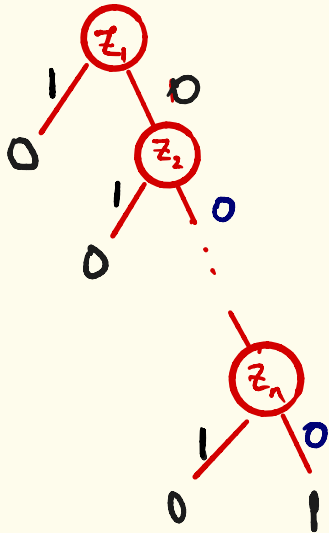
Lifting Theorem

Query Complexity
of f

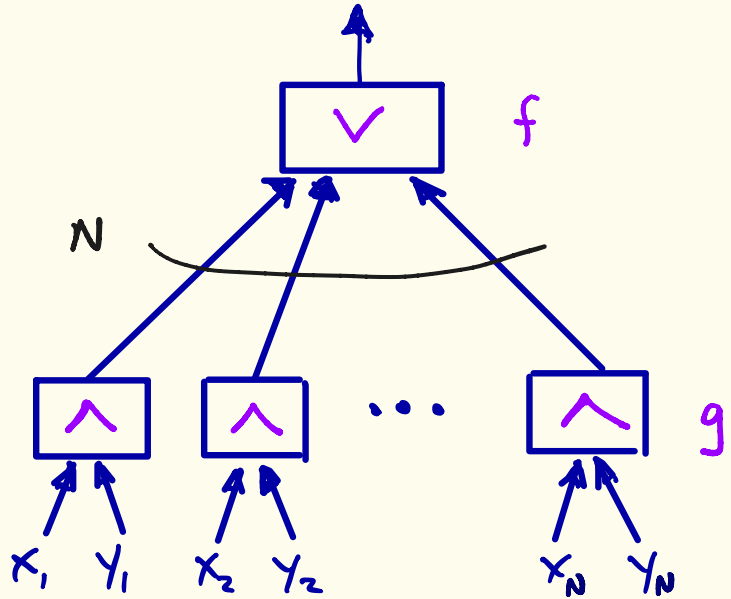
\approx

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 | Deterministic CC | Dec Tree |
| Razborov '03 | Quantum CC | approx Degree |
| Sherstov '07 | discrepancy, sign rank | Threshold degree |
| GLMWZ '15 | Nondet CC | approx Junta degree |
| LRS '15 | semidefinite Rank | SOS degree |
| 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 bound

