Monotone Circuit Lower bounds via Query-to-Communication Lifting

Pritish Kamath

based on joint works with

Ankit
Garg

Mika
Göös

Robert
Robere

Dmitry
Sokolov

Lower Bounds on Algorithms?

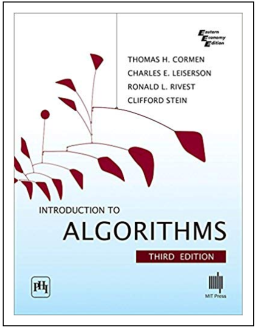
What makes problems computationally hard?

Lower Bounds on Algorithms?

Dynamic Programming

Divide-and-Conquer

Matrix Multiplication

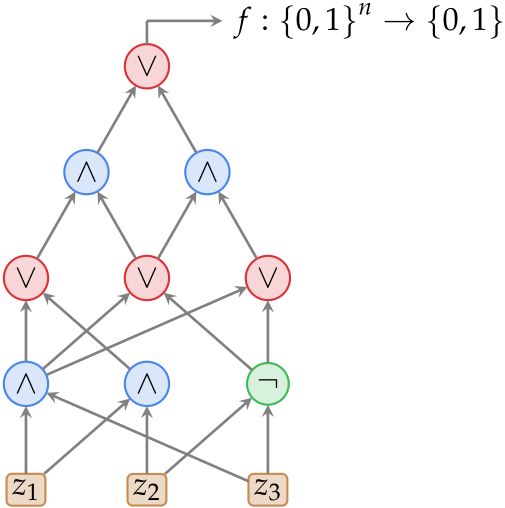


Fibonacci Heaps

Linear/Semidefinite Programming

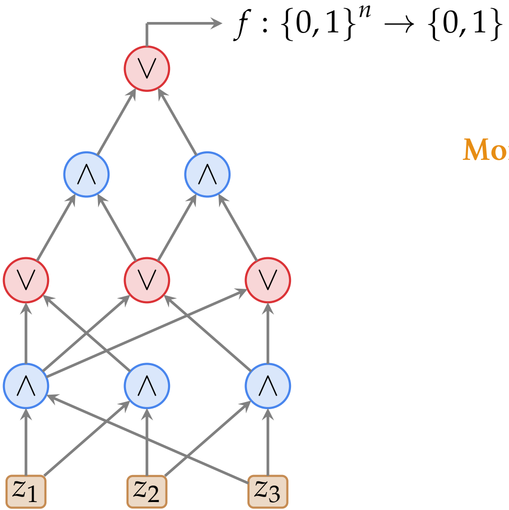
Fast Fourier Transform

Lower Bounds on ~~Algorithms~~ Circuits?



Size: Number of gates

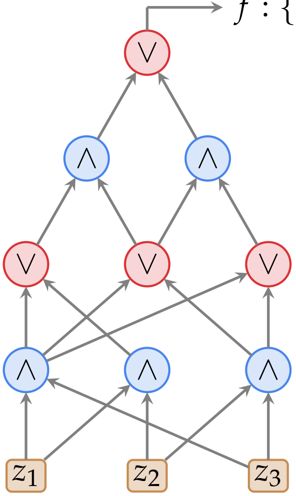
Lower Bounds on Monotone Circuits?



Size: Number of gates

Monotone: $\forall i : x_i \leq y_i \implies f(x) \leq f(y)$

Lower Bounds on Monotone Circuits?



$f : \{0,1\}^n \to \{0,1\}$

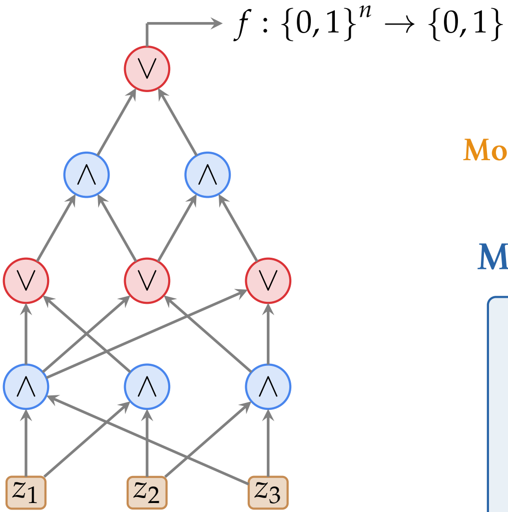
Size: Number of gates

Monotone: $\forall i : x_i \leq y_i \implies f(x) \leq f(y)$

Monotone Circuit Lower Bounds

- [Razborov84, AB85] : k-Clique requires exponential sized monotone circuits

Lower Bounds on Monotone Circuits?



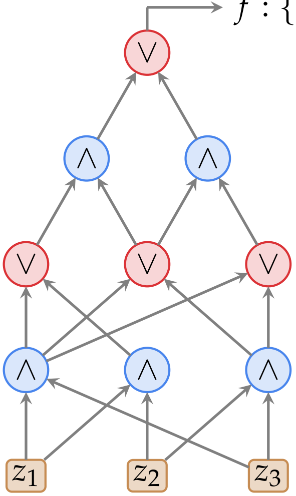
Size: Number of gates

Monotone: $\forall i : x_i \leq y_i \implies f(x) \leq f(y)$

Monotone Circuit Lower Bounds

- [Razborov84, AB85] : k-Clique requires exponential sized monotone circuits
- [Razborov85] : Matching $\in$ P requires super-polynomial sized monotone circuits

Lower Bounds on Monotone Circuits?



$f : \{0,1\}^n \to \{0,1\}$

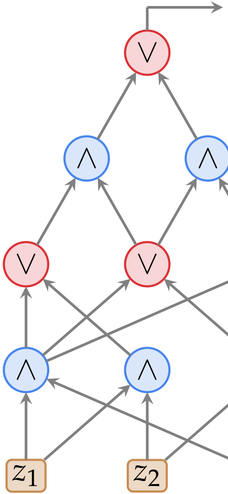
Size: Number of gates

Monotone: $\forall i : x_i \leq y_i \implies f(x) \leq f(y)$

Monotone Circuit Lower Bounds

- [Razborov84, AB85] : k-CLIQUE requires exponential sized monotone circuits
- [Razborov85] : MATCHING $\in$ P requires super-polynomial sized monotone circuits
- [Tardos88] : TARDOS $\in$ P requires exponential sized monotone circuits

Lower Bounds on Monotone Circuits?



$$f : \{0,1\}^n \to \{0,1\}$$

Connections:

- Communication Complexity
  Karchmer–Wigderson games
- Proof Complexity
  Monotone Feasible Interpolation
- LP Extension Complexity
  Hrubeš–Razborov / Göös–Jain–Watson
- Cryptography
  Secret Sharing

Theme of this workshop : Lifting Theorems!

Weak Model

Strong Model

Theme of this workshop : Lifting Theorems!

Weak Model | **Strong Model**

Cannot do X → *Lifting Theorem* → Cannot do $\widetilde{X}$

Theme of this workshop : Lifting Theorems!

Resolution Refutations

Monotone Circuits

Theme of this workshop : Lifting Theorems!

Feasible Interpolation

[BPR97, Kra97]

Resolution Refutations

Monotone Circuits

Theme of this workshop : Lifting Theorems!

Resolution Refutations

Feasible Interpolation
[BPR97, Kra97]

Lifting Theorem
[This talk]

Monotone Circuits

Theme of this workshop : Lifting Theorems!

Feasible Interpolation
[BPR97, Kra97]

Resolution Refutations

Lifting Theorem
[This talk]

Monotone Circuits

THEOREM

n-variate k-CNF $\mathcal{F}$		$n^{O(k)}$-variate function f
Resolution width $\geq w$	$\Longrightarrow$	Monotone circuit size $\geq n^{\Omega(w)}$

Theme of this workshop : Lifting Theorems!

Feasible Interpolation
[BPR97, Kra97]

Lifting Theorem
[This talk]

Stronger Lifting Theorem
[This talk]

Resolution Refutations

Monotone Circuits

Monotone Real Circuits

Theme of this workshop : Lifting Theorems!

Feasible Interpolation
[BPR97, Kra97]

Resolution Refutations

Lifting Theorem
[This talk]

Monotone Circuits

Str

- Wires carry values in $\mathbb{R}$; Inputs/Outputs $\in \{0,1\}$.
- Gates compute arbitrary monotone $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

Monotone Real Circuits

Theme of this workshop : Lifting Theorems!

Resolution Refutations

Feasible Interpolation [BPR97, Kra97] ←

→ *Lifting Theorem* [This talk]

Monotone Circuits

- Wires carry values in $\mathbb{R}$; Inputs/Outputs $\in \{0,1\}$.
- Gates compute arbitrary monotone $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.
- E.g. Can simulate all *monotone* neural networks!

Monotone Real Circuits

Theme of this workshop : Lifting Theorems!

Feasible Interpolation
[BPR97, Kra97]

Resolution Refutations

Lifting Theorem
[This talk]

Monotone Circuits

Stronger Lifting Theorem
[This talk]

Cutting Plane Refutations

Feasible Interpolation

Monotone Real Circuits

COROLLARY

Monotone (Real) Circuit Complexity of XOR-SAT_n is $2^{n^{\Omega(1)}}$.

Corollary

Monotone (Real) Circuit Complexity of Xor-Sat$_n$ is $2^{n^{\Omega(1)}}$.

X : **input**

$\downarrow$

1	$v_1 \oplus v_2 \oplus v_3 = 0$
0	$v_1 \oplus v_2 \oplus v_3 = 1$
$\vdots$	$\vdots$
1	$v_{n-2} \oplus v_{n-1} \oplus v_n = 1$

Corollary

Monotone (Real) Circuit Complexity of Xor-Sat$_n$ is $2^{n^{\Omega(1)}}$.

X : **input**

$$\downarrow$$

$$\textsc{Xor-Sat}_n(X) := 1$$

iff

X is *un*-satisfiable

$$\begin{array}{c|rcl} \mathbf{1} & v_1 \oplus v_2 \oplus v_3 & = & 0 \\ \mathbf{0} & v_1 \oplus v_2 \oplus v_3 & = & 1 \\ \vdots & & \vdots & \\ \mathbf{1} & v_{n-2} \oplus v_{n-1} \oplus v_n & = & 1 \end{array}$$

Corollary

Monotone (Real) Circuit Complexity of $\textsc{Xor-Sat}_n$ is $2^{n^{\Omega(1)}}$.

X : **input**

$\downarrow$

$\textsc{Xor-Sat}_n(X) := 1$

iff

X is *un*-satisfiable

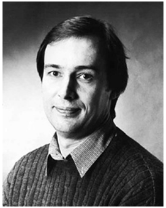
$$\begin{array}{c|rcl} \mathbf{1} & v_1 \oplus v_2 \oplus v_3 & = & 0 \\ \mathbf{0} & v_1 \oplus v_2 \oplus v_3 & = & 1 \\ \vdots & & \vdots & \\ \mathbf{1} & v_{n-2} \oplus v_{n-1} \oplus v_n & = & 1 \end{array}$$

Monotone vs Non-monotone Separations

- $\textsc{Xor-Sat} \in \mathsf{NC}^2$
- $\textsc{Matching} \in \mathsf{RNC}^2$ [Razborov 85]
- $\textsc{Tardos} \in \mathsf{P}$ [Tardos 88]

Corollary

Monotone (Real) Circuit Complexity of $\textsc{Xor-Sat}_n$ is $2^{n^{\Omega(1)}}$.



