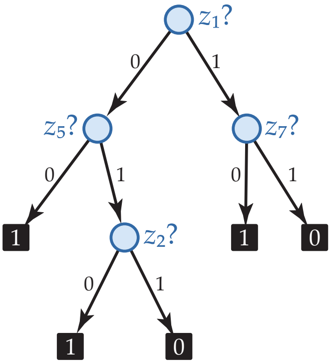
Query-to-Communication Lifting

Mika Göös
Harvard & Simons Institute

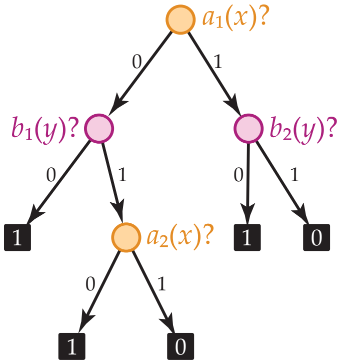
Query vs. Communication

$f(z)$



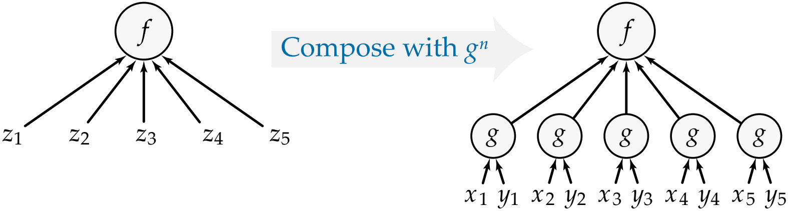
Decision trees

$F(x,y)$



Communication protocols

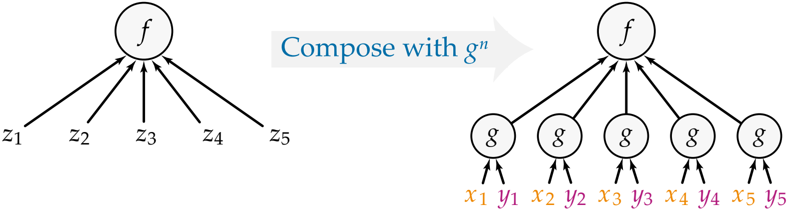
Composed functions $f \circ g^n$



Examples:

- Set-disjointness: $\textsc{Or} \circ \textsc{And}^n$
- Inner-product: $\textsc{Xor} \circ \textsc{And}^n$
- Equality: $\textsc{And} \circ \neg\textsc{Xor}^n$

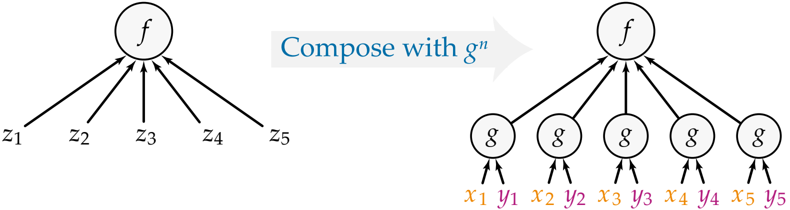
Composed functions $f \circ g^n$



In general: $g\colon \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ is a small gadget

- **Alice** holds $x \in (\{0,1\}^m)^n$
- **Bob** holds $y \in (\{0,1\}^m)^n$

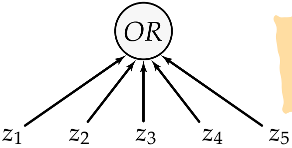
Composed functions $f \circ g^n$



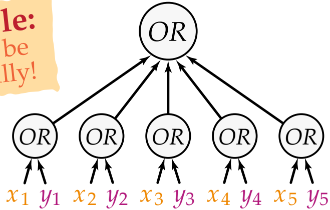
Lifting Theorem Template

$$\mathsf{M}^{\mathsf{cc}}(f \circ g^n) \approx \mathsf{M}^{\mathsf{dt}}(f)$$

Composed functions $f \circ g^n$



Bad example:
Gadget must be chosen carefully!



Lifting Theorem Template

$$\mathsf{M}^{\mathsf{cc}}(f \circ g^n) \approx \mathsf{M}^{\mathsf{dt}}(f)$$

Composed functions $f \circ g^n$

M	Query	Communication	
P	deterministic	deterministic	[RM99, GPW15, dRNV16, HHL16, WYY17, CKLM17]
NP	nondeterministic	nondeterministic	[GLM+15, G15]
many	poly degree	rank	[SZ09, She11, RS10, RPRC16]
many	conical junta deg.	nonnegative rank	[GLM+15, KMR17]
	Sherali–Adams	LP complexity	[CLRS16, KMR17]
	sum-of-squares	SDP complexity	[LRS15]
BPP	randomised	randomised	***new***, [AGJKM17]
P^{NP}	decision list	rectangle overlay	***new***

Lifting Theorem Template

$$M^{cc}(f \circ g^n) \approx M^{dt}(f)$$

Lifting for BPP

with Toniann Pitassi & Thomas Watson

Lifting theorem for BPP

Index gadget $g\colon [m] \times \{0,1\}^m \to \{0,1\}$

$$g(x,y) = y_x$$

$\mathsf{BPP}^{\mathsf{dt}}(f)$ = randomised query complexity of f
$\mathsf{BPP}^{\mathsf{cc}}(F)$ = randomised communication complexity of F

Our result **also [AGJKM17]**

For $m = n^{100}$ and every function $f\colon \{0,1\}^n \to \{0,1\}$,

$$\mathsf{BPP}^{\mathsf{cc}}(f \circ g^n) = \mathsf{BPP}^{\mathsf{dt}}(f) \cdot \Theta(\log n)$$

New applications

$$\mathsf{BPP}^{\mathsf{dt}}(f) \gg \mathsf{M}^{\mathsf{dt}}(f)$$

$$\Downarrow$$

$$\mathsf{BPP}^{\mathsf{cc}}(f \circ g^n) \gg \mathsf{M}^{\mathsf{cc}}(f \circ g^n)$$

~~New~~ applications

$$\mathsf{BPP}^{\mathsf{dt}}(f) \;\gg\; \mathsf{M}^{\mathsf{dt}}(f)$$

$$\Downarrow$$

$$\mathsf{BPP}^{\mathsf{cc}}(f \circ g^n) \;\gg\; \mathsf{M}^{\mathsf{cc}}(f \circ g^n)$$

~~New~~ applications

Classical vs. Quantum

- 2.5-th power total function gap [ABK16,ABB+16]
- *Conjecture:* 2.5 improves to 3 [AA15]
- exponential partial function gap [Raz99,KR11]

BPP vs. Partition numbers

- 1-sided (= Clique vs. Independent Set) [GJPW15]
- 2-sided [AKK16,ABB+16]

Approximate Nash equilibria [BR17]

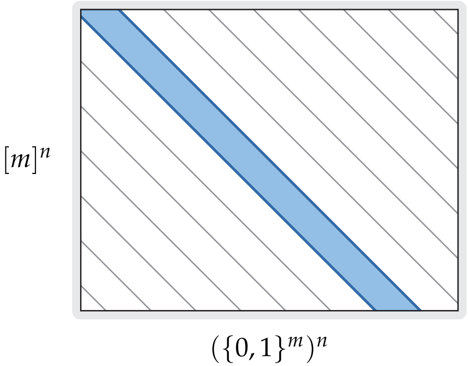
$$\mathsf{BPP}^{\mathsf{cc}}(f \circ g^n) \;\geq\; \mathsf{BPP}^{\mathsf{dt}}(f) \cdot \Omega(\log n)$$

. . . how to begin?

