Monotone Circuit Depth LBs : Putting it all together

Thm 1 [KW equivalence]

$$\text{mCktDepth}(F) = cc(\text{mKW}_F)$$

Thm 2 [Lifted CNF search $\equiv$ KW_F]

$$\text{Search}(\mathcal{C} \circ g^n) \equiv KW_{F_\mathcal{C}}$$ for an associated monotone $F_\mathcal{C}$

Thm 3 [Deterministic Lifting]

For any search problem (ie Search($\mathcal{C}$))

$$\text{Dec-Tree}(\text{Search}(\mathcal{C})) \simeq CC(\text{Search}(\mathcal{C} \circ g^n))$$

Thm 4 (LBs for Search($\mathcal{C}$))

There exist unsat kCNF $\mathcal{C}$ over $z_1 \dots z_n$ st. $\text{DecTree}(\text{Search}(\mathcal{C})) = \Omega(n)$

$DT(\text{Search}(\mathcal{C})) = \Omega(n)$ (Thm 4)

$CC(\text{search}(\mathcal{C} \circ g^n)) = \Omega(n)$ (Thm 3)

$CC(KW_{F_\mathcal{C}}) = \Omega(n)$ (Thm 2)

$\text{mCkt depth}(F_\mathcal{C}) = \Omega(n)$ (Thm 1)

Monotone Circuit Depth LBs : Putting it all together

Thm 1 [KW equivalence]

$\text{mCkt Depth}(F) = cc(\text{mKW}_F)$

DONE ✓

Thm 2 [Lifted CNF search $\equiv KW_F$]

$\text{Search}(\mathcal{C} \circ g^n) \equiv KW_{F_\mathcal{C}}$ for an associated monotone $F_\mathcal{C}$

DONE ✓

Thm 3 [Deterministic Lifting].

For any search problem (ie $\text{Search}(\mathcal{C})$)

$\text{Dec-Tree}(\text{Search}(\mathcal{C})) \simeq CC(\text{Search}(\mathcal{C} \circ g^n))$

TO DO

Thm 4 (LBs for $\text{Search}(\mathcal{C})$)

There exist unsat kCNF $\mathcal{C}$ over $z_1 \ldots z_n$ st. $\text{DecTree}(\text{Search}(\mathcal{C})) = \Omega(n)$

TO DO

$DT(\text{Search}(\mathcal{C})) = \Omega(n)$ (Thm 4)

$CC(\text{Search}(\mathcal{C} \circ g^n)) = \Omega(n)$ (Thm 3)

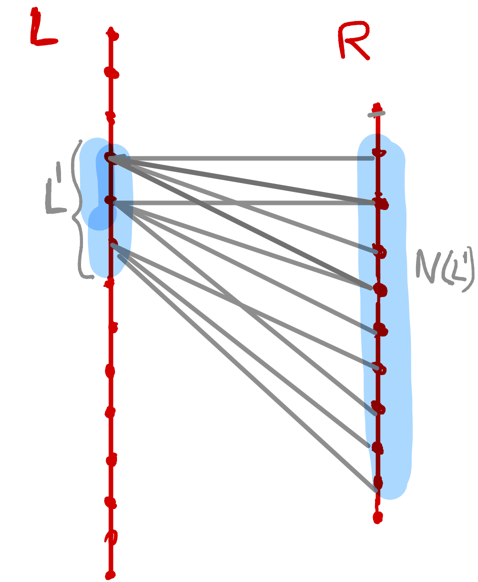
$CC(KW_{F_\mathcal{C}}) = \Omega(n)$ (Thm 2)

$\text{mCkt depth}(F_\mathcal{C}) = \Omega(n)$ (Thm 1)

THEOREM 4 LOWER BOUNDS FOR Decision tree depth for Search($\mathcal{C}$)

The hard formulas: Random (expanding) kCNFs:

Fix a bipartite (m, n) expander, left degree K



g is an (s,c)-expander if $\forall\, L' \subseteq L$ $|L'| \leq s$

$$|N(L')| \geq c \cdot |L'|$$

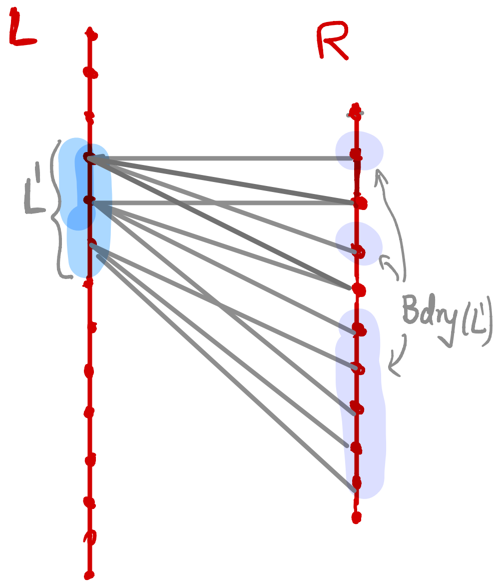
g is an (s,c')-boundary expander if $\forall L'$ $|L'| \leq s$

$$|\mathrm{Bdry}(L')| \geq c' |L'|$$

Claim A random left k-regular bipartite graph $|L| = m = cn$ $|R| = n$ is a $\left(\frac{n}{4}, \frac{K}{10}\right)$-boundary expander whp

THEOREM 4 LOWER BOUNDS FOR Decision tree depth for Search($\mathcal{C}$)

The hard formulas: Random (expanding) kCNFs:



Fix a bipartite (m,n) expander, left degree K

G is an **(s,c)-expander** if $\forall\, L' \subseteq L$ $|L'| \leq s$

$$|N(L')| \geq c \cdot |L'|$$

G is an **(s,c')-boundary expander** if $\forall L'$ $|L'| \leq s$

$$|Bdry(L')| \geq c' |L'|$$

Claim A random left k-regular bipartite graph $|L| = m = cn$ $|R| = n$ is a $\left(\frac{n}{4}, \frac{K}{10}\right)$-boundary expander whp