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}

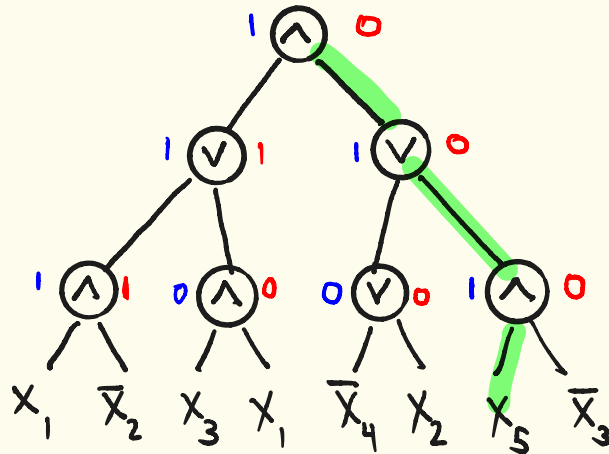
Alice gets $x \in f^{-1}(1)$

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

FIND i SUCH THAT $x_i \neq y_i$

$x = 10011$

$y = 10010$

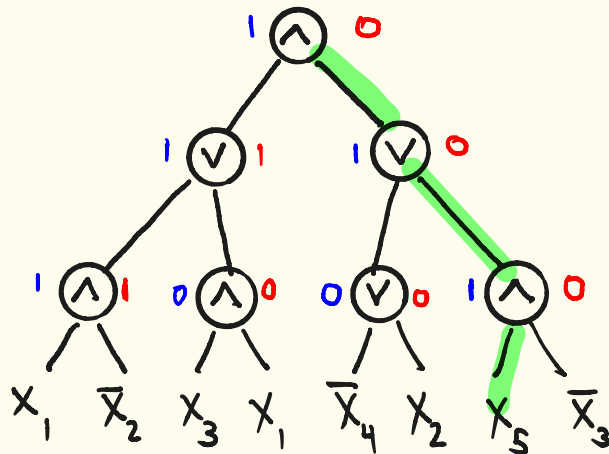


monotone KARCHMER-WIGDERSON GAME KW_f^{cc}

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

$$C = C_1 \wedge C_2 \wedge \dots \wedge C_m \quad \text{over } z_1, \dots, z_N$$

$S_C \subseteq \{0,1\}^N \times [m]$: given $d \in \{0,1\}^N$ output falsified clause

$$C \circ g^N : C_1 \wedge C_2 \wedge \dots \wedge C_m \left[g(x_i, y_i) / z_i \right] \quad \text{over } x_1, \dots, x_N, y_1, \dots, y_N$$

$S_{C \circ g^N}$: Alice: x_1, \dots, x_N Bob: y_1, \dots, y_N

output falsified constraint of $C \circ g^N$

LIFTED SEARCH \equiv monotone KW SEARCH

$f: \{0,1\}^N \rightarrow \{0,1\}$ monotone

monotone KW_f : Alice: $x \in f^{-1}(1)$ Bob: $y \in f^{-1}(0)$
Output $i \in [N]$ such that $x_i = 1$ $y_i = 0$

LIFTED SEARCH \equiv monotone KW SEARCH

$f: \{0,1\}^N \rightarrow \{0,1\}$ monotone

monotone KW_f : Alice: $x \in f^{-1}(1)$ Bob: $y \in f^{-1}(0)$
Output $i \in [N]$ such that $x_i = 1$ $y_i = 0$

THEOREM

Let $c = c_1 \wedge \dots \wedge c_m$ be an unsatisfiable CNF over z_1, \dots, z_N

Then \exists monotone F such that $S_{c \circ g^N} = CC(\text{monotone } KW_F)$

LIFTED SEARCH PROBLEM

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

Alice gets x

Bob gets y

Find a falsified clause

This is saying that
we can always transform
lifted search problem
to an equivalent
KW game!



Theorem [göös-P]

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

Examples

①. \mathcal{C} = Tseitin formula

Search($\mathcal{C} \circ g^N$) \equiv KW game for Clique / Monotone KCSP

②. \mathcal{C} = Pebbling (~~\mathcal{C}~~)

Search($\mathcal{C} \circ g^N$) \equiv KW game for STCONN, GEN

TODAY: SIMPLER PROOF USING SUNFLOWERS

f : N -bit boolean function / search problem

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

Theorem 1 (Deterministic Lifting) [RM, GPW]

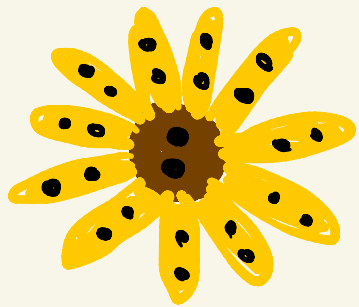
$$DT(f) \cdot \Theta(\log N) = CC(f \circ g^N)$$

Theorem 2 (DAG-Lifting)

$$\text{width}(f) \cdot \Theta \log(N) = \log(\text{DAG-CC}(f \circ g^N))$$

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

SUNFLOWER LEMMA

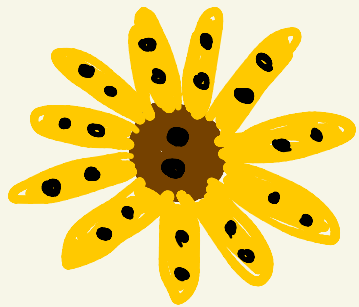


$k=4, p=11$

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



$k=4, p=11$

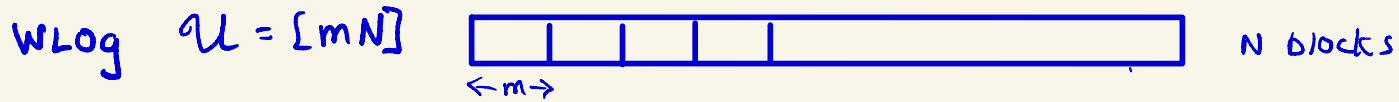
Let \mathcal{X} be a k -uniform set system over \mathcal{U}
If $|\mathcal{X}| > r^k$ then \mathcal{X} contains a sunflower
with p petals.