What we actually prove

Input domain partitioned into **slices**

$$[m]^n \times (\{0,1\}^m)^n = \bigcup_{z \in \{0,1\}^n} (g^n)^{-1}(z)$$

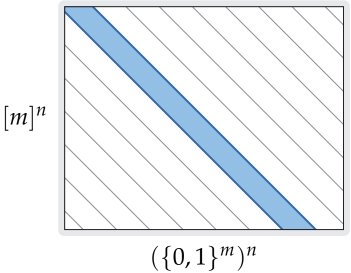


What we actually prove

Simulation

$\forall$ deterministic protocol Π
$\exists$ randomised decision tree of height $|\Pi|$ outputting a random transcript of Π such that 1 $\approx$ 2

1. output of randomised decision tree on input z
2. transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$



What we actually prove

Simulation

$\forall$ deterministic protocol Π
$\exists$ randomised decision tree of height $|\Pi|$ outputting a random transcript of Π such that 1 $\approx$ 2

1. output of randomised decision tree on input z
2. transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$

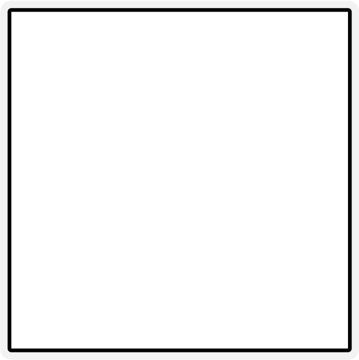
Main theorem:
1. pick $\Pi \sim \boldsymbol{\Pi}$
2. simulate Π via query access to z
3. output value of leaf

$$\mathop{\mathbb{E}}_{(x,y)\sim(g^n)^{-1}(z)} \overbrace{\Pr_{\boldsymbol{\Pi}}[\boldsymbol{\Pi}(x,y) \text{ correct}]}^{>2/3} = \mathop{\mathbb{E}}_{\Pi\sim\boldsymbol{\Pi}} \Pr_{(\boldsymbol{x},\boldsymbol{y})\sim(g^n)^{-1}(z)}[\Pi(\boldsymbol{x},\boldsymbol{y}) \text{ correct}]$$

Goal in pictures

Goal: 1 $\approx$ 2

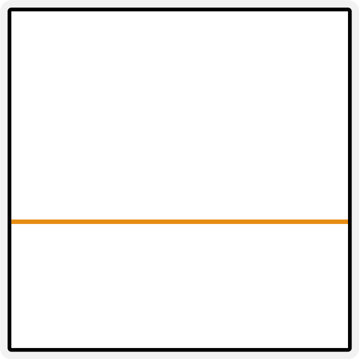
1. output of randomised decision tree on input z
2. transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$

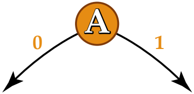


Goal in pictures

Goal: 1 $\approx$ 2

1 output of randomised decision tree on input z
2 transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$

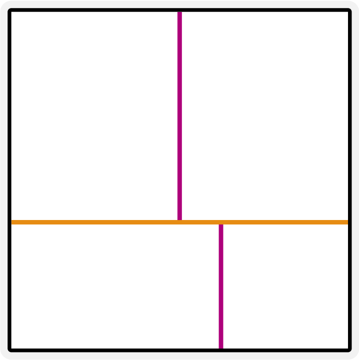


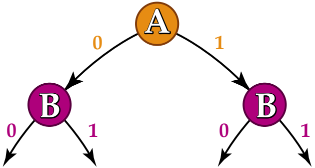


Goal in pictures

Goal: 1 $\approx$ 2

1 output of randomised decision tree on input z
2 transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$

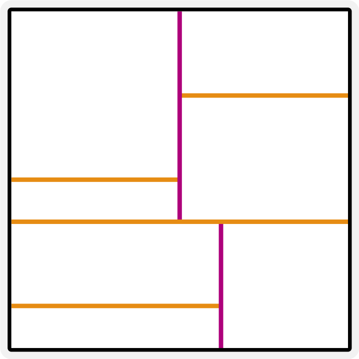


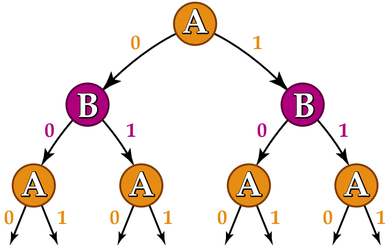


Goal in pictures

Goal: 1 $\approx$ 2

1. output of randomised decision tree on input z
2. transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$

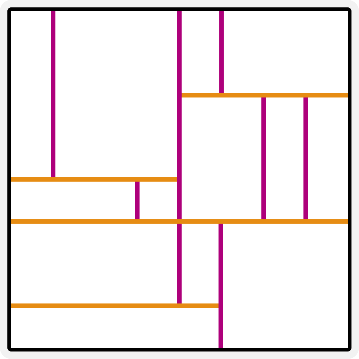


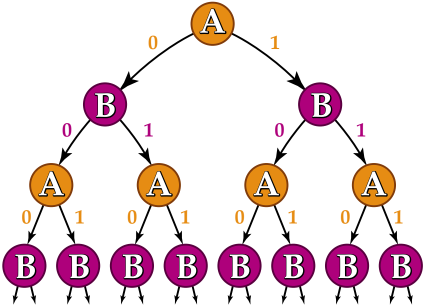


Goal in pictures

Goal: 1 $\approx$ 2

1. output of randomised decision tree on input z
2. transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$

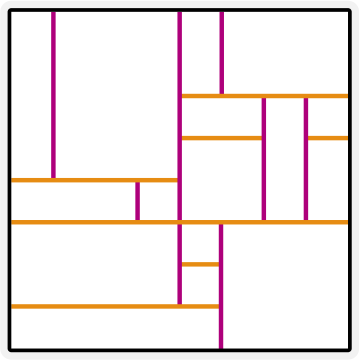


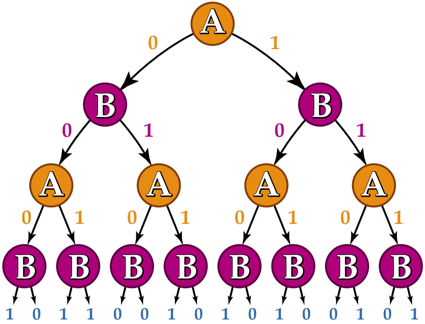


Goal in pictures

Goal: 1 $\approx$ 2

- 1 output of randomised decision tree on input z
- 2 transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$