THEOREM 4 LOWER BOUNDS FOR Decision tree depth for Search($\mathcal{C}$)

The hard formulas: Random (expanding) kCNFs:

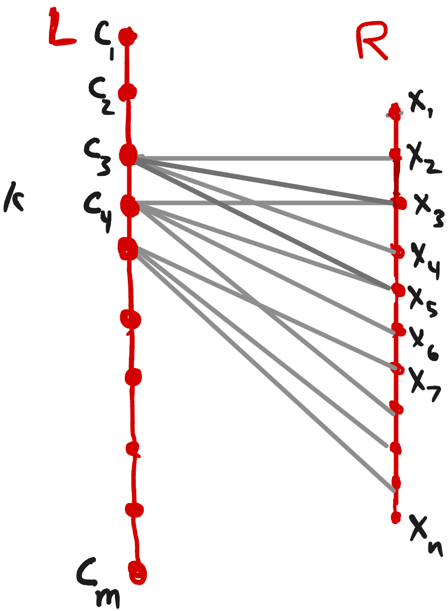
Let $G=(L,R)$ be bipartite graph, $|L|=m$, $|R|=n$, left degree k

G is an (s,c)-expander if $\forall L' \subseteq L$ $|L'| \le s$

$|N(L')| \ge c \cdot |L'|$

G is an (s,c')-boundary expander if $\forall L'$ $|L'| \le s$

$|Bdry(L')| \ge c' |L'|$



From G create CNF $\mathcal{C}$:

vars(C_i) correspond to Neighbors of i in G

$\forall x_j \in vars(C_i)$, randomly pick x_j or $\bar{x}_j$

m = # clauses

n = # vars

k-CNF

Claim 1 Whp (for $m = O(n)$ sufficiently large)
$\mathcal{C}$ is unsat. and every subset of $\frac{n}{2}$ clauses is satisfiable.

Theorem 4 Any Resolution proof (= decision tree for Search ($\mathcal{C}$))
requires depth $\Omega(n)$

Pf of ~~Lemma~~ Thm.

Let Π be a tree-like Res refutation of $\mathcal{C}$ (= dec. tree)

For each node v in Π, Let $S(v)$ = set of clauses in $\mathcal{C}$ labelling leaves of subtree rooted at v

By claim 1, for root vertex r of Π, $|S(r)| \geq \frac{n}{2}$

Find a node $v \in \Pi$ s.t. $\frac{n}{8} \leq |S(v)| \leq \frac{n}{4}$.

By boundary expansion of $\mathcal{C}$, the clause associated with v must contain $\Omega(n)$ variables (since the boundary vars cant be resolved away)

Theorem 4 Any Resolution proof (= decision tree for Search ($\mathcal{C}$)) requires depth $\Omega(n)$

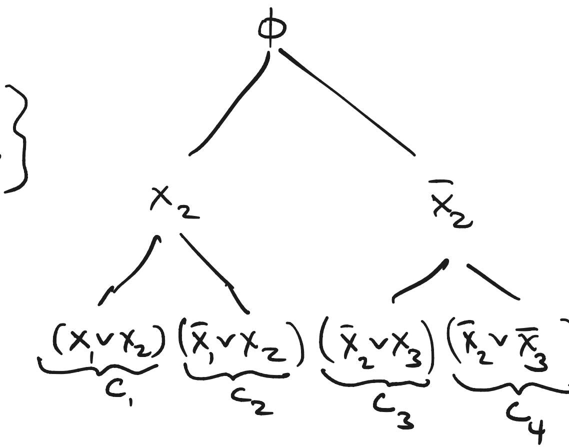
Proof

Let T be a dec. tree for search ($\mathcal{C}$).

Equivalently T is a RES refutation of $\mathcal{C}$

For $v \in T$,

Let $S(v) = \{ c_i \in \mathcal{C}$ such that c_i labels some Leaf of subtree T_v rooted at $v \}$



By claim 1, for $v = \text{root}$, $|S(r)| > \frac{n}{2}$

Find a node $v \in \Pi$ s.t. $\frac{n}{8} \leq |S(v)| \leq \frac{n}{4}$.

By boundary expansion of $\mathcal{C}$, the clause associated with v must contain $\Omega(n)$ variables (since the boundary vars cant be resolved away)

Theorem 3 (Deterministic Lifting)

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 (Deterministic Lifting) [RM, GPW]

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

TODAY: SIMPLER PROOF USING SUNFLOWERS

(with Jun Mertz, Lovett, Meka, Zhang)

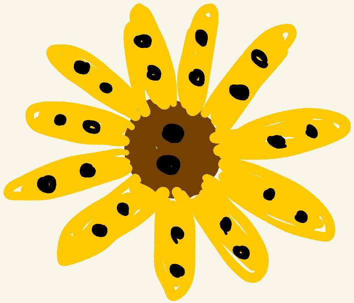
f: N-bit boolean function / search problem

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

Theorem (Deterministic Lifting) [RM, GPW]

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

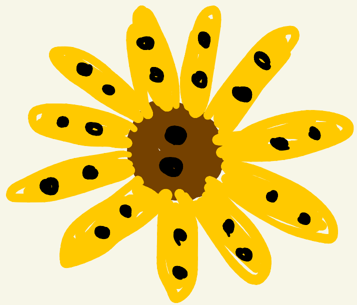
SUNFLOWER LEMMA



$K=4$, $p=11$

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

SUNFLOWER LEMMA



$k=4$, $p=11$

Let X be a k-uniform set system over $\mathcal{U}$.
If $|X| > r^k$ then 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]

Idea behind New Proof

Show $|X| > r^k \Rightarrow$  $\in X$

X is <u>r-spread</u> if $\forall z \subset [n]$, at most $r^{k-|z|}$ sets contain z

<u>Main Lemma</u> X r-spread $\Rightarrow$ X contains $p = r/k$ disjoint sets

Proof (assuming Main Lemma):

