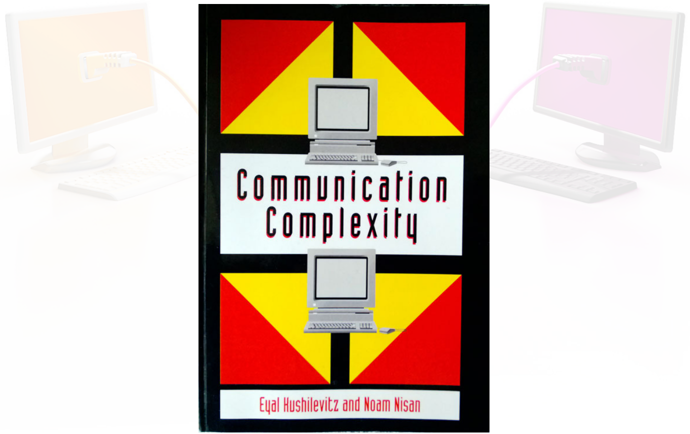
Lower Bounds for

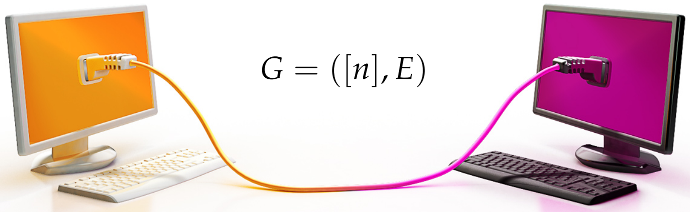
Clique vs. Independent Set

Mika Göös
University of Toronto


Communication Complexity
Eyal Kushilevitz and Noam Nisan

On page 6 . . .

[Yannakakis, STOC'88]



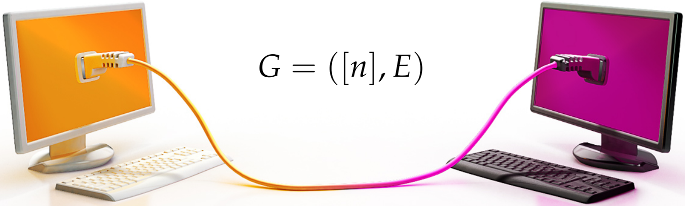
$$G = ([n], E)$$

Alice **Bob**

CIS problem

[Yannakakis, STOC'88]

$G = ([n], E)$



Alice

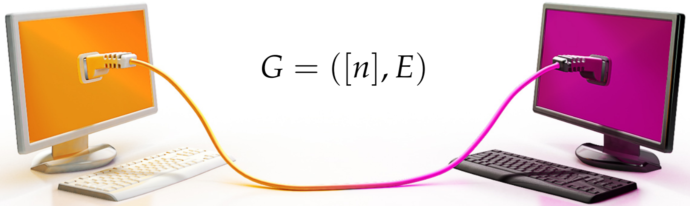
Clique $x \subseteq [n]$ of G

Bob

Independent set $y \subseteq [n]$ of G

CIS problem

[Yannakakis, STOC'88]



$G = ([n], E)$

Alice

Clique $x \subseteq [n]$ of G

Bob

Independent set $y \subseteq [n]$ of G

Compute: $\mathrm{CIS}_G(x, y) = |x \cap y|$

Background

Yannakakis's motivation:

Size of LPs for the vertex packing polytope of G
Breakthrough: [Fiorini et al., STOC'12]

Background

Yannakakis's motivation:

Size of LPs for the vertex packing polytope of G

Breakthrough: [Fiorini et al., STOC'12]

Known bounds:

$\forall G:$ $\quad \mathbf{NP^{cc}}(\mathrm{CIS}_G) = \lceil \log n \rceil$ (guess $x \cap y$)

Background

Yannakakis's motivation:

Size of LPs for the vertex packing polytope of G

Breakthrough: [Fiorini et al., STOC'12]

Known bounds:

$\forall G: \quad \mathbf{NP}^{\mathbf{cc}}(\mathrm{CIS}_G) = \lceil \log n \rceil$ (guess $x \cap y$)