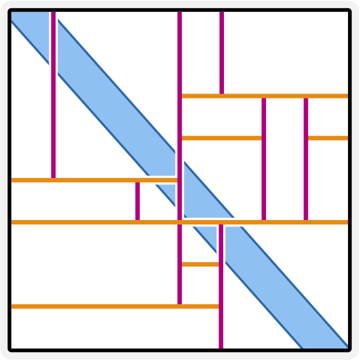


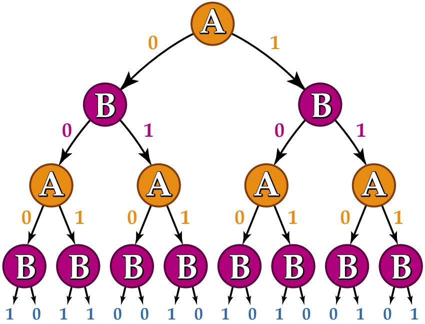


Goal in pictures

Goal: 1 $\approx$ 2

- 1 output of randomised decision tree on input z
- 2 transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$

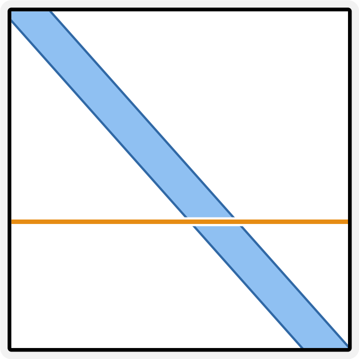


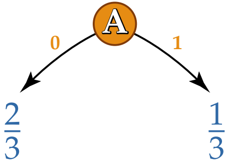


Goal in pictures

Goal: 1 ≈ 2

1. output of randomised decision tree on input z
2. transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$





Idea:

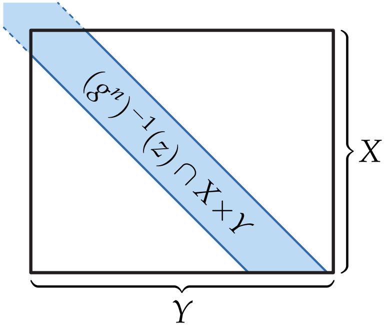
Pretend marginals are uniform!

Pseudorandomness

Uniform Marginals Lemma:

Suppose $X \subseteq [m]^n$ is **dense**
$Y \subseteq (\{0,1\}^m)^n$ is "large"

Then $\forall z \in \{0,1\}^n$ the uniform distribution on $(g^n)^{-1}(z) \cap X \times Y$ has both marginal distributions close to uniform on X and Y

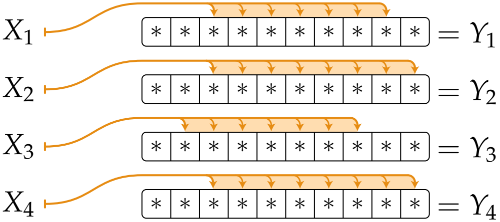


Dense: $\mathbf{H}_\infty(\boldsymbol{X}_I) \geq 0.9 \cdot |I| \log m$ for all $I \subseteq [n]$
[GLMWZ15]

Simulation

When **density** is lost, restore it!

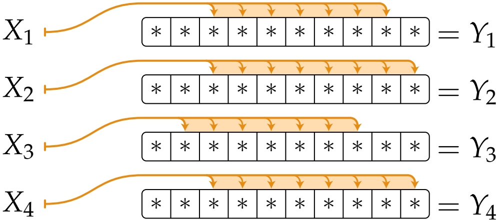
1. Compute partition $X = \bigcup_i X^i$ where each X^i is fixed on some $I \subseteq [n]$ and **dense** on $\bar{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0,1\}^I$
4. Restrict Y so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_{\bar{I}}$ and $X \leftarrow X_{\bar{I}}$ (which is **dense**)



Simulation

When **density** is lost, restore it!

1. Compute partition $X = \bigcup_i X^i$ where each X^i is fixed on some $I \subseteq [n]$ and **dense** on $\bar{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0,1\}^I$
4. Restrict Y so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_{\bar{I}}$ and $X \leftarrow X_{\bar{I}}$ (which is **dense**)



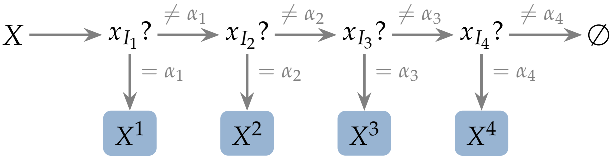
Simulation

When **density** is lost, restore it!

Density-restoring partition [GLMWZ15]

While X is nonempty:

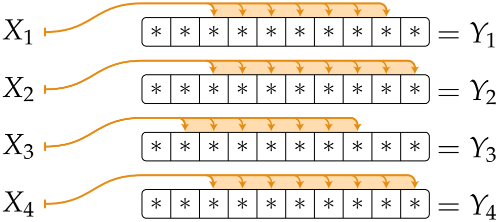
1. Let $I \subseteq [n]$ be **maximal** such that for some α
$$\Pr[\boldsymbol{X}_I = \alpha] > 2^{-0.9|I|\log m}$$
2. Output part $X' = \{x \in X : x_I = \alpha\}$
3. Update $X \leftarrow X \setminus X'$



Simulation

When **density** is lost, restore it!

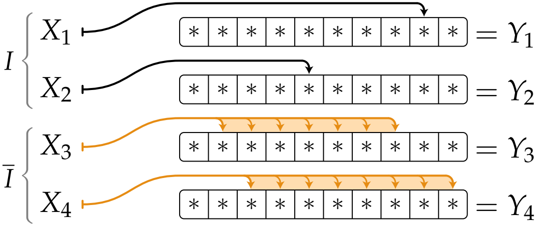
1. Compute partition $X = \bigcup_i X^i$ where each X^i is fixed on some $I \subseteq [n]$ and **dense** on $\bar{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0,1\}^I$
4. Restrict Y so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_{\bar{I}}$ and $X \leftarrow X_{\bar{I}}$ (which is **dense**)



Simulation

When **density** is lost, restore it!