Method of Approximations

Monotone vs Non-monotone Separations

- $\textsc{Xor-Sat} \in \mathsf{NC}^2$
- $\textsc{Matching} \in \mathsf{RNC}^2$ [Razborov 85]
- $\textsc{Tardos} \in \mathsf{P}$ [Tardos 88]

Lifting theorems!

Resolution Refutations

Lifting Theorem
[This talk]

Monotone Circuits

Stronger Lifting Theorem
[This talk]

Monotone Real Circuits

Lifting theorems!

Resolution Refutations

Monotone Circuits

Lifting theorems!

Resolution Refutations

$\Updownarrow$

Query Complexity

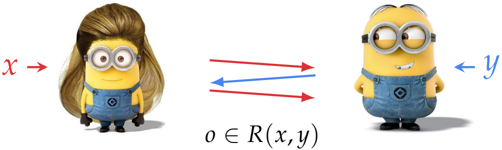
Lifting Theorem $\Rightarrow$

Monotone Circuits

$\Updownarrow$

Communication Complexity

Communication Complexity [Yao79]



$\mathrm{CC}(R) :=$ number of bits

Search Problem R

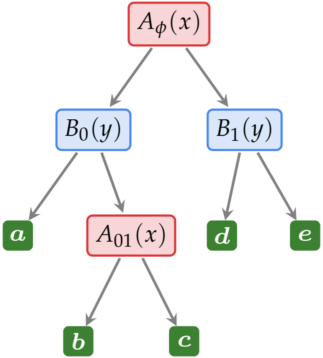
Relation $R \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Alice: $x \in \mathcal{X}$

Bob: $y \in \mathcal{Y}$

Output: $o \in R(x,y)$

Communication Complexity [Yao79]



$$\mathsf{CC}(R) := \text{number of bits}$$
$$= \text{depth of protocol tree}$$

Search Problem R

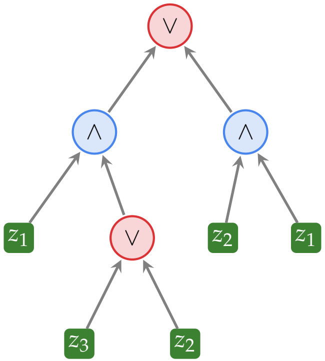
Relation $R \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Alice: $x \in \mathcal{X}$

Bob: $y \in \mathcal{Y}$

Output: $o \in R(x, y)$

Communication Complexity $\iff$ Monotone Circuits



[Karchmer-Wigderson 88]

Search Problem mKW_f

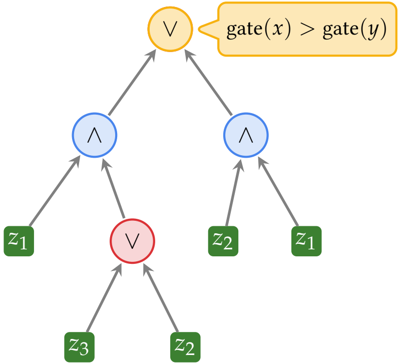
monotone $f : \{0,1\}^n \to \{0,1\}$

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

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

Output: i s.t. $x_i = 1, y_i = 0$

Communication Complexity $\Longleftrightarrow$ Monotone Circuits



[Karchmer-Wigderson 88]

Search Problem mKW_f

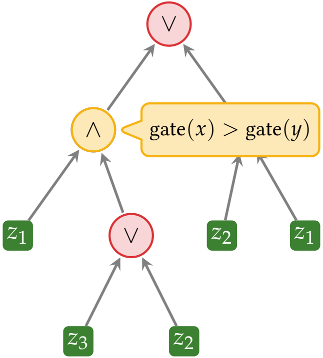
monotone $f : \{0,1\}^n \to \{0,1\}$

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

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

Output: i s.t. $x_i = 1, y_i = 0$

Communication Complexity $\Longleftrightarrow$ Monotone Circuits



[Karchmer-Wigderson 88]

Search Problem mKW_f

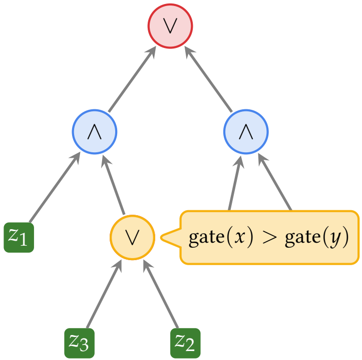
monotone $f : \{0,1\}^n \to \{0,1\}$

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

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

Output: i s.t. $x_i = 1, y_i = 0$

Communication Complexity $\Longleftrightarrow$ Monotone Circuits



[Karchmer-Wigderson 88]

Search Problem mKW_f

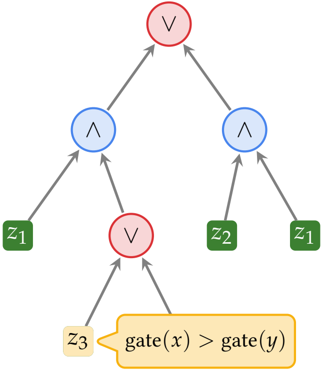
monotone $f : \{0,1\}^n \to \{0,1\}$

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

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

Output: i s.t. $x_i = 1, y_i = 0$

Communication Complexity $\Longleftrightarrow$ Monotone Circuits



[Karchmer-Wigderson 88]

Search Problem mKW_f

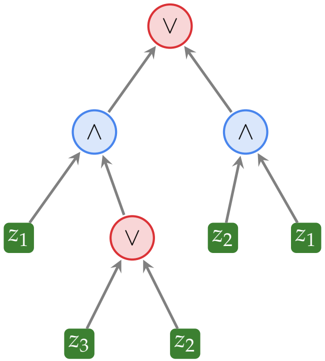
monotone $f : \{0,1\}^n \to \{0,1\}$

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

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

Output: i s.t. $x_i = 1, y_i = 0$

Communication Complexity $\Longleftrightarrow$ Monotone Circuits



[Karchmer-Wigderson 88]

Search Problem mKW_f

monotone $f : \{0,1\}^n \to \{0,1\}$

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

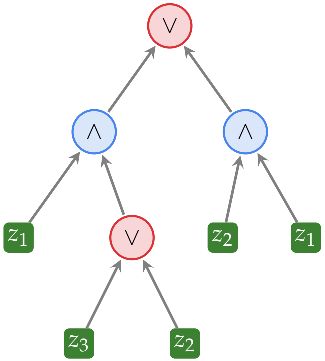
Bob: $y \in f^{-1}(0)$

Output: i s.t. $x_i = 1, y_i = 0$

Theorem [KW 88]

$$\mathsf{CC}(\mathsf{mKW}_f) \;=\; \text{Mon-Circuit-depth}(f)$$

Communication Complexity $\Longleftrightarrow$ Monotone ~~Circuits~~ Formulas



[Karchmer-Wigderson 88]

Search Problem mKW_f

monotone $f : \{0,1\}^n \to \{0,1\}$

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

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

Output: i s.t. $x_i = 1, y_i = 0$

Theorem [KW 88]

$$\mathsf{CC}(\mathsf{mKW}_f) = \Theta(\log(\text{Mon-Formula-size}(f)))$$

Lifting Theorems!

Resolution Refutations

$\Updownarrow$

Query Complexity

Lifting Theorem $\Rightarrow$

Monotone Circuits

$\Updownarrow$

Communication Complexity

Lifting Theorems!

Resolution Refutations

$\Updownarrow$

Query Complexity

Lifting Theorem $\Rightarrow$

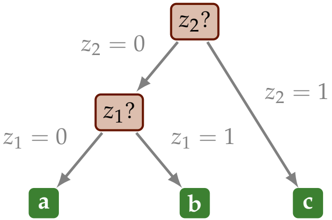
Formulas

Monotone ~~Circuits~~

✓ $\Updownarrow$ Karchmer Wigderson 88

Communication Complexity

Query Complexity



Search Problem S

Relation $S \subseteq \{0,1\}^n \times \mathcal{O}$

Input: $z \in \{0,1\}^n$

Output: $o \in S(z)$

$$\begin{aligned} \mathsf{DT}(R) &:= \text{number of bits queried} \\ &= \text{depth of decision tree} \end{aligned}$$

Resolution Refutations

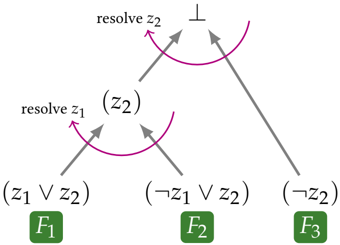
unsatisfiable $\mathcal{F} = F_1 \wedge F_2 \wedge \cdots \wedge F_m$

Resolution Refutations

unsatisfiable $\mathcal{F} = F_1 \wedge F_2 \wedge \cdots \wedge F_m$

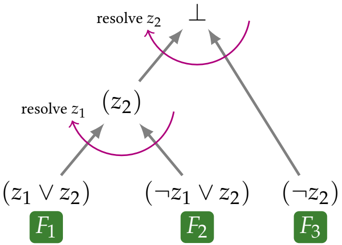
$(z_1 \vee z_2)$ F_1 $(\neg z_1 \vee z_2)$ F_2 $(\neg z_2)$ F_3

Resolution Refutations



unsatisfiable $\mathcal{F} = F_1 \wedge F_2 \wedge \cdots \wedge F_m$

Query Complexity $\Longleftrightarrow$ Resolution Refutations



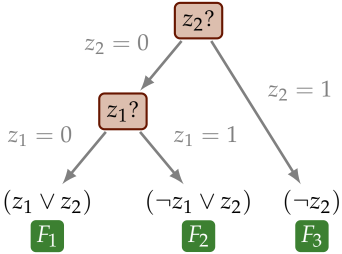
Search Problem $S_{\mathcal{F}}$

unsatisfiable $\mathcal{F} = F_1 \land F_2 \land \cdots \land F_m$

Input: $z \in \{0,1\}^n$

Output: i s.t. $F_i(z) = 0$

Query Complexity $\Longleftrightarrow$ Resolution Refutations



Search Problem $S_{\mathcal{F}}$

unsatisfiable $\mathcal{F} = F_1 \wedge F_2 \wedge \cdots \wedge F_m$

Input: $z \in \{0,1\}^n$

Output: i s.t. $F_i(z) = 0$

Folklore Observation

$$\mathsf{DT}(S_{\mathcal{F}}) \;=\; \text{Resolution-depth}(\mathcal{F})$$

Lifting Theorems!

Resolution Refutations

$\Updownarrow$

Query Complexity

Lifting Theorem $\Rightarrow$

Monotone Formulas

✓ $\Updownarrow$ Karchmer Wigderson 88

Communication Complexity

Lifting Theorems!