$\forall G: \quad \mathbf{coNP}^{\mathbf{cc}}(\mathrm{CIS}_G) \leq O(\log^2 n)$

Background

Yannakakis's motivation:

Size of LPs for the vertex packing polytope of G

Breakthrough: [Fiorini et al., STOC'12]

Known bounds:

$\forall G:$ $\quad \mathbf{NP}^{\mathbf{cc}}(\mathrm{CIS}_G) = \lceil \log n \rceil$ $\quad$ (guess $x \cap y$)

$\forall G:$ $\quad \mathbf{coNP}^{\mathbf{cc}}(\mathrm{CIS}_G) \leq O(\log^2 n)$

Yannakakis's question:

$\forall G:$ $\quad \mathbf{coNP}^{\mathbf{cc}}(\mathrm{CIS}_G) \leq O(\log n)$?

Background

Alon–Saks–Seymour conjecture:

$\forall G :$ $\qquad \chi(G) \leq \mathrm{bp}(G) + 1 \qquad ?$

Yannakakis's question:

$\forall G :$ $\qquad \mathbf{coNP^{cc}}(\mathrm{CIS}_G) \leq O(\log n) \qquad ?$

Background

Alon–Saks–Seymour conjecture:

$\forall G:$ ~~$\chi(G) \leq \mathrm{bp}(G) + 1$~~ ?

[Huang–Sudakov, 2010]: $\exists G: \ \chi(G) \geq \mathrm{bp}(G)^{6/5}$

Yannakakis's question:

$\forall G:$ $\mathbf{coNP}^{\mathbf{cc}}(\mathrm{CIS}_G) \leq O(\log n)$?

Background

Polynomial Alon–Saks–Seymour conjecture:

$\forall G :$ $\chi(G) \leq \mathbf{poly}(\mathrm{bp}(G))$?

Yannakakis's question:

$\forall G :$ $\mathbf{coNP^{cc}}(\mathrm{CIS}_G) \leq O(\log n)$?

Background

Polynomial Alon–Saks–Seymour conjecture:

$\forall G:$ $\chi(G) \leq \mathbf{poly}(\mathrm{bp}(G))$?

[Alon–Haviv] $\Downarrow$ $\Uparrow$ [Bousquet et al.]

Yannakakis's question:

$\forall G:$ $\mathbf{coNP}^{\mathbf{cc}}(\mathrm{CIS}_G) \leq O(\log n)$?

Background

Po[redacted]ynomial Alon–Saks–Seymour conj[redacted]re:

∀G : [redacted]$(G) \le$ **poly**$($bp(G)[redacted] ?

[Alon–Haviv] $\Downarrow$ $\Uparrow$ [Bousquet et al.]

Yannaka[redacted]question:

$\forall$G[redacted] $\mathbf{coNP^{cc}}(\mathrm{CIS}_G) \le O(\log n)$?

Our result

Main theorem

$$\exists G : \quad \mathbf{coNP^{cc}}(\mathrm{CIS}_G) \;\geq\; \Omega(\log^{1.128} n)$$

Our result

Main theorem

$$\exists G: \quad \mathbf{coNP^{cc}}(\mathrm{CIS}_G) \;\geq\; \Omega(\log^{1.128} n)$$

Prior bounds

Measure	Lower bound	Reference
$\mathbf{P^{cc}}$	$2 \cdot \log n$	Kushilevitz, Linial, and Ostrovsky (1999)
$\mathbf{coNP^{cc}}$	$6/5 \cdot \log n$	Huang and Sudakov (2010)
$\mathbf{coNP^{cc}}$	$3/2 \cdot \log n$	Amano (2014)
$\mathbf{coNP^{cc}}$	$2 \cdot \log n$	Shigeta and Amano (2014)

Our result

Main theorem

$$\exists G : \quad \mathbf{coNP^{cc}}(\mathrm{CIS}_G) \;\geq\; \Omega(\log^{1.128} n)$$

Proof strategy:

Query complexity $\longrightarrow$ Communication complexity

Cf. lower bounds for log-rank
[Nisan–Wigderson, 1995]