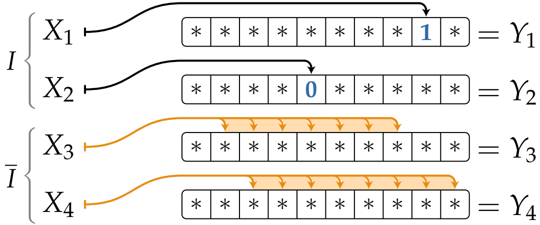
1. Compute partition $X = \bigcup_i X^i$ where each X^i is fixed on some $I \subseteq [n]$ and **dense** on $\bar{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0,1\}^I$
4. Restrict Y so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_{\bar{I}}$ and $X \leftarrow X_{\bar{I}}$ (which is **dense**)



Simulation

When **density** is lost, restore it!

1. Compute partition $X = \bigcup_i X^i$ where each X^i is fixed on some $I \subseteq [n]$ and **dense** on $\overline{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0,1\}^I$
4. Restrict Y so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_{\overline{I}}$ and $X \leftarrow X_{\overline{I}}$ (which is **dense**)



Simulation

When **density** is lost, restore it!

1. Compute partition $X = \bigcup_i X^i$ where each X^i is fixed on some $I \subseteq [n]$ and **dense** on $\bar{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0,1\}^I$
4. Restrict Y so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_{\bar{I}}$ and $X \leftarrow X_{\bar{I}}$ (which is **dense**)

Correctness

1. #queries $\leq |\Pi|$ (whp)
2. Resulting transcript is close to that generated by random input from $(g^n)^{-1}(z)$

Application (via P^{NP} *lifting)*

with Pritish Kamath, Toniann Pitassi & Thomas Watson

Monochromatic rectangles

$$\mathrm{mon}(F) \;:=\; \min_{R \text{ mono}} \log \frac{1}{\mu(R)}$$

1	0	0	1	1	1
0	1	0	1	1	1
0	0	1	1	1	1
0	1	1	0	0	0
0	0	1	1	1	1
1	0	1	1	0	1

Monochromatic rectangles

$$\mathsf{mon}(F) \;:=\; \max_{\mu \text{ product}} \; \min_{R \text{ mono}} \; \log \frac{1}{\mu(R)}$$

1	0	0	1	1	1
0	1	0	1	1	1
0	0	1	1	1	1
0	1	1	0	0	0
0	0	1	1	1	1
1	0	1	1	0	1

Monochromatic rectangles

$$\mathsf{mon}(F) := \max_{\mu \text{ product}} \min_{R \text{ mono}} \log \frac{1}{\mu(R)}$$

Basic questions

- Log-rank conjecture? $\iff \forall F\colon\ \mathsf{mon}(F) \leq \log^{O(1)} \mathsf{rk}(F)$
- Protocols from mon? $\iff \forall F\colon\ \mathsf{PSPACE}^{\mathsf{cc}}(F) \leq \mathsf{mon}(F)^{O(1)}$

Monochromatic rectangles

$$\mathsf{mon}(F) \;:=\; \max_{\mu\ \text{product}} \; \min_{R\ \text{mono}} \; \log \frac{1}{\mu(R)}$$

Basic questions

- Log-rank conjecture? $\iff$ $\forall F\colon$ $\mathsf{mon}(F) \le \log^{O(1)} \mathsf{rk}(F)$
- Protocols from mon? $\iff$ $\forall F\colon$ $\mathsf{PSPACE}^{\mathsf{cc}}(F) \le \mathsf{mon}(F)^{O(1)}$

Known

- $\forall F\colon$ non-product-$\mathsf{mon}(F) \;=\; \mathsf{P}^{\mathsf{cc}}(F)^{\Theta(1)}$ [AUY83,KKN95]
- $\forall F\colon$ $\mathsf{mon}(F) \;\le\; \mathsf{P}^{\mathsf{NPcc}}(F)$ [IW10,PSS14]
- $\exists F\colon$ $\mathsf{P}^{\mathsf{NPcc}}(F) \;\le\; \log n \;\lll\; n^{\Omega(1)} \;\le\; \mathsf{PP}^{\mathsf{cc}}(F)$ [BVdW07]

Monochromatic rectangles

$$\mathsf{mon}(F) := \max_{\mu \text{ product}} \min_{R \text{ mono}} \log \frac{1}{\mu(R)}$$

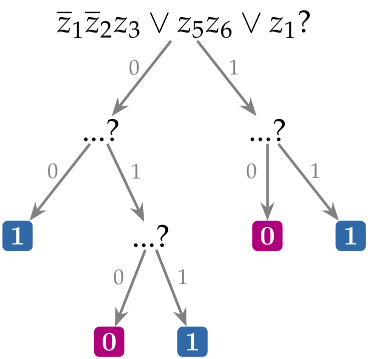
Lifting application:

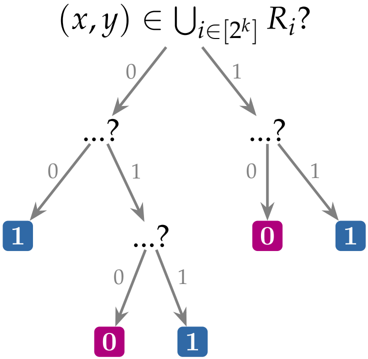
$$\exists F: \quad \mathsf{mon}(F) \le \log^{O(1)} n \lll n^{\Omega(1)} \le \mathsf{P}^{\mathsf{NP}^{\mathsf{cc}}}(F)$$

Known

- $\forall F:$ non-product-$\mathsf{mon}(F) = \mathsf{P}^{\mathsf{cc}}(F)^{\Theta(1)}$ [AUY83,KKN95]
- $\forall F:$ $\mathsf{mon}(F) \le \mathsf{P}^{\mathsf{NPcc}}(F)$ [IW10,PSS14]
- $\exists F:$ $\mathsf{P}^{\mathsf{NPcc}}(F) \le \log n \lll n^{\Omega(1)} \le \mathsf{PP}^{\mathsf{cc}}(F)$ [BVdW07]

P^{NP} decision trees / protocols



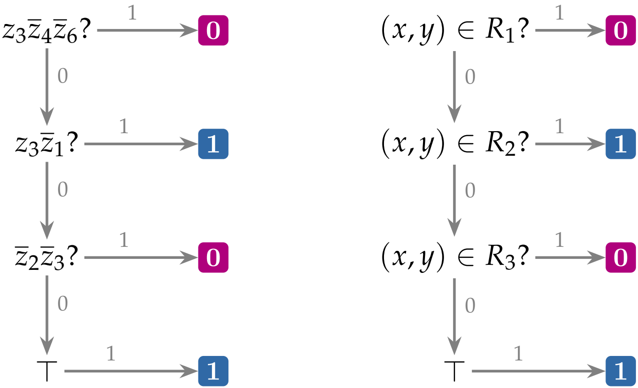


Oracle query cost:

$\mathsf{NP}^{\mathsf{dt}}$ = DNF width **vs.** $\mathsf{NP}^{\mathsf{cc}}$ = log #rectangles