Resolution Depth

Folklore! $\Updownarrow$ ✓

Query Complexity

Lifting Theorem $\Rightarrow$

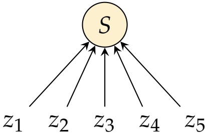
Monotone Formulas

✓ $\Updownarrow$ Karchmer Wigderson 88

Communication Complexity

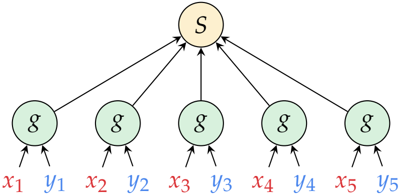
Query-to-Communication Lifting

$S \subseteq \{0,1\}^n \times \mathcal{O}$



Compose with
$g : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

$S \circ g^n \subseteq \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{O}$



Indexing Gadget

$$g : [m] \times \{0,1\}^m \to \{0,1\}$$
$$g(x, y) = y_x$$

$m = n^{O(1)}$

Lifting Theorem [Raz-McKenzie 99, ...]

Fixed g, such that for all S:

$$\mathsf{CC}(S \circ g^n) \geq \Omega(\mathsf{DT}(S) \cdot \log m)$$

Lifting Theorems!

Resolution Depth

Monotone Formulas

Folklore!

Karchmer
Wigderson 88

Query Complexity

Lifting Theorem

Communication Complexity

Lifting Theorems!

Resolution Depth

Folklore! ⇕ ✓

Query Complexity

✓

Lifting Theorem ⇒

Raz-McKenzie 99

Monotone Formulas

✓ ⇕ Karchmer Wigderson 88

Communication Complexity

Lifting Theorems!

[Raz-McKenzie 99, ...]

$$\text{Monotone-NC}^{i+1} \quad \not\subseteq \quad \text{Monotone-NC}^{i}$$

Resolution Depth

Folklore! $\Updownarrow$ ✓

Query Complexity

✓

Lifting Theorem $\Rightarrow$

Raz-McKenzie 99

Monotone Formulas

✓ $\Updownarrow$ Karchmer Wigderson 88

Communication Complexity

Lifting Theorems!

[Raz-McKenzie 99, ...]

Monotone Formula Complexity of $\textsc{Xor-Sat}_n$ is $2^{n^{\Omega(1)}}$.

Resolution Depth

Monotone Formulas

Folklore! $\Updownarrow$ ✓

✓ $\Updownarrow$ Karchmer Wigderson 88

✓

Query Complexity — *Lifting Theorem* $\Rightarrow$ Communication Complexity

Raz-McKenzie 99

Lifting Theorems!

[Raz-McKenzie 99, ...]

Monotone Formula Complexity of $\textsc{Xor-Sat}_n$ is $2^{n^{\Omega(1)}}$.

Bottleneck: Decision Trees & Communication Protocols are all *tree*-like objects.

Resolution Depth

Folklore! $\Updownarrow$ ✓

Query Complexity

Lifting Theorem ✓

Raz-McKenzie 99

Monotone Formulas

✓ $\Updownarrow$ Karchmer Wigderson 88

Communication Complexity

Lifting Theorems!

[Raz-McKenzie 99, ...]

Monotone Formula Complexity of $\textsc{Xor-Sat}_n$ is $2^{n^{\Omega(1)}}$.

Bottleneck: Decision Trees & Communication Protocols are all *tree*-like objects.

Challenge: We need to study *DAG*-like objects!

Resolution Depth

Folklore! $\Updownarrow$ ✓

Query Complexity

✓

Lifting Theorem $\Rightarrow$

Raz-McKenzie 99

Monotone Formulas

✓ $\Updownarrow$ Karchmer Wigderson 88

Communication Complexity

Communication dags [Razborov 95, Sokolov 17]

Unprovability of Lower Bounds on Circuit Size in Certain Fragments of Bounded Arithmetic

Alexander A. Razborov*
School of Mathematics
Institute for Advanced Study
Princeton, NJ 08540
and
Steklov Mathematical Institute
Vavilova 42, 117966, GSP–1
Moscow, RUSSIA

To appear in *Izvestiya of the RAN*

Abstract

We show that if strong pseudorandom generators exist then the statement "α encodes a circuit of size $n^{(\log^* n)}$ for SATISFIABILITY" is not refutable in $S_2^2(\alpha)$. For refutation in $S_2^1(\alpha)$, this is proven under the weaker assumption of the existence of generators secure against the attack by small depth circuits, and for another system which is strong enough to prove exponential lower bounds for constant-depth circuits, this is shown without using any unproven hardness assumptions.

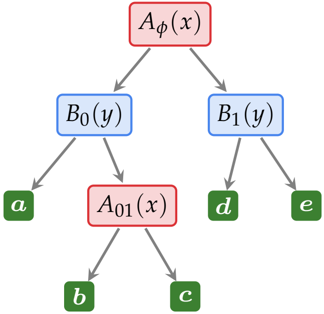
These results can be also viewed as direct corollaries of interpolation-like theorems for certain "split versions" of classical systems of Bounded Arithmetic introduced in this paper.

*Supported by the grant # 93-6-6 of the Alfred P. Sloan Foundation and by the grant # 93-011-16015 of the Russian Foundation for Fundamental Research

Communication dags [Razborov 95, Sokolov 17]

$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Communication Tree:



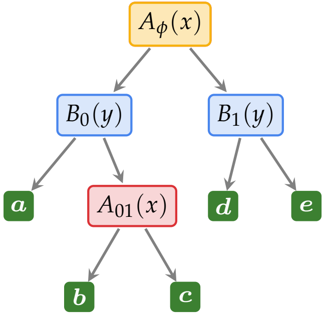
Communication dags [Razborov 95, Sokolov 17]

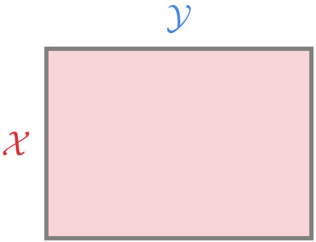
Communication Tree:

Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$

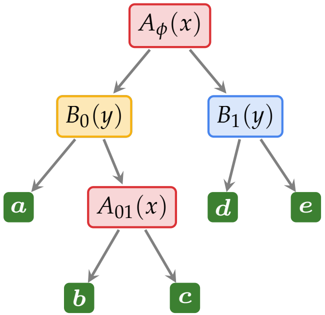
$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$





Communication dags [Razborov 95, Sokolov 17]

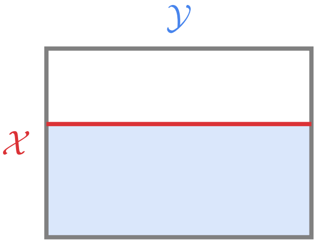
$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$



Communication Tree:

Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$
- **Internal node:** $R_v = R_u \sqcup R_w$



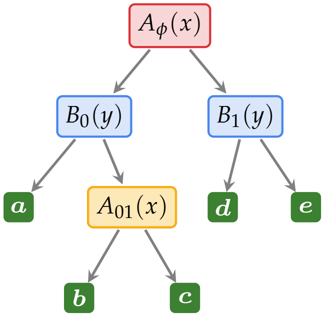
Communication dags [Razborov 95, Sokolov 17]

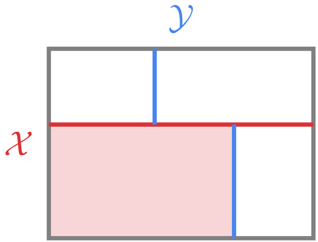
$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Communication Tree:

Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$
- **Internal node:** $R_v = R_u \sqcup R_w$





Communication dags [Razborov 95, Sokolov 17]

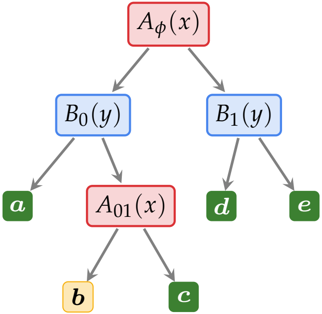
$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

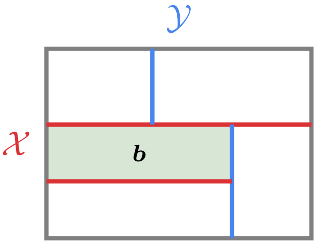
Communication Tree:

Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$
- **Internal node:** $R_v = R_u \sqcup R_w$
- **Leaf:** R_v is labelled by $o_v \in \mathcal{O}$

  valid answer to F for all $(x, y) \in R_\ell$





Communication dags [Razborov 95, Sokolov 17]

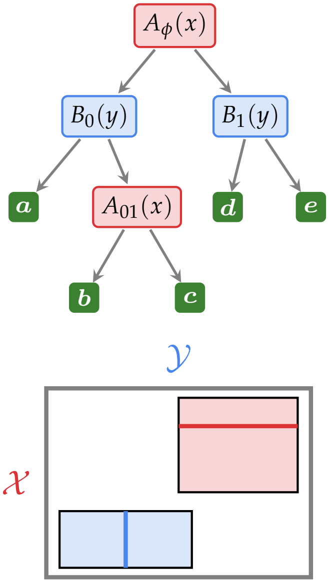
$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Communication Tree:

Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$
- **Internal node:** $R_v = R_u \sqcup R_w$
- **Leaf:** R_v is labelled by $o_v \in \mathcal{O}$

  valid answer to F for all $(x, y) \in R_\ell$



No need for an "explicit" Alice/Bob reference!

Communication dags [Razborov 95, Sokolov 17]

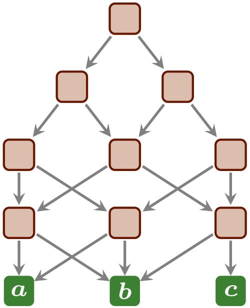
$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

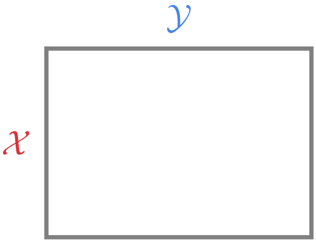
Communication DAG:

Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$
- **Internal node:** $R_v = R_u \sqcup R_w$
- **Leaf:** R_v is labelled by $o_v \in \mathcal{O}$

  valid answer to F for all $(x, y) \in R_\ell$





No need for an "explicit" Alice/Bob reference!

Communication dags [Razborov 95, Sokolov 17]

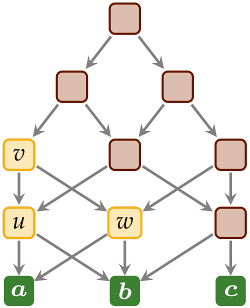
$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

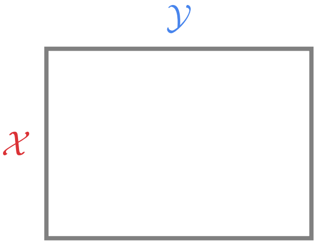
Communication DAG:

Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$
- **Internal node:** $\cancel{R_v = R_u \sqcup R_w}$ $R_v \subseteq R_u \cup R_w$
- **Leaf:** R_v is labelled by $o_v \in \mathcal{O}$

  valid answer to F for all $(x, y) \in R_\ell$





No need for an "explicit" Alice/Bob reference!

Communication dags [Razborov 95, Sokolov 17]

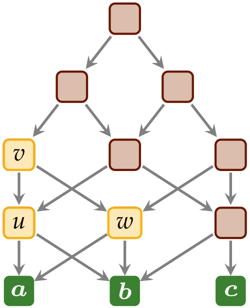
$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

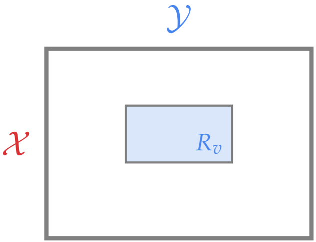
Communication DAG:

Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$
- **Internal node:** $\cancel{R_v = R_u \sqcup R_w}$ $R_v \subseteq R_u \cup R_w$
- **Leaf:** R_v is labelled by $o_v \in \mathcal{O}$

  valid answer to F for all $(x, y) \in R_\ell$





No need for an "explicit" Alice/Bob reference!