Old: True for $r \sim p^k$

Conjecture: True for $r \sim p$

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

$$|X| \text{ large} \Rightarrow \text{flower} \in X$$

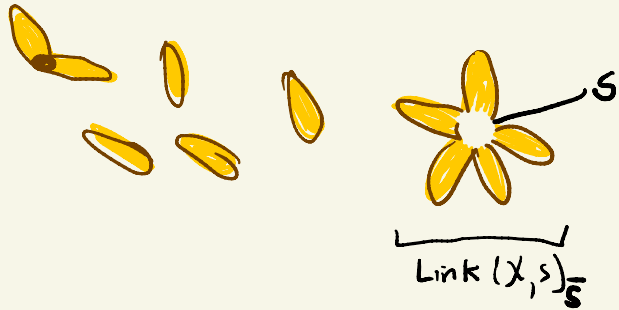


each $x \in X$ contains at most one element per block

X is r-spread iff

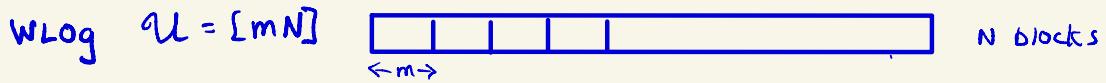
$$\forall I \subseteq [N] \quad \forall S \subseteq [m]^I$$

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



$$|X| \text{ large} \Rightarrow \text{flower} \in X$$

$$x \in [m]^N$$

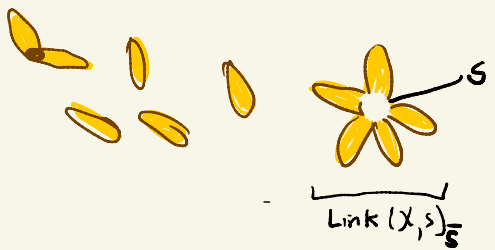


each $x \in X$ contains at most one element per block

X is r -spread iff

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

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

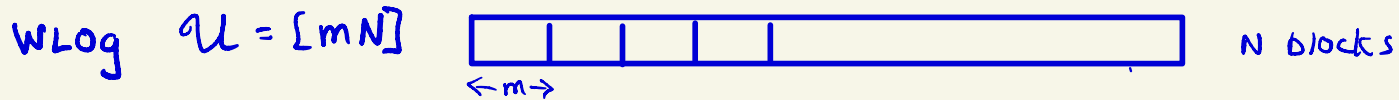


Equivalently X is $\log r$ -dense: $\forall I \subseteq [N] \quad H_\infty(X_I) \geq \log r \cdot |I|$

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)

$$|X| \text{ large} \Rightarrow \text{flower} \in X$$



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

X is r-spread iff

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

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



Lemma X r-spread $\Rightarrow X$ contains $p = \frac{r}{N}$ disjoint sets

Robust Sunflowers

(Rossman)

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

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

$$\Pr_{y \in \frac{1}{2}\mathcal{U}} [\forall x \in \mathcal{X} \quad x \not\subseteq y] \leq \epsilon$$

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

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

$$\text{Then } \Pr_y [X_{DNF}(y) \neq 1] \leq \epsilon$$

Robust Sunflowers

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

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

$$\Pr_{\substack{y \subseteq \mathcal{U} \\ |y| = \frac{1}{2}}} [\forall x \in \mathcal{X} \quad x \not\subseteq y] \leq \epsilon$$