$k = 1$

$k \geq 2$ either X is r-spread

ow $\exists\ z$ such that $> r^{k-|z|}$ sets contain z

recurse on $X' = \{ s \in X \mid z \subseteq s \}$

$|X| > r^k \Rightarrow$  $\in X$

X is r-spread if $\forall Z \subseteq [n]$, at most $r^{k-|Z|}$ sets contain Z
and $|X| \geq r^k$

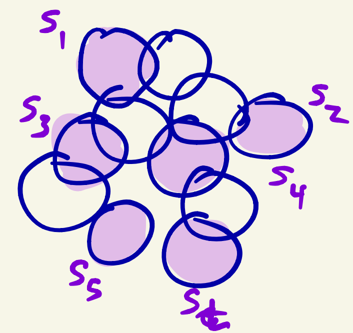
Lemma X r-spread $\Rightarrow X$ contains $p = r/k$ disjoint sets

Proof of Lemma for $r = pk$:

Let $B = \{S_1, \dots, S_t\}$ be maximal collection of disjoint sets in X, $t < p$

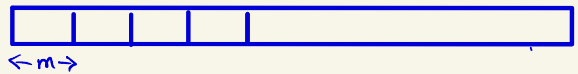
Then some element contained in $\geq \frac{|X|}{|B|k}$ sets

$$\frac{|X|}{|B| \cdot k} \geq \frac{(pk)^k}{pk} = (pk)^{k-1},$$ so X not r-spread



BLOCK-RESPECTING SET SYSTEMS : r-SPREAD ≡ log r-dense

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



N blocks

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

$\mathcal{X}$ is r-spread ≡ $\mathcal{X}$ is log r-dense

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

$|\mathrm{Link}(\mathcal{X}, S)_{\bar{S}}| \le \dfrac{|\mathcal{X}|}{r^{|I|}}$

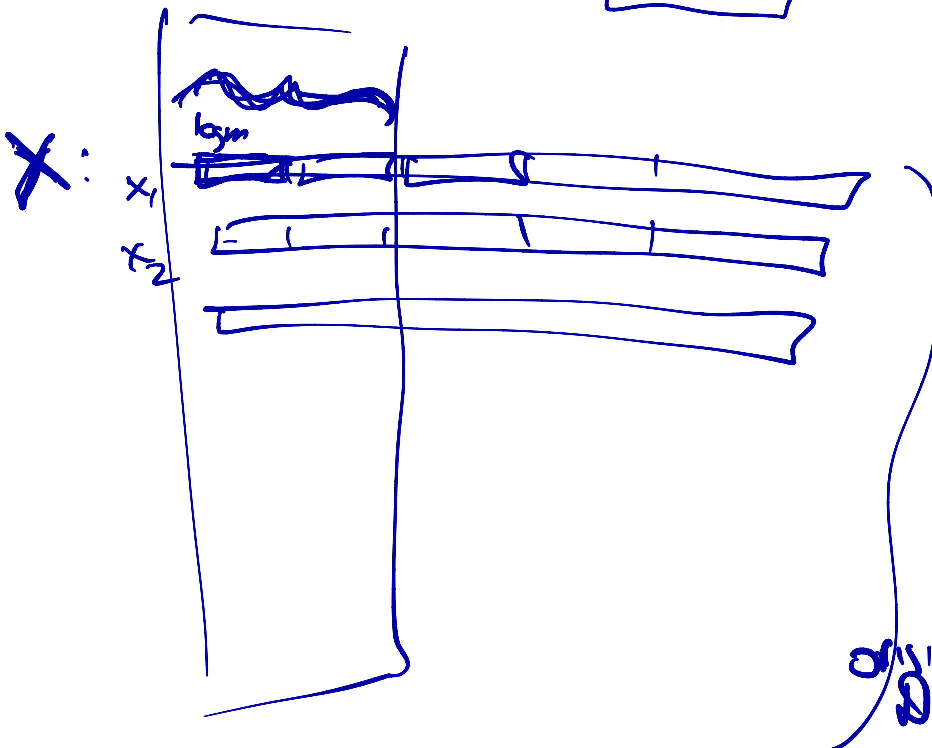
$\forall I \subseteq [N]\ H_\infty(\mathcal{X}_I) \geq \overbrace{\log r \cdot |I|}$

where $H_\infty(\mathcal{X}) = \min\limits_{x \in \mathcal{X}} \log\left(\dfrac{1}{\Pr[\mathcal{X} = x]}\right)$

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

If $X = [m]^N$

then $\forall I$, $\underbrace{H_\infty(X_I)} = \overbrace{\underbrace{|I| \cdot \log m}}$ $\quad .9\,|I|\lg m$



$I = \{1, 2\}$

$X \subseteq [m]^N$

$I = \{1\,2\}$

$X_I =$

original dist:

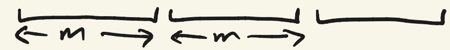
$D:$ $x \in X$ then $pr(x) = \frac{1}{|X|}$

$x \notin X$ then $pr(x) = 0$

Robust Sunflowers

N blocks, each size m

Let $\mathcal{X}$ be a block-respecting set system over $[mN]$ =



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

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

$\mathcal{X}_{DNF} = x_1 x_7 x_9 \vee x_3 x_4 x_8 \vee x_2 x_6 x_8$

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

Then $\Pr_y [\mathcal{X}_{DNF}(y) \neq 1] \leq \varepsilon$

$\boxed{\begin{array}{l} \underline{\textbf{Theorem}} \text{ [ALWS] Let } \mathcal{X} \text{ be } \log r\text{-dense, } r = c \log(\tfrac{N}{\varepsilon}). \text{ Then} \\ \qquad \Pr[\mathcal{X}_{DNF}(y) \neq 1] \leq \varepsilon \end{array}}$

true even for Nonmonotone DNF

$\log r = .9 \log m$

Robust Sunflowers

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

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

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

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

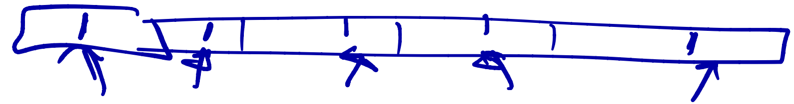
y : random vector in $\{0,1\}^{|\mathcal{U}|}$, $\Pr[y_i = 1] = \frac{1}{2}$