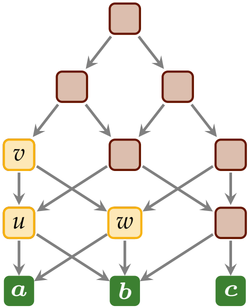
Communication dags [Razborov 95, Sokolov 17]

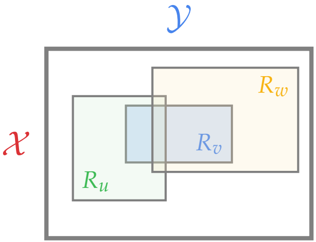
$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Communication DAG:

Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$
- **Internal node:** $\cancel{R_v = R_u \sqcup R_w}$ $R_v \subseteq R_u \cup R_w$
- **Leaf:** R_v is labelled by $o_v \in \mathcal{O}$
  valid answer to F for all $(x, y) \in R_\ell$





No need for an "explicit" Alice/Bob reference!

Communication dags [Razborov 95, Sokolov 17]

$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

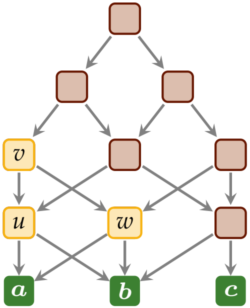
Communication DAG:

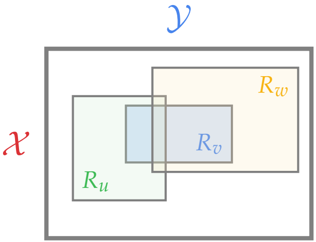
Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$
- **Internal node:** $\cancel{R_v = R_u \sqcup R_w}$ $R_v \subseteq R_u \cup R_w$
- **Leaf:** R_v is labelled by $o_v \in \mathcal{O}$

  valid answer to F for all $(x, y) \in R_\ell$

$\text{dag}^{\text{cc}}(F) :=$ log number of nodes in DAG.





Communication dags [Razborov 95, Sokolov 17]

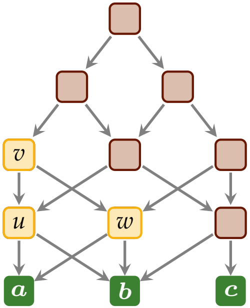
$F \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

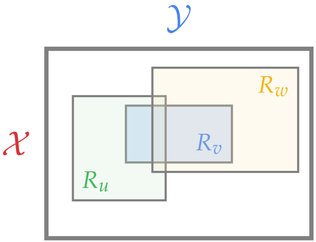
Communication DAG:

Every node v corresponds to rectangle $R_v \subseteq \mathcal{X} \times \mathcal{Y}$ such that,

- **Root:** $R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$
- **Internal node:** $\cancel{R_v = R_u \sqcup R_w}$ $R_v \subseteq R_u \cup R_w$
- **Leaf:** R_v is labelled by $o_v \in \mathcal{O}$

  valid answer to F for all $(x, y) \in R_\ell$





$\mathrm{dag}^{\mathrm{cc}}(F) :=$ log number of nodes in DAG.

Theorem [Razborov 95, Sokolov 17]

$$\mathrm{dag}^{\mathrm{cc}}(\mathrm{mKW}_f) = \log \text{Mon-Circuit-Size}(f)$$

Lifting Theorems!

Resolution Refutations

$\Updownarrow$

Query Complexity

Lifting Theorem

Monotone Circuits

$\Updownarrow$

Communication Complexity

Lifting Theorems!

Resolution Refutations

$\Updownarrow$

Query Complexity

Lifting Theorem

Monotone Circuit Size

✓ $\Updownarrow$ [Razborov 95] [Sokolov 17]

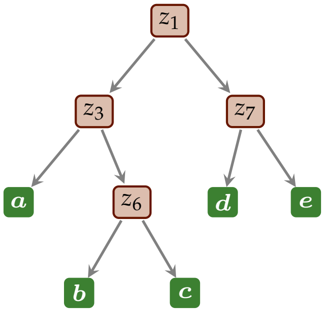
Dag Comm. Complexity

Query dags

Query dags

Decision Tree:

$$S \subseteq \{0,1\}^n \times \mathcal{O}$$



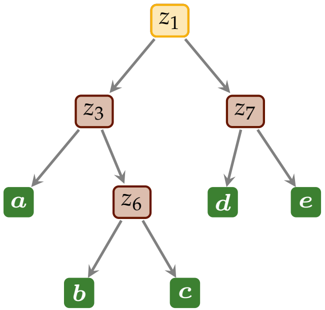
Query dags

$$S \subseteq \{0,1\}^n \times \mathcal{O}$$

Decision Tree:

Every node v corresponds to sub-cube $C_v \subseteq \{0,1\}^n$ such that,

- **Root:** $C_{\text{root}} = \{0,1\}^n$



$* * * * * * * * * *$

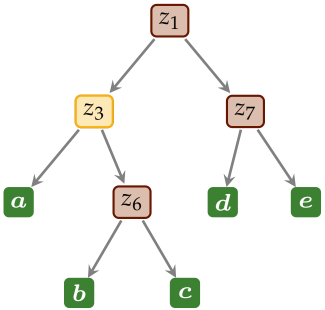
Query dags

Decision Tree:

Every node v corresponds to sub-cube $C_v \subseteq \{0,1\}^n$ such that,

- **Root:** $C_{\text{root}} = \{0,1\}^n$
- **Internal node:** $C_v = C_u \sqcup C_w$

$$S \subseteq \{0,1\}^n \times \mathcal{O}$$



$$0 * * * * * * * * *$$

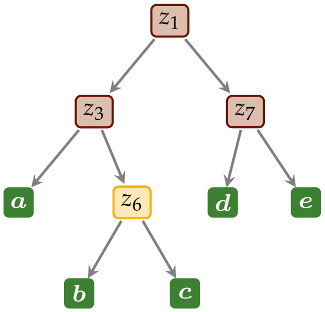
Query dags

$$S \subseteq \{0,1\}^n \times \mathcal{O}$$

Decision Tree:

Every node v corresponds to sub-cube $C_v \subseteq \{0,1\}^n$ such that,

- **Root:** $C_{\text{root}} = \{0,1\}^n$
- **Internal node:** $C_v = C_u \sqcup C_w$



$$0 * 1 * * * * * * *$$

Query dags

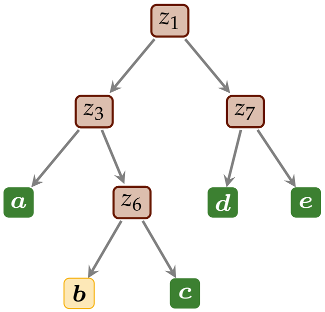
$S \subseteq \{0,1\}^n \times \mathcal{O}$

Decision Tree:

Every node v corresponds to sub-cube $C_v \subseteq \{0,1\}^n$ such that,

- **Root:** $C_{\text{root}} = \{0,1\}^n$
- **Internal node:** $C_v = C_u \sqcup C_w$
- **Leaf:** C_v is labelled by $o \in \mathcal{O}$

  valid answer to S for all $z \in \{0,1\}^n$



$$0 * 1 * * 0 * * * *$$

Query dags

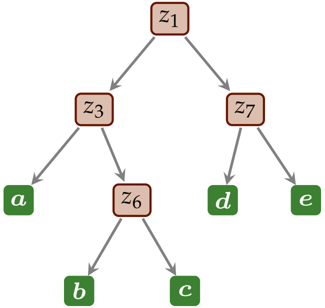
$S \subseteq \{0,1\}^n \times \mathcal{O}$

Decision Tree:

Every node v corresponds to sub-cube $C_v \subseteq \{0,1\}^n$ such that,

- **Root:** $C_{\text{root}} = \{0,1\}^n$
- **Internal node:** $C_v = C_u \sqcup C_w$
- **Leaf:** C_v is labelled by $o \in \mathcal{O}$
  valid answer to S for all $z \in \{0,1\}^n$

$\mathsf{DT}(S) :=$ max **width** of a node



$$0 * 1 * * 0 * * * *$$

Query dags

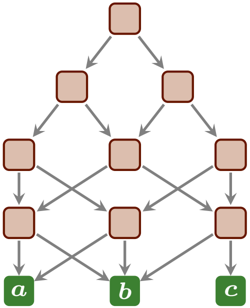
$S \subseteq \{0,1\}^n \times \mathcal{O}$

Decision DAG:

Every node v corresponds to sub-cube $C_v \subseteq \{0,1\}^n$ such that,

- **Root:** $C_{\text{root}} = \{0,1\}^n$
- **Internal node:** $C_v = C_u \sqcup C_w$
- **Leaf:** C_v is labelled by $o \in \mathcal{O}$
  valid answer to S for all $z \in \{0,1\}^n$

$\mathsf{DT}(S) :=$ max **width** of a node



Query dags

$S \subseteq \{0,1\}^n \times \mathcal{O}$

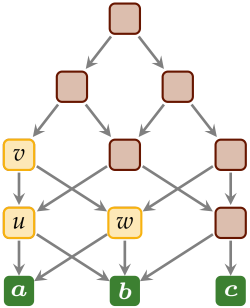
Decision DAG:

Every node v corresponds to sub-cube $C_v \subseteq \{0,1\}^n$ such that,

- **Root:** $C_{\mathrm{root}} = \{0,1\}^n$
- **Internal node:** $\cancel{C_v = C_u \sqcup C_w}$ $C_v \subseteq C_u \cup C_w$
- **Leaf:** C_v is labelled by $o \in \mathcal{O}$

  valid answer to S for all $z \in \{0,1\}^n$

$\mathsf{dag}^{\mathsf{dt}}(S) :=$ max **width** of a node



Query dags

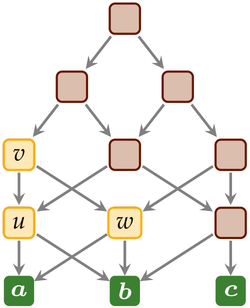
Decision DAG:

Every node v corresponds to sub-cube $C_v \subseteq \{0,1\}^n$ such that,

- **Root:** $C_{\text{root}} = \{0,1\}^n$
- **Internal node:** $\cancel{C_v = C_u \sqcup C_w}$ $C_v \subseteq C_u \cup C_w$
- **Leaf:** C_v is labelled by $o \in \mathcal{O}$
  valid answer to S for all $z \in \{0,1\}^n$

$\mathsf{dag}^{\mathsf{dt}}(S) :=$ max **width** of a node

$S \subseteq \{0,1\}^n \times \mathcal{O}$



$$C_v \subseteq C_u \cup C_w$$

$$C_v = 1 * 0 * * 0 * * 1 *$$
$$C_u = 1 * 0 0 * * * * * *$$
$$C_w = * * * 1 * 0 * * 1 *$$

Query dags

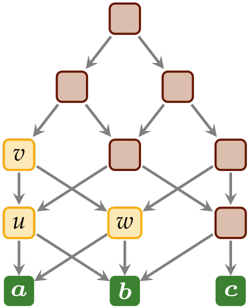
$S \subseteq \{0,1\}^n \times \mathcal{O}$