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

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

$$\text{Then } \Pr_y [X_{\text{DNF}}(y) \neq 1] \leq \epsilon$$

Theorem [ALWS] Let \mathcal{X} be r -spread, $r = \lceil \log(\frac{N}{\epsilon}) \rceil$. Then

$$\Pr [X_{\text{DNF}}(y) \neq 1] \leq \epsilon$$

↖ true even for nonmonotone DNF

Robust Sunflowers

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

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

$$\Pr_{\substack{y \subseteq \mathcal{U} \\ |y| = \frac{1}{2}}} [\forall x \in \mathcal{X} \quad x \not\subseteq y] \leq \epsilon$$

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

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

$$\text{Then } \Pr_y [X_{\text{DNF}}(y) \neq 1] \leq \epsilon$$

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

$$\Pr_y [X_{\text{DNF}}(y) \neq 1] \leq \epsilon$$

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

(exponential improvement when ϵ very small)

BACK TO

LIFTING THEOREM

f : N -bit boolean function / search problem

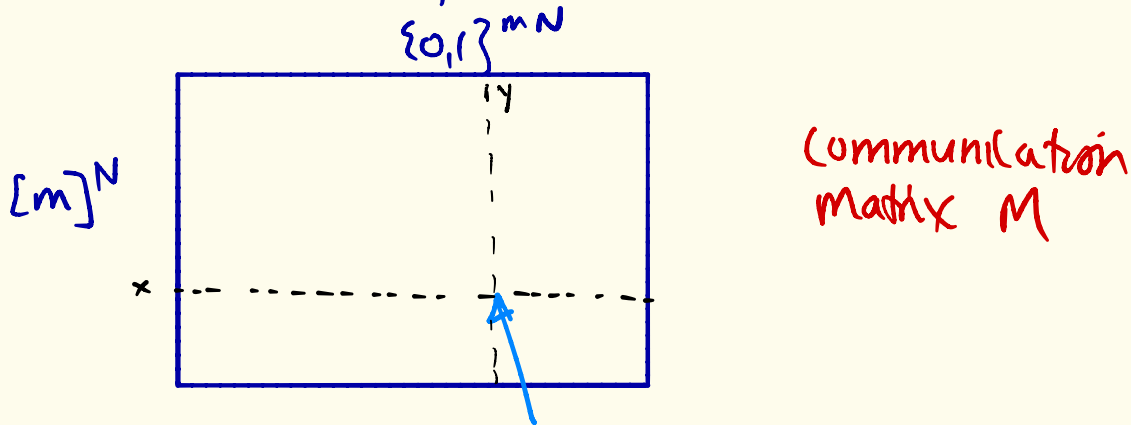
g : index gadget $g(x, y) = y_x$

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

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 $f \circ \text{IND}^N$

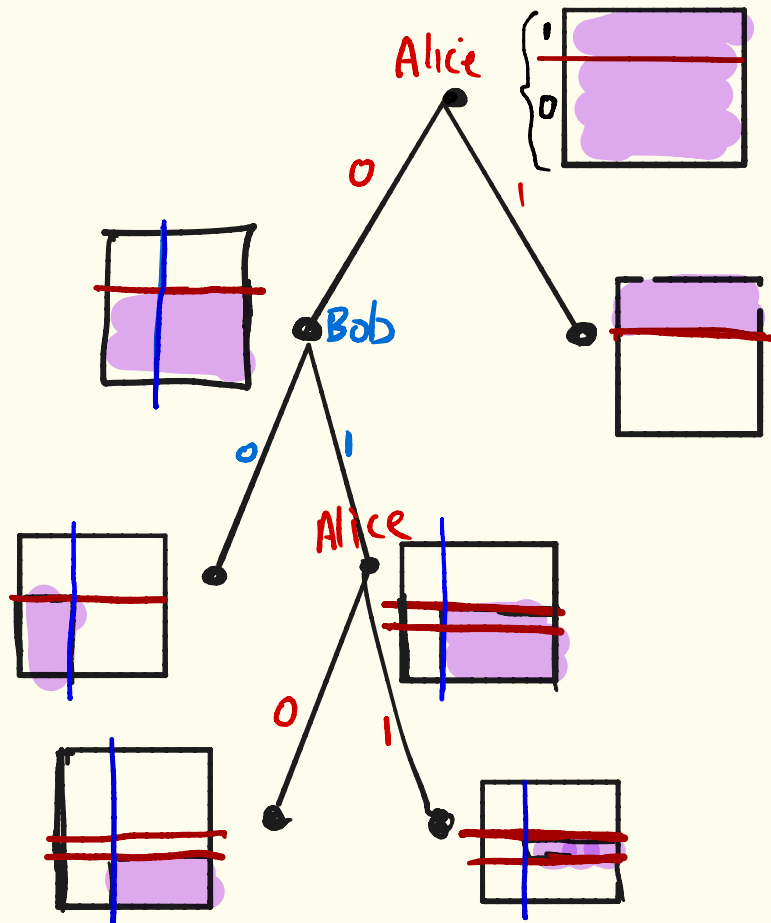


(x, y) -entry (labelled by

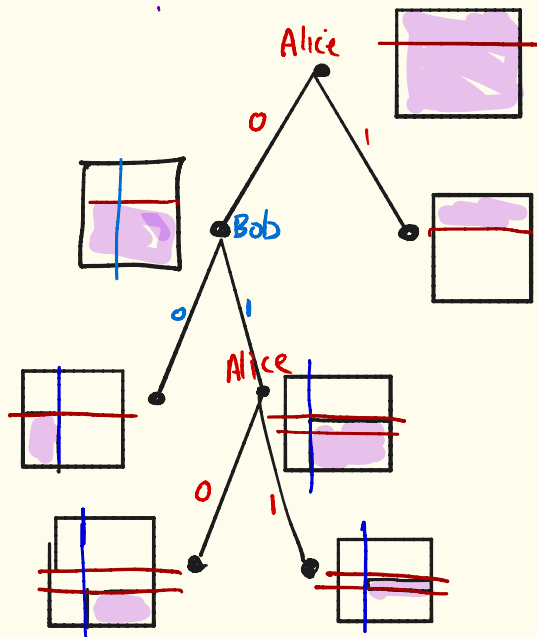
$$z = \text{IND}(x, y_1), \dots, \text{IND}(x_N, y_N)$$

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

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 $f \circ \text{IND}^N \rightarrow$ Construct decision tree T for f
of depth $\sim \text{height}(\Pi) / \log N$

Simulation

Invariant: $X \times Y = [m]^N \times \{0,1\}^{mN}$

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

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 $z_I = \{z_i, i \in I\}$ 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

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 $X \times Y$:

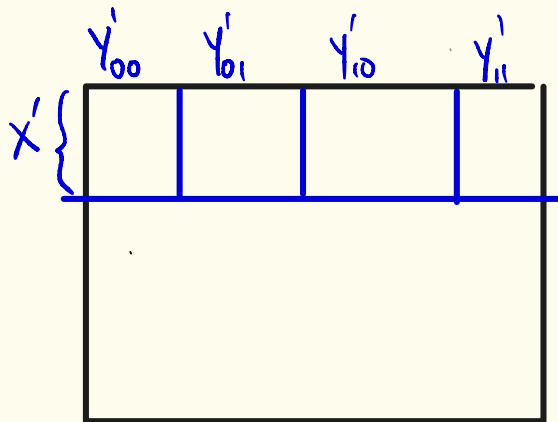
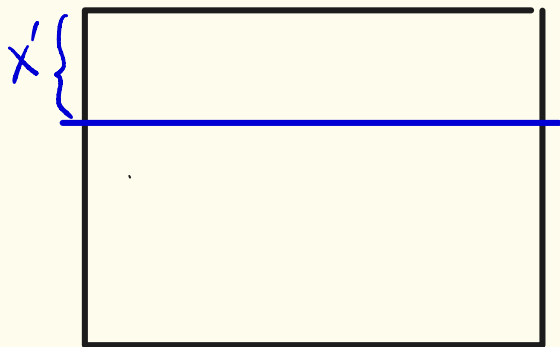
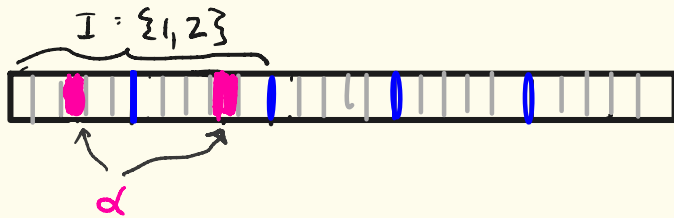
$$X' = \{x \in X \mid x_I = \alpha\}$$