Decision lists: $\mathrm{DL}^{\mathrm{dt}}$ and $\mathrm{DL}^{\mathrm{cc}}$

Equivalent (up to quadratic factors): [Riv87,PSS14]



Conjunction width **vs.** log #rectangles

Lifting theorems

Lifting for P^{NP}

For poly-size index gadget g and every $f\colon \{0,1\}^n \to \{0,1\}$,

$$\mathsf{P}^{\mathsf{NPcc}}(f \circ g^n) \;\geq\; \sqrt{\mathsf{P}^{\mathsf{NPdt}}(f) \cdot \Omega(\log n)}$$

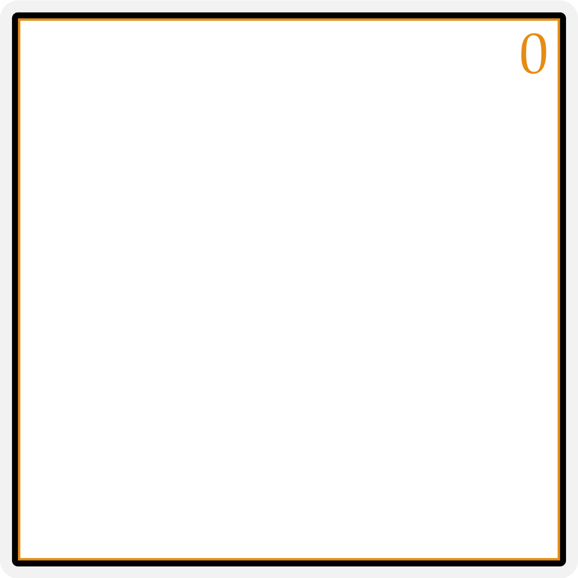
Lifting for decision lists

For poly-size index gadget g and every $f\colon \{0,1\}^n \to \{0,1\}$,

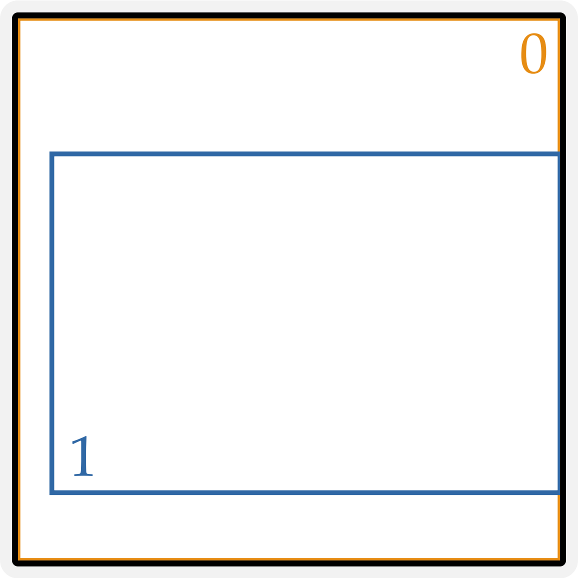
$$\mathsf{DL}^{\mathsf{cc}}(f \circ g^n) \;=\; \mathsf{DL}^{\mathsf{dt}}(f) \cdot \Theta(\log n)$$

$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]

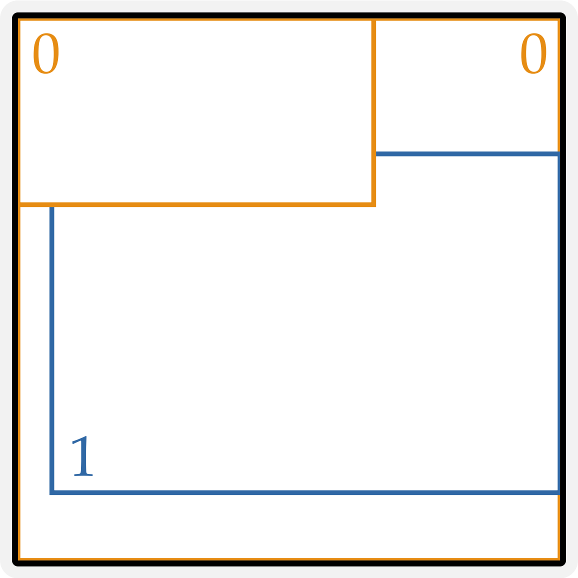
$\mathsf{mon}(F) \le \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



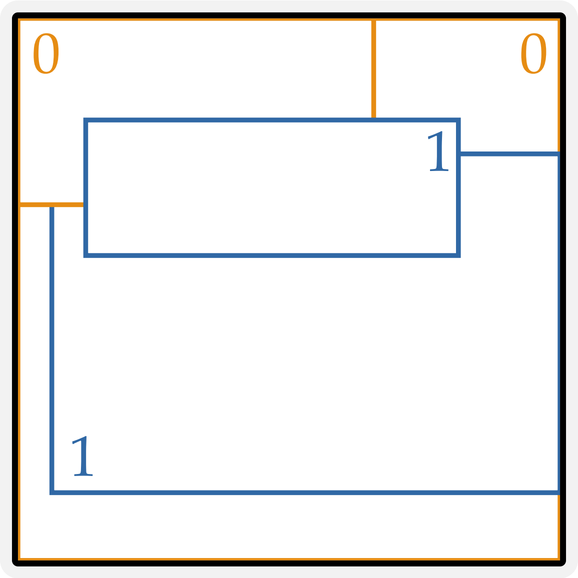
$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



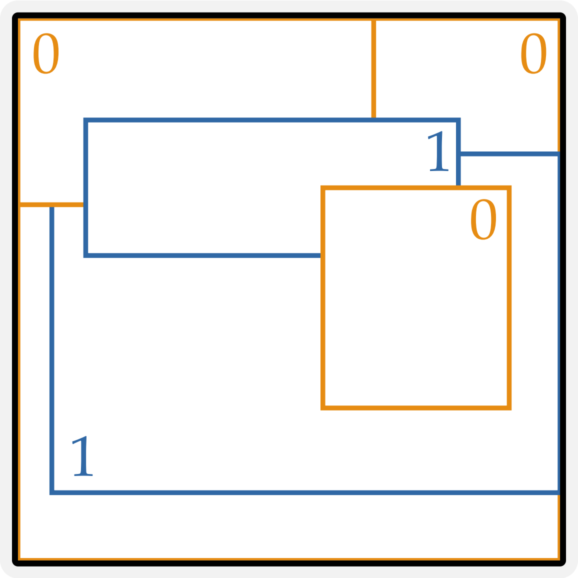
$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