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

$$\boxed{\begin{array}{l}\underline{\text{Theorem}} \text{ [ALWS] Let } \mathcal{X} \text{ be } \log r\text{-dense, } r \geq c \log(N/\varepsilon)\text{. Then} \\ \qquad \Pr_y [X_{DNF}(y) \neq 1] \leq \varepsilon\end{array}}$$

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

(exponential improvement when ε very small)

For us: vars are 

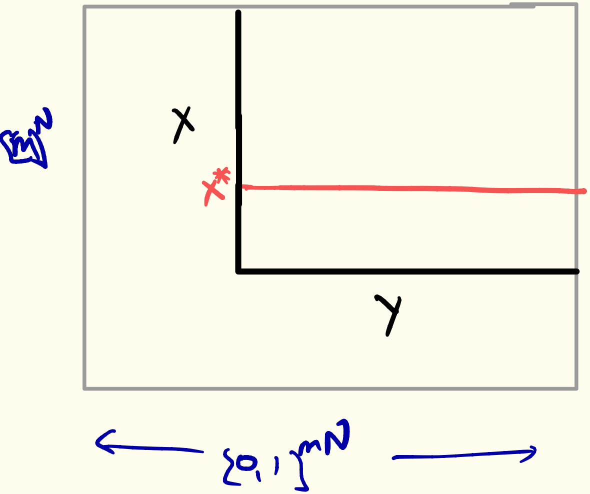
Vars $\vec{Y}$ = mN vars

each $x \in X$ maps to a term t_x of size N

$$t_x = \bigwedge_{i=1}^{N} Y(i, x_i)$$

$$\text{DNF} = \bigvee_{x \in X} t_x$$

FULL RANGE LEMMA (via )



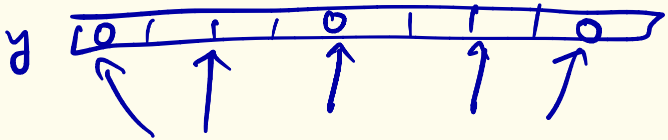
$m \sim N^{10}$

$m = N^{10}$

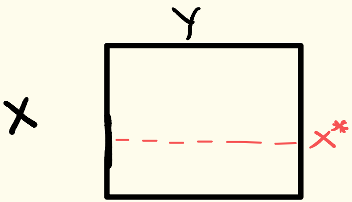
Let $X \subseteq [m]^N$ be $.9 \log m$-dense
$Y \subseteq \{0,1\}^{mN}$ be large $(> 2^{mN - N^3})$

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

$IND^N(x^*, y) \in \{0,1\}^N$



FULL RANGE LEMMA (via )



X $.9 \log m$ dense, Y Large $\left(|Y| \geq 2^{mN - N^3}\right) \Rightarrow$

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

<u>Proof</u> Assume $\forall x \; \exists \beta_x$ st $\forall \alpha \in Y \;\; \mathrm{IND}^N(x, \alpha) \neq \beta_x$

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

create DNF $f = \bigvee_{x \in X} Y_x$

By Robust sunflower lemma, $\Pr_{\alpha \in \{0,1\}^{mN}} \left[f|_\alpha \neq 1 \right] \leq 2^{-N^4}$

Since Y is large, $\exists \alpha \in Y$ s.t. $f|_\alpha = 1$. #

BACK TO: DETERMINISTIC LIFTING THEOREM

f: N-bit boolean function / search problem

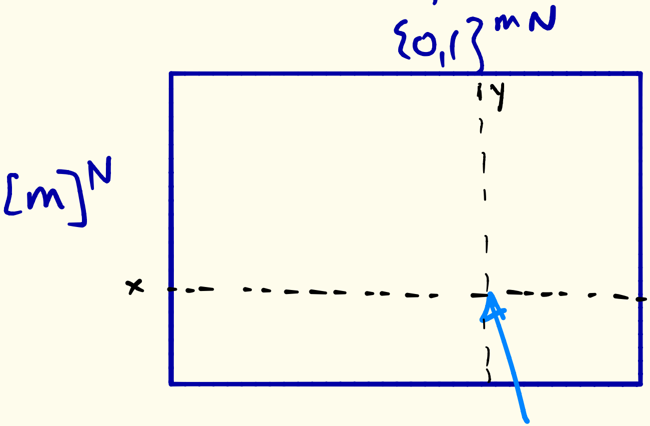
g: index gadget $\quad g(x,y) = y_x$

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

Theorem (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 $f \circ \mathrm{IND}^N$