Decision DAG:

Every node v corresponds to sub-cube $C_v \subseteq \{0,1\}^n$ such that,

- **Root:** $C_{\text{root}} = \{0,1\}^n$
- **Internal node:** $\cancel{C_v = C_u \sqcup C_w}$ $C_v \subseteq C_u \cup C_w$
- **Leaf:** C_v is labelled by $o \in \mathcal{O}$
  valid answer to S for all $z \in \{0,1\}^n$

$\text{dag}^{\text{dt}}(S) :=$ max **width** of a node



$$C_v \subseteq C_u \cup C_w$$

$$\begin{aligned} C_v &= 1 * 0 * * 0 * * 1 * \\ C_u &= 1 * 0\ 0 * * * * * * \\ C_w &= * * * 1 * 0 * * 1 * \end{aligned}$$

Theorem

$$\text{dag}^{\text{dt}}(S_{\mathcal{F}}) \;=\; \text{Resolution-Width}(\mathcal{F})$$

Query dags

$S \subseteq \{0,1\}^n \times \mathcal{O}$

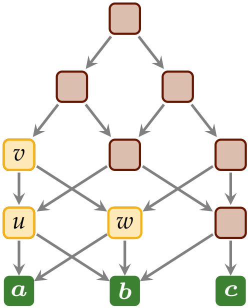
Explorer vs. Adversary game: [Pud00, AD08]

- Game state is $\rho \in \{0,1,*\}^n$.
- In each round, Explorer makes a choice:

Query. *Explorer* chooses $i \in [n]$
Adversary responds $b \in \{0,1\}$
Update $\rho_i = b$

Forget. *Explorer* chooses $i \in [n]$
Update $\rho_i = *$

- Game ends when solution to S can be deduced from ρ.



$C_v \subseteq C_u \cup C_w$

$\mathrm{dag}^{\mathrm{dt}}(S) :=$ least d such that,
Explorer has a strategy that maintains ρ of width $\leq d$.

$$C_v = 1 * 0 * * 0 * * 1 *$$
$$C_u = 1 * 0\ 0 * * * * * *$$
$$C_w = * * * 1 * 0 * * 1 *$$

Lifting Theorems!

Resolution Refutations

$\Updownarrow$

Query Complexity

Lifting Theorem

Monotone Circuit Size

✓ $\Updownarrow$ [Razborov 95] [Sokolov 17]

Dag Comm. Complexity

Lifting Theorems!

Resolution Width

[Pud00, AD08]$^+$ $\Updownarrow$ ✓

Dag Query Complexity

Lifting Theorem

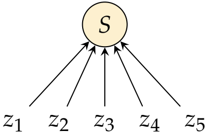
Monotone Circuit Size

✓ $\Updownarrow$ [Razborov 95] [Sokolov 17]

Dag Comm. Complexity

Lifting Theorems!

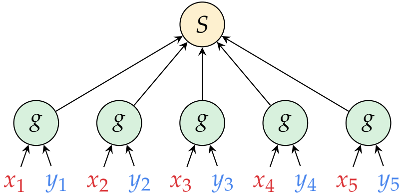
$S \subseteq \{0,1\}^n \times \mathcal{O}$



Compose with

$\mathsf{Ind}_m : [m] \times \{0,1\}^m \to \{0,1\}$

$S \circ g^n \subseteq [m]^n \times (\{0,1\}^m)^n \times \mathcal{O}$



$$\Omega(\mathsf{dag}^{\mathsf{dt}}(S) \cdot \log n) \quad \leq \quad \mathsf{dag}^{\mathsf{cc}}(S \circ g^n)$$

Dag Query Complexity — *Lifting Theorem [GGKS 18]* → Dag Comm. Complexity

Rectangles are Non-negative Juntas

[Göös-Lovett-Meka-Watson-Zuckerman 16]

+ [Göös-**K**-Pitassi-Watson 17, Göös-Pitassi-Watson 17]

Rectangle $R \subseteq [m]^n \times (\{0,1\}^m)^n$

$$g^n(R) \text{ is like } (\underbrace{b_1, b_2, \ldots, b_d}_{\text{fixed}}, \underbrace{*, *, \ldots, *}_{\text{random}})$$

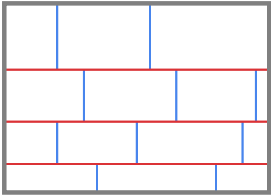
R is ρ-like for $\rho \in \{0,1,*\}^n$ with $|\text{fix}(\rho)| \leq d$.

Rectangles are Non-negative Juntas

[Göös-Lovett-Meka-Watson-Zuckerman 16]

+ [Göös-**K**-Pitassi-Watson 17, Göös-Pitassi-Watson 17]

$\rightsquigarrow$

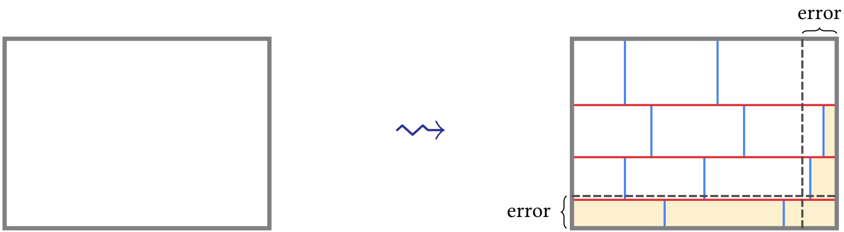


Rectangle $R \subseteq [m]^n \times (\{0,1\}^m)^n$

$R = \bigsqcup_i R_i$

Rectangles are Non-negative Juntas

[Göös-Lovett-Meka-Watson-Zuckerman 16]
+ [Göös-**K**-Pitassi-Watson 17, Göös-Pitassi-Watson 17]



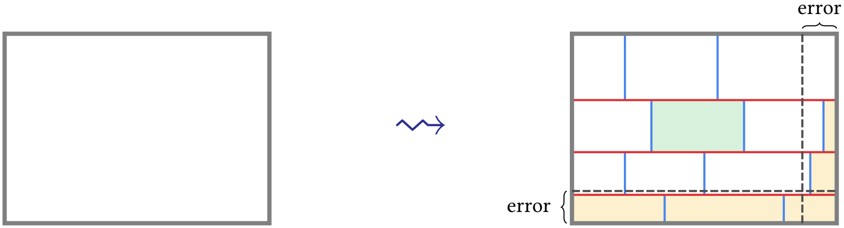
Rectangle $R \subseteq [m]^n \times (\{0,1\}^m)^n$

$R = \bigsqcup_i R_i$

- **Error** R_i : contained in $m^{-\Omega(d)}$ fraction of all rows/columns.

Rectangles are Non-negative Juntas

[Göös-Lovett-Meka-Watson-Zuckerman 16]
+ [Göös-**K**-Pitassi-Watson 17, Göös-Pitassi-Watson 17]



Rectangle $R \subseteq [m]^n \times (\{0,1\}^m)^n$

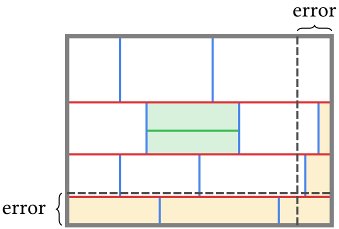
$R = \bigsqcup_i R_i$

- **Error** R_i : contained in $m^{-\Omega(d)}$ fraction of all rows/columns.
- **Non-Error** R_i : ρ-like with $|\mathrm{fix}(\rho)| \leq d$.

Rectangles are Non-negative Juntas

[Göös-Lovett-Meka-Watson-Zuckerman 16]
+ [Göös-**K**-Pitassi-Watson 17, Göös-Pitassi-Watson 17]

$\rightsquigarrow$



Rectangle $R \subseteq [m]^n \times (\{0,1\}^m)^n$

$R = \bigsqcup_i R_i$

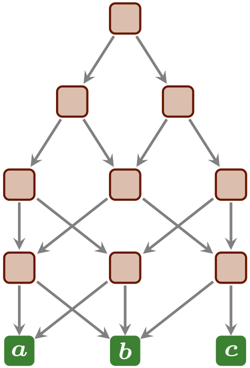
- **Error** R_i : contained in $m^{-\Omega(d)}$ fraction of all rows/columns.
- **Non-Error** R_i : ρ-like with $|\mathrm{fix}(\rho)| \leq d$.
  (in fact, support achieved on a single row)

Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \leq O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \le O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

Given n^d-sized Communication DAG for $S \circ g^n$

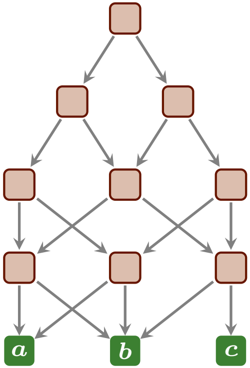
Extract width-$O(d)$ Explorer strategy for S



Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \le O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

Pre-processing:

- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \le d$.
  (Simplified proof: assume no error rectangles)



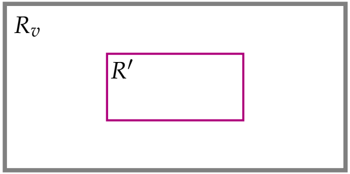
Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \leq O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

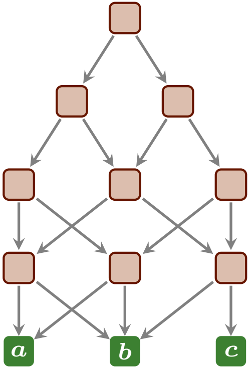
Pre-processing:

- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \leq d$.
  (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.





Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \leq O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

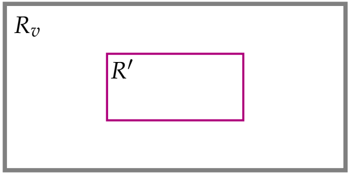
Pre-processing:

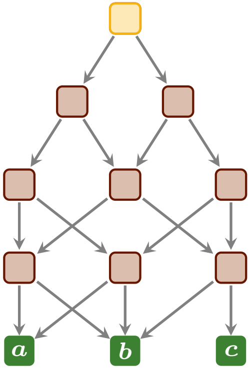
- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \leq d$.
  (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\mathrm{root}} = \mathcal{X} \times \mathcal{Y}$.