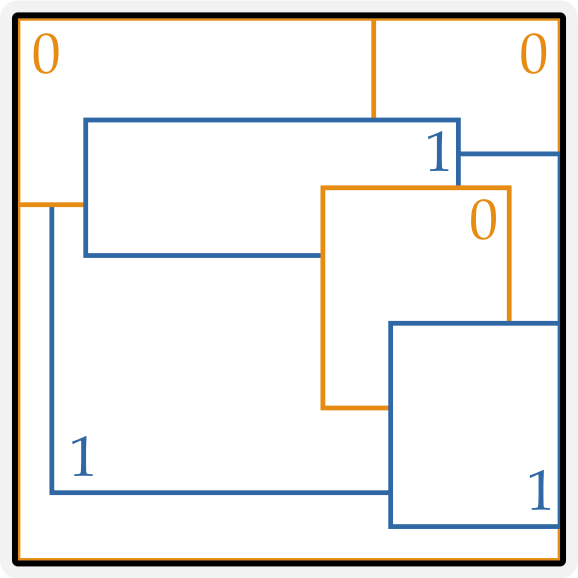
$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



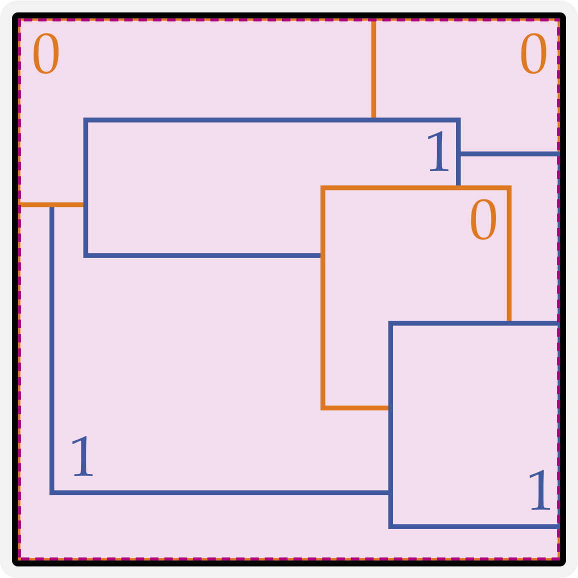
$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



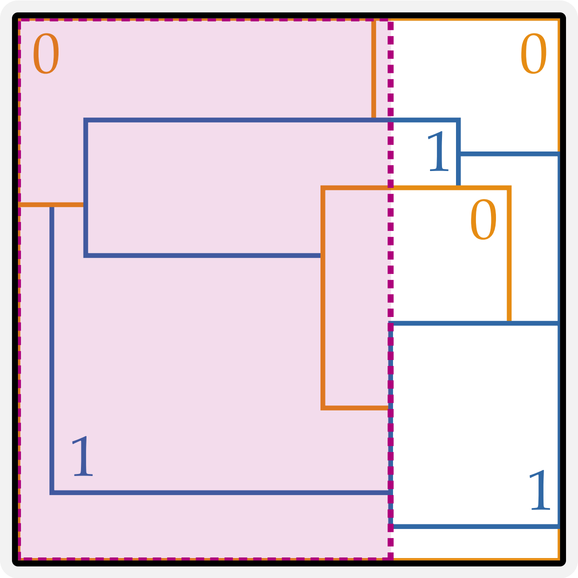
$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



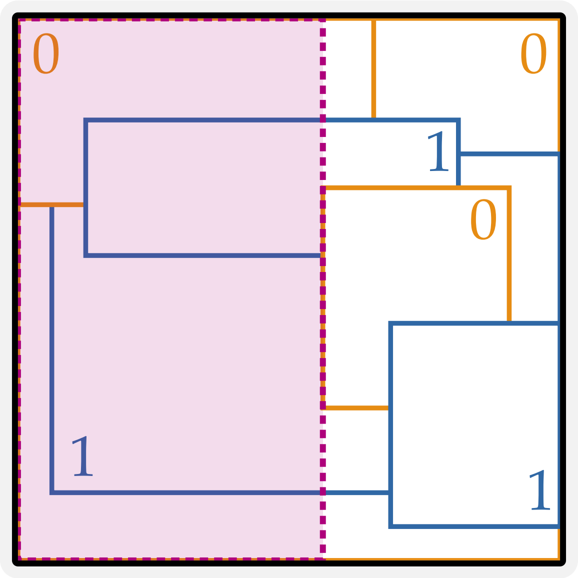
$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



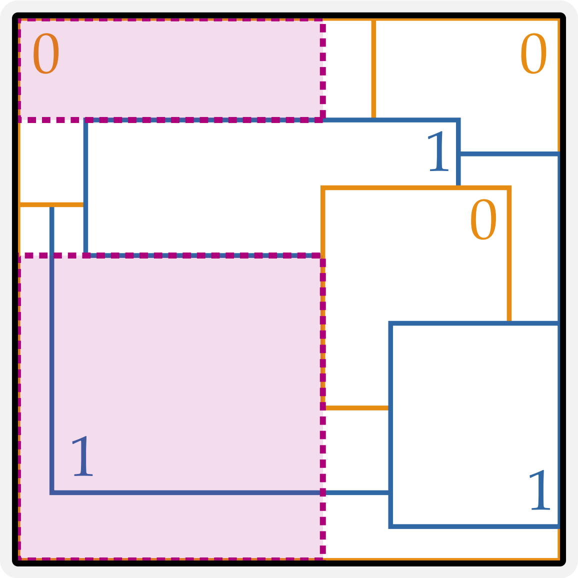
$\mathsf{mon}(F) \le \mathsf{DL^{cc}}(F)$ [IW10,PSS14]



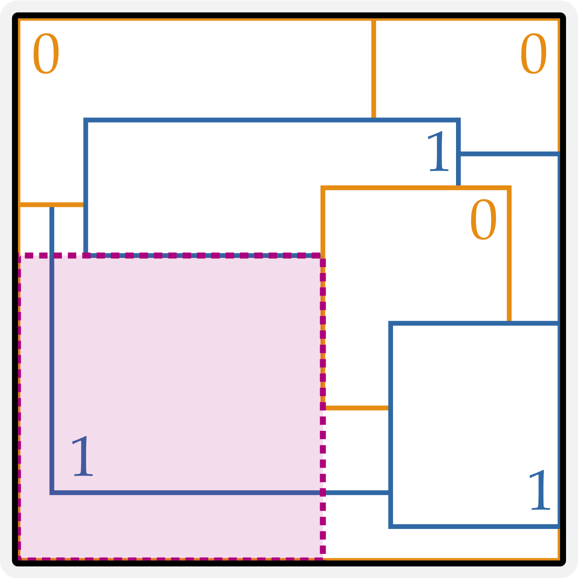
$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