Communication matrix M

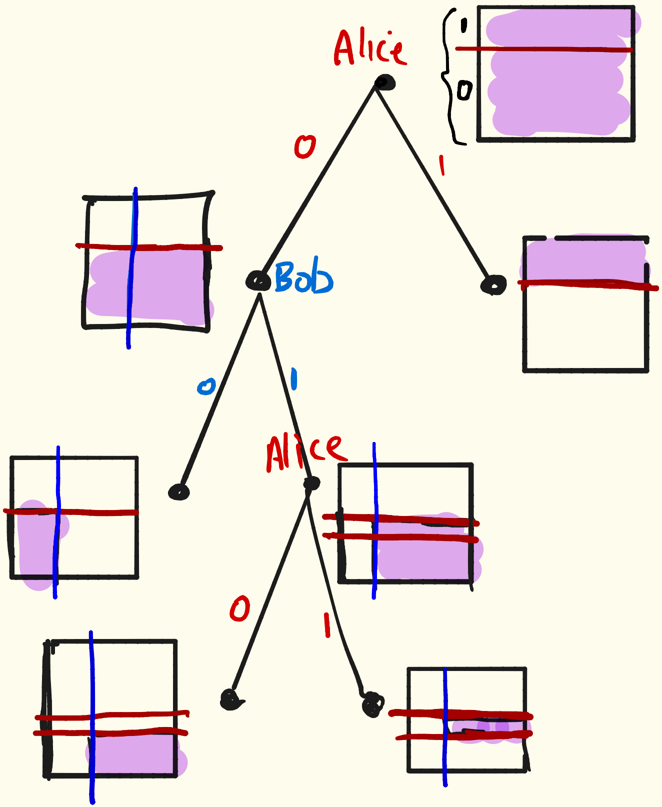
(x,y)-entry labelled by

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

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

ans to $z_1, \ldots, z_N$

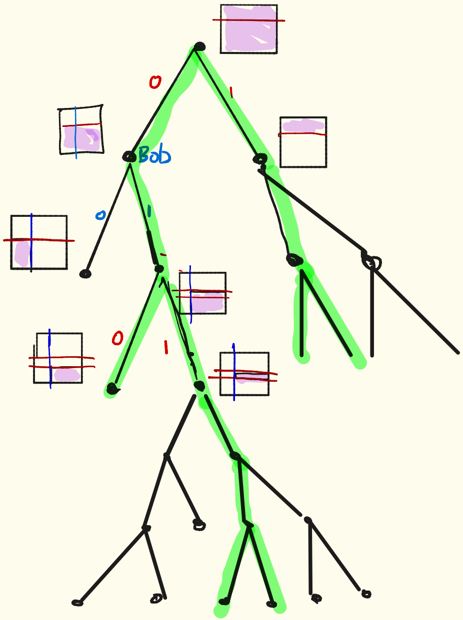
Protocol Π is a tree, partitions M into subrectangles



each vertex v of Π labelled with subrectangle $R_v = X_v \times Y_v$

given Π for $f \circ \mathrm{IND}^N \longrightarrow$ construct decision tree T for f

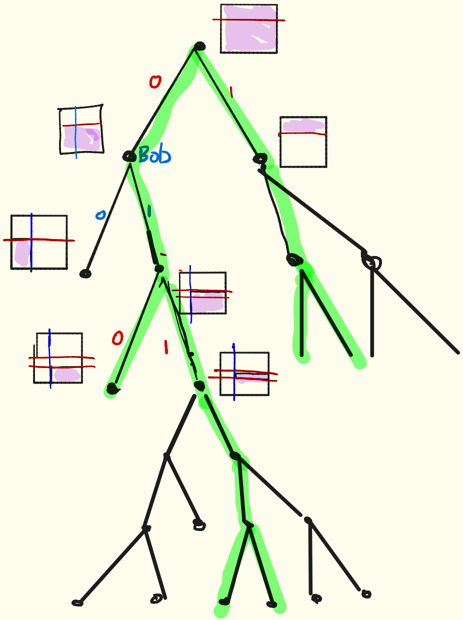
of depth $\sim \text{height}(\Pi) / \log N$



Π has height $d = 6$

T has height $\frac{d}{\log m} = 3$

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



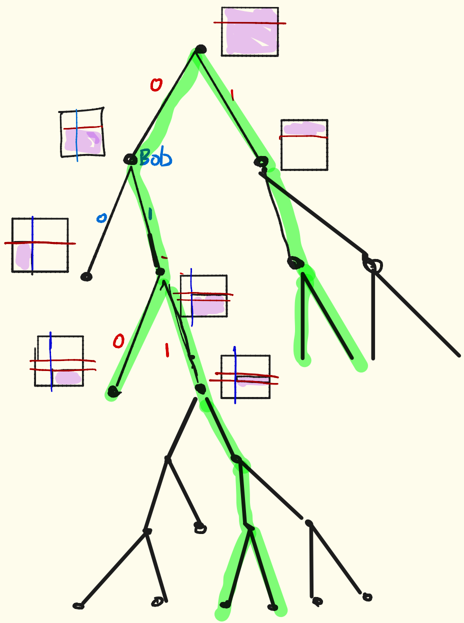
<u>want</u>:

Let v be a vertex in T, and let ρ_v be the partial assignment associated with v.

Let R_v be the rectangle in associated vertex of Π

then $\forall \beta \in \{0,1\}^n$ extending ρ_v,
$\exists$ some $(x,y) \in R_v$ s.t. $\mathrm{IND}^n(x,y) = \beta$

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



Strategy (high level):

- As long as not much info is revealed about any subset of coordinates, go to larger side
- Otherwise find maximal subset of coordinates where minentropy is low, set these coordinates of x and query them in T
- Need to maintain invariant that on all unset coordinates, little info has been revealed

Simulation : Warmup

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

still large

- When Alice sends a bit, go to larger side

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

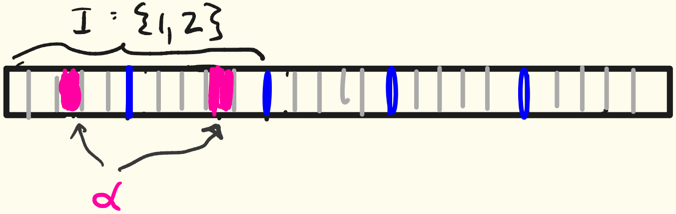
- Find maximal subset $I \subseteq [N]$ and value $\alpha \in [m]^J$ that is too likely.
- Query variables $z_I = \{x_i, i \in I\}$ in T. Say $z_J = \beta$
- This induces a refinement of $X \times Y$:

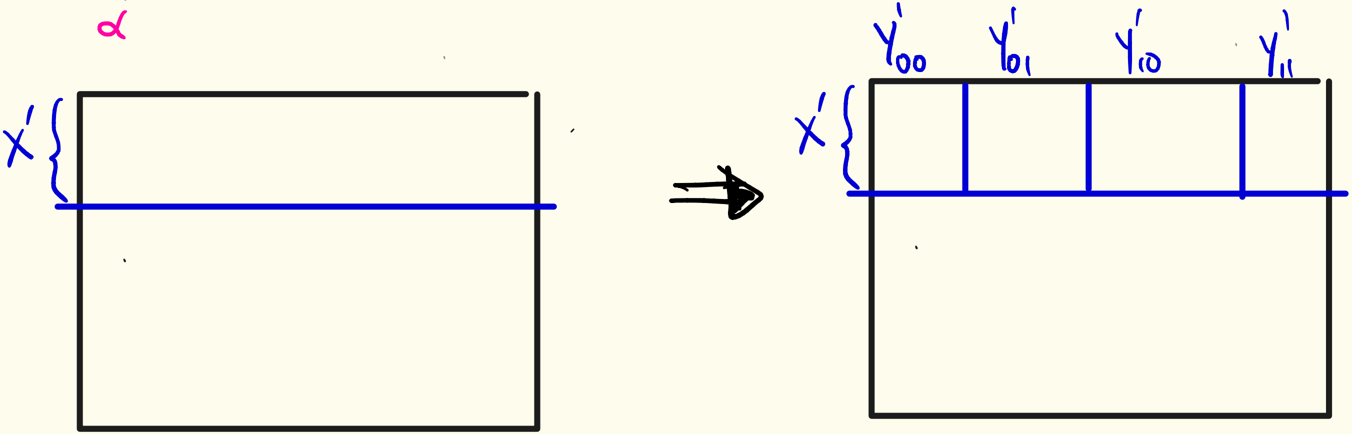
$$X' = \{x \in X \mid x_I = \alpha\}$$
$$Y'_\beta = \{y \in Y \mid \text{IND}(\alpha, y_i) = \beta\}$$

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

REFINEMENT (of Y wrt X')

X no longer $.9 \log m$ dense



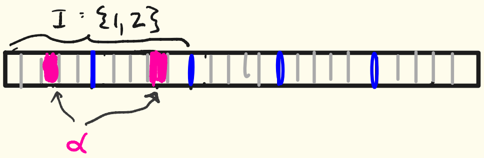


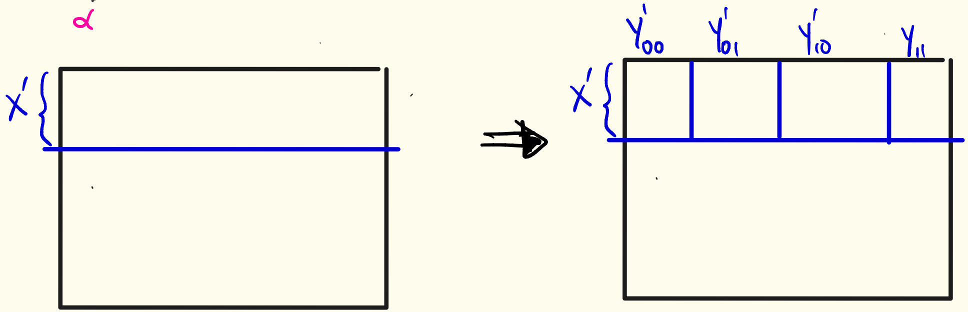
$$X' = \{x \in X \mid x_I = \alpha\}$$

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

REFINEMENT (of Y wrt X')

X no longer $.9 \log m$ 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 $[N] - I$

FULL RANGE LEMMA tells us that Y'_β is not empty $\forall \beta$

★ Need to show Y'_β is large (otherwise decision tree T can err)

Simulation:

Invariant: $\rho \in \{0,1,*\}^N$, $J = \text{fixed}(\rho)$

R is $X \times Y$ ρ-structured:

- X, Y are fixed on blocks J and $\text{IND}_m^J(X_J, Y_J) = \rho[J]$
- $X_{\bar{J}}$ is $.9 \log m$ dense
- $Y_{\bar{J}}$ is large $\left(> 2^{m|\bar{J}| - N\log m} \right)$

Invariant: R is ρ-structured
- X, Y are fixed on J, $\mathrm{IND}^J(X_J, Y_J) = \rho$
- $X_{\bar{J}}$ is $.9 \log m$ dense
- $Y_{\bar{J}}$ is large

Simulation:

- Initially (at root of Π), $X = [m]^N$, $Y = \{0,1\}^{mN}$

Y still large

- 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:

  - Restore density via Rectangle Partition
  - By Main Lemma, $\exists X^j, \alpha_j, I^j$ and $\{Y^{j,\beta}\}_{\beta \in \{0,1\}^{|I^j|}}$ s.t. $\forall \beta$ $Y^{j,\beta}$ is large, X^j dense

  - Query variables z_i, $i \in I^j$ in T. Say $z_I = \beta$

Rectangle Partition Procedure

Input $X \times Y$

Phase I : Density restoration of X

Repeatedly find max subset of coordinates violating blockwise density. Set the coordinates to most likely value

Induces partition of X into $X^1, X^2, \ldots, X^q$ (plus small error part)

Phase II : For each X^i, Refine Y

Phase I: Density Restoration (for $X \subseteq [m]^n$)

$$
\begin{tikzcd}
X \arrow[r] \arrow[d, "I_1 = \alpha_1"'] & X^{\geq 2} := X \setminus X^1 \arrow[r] \arrow[d, "I_2 = \alpha_2"'] & X^{\geq 3} \arrow[r] \arrow[d, "I_3 = \alpha_3"'] & \cdots \arrow[r] \arrow[d] & |X^{\geq j+1}| < \frac{|X|}{2} \\
X^1 & X^2 & X^3 & X^j &
\end{tikzcd}
$$

I_j = max subset of $[n]$ that violates $.9 \log m$-blockwise minentropy on I_j, $\alpha_j \in [m]^{I_j}$ is assignment to blocks I_j violating minentropy (ie. $\Pr[x[I_j] = \alpha] > 2^{-.9 |I_j| \log m}$)

Phase I: Density Restoration of X

Initially $X^{\geq 1} := X$, $j = 1$

While $|X^{\geq j}| \geq |X|/2$ do:

Let I_j = max subset of $[n]$ violating $.9\log m$ density of $X^{\geq j}$

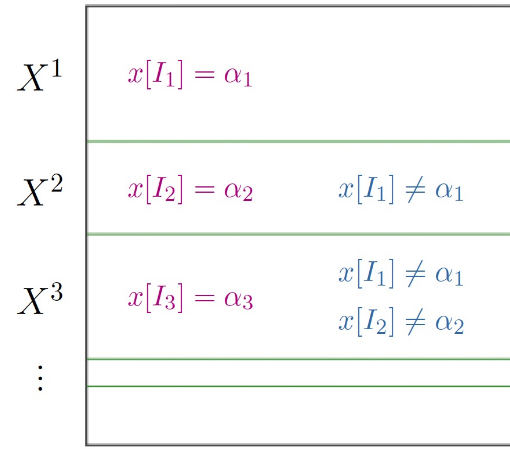
Let $\alpha_j \in [m]^{I_j}$ be outcome witnessing this

$$\Pr_{x \sim X^{\geq j}} \left(x[I_j] = \alpha_j \right) \geq 2^{-.9|I_j|\log m}$$

Let $X^j = \{ x \in X^{\geq j} \mid x[I_j] = \alpha_j \}$

Let $X^{j+1} = X^{\geq j} \setminus X^j$

$j = j+1$



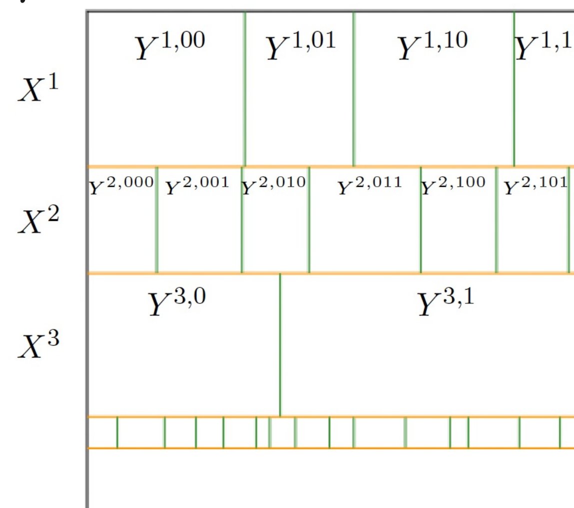
Phase II: For each X^i, refine Y

For each (I_j, α_j) from phase I, $\beta \in \{0,1\}^{I_j}$ do:

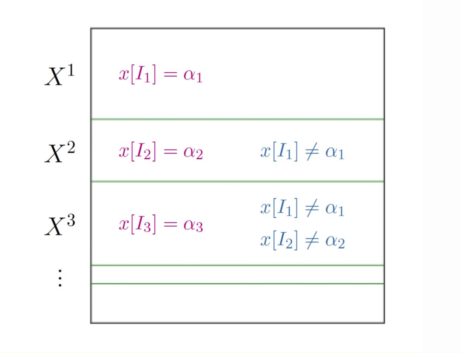
Let $Y' = \{ y \in Y \mid y[I_j, \alpha_j] = \beta \}$

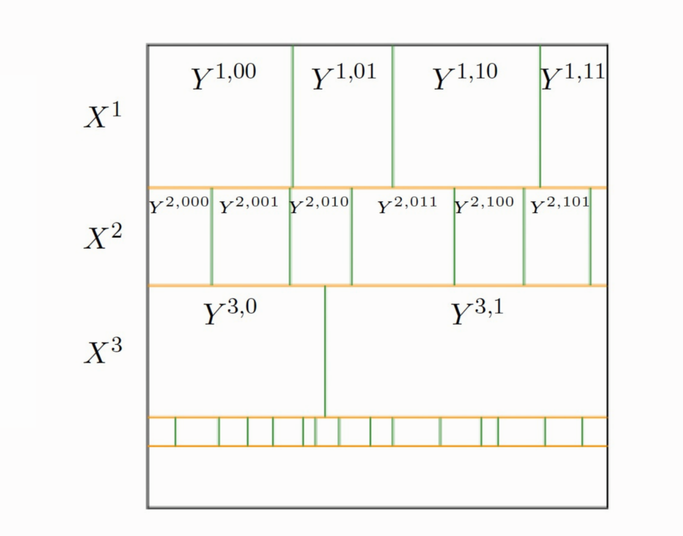
Let $\eta^{j,\beta} \in (\{0,1\}^m)^{|I_j|}$ be the string maximizing $|\{ y \in Y' \mid y[I_j] = \eta^{j,\beta} \}|$

Let $Y^{j,\beta} = \{ y \in Y' \mid y[I_j] = \eta^{j,\beta} \}$



Rectangle Partition Procedure





Claim 4.2

$\forall j \;\; X^j \times Y^{j,\beta}$ is fixed on I_j and $IND^{I_j}(X^j_{I_j}, Y^{j,\beta}_{I_j}) = \beta$

Claim 4.3 $\forall j$ $X^{j}_{\overline{I_j}}$ is $.9\log m$ dense

Proof (sketch)

We picked maximal block I_j that violated blockwise mintropy & set I_j to most likely value.