Proof Outline: $\mathrm{dag}^{\mathrm{dt}}(S) \leq O(\mathrm{dag}^{\mathrm{cc}}(S \circ g^n) / \log n)$

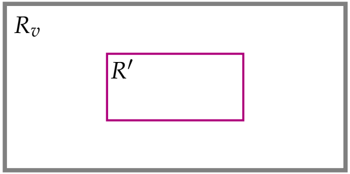
Pre-processing:

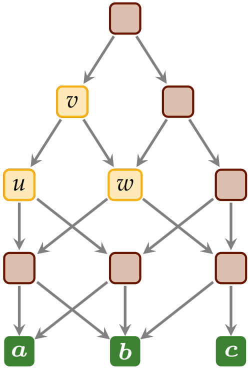
- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \leq d$.
  (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\text{root}} = \mathcal{X} \times \mathcal{Y}$.
2. **Internal node:** $\rho = 0\ 1\ 1\ 0 * * * * * * * * * *$





Proof Outline: $\mathrm{dag}^{\mathrm{dt}}(S) \leq O(\mathrm{dag}^{\mathrm{cc}}(S \circ g^n) / \log n)$

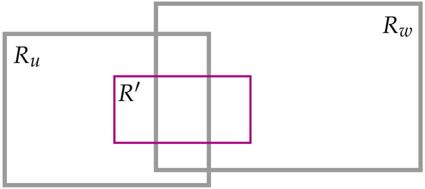
Pre-processing:

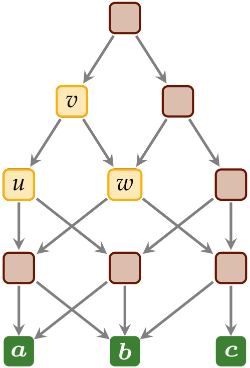
- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \leq d$.
  (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\mathrm{root}} = \mathcal{X} \times \mathcal{Y}$.
2. **Internal node:** $\rho = 0\ 1\ 1\ 0 * * * * * * * * * *$





Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \leq O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

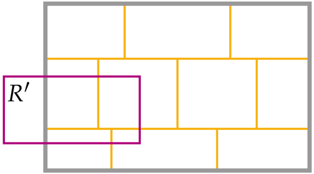
Pre-processing:

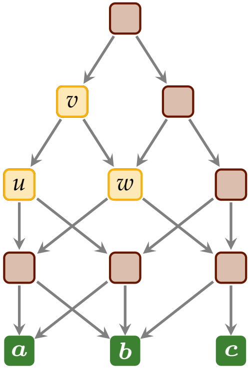
- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \leq d$.
  (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\mathrm{root}} = \mathcal{X} \times \mathcal{Y}$.
2. **Internal node:** $\rho = 0\ 1\ 1\ 0 * * * * * * * * * *$





Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \le O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

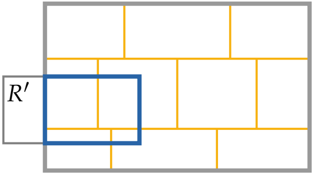
Pre-processing:

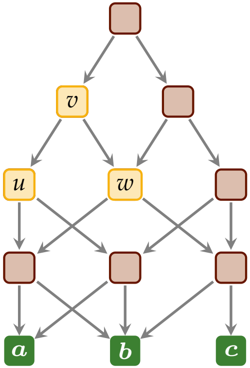
- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \le d$.
  (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\mathrm{root}} = \mathcal{X} \times \mathcal{Y}$.
2. **Internal node:** $\rho = 0\ 1\ 1\ 0 * * * * * * * * * *$





Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \le O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

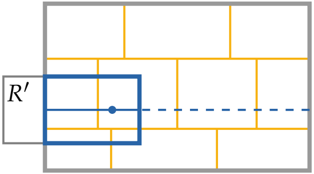
Pre-processing:

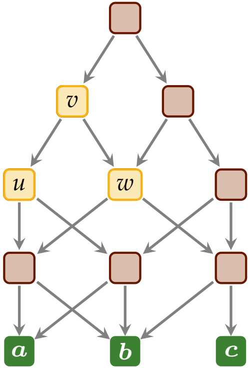
- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \le d$.
  (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\mathrm{root}} = \mathcal{X} \times \mathcal{Y}$.
2. **Internal node:** $\rho = 0\ 1\ 1\ 0 * * * * ?\ ?\ ? * * *$





Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \leq O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

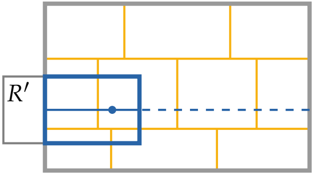
Pre-processing:

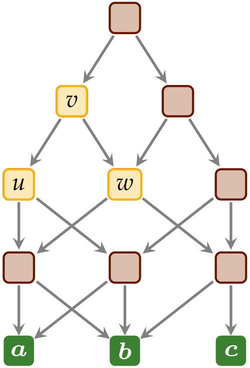
- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \leq d$. (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\mathrm{root}} = \mathcal{X} \times \mathcal{Y}$.
2. **Internal node:** $\rho = 0\ 1\ 1\ 0\ *\ *\ *\ *\ 1\ 0\ 0\ *\ *\ *$





Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \leq O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

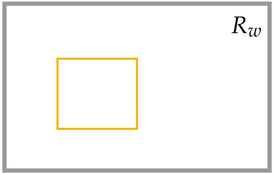
Pre-processing:

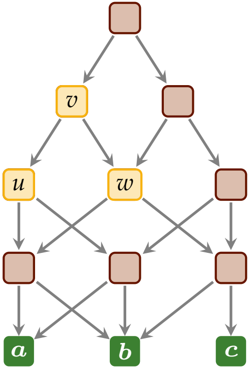
- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \leq d$.
  (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\mathrm{root}} = \mathcal{X} \times \mathcal{Y}$.
2. **Internal node:** $\rho = 0\ 1\ 1\ 0 * * * *\ 1\ 0\ 0 * * *$





Proof Outline: $\mathrm{dag}^{\mathrm{dt}}(S) \leq O(\mathrm{dag}^{\mathrm{cc}}(S \circ g^n) / \log n)$

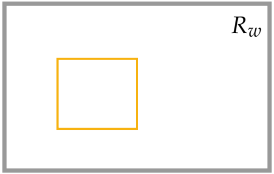
Pre-processing:

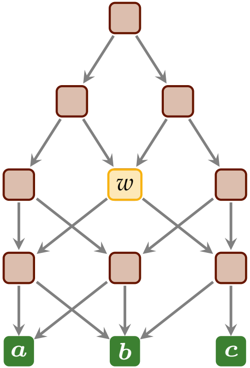
- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \leq d$.
  (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\mathrm{root}} = \mathcal{X} \times \mathcal{Y}$.
2. **Internal node:** $\rho = * * * 0 * * * * 1 0 0 * * *$





Proof Outline: $\mathrm{dag}^{\mathrm{dt}}(S) \le O(\mathrm{dag}^{\mathrm{cc}}(S \circ g^n) / \log n)$

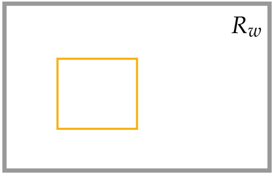
Pre-processing:

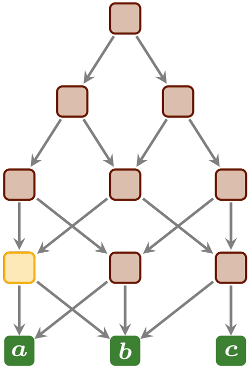
- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \le d$.
  (Simplified proof: assume no error rectangles)

Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\mathrm{root}} = \mathcal{X} \times \mathcal{Y}$.
2. **Internal node:** $\rho = * * * \; 0 \; * * * * \; 1 \; 0 \; 0 \; * * *$





Proof Outline: $\mathsf{dag}^{\mathsf{dt}}(S) \le O(\mathsf{dag}^{\mathsf{cc}}(S \circ g^n) / \log n)$

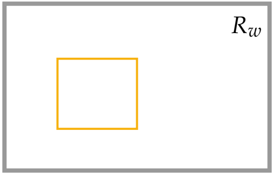
Pre-processing:

- Partition all $R_v = \bigsqcup_i R_v^i$, each R_v^i is ρ-like for $|\mathrm{fix}(\rho)| \le d$.
  (Simplified proof: assume no error rectangles)

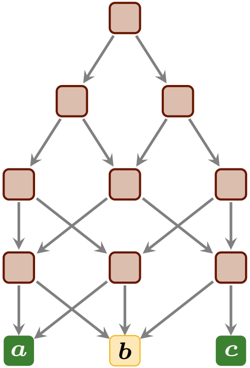
Extract width-$O(d)$ explorer strategy:

- **Invariant:** Game state ρ : maintain ρ-like $R' \subseteq R_v$.

1. **Root:** $\rho = *^n$ and $R' = R_{\mathrm{root}} = \mathcal{X} \times \mathcal{Y}$.
2. **Internal node:** $\rho = * * * 0 * * * * 1 0 0 * * *$



3. **Leaf:** Output o_v valid for $R \supseteq R'$ and hence for ρ. **Game ends!**



Lifting Theorems!

Resolution Width

[Pud00, AD08]$^+$ $\Updownarrow$ ✓

Dag Query Complexity

Lifting Theorem [GGKS 18] $\Rightarrow$

Monotone Circuits

✓ $\Updownarrow$ Razborov 95, Sokolov 17

Dag Comm. Complexity

Lifting Theorems!

Theorem

n-variate k-CNF $\mathcal{F}$	$\Longrightarrow$	$n^{O(k)}$-variate function f
Resolution width $\geq$ w		Monotone circuit size $\geq n^{\Omega(w)}$

Resolution Width

Monotone Circuits

[Pud00, AD08]$^{+}$ $\Updownarrow$ ✓

✓ $\Updownarrow$ Razborov 95
Sokolov 17

Dag Query Complexity

Lifting Theorem
[GGKS 18]

Dag Comm. Complexity

Lifting Theorems!

COROLLARY

Monotone Circuit Complexity of $\textsc{Xor-Sat}_n$ is $2^{n^{\Omega(1)}}$.

Resolution Width

[Pud00, AD08]+ $\Updownarrow$ ✓

Dag Query Complexity

Lifting Theorem
[GGKS 18]

Monotone Circuits

✓ $\Updownarrow$ Razborov 95, Sokolov 17

Dag Comm. Complexity

Lifting Theorems!

Resolution Width

Lifting Theorem
[GGKS 18]

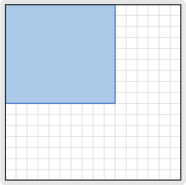
Monotone Circuits

Stronger Lifting Theorem
[GGKS 18]

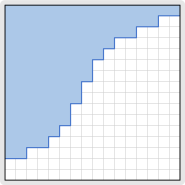
Monotone Real Circuits

Lifting Theorems!

Resolution Width



Rectangle

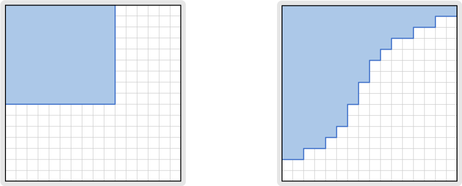


Triangle

Monotone Real Circuits

Lifting Theorems!

Resolution Width



Rectangle

Triangle

Key technique. Partitioning triangles into junta-like rectangles!

Monotone Real Circuits

Lifting Theorems!

Resolution Width

Lifting Theorem
[GGKS 18]

Monotone Circuits

Stronger Lifting Theorem
[GGKS 18]

Cutting Plane Refutations

Feasible Interpolation

Monotone Real Circuits

Lifting Theorems!

Resolution Width

Lifting Theorem
[GGKS 18]

Monotone Circuits

Stron

- Proof of refutations where lines are Linear Threshold Functions
- Encode clause $z_1 \vee z_2 \vee \neg z_3$ as $z_1 + z_2 + (1 - z_3) \geq 1$.
- Proof of refutation ends in $0 \geq 1$.

Cutting Plane Refutations

Feasible Interpolation

Monotone Real Circuits

Lifting Theorems!