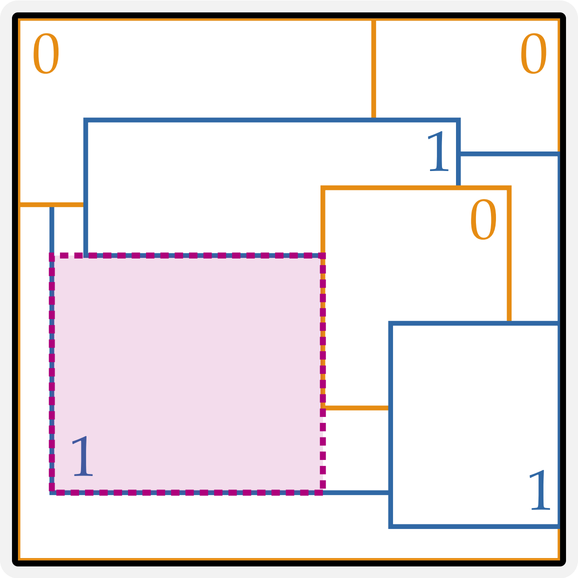
$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



$\mathsf{mon}(F) \leq \mathsf{DL}^{\mathsf{cc}}(F)$ [IW10,PSS14]



Construction

Lifting application:

$$\exists F = f \circ g^n : \quad \mathsf{mon}(F) \lll \mathsf{P}^{\mathsf{NP}^{\mathsf{cc}}}(F)$$

$\forall\cdot$US-complete f

Input:

$M \in \{0,1\}^{\sqrt{n}\times\sqrt{n}}$

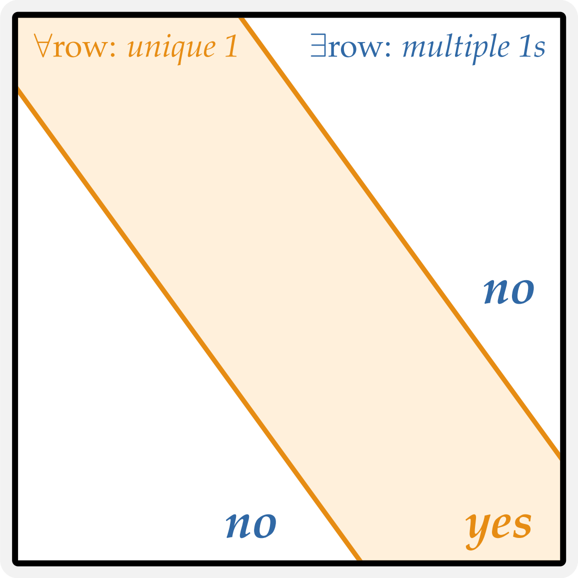
Output:

yes iff

$\forall$ row has unique 1

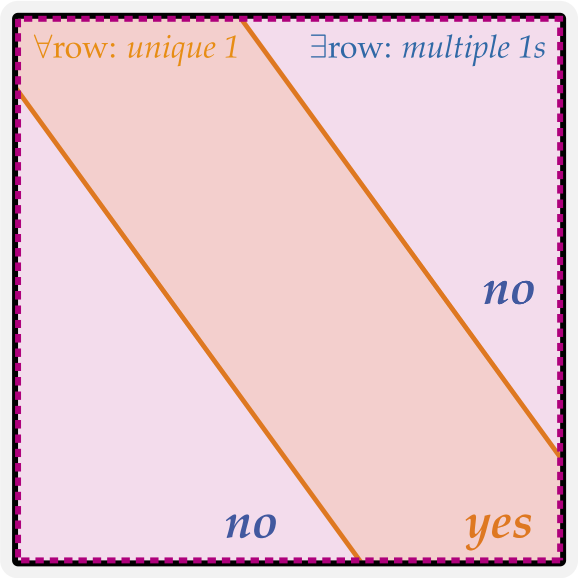
	1				
				1	
		1			
			1		
				1	
1					

$\mathsf{mon}(F) \leq \log^{O(1)} n$



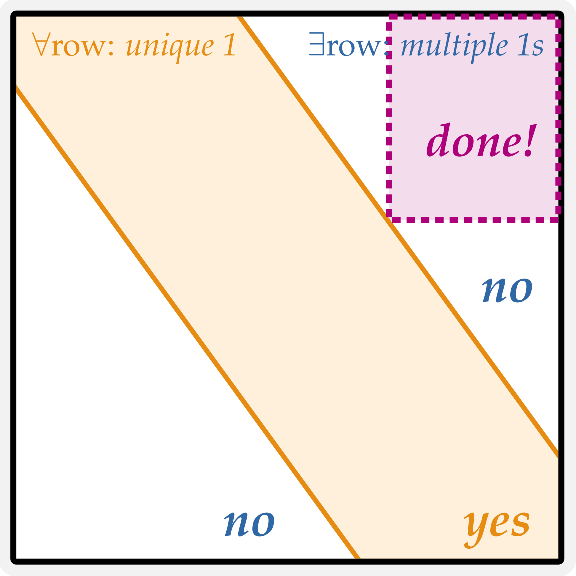
$F \in \forall{\cdot}\mathsf{US}^{\mathsf{cc}}$

$\mathsf{mon}(F) \le \log^{O(1)} n$



$F \in \forall\cdot\mathsf{US}^{\mathsf{cc}}$

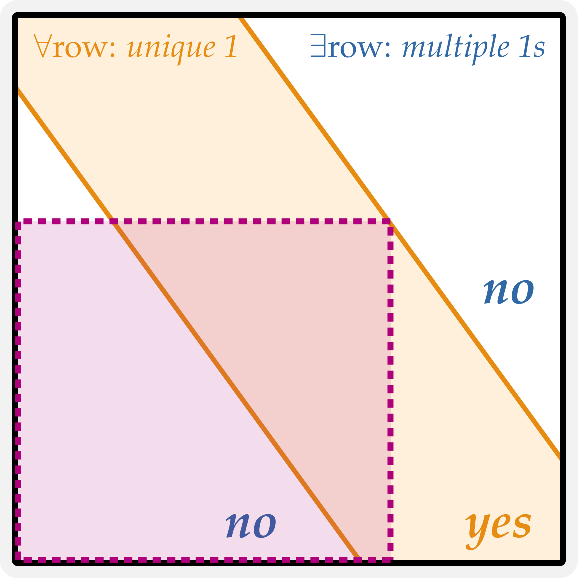
$\mathsf{mon}(F) \leq \log^{O(1)} n$



$F \in \forall\cdot\mathsf{US}^{\mathsf{cc}}$

↓ [IW10,PSS14]

$\mathsf{mon}(F) \leq \log^{O(1)} n$

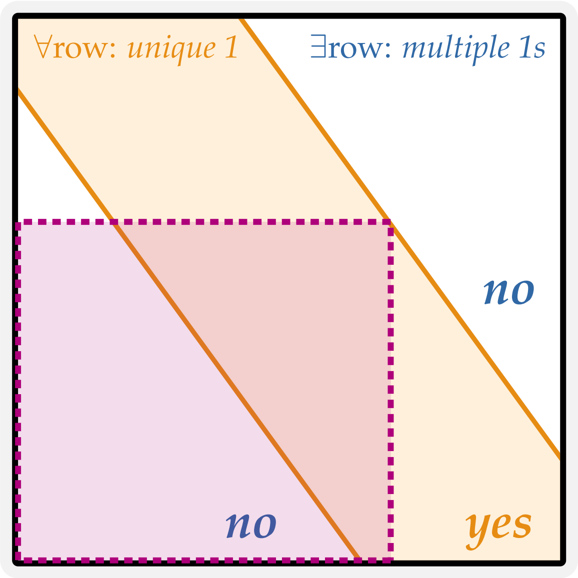


$F \in \forall{\cdot}\mathsf{US}^{\mathsf{cc}}$

↓ [IW10,PSS14]