$\therefore$ $X^{j}_{\overline{I_j}}$ has blockwise density restored on remaining blocks

(Says: fixing maximal subset I_j of coordinates to most likely value restores density on remaining unfixed coordinates $\overline{I_j}$)

Deficiency: $D_\infty(S) = \log|S| - H_\infty(S)$ ← number of bits of information learned

Claim 4.4 (deficiency of each X^j drops by $\Omega(|I_j|\log m)$)

For all (I_j, α_j), $D_\infty(X^j_{\overline{I_j}}) \leq D_\infty(X) - \frac{1}{10}|I_j|\log m + 1$

(says if X^j sets blocks I_j then protocol must have sent $\sim |I_j|\log m$ bits)

Claim 4.4 (deficiency of each X^j drops by $\Omega(|J_j|\log m)$)

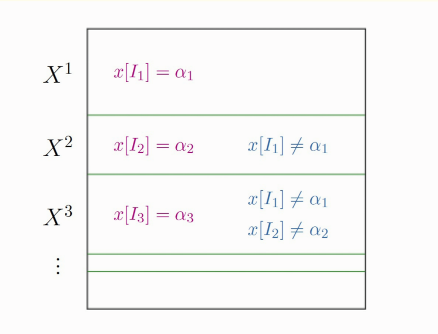
For all (I_j, α_j), $D_\infty(X^j_{\overline{I_j}}) \leq D_\infty(X) - \frac{1}{10}|I_j|\log m + 1$

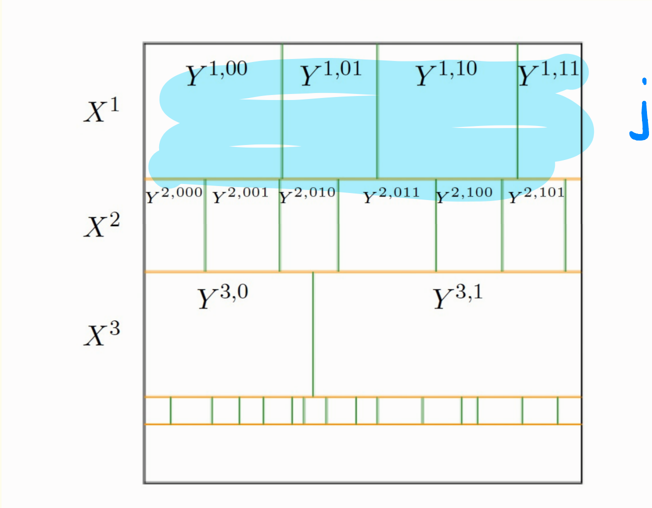
(says if X^j sets blocks I_j then protocol must have sent $\sim |I_j|\log m$ bits)

Proof (uses $|X^{\geq j}| \geq |X|/2$)

$$
\begin{aligned}
D_\infty(X^j_{\overline{I_j}}) &= |\overline{I}_j|\log m - \log|X^j| \\
&\leq (n-|I_j|)\log m - \log\left(|X^{\geq j}| \cdot 2^{-.9|I_j|\log m}\right) \\
&\leq n\log m - |I_j|\log m - \log|X^{\geq j}| + .9|I_j|\log m - \log|X| + \log|X| \\
&= (n\log m - \log|X|) - \tfrac{1}{10}\cdot|I_j|\cdot\log m + \log\left(|X|/|X^{\geq j}|\right) \qquad |X^{\geq j}| \geq \tfrac{|X|}{2} \\
&\leq D_\infty(X) - \tfrac{1}{10}|I_j|\log m + 1
\end{aligned}
$$

Rectangle Partition Procedure : MAIN LEMMA 4.5





$j=1$

MAIN LEMMA (4.5)

Let $X = \bigcup_j X^j$ be $.9\log m - o(1)$ dense; Y large. Then

$$\exists j \;\forall \beta \in \{0,1\}^{I_j} \quad Y^j_\beta = \{ y \in Y \mid \mathrm{IND}(\alpha_j, Y_{I_j}) = \beta \} \text{ is large}$$

Claims 4.2, 4.3 and Main Lemma 4.5
show that our invariant holds.

Claim 4.4 shows that depth $(T) \sim d / \log n$

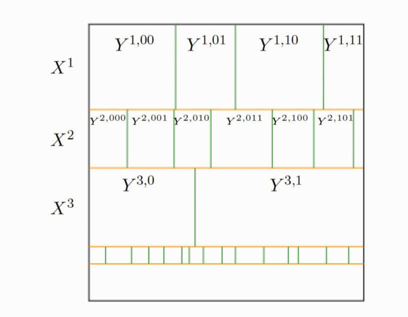
depth of cc protocol π

Main Lemma (4.5)

Let $X = \bigcup_j X^j$ be $.9\log m - O(1)$ dense, Y large

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

$$|Y^{j,\beta}_{\bar{I}_j}| \geq |Y| / 2^{3|I_j|\log m}$$



Proof idea:

Recall FULL RANGE LEMMA (via 🌻):

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

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

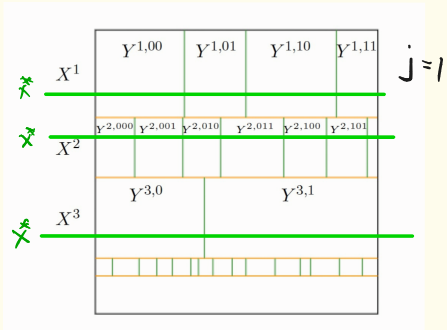
- applying Full Range Lemma to each block X^j, each one contains some x^* with full range

Main Lemma (4.5)

Let $X = \bigcup_j X^j$ be $.9 \log m - o(1)$ dense, Y large

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

$$|Y^{j,\beta}| \geq |Y| / 2^{3|I_j| \log m}$$



Proof idea:

Recall **FULL RANGE LEMMA** (via ):

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

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

① applying Full Range Lemma to each block X^j, each one contains some x^* with full range

② Assume for contradiction $\forall j \ \exists \beta \in \{0,1\}^{I_j}$ s.t. $|Y^{j,\beta}|$ too small

$Y' = Y$ − Bad ones

calculation shows $|Y'| \geq |Y|/2$ so Y' still large

Apply Full range Lemma on X, Y' which contradicts ①

$|Y_{BAD}|$ IS SMALL:

- Assume for contradiction $\forall j$ $\exists \beta$ such that

$$|Y^{j,\beta}| < |Y| / 2^{4|I_j| \log m}$$

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

$$|Y_{BAD}| \leq \sum_{k=1}^{n} \binom{n}{k} m^k \, |Y| / 2^{4k \log m}$$

$$\leq \sum_{k=1}^{n} m^{2k} \, |Y| / m^{4k}$$

$$< |Y|/2$$