$$Y'_\beta = \{y \in Y \mid \text{IND}(\alpha, y_I) = \beta\}$$

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

REFINEMENT (after querying Z_I)

X no longer .9 dense:

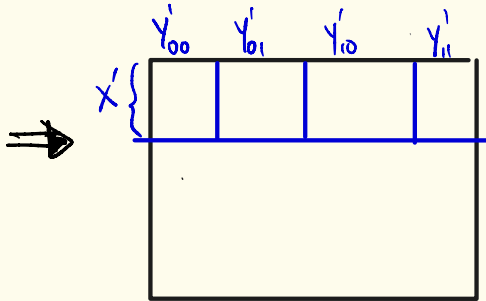
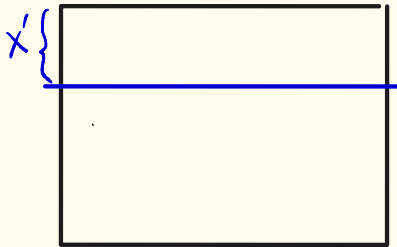
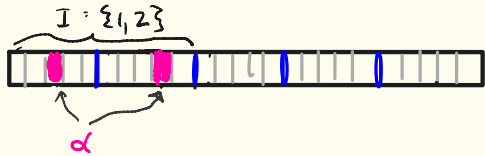


$$X' = \{x \in X \mid x_I = \alpha\}$$

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

REFINEMENT (after querying Z_I)

X no longer $.9$ dense:



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

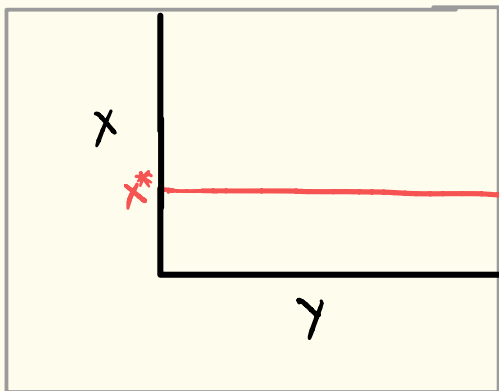
$$Y'_\beta = \{y \in Y \mid \text{IND}^I(\alpha, y_I) = \beta\}$$

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)

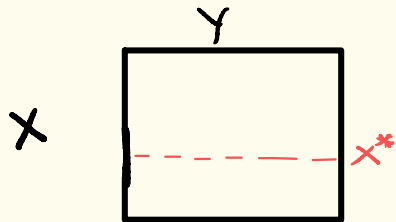
FULL RANGE LEMMA (via)



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

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

FULL RANGE LEMMA (via)



X .91 logm dense, Y large ($|Y| \geq 2^{mN - N^2}$) \Rightarrow

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

Proof Assume $\forall x \exists \beta_x$ st $\forall y \in Y \text{IND}^N(x, y) \neq \beta_x$

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

By Robust sunflower lemma, at most 2^{-N} 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^1 are large (Not hard)