Models of communication

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

$$F\colon \mathcal{X} \times \mathcal{Y} \to \{0,1\}$$

Models of communication

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

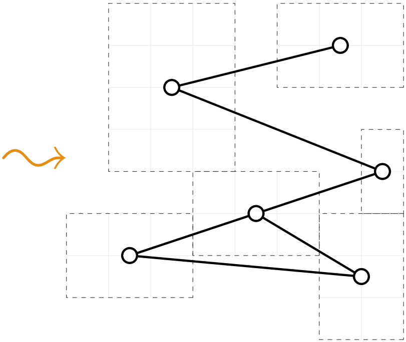
$\mathbf{NP}^{\mathbf{cc}}$

Models of communication

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

$\mathbf{UP}^{\mathbf{cc}}$

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



CIS_G is complete for $\mathbf{UP}^{\mathrm{cc}}$: $F \leq \mathrm{CIS}_G$

$$\mathbf{UP}^{\mathrm{cc}}(F) = \mathbf{UP}^{\mathrm{cc}}(\mathrm{CIS}_G) = \log n$$

Proof strategy

Restatement of Main theorem:

$\exists F\colon \mathcal{X} \times \mathcal{Y} \to \{0,1\} \qquad \mathbf{coNP^{cc}}(F) \;\geq\; \mathbf{UP^{cc}}(F)^{1.128}$

Proof strategy

Restatement of Main theorem:

$\exists F\colon \mathcal{X} \times \mathcal{Y} \to \{0,1\} \qquad \mathbf{coNP^{cc}}(F) \geq \mathbf{UP^{cc}}(F)^{1.128}$

Query separation:

$\exists f\colon \{0,1\}^n \to \{0,1\} \qquad \mathbf{coNP^{dt}}(f) \geq \mathbf{UP^{dt}}(f)^{1.128}$

Proof strategy

Restatement of Main theorem:

$\exists F \colon \mathcal{X} \times \mathcal{Y} \to \{0,1\} \qquad \mathbf{coNP^{cc}}(F) \;\geq\; \mathbf{UP^{cc}}(F)^{1.128}$

Query separation:

$\exists f \colon \{0,1\}^n \to \{0,1\} \qquad \mathbf{coNP^{dt}}(f) \;\geq\; \mathbf{UP^{dt}}(f)^{1.128}$

Decision tree complexity measures:

$\mathbf{NP^{dt}}$ = DNF width = 1-certificate complexity

$\mathbf{coNP^{dt}}$ = CNF width = 0-certificate complexity

$\mathbf{UP^{dt}}$ = Unambiguous DNF width

Proof strategy

Restatement of Main theorem:

$\exists F\colon \mathcal{X} \times \mathcal{Y} \to \{0,1\} \qquad \mathbf{coNP^{cc}}(F) \;\geq\; \mathbf{UP^{cc}}(F)^{1.128}$

Query separation:

$\exists f\colon \{0,1\}^n \to \{0,1\} \qquad \mathbf{coNP^{dt}}(f) \;\geq\; \mathbf{UP^{dt}}(f)^{1.128}$

Agenda:

- **Step 1:** Query separation
- **Step 2:** Simulation theorem [GLMWZ, 2015]

Step 1: Query separation

Warm-up

Example: Let $f(x_1, x_2, x_3) = 1$ iff $x_1 + x_2 + x_3 \in \{1, 2\}$

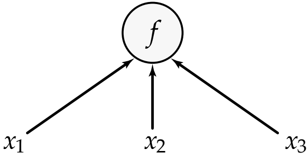
- $\mathbf{UP^{dt}}(f) = 2$ because $f \equiv x_1\bar{x}_2 \vee x_2\bar{x}_3 \vee x_3\bar{x}_1$
- $\mathbf{coNP^{dt}}(f) = 3$ because 0-input $\vec{0}$ is *fully sensitive*

Warm-up

Example: Let $f(x_1, x_2, x_3) = 1$ iff $x_1 + x_2 + x_3 \in \{1, 2\}$

- $\mathbf{UP^{dt}}(f) = 2$ because $f \equiv x_1\bar{x}_2 \vee x_2\bar{x}_3 \vee x_3\bar{x}_1$
- $\mathbf{coNP^{dt}}(f) = 3$ because 0-input $\vec{0}$ is *fully sensitive*

Recursive composition:



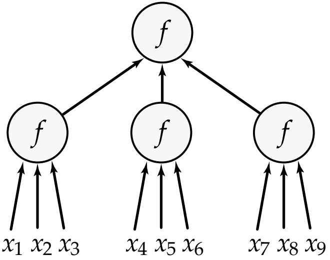
$$f^1(\cdot) := f(\cdot)$$
$$f^{i+1}(\cdot) := f(f^i(\cdot), f^i(\cdot), f^i(\cdot))$$

Warm-up

Example: Let $f(x_1, x_2, x_3) = 1$ iff $x_1 + x_2 + x_3 \in \{1, 2\}$

- $\mathbf{UP}^{\mathbf{dt}}(f) = 2$ because $f \equiv x_1\bar{x}_2 \vee x_2\bar{x}_3 \vee x_3\bar{x}_1$
- $\mathbf{coNP}^{\mathbf{dt}}(f) = 3$ because 0-input $\vec{0}$ is *fully sensitive*

Recursive composition:



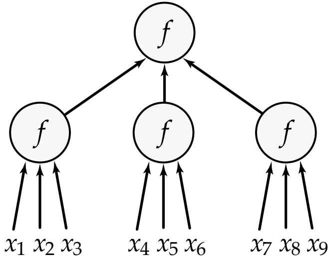
$$f^1(\cdot) := f(\cdot)$$
$$f^{i+1}(\cdot) := f(f^i(\cdot), f^i(\cdot), f^i(\cdot))$$

Warm-up

Example: Let $f(x_1, x_2, x_3) = 1$ iff $x_1 + x_2 + x_3 \in \{1,2\}$

- $\mathbf{UP}^{\mathbf{dt}}(f) = 2$ because $f \equiv x_1\bar{x}_2 \vee x_2\bar{x}_3 \vee x_3\bar{x}_1$
- $\mathbf{coNP}^{\mathbf{dt}}(f) = 3$ because 0-input $\vec{0}$ is *fully sensitive*

Recursive composition:



$$f^1(\cdot) := f(\cdot)$$
$$f^{i+1}(\cdot) := f(f^i(\cdot), f^i(\cdot), f^i(\cdot))$$

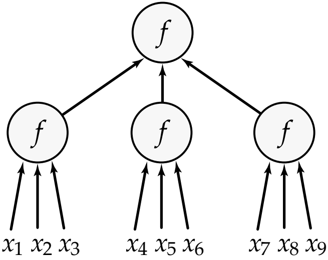
Hope: $$\frac{\mathbf{coNP}^{\mathbf{dt}}(f^i)}{\mathbf{UP}^{\mathbf{dt}}(f^i)} \geq \left(\frac{3}{2}\right)^i$$

Warm-up

Problem!

In order to certify "$f^i(\cdot) = 1$", (should be *easy*)
might need to certify "$f^{i-1}(\cdot) = 0$" (should be *hard*)

Recursive composition:



$$f^1(\cdot) := f(\cdot)$$
$$f^{i+1}(\cdot) := f(f^i(\cdot), f^i(\cdot), f^i(\cdot))$$

Hope: $\frac{\mathbf{coNP}^{\mathrm{dt}}(f^i)}{\mathbf{UP}^{\mathrm{dt}}(f^i)} \geq \left(\frac{3}{2}\right)^i$

Warm-up

Problem!

In order to certify "$f^i(\cdot) = 1$", (should be *easy*)
might need to certify "$f^{i-1}(\cdot) = 0$" (should be *hard*)

Solution: Enlarge input/output alphabets

$$f\colon (\{0\} \cup \Sigma)^n \to \{0\} \cup \Sigma$$

Warm-up

Problem!

