Lifting Applied to Proof Complexity

Marc Vinyals

Technion
Haifa, Israel

FSTTCS Workshop on Extension Complexity and Lifting Theorems

Supported by ERC project “HARMONIC”

SAT

Is this formula satisfiable?

$x_{11} \lor x_{12}$	$x_{21} \lor x_{22}$	$x_{31} \lor x_{32}$
$\overline{x_{11}} \lor \overline{x_{21}}$	$\overline{x_{11}} \lor \overline{x_{31}}$	$\overline{x_{21}} \lor \overline{x_{31}}$
$\overline{x_{12}} \lor \overline{x_{22}}$	$\overline{x_{12}} \lor \overline{x_{32}}$	

SAT

Is this formula satisfiable?

$x_{11} \vee x_{12}$	$x_{21} \vee x_{22}$	$x_{31} \vee x_{32}$
$\overline{x_{11}} \vee \overline{x_{21}}$	$\overline{x_{11}} \vee \overline{x_{31}}$	$\overline{x_{21}} \vee \overline{x_{31}}$
$\overline{x_{12}} \vee \overline{x_{22}}$	$\overline{x_{12}} \vee \overline{x_{32}}$	

Yes

SAT

Is this formula satisfiable?

$$x_{11} \vee x_{12} \qquad x_{21} \vee x_{22} \qquad x_{31} \vee x_{32}$$
$$\overline{x_{11}} \vee \overline{x_{21}} \qquad \overline{x_{11}} \vee \overline{x_{31}} \qquad \overline{x_{21}} \vee \overline{x_{31}}$$
$$\overline{x_{12}} \vee \overline{x_{22}} \qquad \overline{x_{12}} \vee \overline{x_{32}}$$

Yes

$x_{11} = 1, x_{12} = 0, x_{21} = 0, x_{22} = 1, x_{31} = 0, x_{32} = 1.$

SAT

Is this formula satisfiable?

$$x_{11} \vee x_{12} \qquad x_{21} \vee x_{22} \qquad x_{31} \vee x_{32}$$

$$\overline{x_{11}} \vee \overline{x_{21}} \qquad \overline{x_{11}} \vee \overline{x_{31}} \qquad \overline{x_{21}} \vee \overline{x_{31}}$$

$$\overline{x_{12}} \vee \overline{x_{22}} \qquad \overline{x_{12}} \vee \overline{x_{32}} \qquad \overline{x_{22}} \vee \overline{x_{32}}$$

SAT

Is this formula satisfiable?

$$
\begin{array}{ccc}
x_{11} \vee x_{12} & x_{21} \vee x_{22} & x_{31} \vee x_{32} \\
\overline{x_{11}} \vee \overline{x_{21}} & \overline{x_{11}} \vee \overline{x_{31}} & \overline{x_{21}} \vee \overline{x_{31}} \\
\overline{x_{12}} \vee \overline{x_{22}} & \overline{x_{12}} \vee \overline{x_{32}} & \overline{x_{22}} \vee \overline{x_{32}}
\end{array}
$$

No

SAT

Is this formula satisfiable?

$$x_{11} \vee x_{12} \qquad x_{21} \vee x_{22} \qquad x_{31} \vee x_{32}$$
$$\overline{x_{11}} \vee \overline{x_{21}} \qquad \overline{x_{11}} \vee \overline{x_{31}} \qquad \overline{x_{21}} \vee \overline{x_{31}}$$
$$\overline{x_{12}} \vee \overline{x_{22}} \qquad \overline{x_{12}} \vee \overline{x_{32}} \qquad \overline{x_{22}} \vee \overline{x_{32}}$$

No

I promise

SAT

Is this formula satisfiable?

$$x_{11} \lor x_{12} \qquad x_{21} \lor x_{22} \qquad x_{31} \lor x_{32}$$
$$\overline{x_{11}} \lor \overline{x_{21}} \qquad \overline{x_{11}} \lor \overline{x_{31}} \qquad \overline{x_{21}} \lor \overline{x_{31}}$$
$$\overline{x_{12}} \lor \overline{x_{22}} \qquad \overline{x_{12}} \lor \overline{x_{32}} \qquad \overline{x_{22}} \lor \overline{x_{32}}$$

