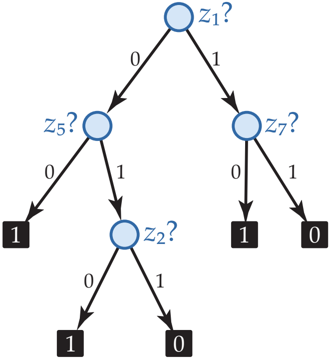
Query-to-Communication Lifting for BPP

(incl. a pseudorandomness lemma)

Mika Göös — *Harvard & Simons Institute*
Toniann Pitassi — *University of Toronto*
Thomas Watson — *University of Memphis*

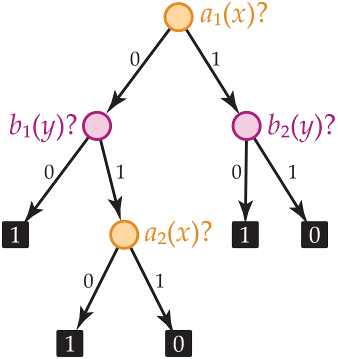
Query vs. Communication

$f(z)$



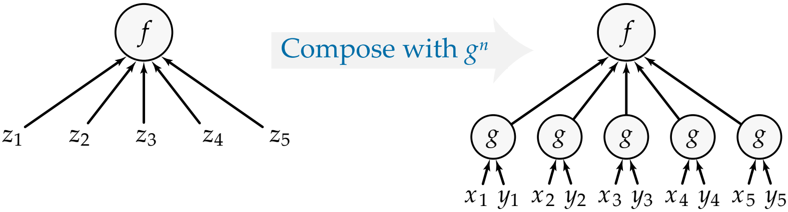
Decision trees

$F(x,y)$



Communication protocols

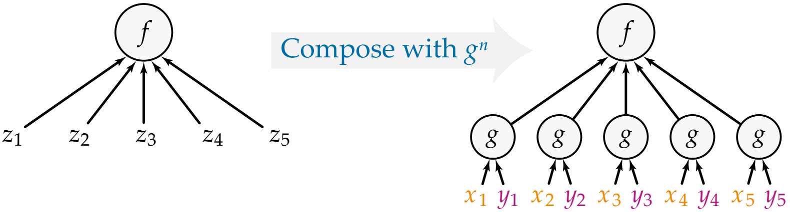
Composed functions $f \circ g^n$



Examples:

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

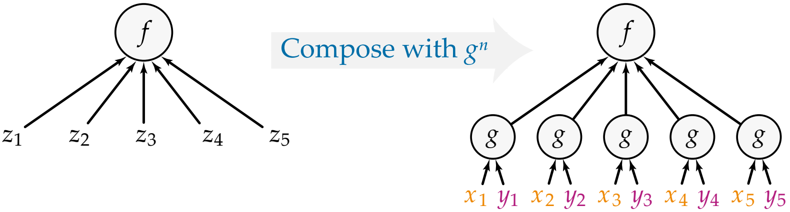
Composed functions $f \circ g^n$



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 $f \circ g^n$

M	Query	Communication	
P	deterministic	deterministic	[RM99, GPW15, dRNV16, HHL16]
NP	nondeterministic	nondeterministic	[GLM$^+$15, G15]
many	poly degree	rank	[SZ09, She11, RS10, RPRC16]
many	conical junta deg.	nonnegative rank	[GLM$^+$15, KMR17]
P^{NP}	decision list	rectangle overlay	[GKPW17]
	Sherali–Adams	LP complexity	[CLRS16, KMR17]
	sum-of-squares	SDP complexity	[LRS15]

Lifting Theorem Template:

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

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

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]

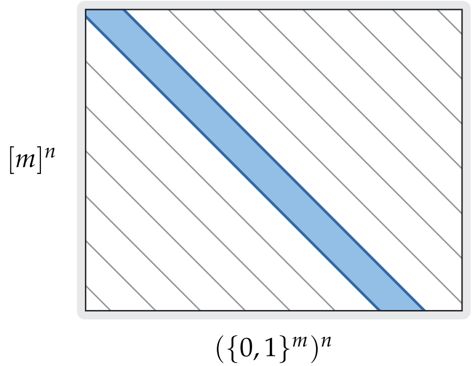
$$\mathsf{BPP}^{\mathsf{cc}}(f \circ g^n) \;\geq\; \mathsf{BPP}^{\mathsf{dt}}(f) \cdot \Omega(\log n)$$

...how to begin?