$F|_{\mu}$

$\mathsf{mon}(F) \leq \log^{O(1)} n$

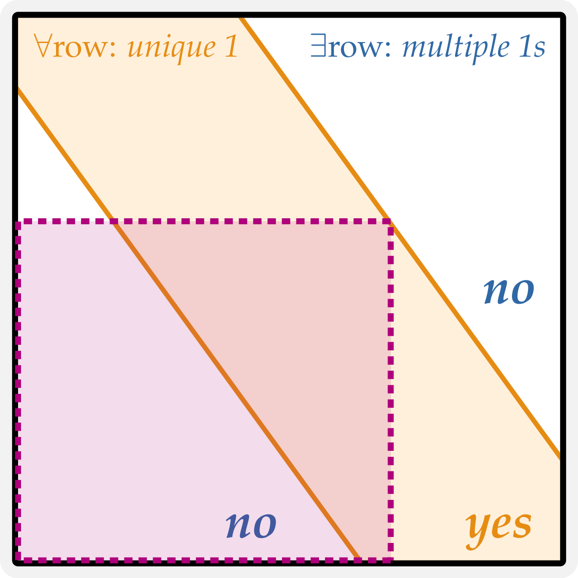


$F \in \forall\cdot\mathsf{US}^{\mathsf{cc}}$

↓ [IW10,PSS14]

$F|_{\mu} \in \forall\cdot\mathsf{UP}^{\mathsf{cc}}$

$\mathsf{mon}(F) \leq \log^{O(1)} n$



$F \in \forall{\cdot}\mathsf{US}^{\mathsf{cc}}$

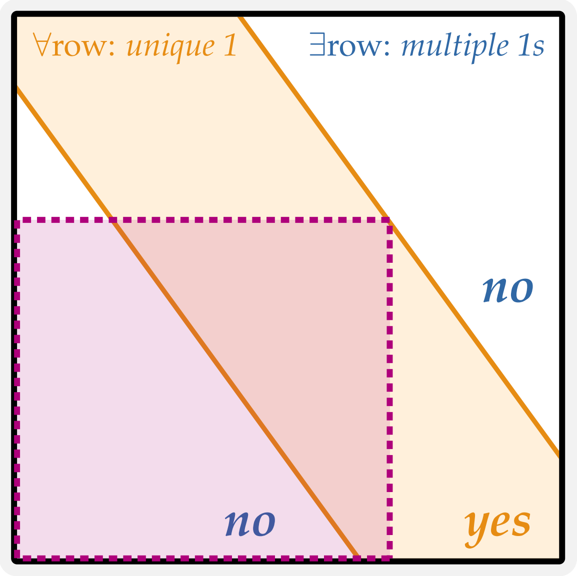
↓ [IW10,PSS14]

$F|_{\mu} \in \forall{\cdot}\mathsf{UP}^{\mathsf{cc}}$

↓ [Yan89]

$F|_{\mu} \in \forall{\cdot}\mathsf{P}^{\mathsf{cc}}$

$\mathsf{mon}(F) \leq \log^{O(1)} n$



$F \in \forall\cdot\mathsf{US}^{\mathsf{cc}}$

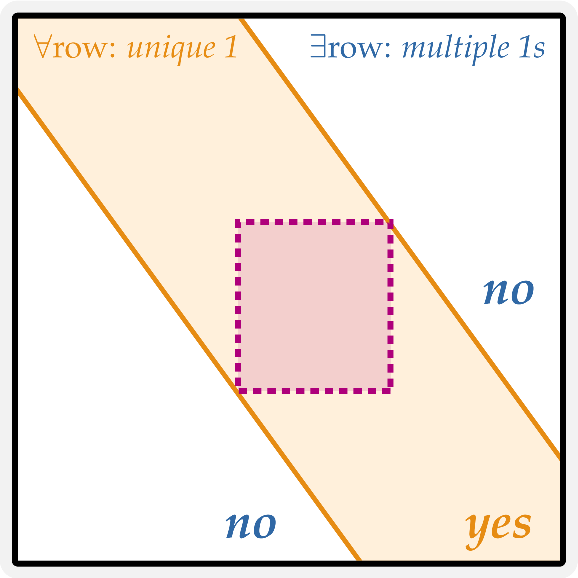
↓ [IW10,PSS14]

$F|_\mu \in \forall\cdot\mathsf{UP}^{\mathsf{cc}}$

↓ [Yan89]

$F|_\mu \in \forall\cdot\mathsf{P}^{\mathsf{cc}}$
$= \mathsf{coNP}^{\mathsf{cc}}$

$\mathsf{mon}(F) \leq \log^{O(1)} n$



$F \in \forall\cdot\mathsf{US}^{\mathsf{cc}}$

↓ [IW10,PSS14]

$F|_\mu \in \forall\cdot\mathsf{UP}^{\mathsf{cc}}$

↓ [Yan89]

$F|_\mu \in \forall\cdot\mathsf{P}^{\mathsf{cc}}$
$= \mathsf{coNP}^{\mathsf{cc}}$

↓ [IW10,PSS14]

done!

Some problems

Problems

- Exhibit F with $\mathsf{mon}(F) \lll \mathsf{UPP^{cc}}(F)$
- Lifting using **constant-size** gadgets?
- Lifting for BQP? [ABG+17]

Challenges

- Disprove the log-rank conjecture 
- Explicit lower bounds against $\mathsf{PH^{cc}}$?
  Or even $\mathsf{SZK^{cc}} \subseteq \mathsf{AM^{cc}} \subseteq \Pi_2\mathsf{P^{cc}}$? [BCHTV16]

Problems

- Exhibit F with $\mathsf{mon}(F) \lll \mathsf{UPP}^{\mathsf{cc}}(F)$
- Lifting using **constant-size** gadgets?
- Lifting for BQP? [ABG+17]

Challenges

- Disprove the log-rank conjecture 
- Explicit lower bounds against $\mathsf{PH}^{\mathsf{cc}}$?
  Or even $\mathsf{SZK}^{\mathsf{cc}} \subseteq \mathsf{AM}^{\mathsf{cc}} \subseteq \Pi_2\mathsf{P}^{\mathsf{cc}}$? [BCHTV16]

Cheers!