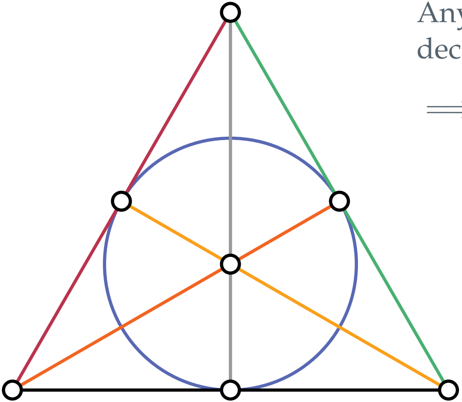
In order to certify "$f^i(\cdot) = 1$", (should be *easy*)
might need to certify "$f^{i-1}(\cdot) = 0$" (should be *hard*)

Solution: Enlarge input/output alphabets

$$f\colon (\{0\} \cup \Sigma)^n \to \{0\} \cup \Sigma$$

Now: In order to certify "$f^i(\cdot) = \sigma$" for $\sigma \in \Sigma$,
only need to certify "$f^{i-1}(\cdot) = \sigma'$" for $\sigma' \in \Sigma$

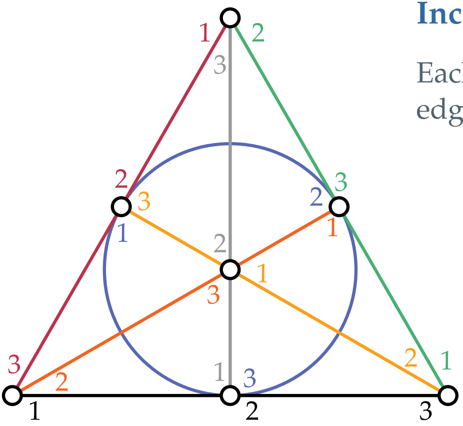
Defining f



Any two certificates in an $\mathbf{UP}^{\mathbf{dt}}$ decision tree intersect in variables

$\implies$ **Finite projective planes!**

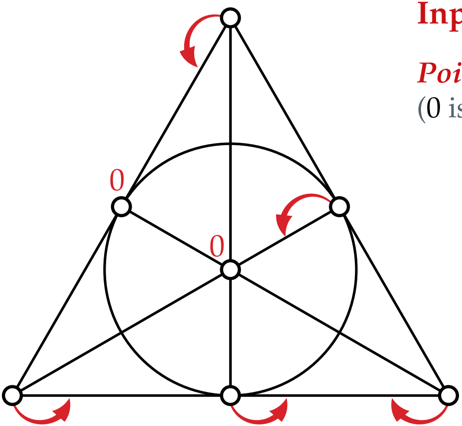
Defining f



Incidence ordering:

Each node orders its incident edges using numbers from $[3]$

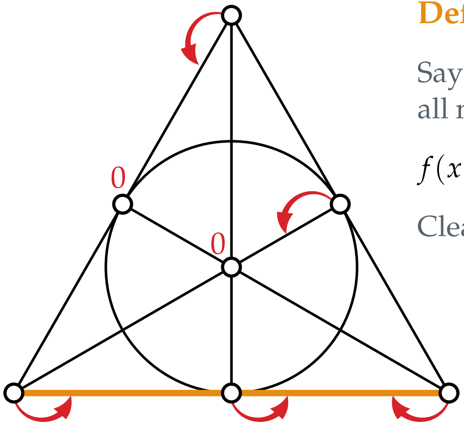
Defining f



Inputs to nodes:

Pointer values from $\{0\} \cup \underbrace{[3]}_{=\Sigma}$
(0 is a *null pointer*)

Defining f



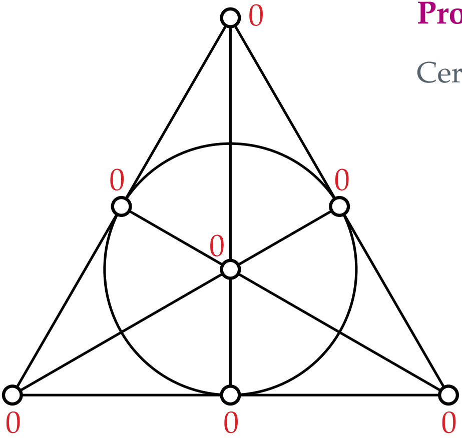
Defining $f\colon (\{0\} \cup [3])^7 \to \{0,1\}$

Say edge e is ***satisfied*** on input x iff all nodes $v \in e$ point to e under x