What we actually prove

Input domain partitioned into **slices**

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

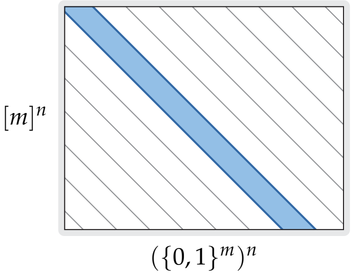


What we actually prove

Simulation

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

- $\boxed{1}$ output of randomised decision tree on input z
- $\boxed{2}$ 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 $\boxed{1} \approx \boxed{2}$

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

Main theorem:

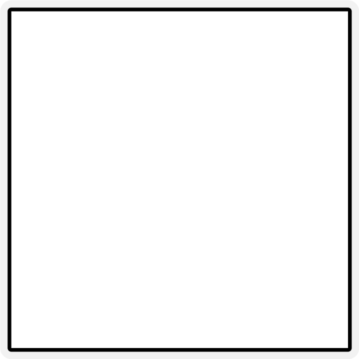
1. pick $\Pi \sim \boldsymbol{\Pi}$
2. simulate Π via query access to z
3. output value of leaf

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

Goal in pictures

Goal: $\boxed{1} \approx \boxed{2}$

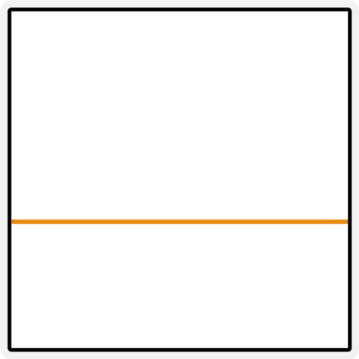
- $\boxed{1}$ output of randomised decision tree on input z
- $\boxed{2}$ transcript generated by Π on input $(\boldsymbol{x}, \boldsymbol{y}) \sim (g^n)^{-1}(z)$