Theorem

n-variate k-CNF $\mathcal{F}$	$\Longrightarrow$	$n^{O(1)}$-variate $2k$-CNF $\widetilde{\mathcal{F}}$
Resolution width $\geq\ w$		Cutting Planes length $\geq n^{\Omega(w)}$

Resolution Width — *Lifting Theorem* [GGKS 18] → Monotone Circuits

- Proof of refutations where lines are Linear Threshold Functions
- Encode clause $z_1 \vee z_2 \vee \neg z_3$ as $z_1 + z_2 + (1 - z_3) \geq 1$.
- Proof of refutation ends in $0 \geq 1$.

Cutting Plane Refutations ← *Feasible Interpolation* — Monotone Real Circuits

Is there a broader context to these lifting theorems?

(or does it sit alone in a corner?)

Query

Total Search Problem $S_{\mathcal{F}}$

unsatisfiable k-CNF $\mathcal{F} = F_1 \wedge \cdots \wedge F_m$

Input: $z \in \{0,1\}^n$

Output: i s.t. $F_i(z) = 0$

Communication

Total Search Problem mKW_f

monotone $f : \{0,1\}^n \to \{0,1\}$

Input: $(x, y) \in f^{-1}(1) \times f^{-1}(0)$

Output: i s.t. $x_i = 1$, $y_i = 0$

Query

Total Search Problem $S_{\mathcal{F}}$

unsatisfiable k-CNF $\mathcal{F} = F_1 \wedge \cdots \wedge F_m$

Input: $z \in \{0,1\}^n$

Output: i s.t. $F_i(z) = 0$

Non-deterministic query cost of $S_{\mathcal{F}} = k$

Communication

Total Search Problem mKW_f

monotone $f : \{0,1\}^n \to \{0,1\}$

Input: $(x, y) \in f^{-1}(1) \times f^{-1}(0)$

Output: i s.t. $x_i = 1$, $y_i = 0$

Non-deterministic comm. cost of $\mathsf{mKW}_f = \log n$

Query

Total Search Problem $S_{\mathcal{F}}$

unsatisfiable k-CNF $\mathcal{F} = F_1 \wedge \cdots \wedge F_m$

Input: $z \in \{0,1\}^n$

Output: i s.t. $F_i(z) = 0$

Non-deterministic query cost of $S_{\mathcal{F}} \;=\; k$

Observation. [LNNW95]

$\{S_{\mathcal{F}}\}_{\mathcal{F}}$ is *complete* for total search problems with non-deterministic query cost k

Communication

Total Search Problem mKW_f

monotone $f : \{0,1\}^n \to \{0,1\}$

Input: $(x, y) \in f^{-1}(1) \times f^{-1}(0)$

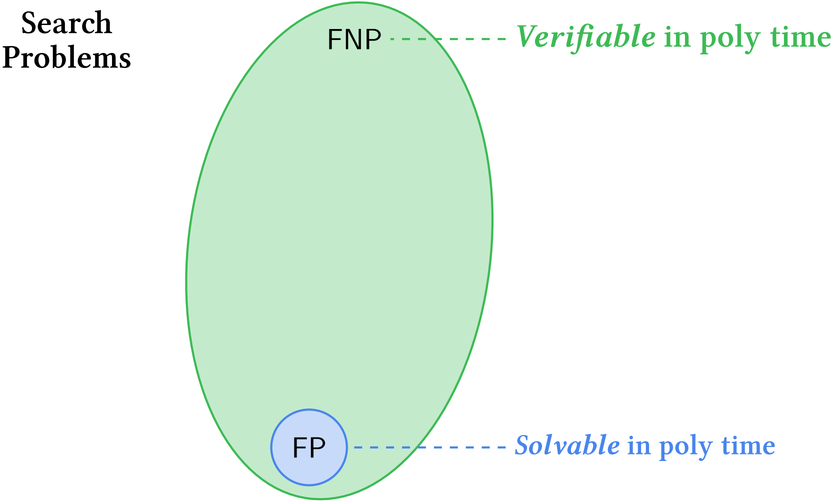
Output: i s.t. $x_i = 1,\; y_i = 0$

Non-deterministic comm. cost of $\mathsf{mKW}_f \;=\; \log n$

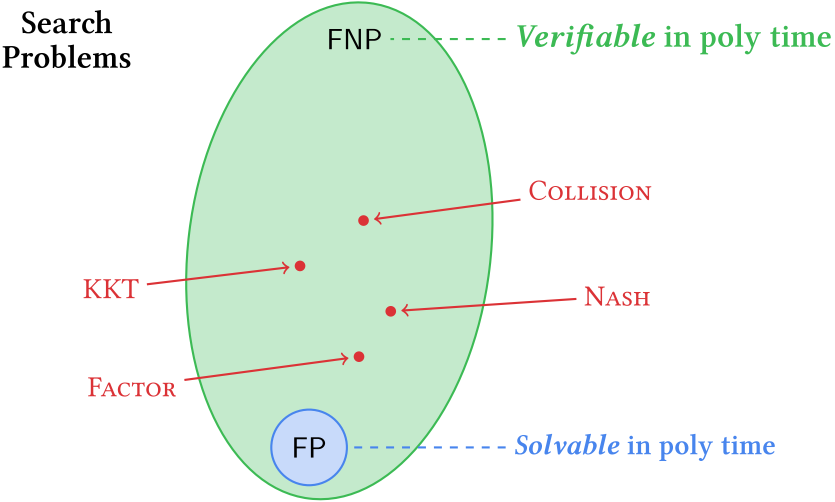
Observation. [Gál01]

$\left\{\mathsf{mKW}_f\right\}_f$ is *complete* for total search problems with non-deterministic comm. cost $\log n$

TFNP — Total Search Problems in NP

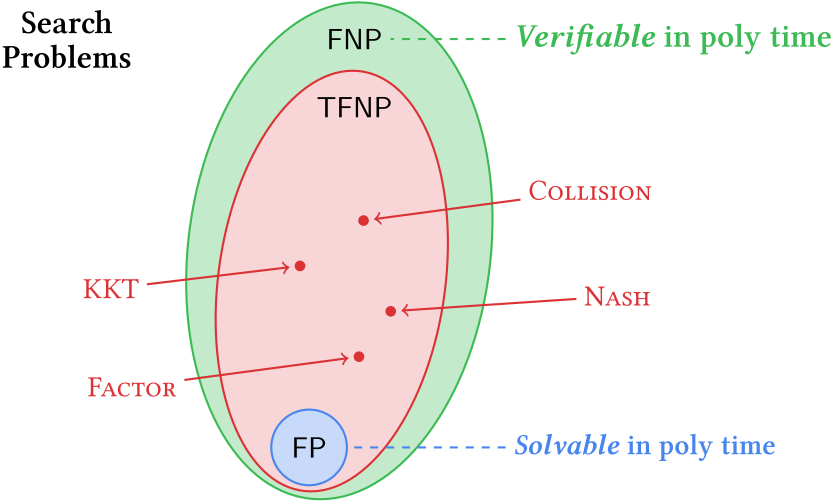


TFNP — Total Search Problems in NP



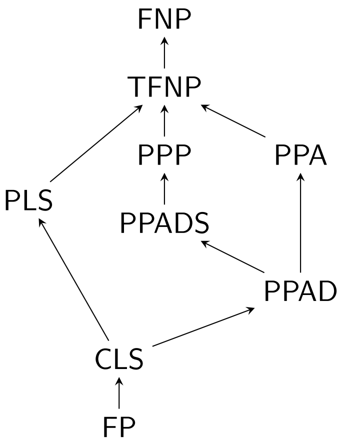
TFNP — Total Search Problems in NP

[Johnson-Papadimitriou-Yannakakis '85]
[Megiddo-Papadimitriou '89]
[Papadimitriou '91]



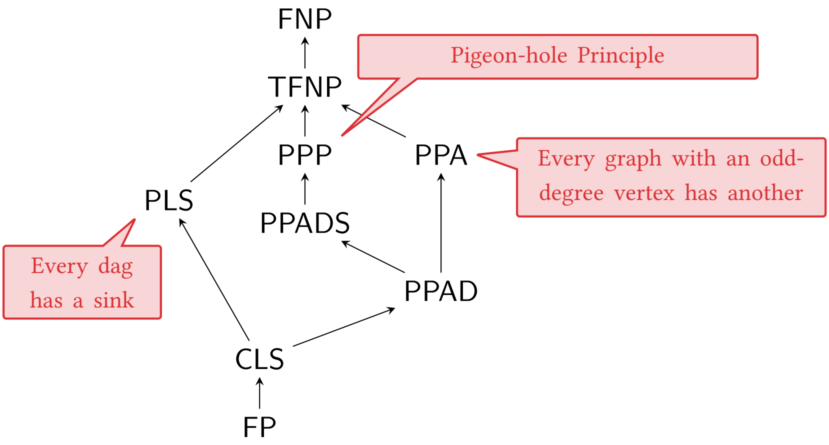
TFNP — Total Search Problems in NP

[Johnson-Papadimitriou-Yannakakis '85]
[Megiddo-Papadimitriou '89]
[Papadimitriou '91]



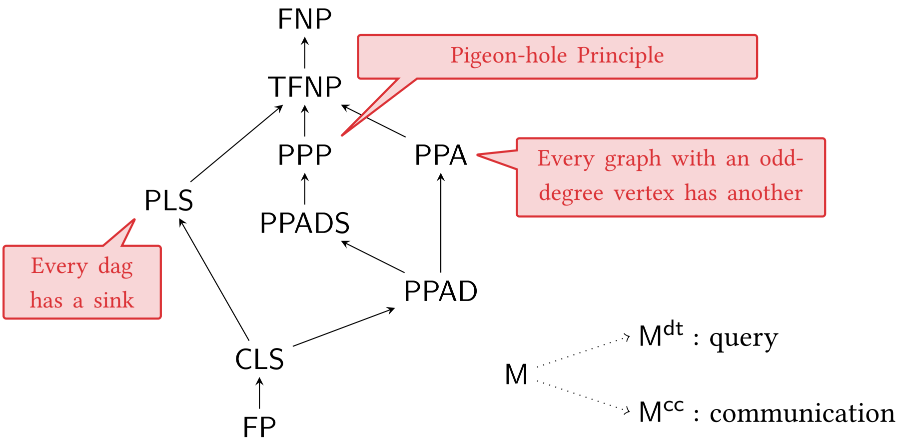
TFNP — Total Search Problems in NP

[Johnson-Papadimitriou-Yannakakis '85]
[Megiddo-Papadimitriou '89]
[Papadimitriou '91]



TFNP — Total Search Problems in NP

[Johnson-Papadimitriou-Yannakakis '85]
[Megiddo-Papadimitriou '89]
[Papadimitriou '91]



Complexity Classes in Communication Complexity Theory [Babai-Frankl-Simon 86]

The Landscape of Communication Complexity Classes [Göös-Pitassi-Watson 15]

Lifting Theorems!

Resolution Depth

Folklore! $\Updownarrow$

Query Complexity

Lifting Theorem
[Raz-McKenzie 99]

Monotone Formulas

$\Updownarrow$ Karchmer Wigderson88

Comm. Complexity

Lifting Theorems!

Resolution Depth

Folklore! $\Updownarrow$

$\mathsf{FP}^{\mathsf{dt}}$

Lifting Theorem
[Raz-McKenzie 99]

Monotone Formulas

$\Updownarrow$ Karchmer Wigderson88

$\mathsf{FP}^{\mathsf{cc}}$

Lifting Theorems!