$f(x) = 1$ iff x satisfies an edge

Clearly $\mathbf{UP}^{\mathbf{dt}}(f) = 3$

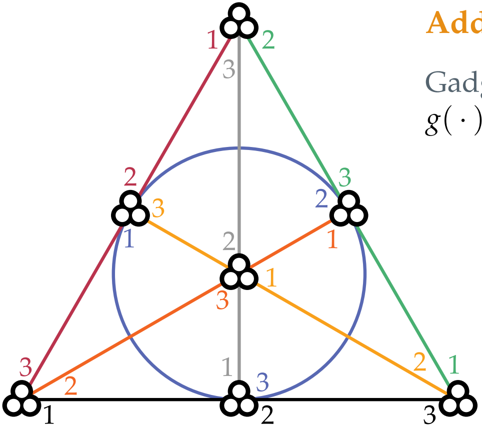
Defining f



Problem!

Certifying "$f(\vec{0}) = 0$" too easy!

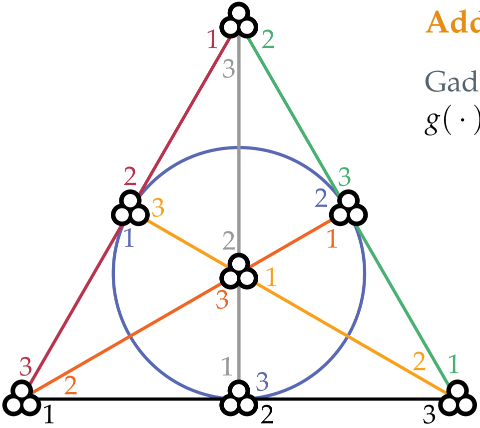
Defining f



Add input weights: $f \circ g^7$

Gadget g is such that deciding if $g(\cdot) = i$ for $i \in [3]$ costs i queries

Defining f

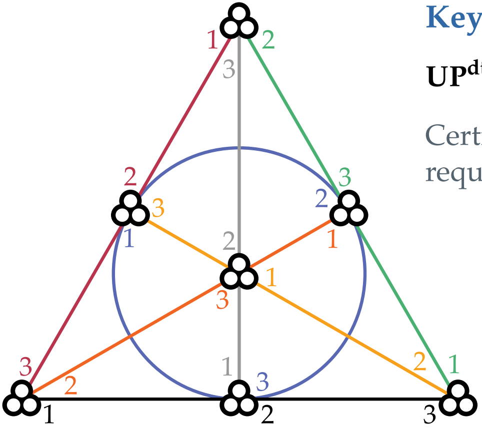


Add input weights: $f \circ g^7$

Gadget g is such that deciding if $g(\cdot) = i$ for $i \in [3]$ costs i queries

$1**$	$\mapsto$	1
$2**$	$\mapsto$	2
$02*$	$\mapsto$	2
$3**$	$\mapsto$	3
$03*$	$\mapsto$	3
003	$\mapsto$	3
Else	$\mapsto$	0

Defining f

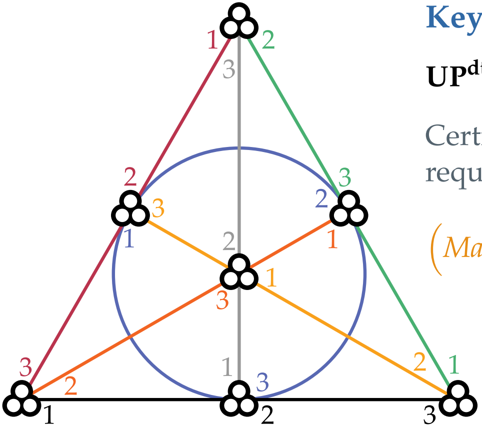


Key properties:

$\mathbf{UP}^{\mathbf{dt}}(f \circ g^7) = 1 + 2 + 3 = 6$

Certifying "$(f \circ g^7)(\vec{0}) = 0$" requires (# edges) = 7 queries

Defining f



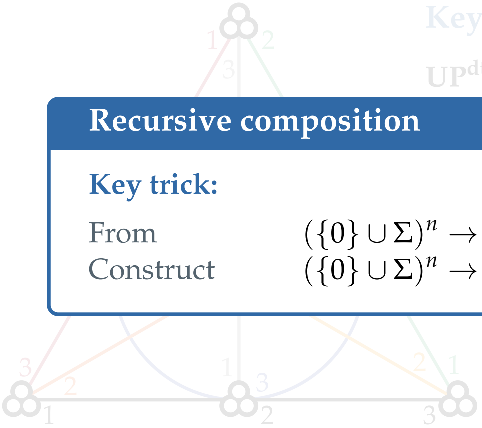
Key properties:

$\mathbf{UP}^{\mathbf{dt}}(f \circ g^7) = 1 + 2 + 3 = 6$

Certifying "$(f \circ g^7)(\vec{0}) = 0$" requires (# edges) = 7 queries

$\Big($*Magic numerology:* $57 \approx 36^{1.128}\Big)$

Defining f



Key properties:

$\mathrm{UP}^{\mathrm{dt}}(f \circ g^7) = 1 + 2 + 3 = 6$

Recursive composition

Key trick:

From	$(\{0\} \cup \Sigma)^n \to \{0, \mathbf{1}\}$
Construct	$(\{0\} \cup \Sigma)^n \to \{0\} \cup \{\textbf{pointers}\}$

Query separation:

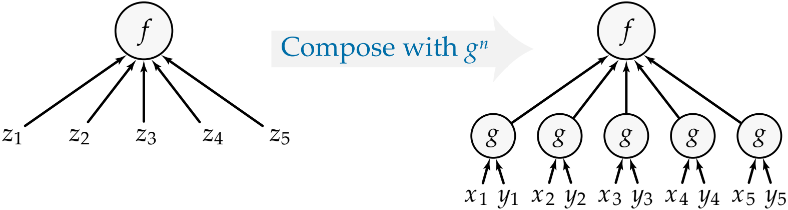
$\exists f\colon \{0,1\}^n \to \{0,1\}$ $\qquad \mathbf{coNP^{dt}}(f) \;\geq\; \mathbf{UP^{dt}}(f)^{1.128}$

Step 2: Simulation theorem from

"Rectangles Are Nonnegative Juntas"

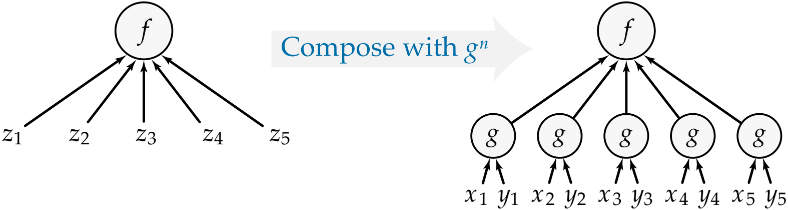
Mika Göös, Shachar Lovett, Raghu Meka, Thomas Watson, and David Zuckerman (STOC'15)

Composed functions $f \circ g^n$



Examples: Set-disjointness: $\text{OR} \circ \text{AND}^n$
Inner-product: $\text{XOR} \circ \text{AND}^n$

Composed functions $f \circ g^n$



Examples: Set-disjointness: $\mathrm{OR} \circ \mathrm{AND}^n$
Inner-product: $\mathrm{XOR} \circ \mathrm{AND}^n$

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

- **Alice** holds $x \in \{0,1\}^{bn}$
- **Bob** holds $y \in \{0,1\}^{bn}$

We choose: $g =$ inner-product with $b = \Theta(\log n)$ bits per party

Approximation by juntas

Conical d-junta:

Nonnegative combination of d-conjunctions
(Example: $0.4 \cdot z_1\bar{z}_2 + 0.66 \cdot z_2\bar{z}_3 + 0.35 \cdot z_3\bar{z}_1$)

Approximation by juntas

Conical d-junta:

Nonnegative combination of d-conjunctions
(Example: $0.4 \cdot z_1\bar{z}_2 + 0.66 \cdot z_2\bar{z}_3 + 0.35 \cdot z_3\bar{z}_1$)

Main Structure Theorem:

Suppose Π is cost-d randomised protocol for $f \circ g^n$
Then there exists a conical d-junta h s.t. $\forall z \in \mathrm{dom}\, f$:

$$\Pr_{(\boldsymbol{x},\boldsymbol{y})\sim(g^n)^{-1}(z)}[\,\Pi(\boldsymbol{x},\boldsymbol{y}) \text{ accepts}\,] \;\approx\; h(z)$$