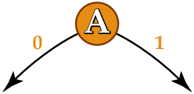


Goal in pictures

Goal: $\boxed{1} \approx \boxed{2}$

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



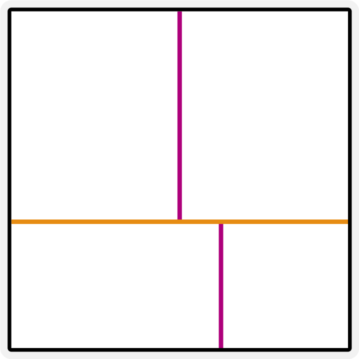


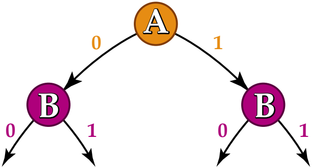
Goal in pictures

Goal: $\boxed{1} \approx \boxed{2}$

$\boxed{1}$ output of randomised decision tree on input z

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

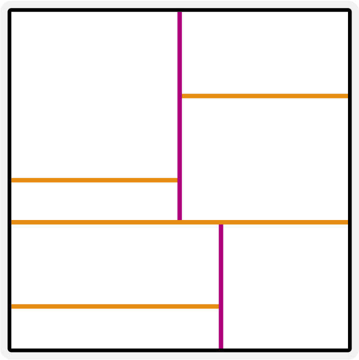


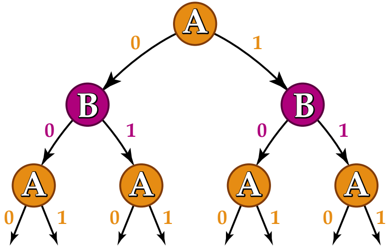


Goal in pictures

Goal: $\boxed{1} \approx \boxed{2}$

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

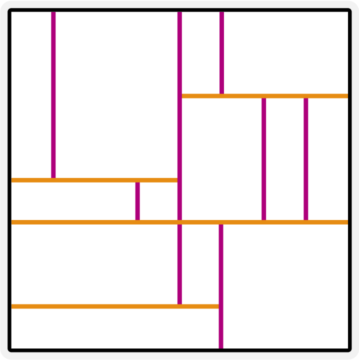


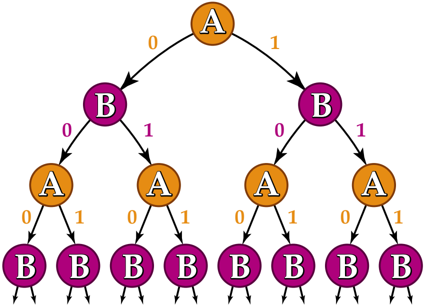


Goal in pictures

Goal: $\boxed{1} \approx \boxed{2}$

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

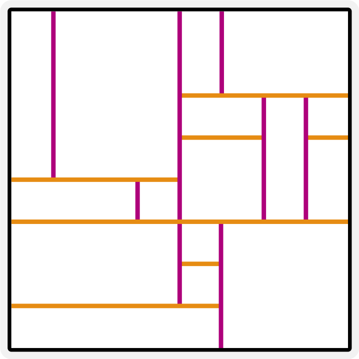


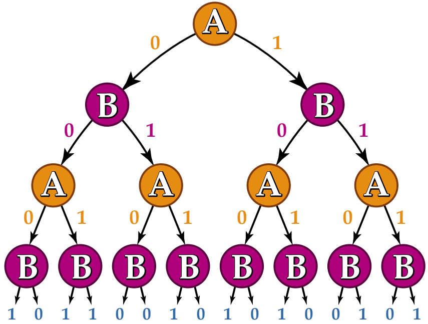


Goal in pictures

Goal: $\boxed{1} \approx \boxed{2}$

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

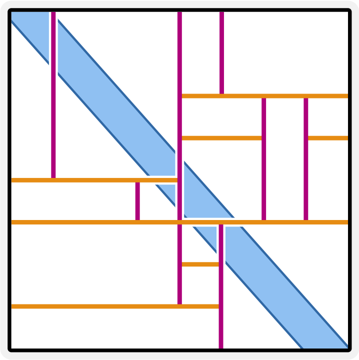


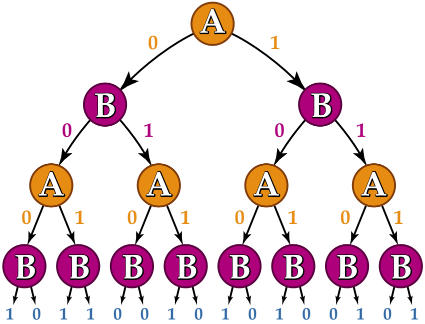


Goal in pictures

Goal: $\boxed{1} \approx \boxed{2}$

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

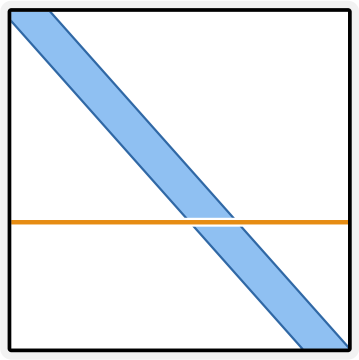


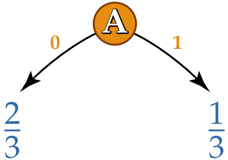


Goal in pictures

Goal: $\boxed{1} \approx \boxed{2}$

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





Idea:

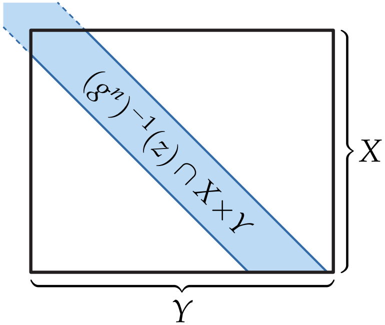
Pretend marginals are uniform!

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

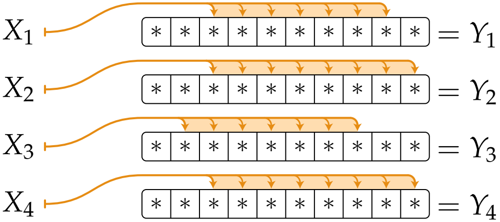


Dense: [GLMWZ15] $\mathbf{H}_\infty(\boldsymbol{X}_I) \geq 0.9 \cdot |I| \log m$ for all $I \subseteq [n]$

Simulation

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

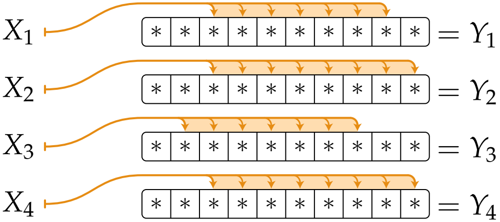
1. Compute partition $X = \bigcup_i X^i$ where each X^i is fixed on some $I \subseteq [n]$ and **dense** on $\bar{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0,1\}^I$
4. Restrict Y so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_{\bar{I}}$ and $X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



Simulation

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

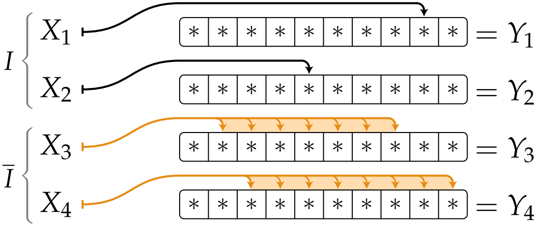
1. Compute partition $X = \bigcup_i X^i$ where each X^i is fixed on some $I \subseteq [n]$ and **dense** on $\bar{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0,1\}^I$
4. Restrict Y so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_{\bar{I}}$ and $X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



Simulation

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

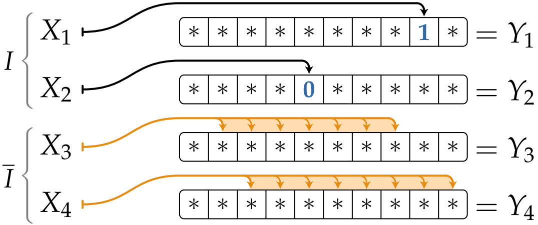
1. Compute partition $X = \bigcup_i X^i$ where each X^i is fixed on some $I \subseteq [n]$ and **dense** on $\bar{I}$ [GLMWZ15]
2. Update $X \leftarrow X^i$ with probability $|X^i|/|X|$
3. Query $z_I \in \{0,1\}^I$
4. Restrict Y so that $g^I(X_I, Y_I) = z_I$
5. Update $Y \leftarrow Y_{\bar{I}}$ and $X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

Some problems

Maybe doable

- Lifting for BQP? [ABG+17]
- Lifting using **constant-size** gadgets?

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]

Maybe doable

- Lifting for BQP? [ABG+17]
- Lifting using **constant-size** gadgets?

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!