Resolution Width

[Pud00, AD08]$^{+}$ $\Updownarrow$

Query Dags

Lifting Theorem
[GGKS 18]

Monotone Circuits

$\Updownarrow$ Razborov95
Sokolov17

Communication Dags

Lifting Theorems!

Every dag has a sink

Resolution Width

[Pud00, AD08]$^+$ $\Updownarrow$

$\mathsf{PLS}^{\mathsf{dt}}$

Lifting Theorem [GGKS 18] $\Rightarrow$

Monotone Circuits

$\Updownarrow$ Razborov95 Sokolov17

$\mathsf{PLS}^{\mathsf{cc}}$

Lifting Theorems!

$\mathbb{F}$-Nullstellensatz

Pitassi
Robere18 $\Updownarrow$

Algebraic Gaps

Lifting Theorem
[Pitassi-Robere 18]

Monotone $\mathbb{F}$-Span Programs

$\Updownarrow$ Gál01

Algebraic Tiling

Lifting Theorems!

Every graph with an odd degree vertex has another

$\mathbb{F}_2$-Nullstellensatz

Pitassi Robere18 $\Updownarrow$ [GKRS 19]

$\mathsf{PPA}^{\mathsf{dt}}$

Lifting Theorem

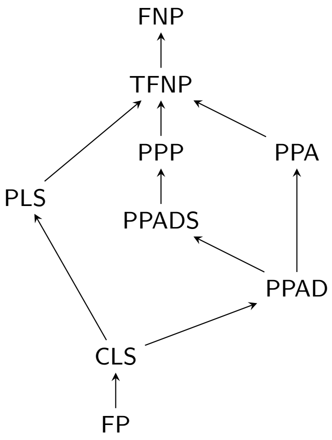
[Pitassi-Robere 18]

Monotone $\mathbb{F}_2$-Span Programs

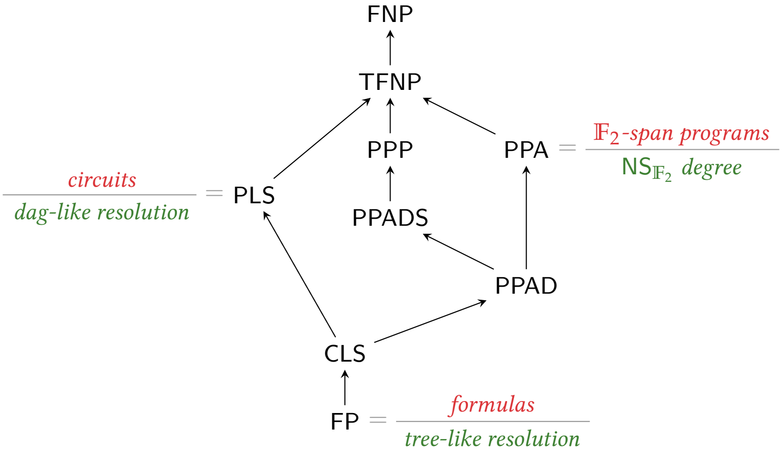
[GKRS 19] $\Updownarrow$ Gál01

$\mathsf{PPA}^{\mathsf{cc}}$

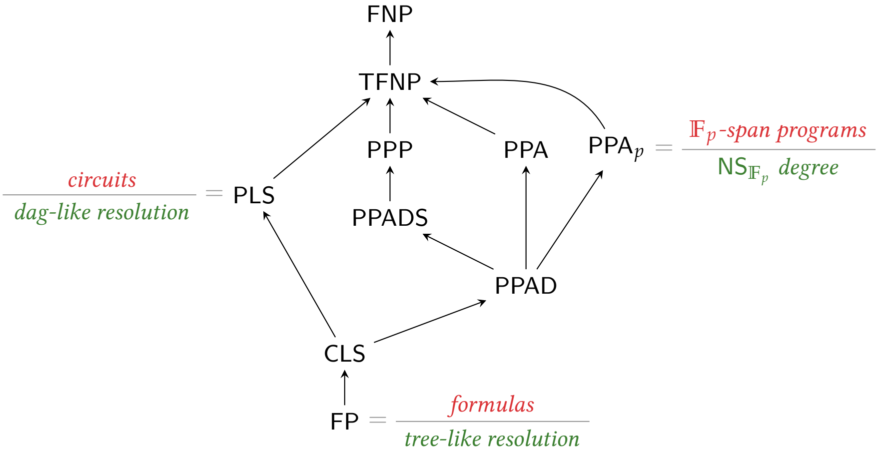
TFNP in Query & Communication



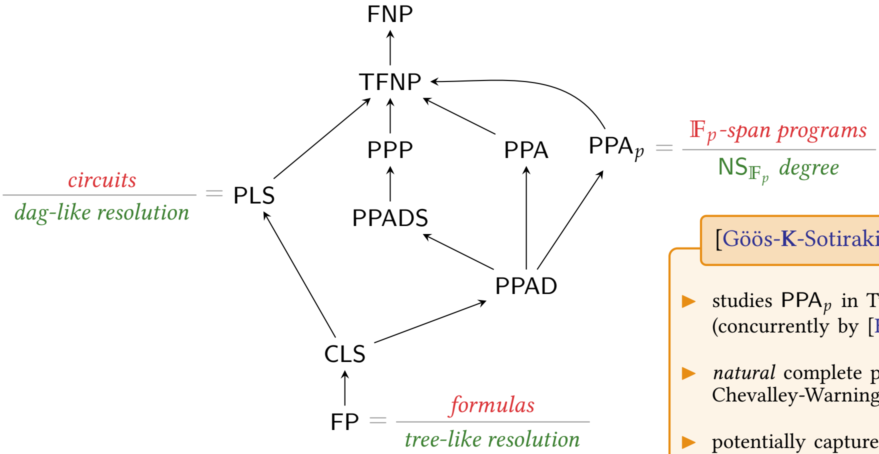
TFNP in Query & Communication



TFNP in Query & Communication



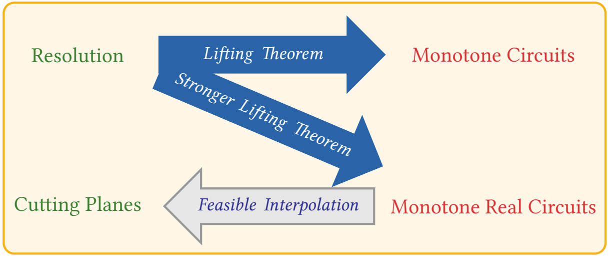
TFNP in Query & Communication



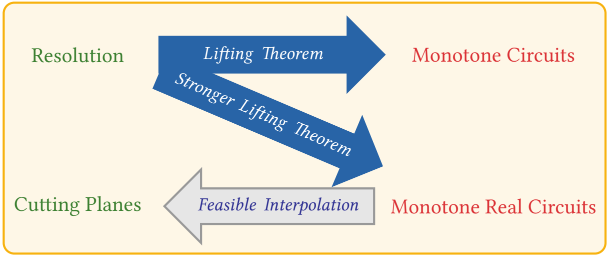
[Göös-K-Sotiraki-Zampetakis 19]

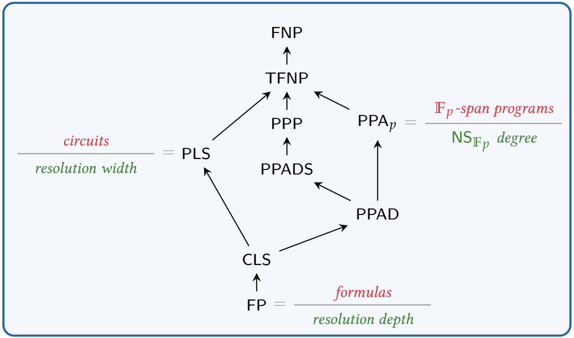
- studies PPA$_p$ in Turing machine world (concurrently by [Hollender 19])
- *natural* complete problem based on Chevalley-Warning theorem.
- potentially captures many more natural problems!

In Conclusion...

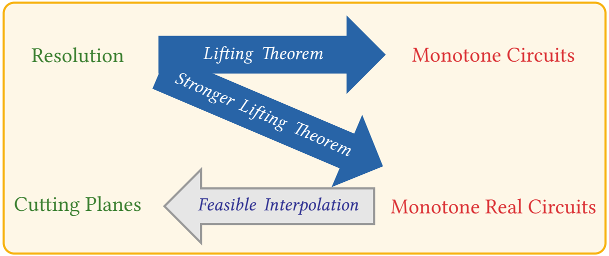


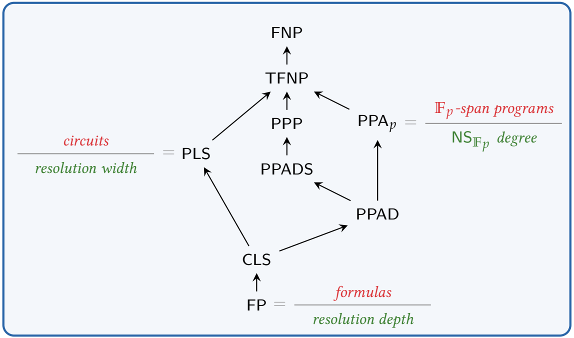
In Conclusion...





In Conclusion...

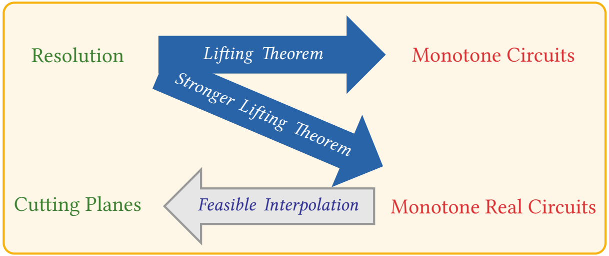


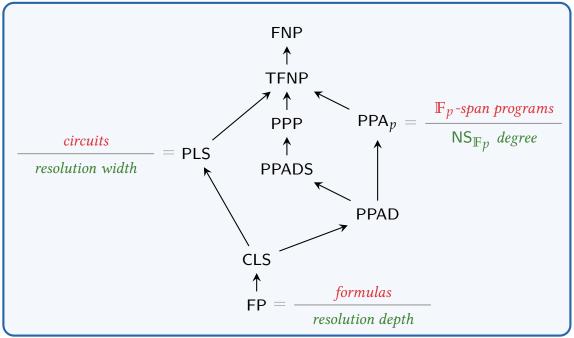


Open Questions

- Lifting with constant-sized gadgets? (Implies $2^{\Omega(n)}$ monotone circuit lower bound.)
- Lifting for dag models with other shapes? (We showed for rectangles and triangles.)
- Exponential monotone circuit lower bound for Perfect-Matching?
- Characterizations & Lifting theorems for other TFNP subclasses?
- TFNP characterizations of Proof systems & Computational models?

In Conclusion...





Open Questions

- Lifting with constant-sized gadgets? (Implies $2^{\Omega(n)}$ monotone circuit lower bound.)
- Lifting for dag models with other shapes? (We showed for rectangles and triangles.)
- Exponential monotone circuit lower bound for Perfect-Matching?
- Characterizations & Lifting theorems for other TFNP subclasses?
- TFNP characterizations of Proof systems & Computational models?

Thanks!
Questions?