Approximation by juntas

Conical d-junta:

Nonnegative combination of d-conjunctions
(Example: $0.4 \cdot z_1\bar{z}_2 + 0.66 \cdot z_2\bar{z}_3 + 0.35 \cdot z_3\bar{z}_1$)

Main Structure Theorem:

Suppose Π is cost-d randomised protocol for $f \circ g^n$
Then there exists a conical d-junta h s.t. $\forall z \in \mathrm{dom}\, f$:

$$\Pr_{(\boldsymbol{x},\boldsymbol{y})\sim(g^n)^{-1}(z)}[\,\Pi(\boldsymbol{x},\boldsymbol{y}) \text{ accepts}\,] \;\approx\; h(z)$$

Cf. Polynomial approximation [Razborov, Sherstov, Shi–Zhu,...]**:**

Approximate poly-degree of AND $= \Theta(\sqrt{n})$
Approximate junta-degree of AND $= \Theta(n)$

Corollaries

Simulation for NP:

$$\mathbf{NP}^{\mathbf{cc}}(f \circ g^n) = \Theta(\mathbf{NP}^{\mathbf{dt}}(f) \cdot b)$$

…recall $b = \Theta(\log n)$

Conical d-junta: $0.4 \cdot z_1\bar{z}_2 + 0.66 \cdot z_2\bar{z}_3 + 0.35 \cdot z_3\bar{z}_1$

$\rightsquigarrow$

d-DNF: $z_1\bar{z}_2 \lor z_2\bar{z}_3 \lor z_3\bar{z}_1$

Corollaries

Simulation for NP:

$$\mathbf{NP}^{\mathbf{cc}}(f \circ g^n) = \Theta(\mathbf{NP}^{\mathbf{dt}}(f) \cdot b)$$

…recall $b = \Theta(\log n)$

Trivially: $\mathbf{UP}^{\mathbf{cc}}(f \circ g^n) \leq O(\mathbf{UP}^{\mathbf{dt}}(f) \cdot b)$

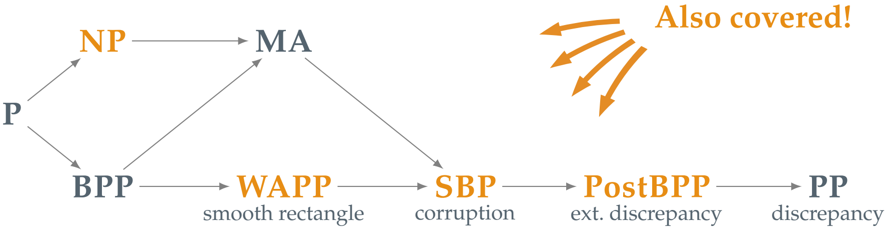
Main theorem follows!

Corollaries

Simulation for NP:

$$\mathbf{NP}^{\mathrm{cc}}(f \circ g^n) = \Theta(\mathbf{NP}^{\mathrm{dt}}(f) \cdot b)$$

…recall $b = \Theta(\log n)$



Summary

Main result

- $\exists G: \quad \mathbf{coNP^{cc}}(\mathrm{CIS}_G) \geq \Omega(\log^{1.128} n)$

Open problems

- Better separation for $\mathbf{coNP^{dt}}$ vs. $\mathbf{UP^{dt}}$?
- Simulation theorems for new models (e.g., **BPP**)
- Improve gadget size down to $b = O(1)$
  (Would give new proof of $\Omega(n)$ bound for set-disjointness)

Summary

Main result

- $\exists G: \quad \mathbf{coNP^{cc}}(\mathrm{CIS}_G) \geq \Omega(\log^{1.128} n)$

Open problems

- Better separation for $\mathbf{coNP^{dt}}$ vs. $\mathbf{UP^{dt}}$?
- Simulation theorems for new models (e.g., **BPP**)
- Improve gadget size down to $b = O(1)$
  (Would give new proof of $\Omega(n)$ bound for set-disjointness)

Cheers!