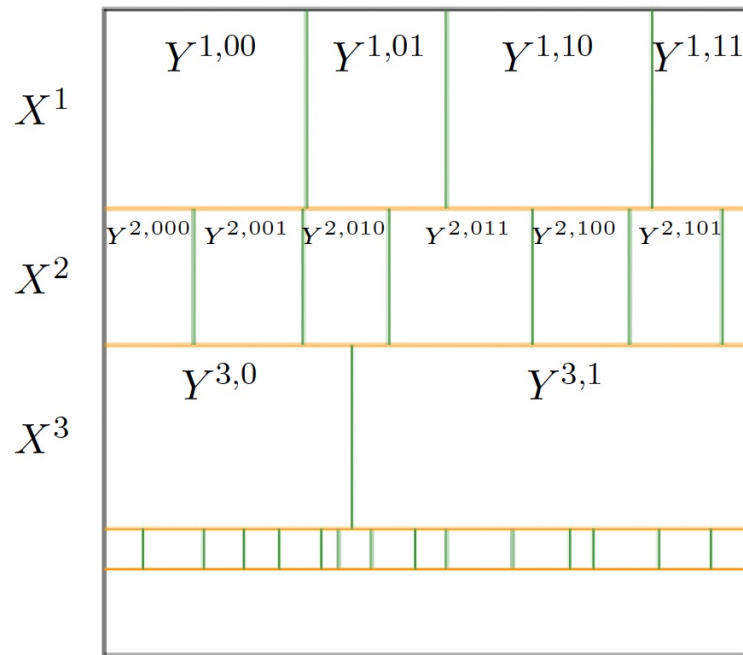
| | | |
|----------|---------------------|--|
| X^1 | $x[I_1] = \alpha_1$ | |
| X^2 | $x[I_2] = \alpha_2$ | $x[I_1] \neq \alpha_1$ |
| X^3 | $x[I_3] = \alpha_3$ | $x[I_1] \neq \alpha_1$ $x[I_2] \neq \alpha_2$ |
| \vdots | | |
| | | |

Partition all of X

Extending Full Range Lemma

| | | |
|----------|---------------------|--|
| X^1 | $x[I_1] = \alpha_1$ | |
| X^2 | $x[I_2] = \alpha_2$ | $x[I_1] \neq \alpha_1$ |
| X^3 | $x[I_3] = \alpha_3$ | $x[I_1] \neq \alpha_1$ $x[I_2] \neq \alpha_2$ |
| \vdots | | |

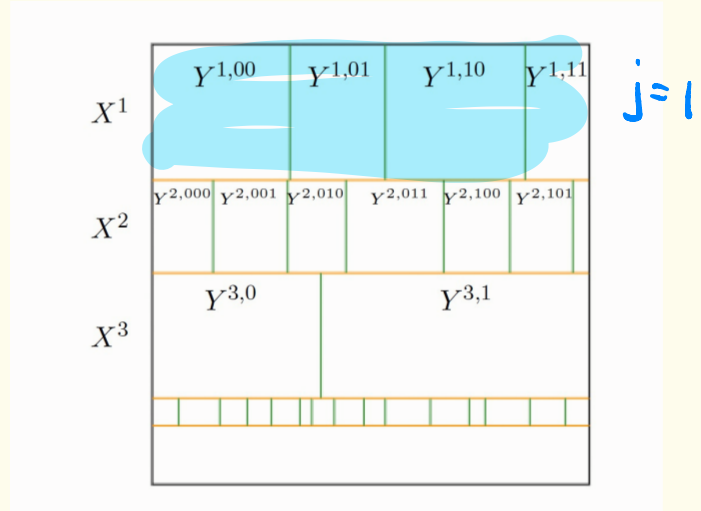
Partition all of x



Refinement of Y

Extending Full Range Lemma

| | | |
|----------|---------------------|--|
| X^1 | $x[I_1] = \alpha_1$ | |
| X^2 | $x[I_2] = \alpha_2$ | $x[I_1] \neq \alpha_1$ |
| X^3 | $x[I_3] = \alpha_3$ | $x[I_1] \neq \alpha_1$ $x[I_2] \neq \alpha_2$ |
| \vdots | | |



Theorem

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

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

Proof sketch

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

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

- $Y_{\text{BAD}} = \{y \in Y \mid \exists j \text{IND}(\alpha_j, Y_{I_j}) = \beta_j\}$

- $|Y_{\text{BAD}}| < |Y|/2$ since Y is large

- Apply Full Range Lemma to $Y - Y_{\text{BAD}}$ 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 $\exists I \subseteq [N]$, $|I| \leq c\Delta$, $\alpha \in \{0,1\}^I$ st.

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

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