No
I promise
Enumerate all 2^6 assignments

Resolution

$x_{11} \lor x_{12}$	$x_{21} \lor x_{22}$	$x_{31} \lor x_{32}$
$\overline{x_{11}} \lor \overline{x_{21}}$	$\overline{x_{11}} \lor \overline{x_{31}}$	$\overline{x_{21}} \lor \overline{x_{31}}$
$\overline{x_{12}} \lor \overline{x_{22}}$	$\overline{x_{12}} \lor \overline{x_{32}}$	$\overline{x_{22}} \lor \overline{x_{32}}$

Resolution

$x_{11} \lor x_{12}$	$x_{21} \lor x_{22}$	$x_{31} \lor x_{32}$
$\overline{x_{11}} \lor \overline{x_{21}}$	$\overline{x_{11}} \lor \overline{x_{31}}$	$\overline{x_{21}} \lor \overline{x_{31}}$
$\overline{x_{12}} \lor \overline{x_{22}}$	$\overline{x_{12}} \lor \overline{x_{32}}$	$\overline{x_{22}} \lor \overline{x_{32}}$

$$x_{31} \lor \overline{x_{22}}$$

Resolution

$x_{11} \lor x_{12}$ $\quad$ $x_{21} \lor x_{22}$ $\quad$ $x_{31} \lor x_{32}$

$\overline{x_{11}} \lor \overline{x_{21}}$ $\quad$ $\overline{x_{11}} \lor \overline{x_{31}}$ $\quad$ $\overline{x_{21}} \lor \overline{x_{31}}$

$\overline{x_{12}} \lor \overline{x_{22}}$ $\quad$ $\overline{x_{12}} \lor \overline{x_{32}}$ $\quad$ $\overline{x_{22}} \lor \overline{x_{32}}$

$x_{31} \lor \overline{x_{22}}$

$x_{31} \lor x_{21}$

Resolution

$x_{11} \lor x_{12}$	$x_{21} \lor x_{22}$	$x_{31} \lor x_{32}$
$\overline{x_{11}} \lor \overline{x_{21}}$	$\overline{x_{11}} \lor \overline{x_{31}}$	$\overline{x_{21}} \lor \overline{x_{31}}$
$\overline{x_{12}} \lor \overline{x_{22}}$	$\overline{x_{12}} \lor \overline{x_{32}}$	$\overline{x_{22}} \lor \overline{x_{32}}$

$x_{31} \lor \overline{x_{22}}$

$x_{31} \lor x_{21}$

$\overline{x_{11}} \lor x_{21}$

Resolution

$x_{11} \vee x_{12}$	$x_{21} \vee x_{22}$	$x_{31} \vee x_{32}$
$\overline{x_{11}} \vee \overline{x_{21}}$	$\overline{x_{11}} \vee \overline{x_{31}}$	$\overline{x_{21}} \vee \overline{x_{31}}$
$\overline{x_{12}} \vee \overline{x_{22}}$	$\overline{x_{12}} \vee \overline{x_{32}}$	$\overline{x_{22}} \vee \overline{x_{32}}$

$x_{31} \vee \overline{x_{22}}$

$x_{31} \vee x_{21}$

$\overline{x_{11}} \vee x_{21}$

$\overline{x_{11}}$

Resolution

$x_{11} \lor x_{12}$	$x_{21} \lor x_{22}$	$x_{31} \lor x_{32}$
$\overline{x_{11}} \lor \overline{x_{21}}$	$\overline{x_{11}} \lor \overline{x_{31}}$	$\overline{x_{21}} \lor \overline{x_{31}}$
$\overline{x_{12}} \lor \overline{x_{22}}$	$\overline{x_{12}} \lor \overline{x_{32}}$	$\overline{x_{22}} \lor \overline{x_{32}}$

$x_{31} \lor \overline{x_{22}}$

$x_{31} \lor x_{21}$

$\overline{x_{11}} \lor x_{21}$

$\overline{x_{11}}$

$\cdots$

x_{11}

Resolution

$x_{11} \lor x_{12}$ $x_{21} \lor x_{22}$ $x_{31} \lor x_{32}$

$\overline{x_{11}} \lor \overline{x_{21}}$ $\overline{x_{11}} \lor \overline{x_{31}}$ $\overline{x_{21}} \lor \overline{x_{31}}$

$\overline{x_{12}} \lor \overline{x_{22}}$ $\overline{x_{12}} \lor \overline{x_{32}}$ $\overline{x_{22}} \lor \overline{x_{32}}$

$x_{31} \lor \overline{x_{22}}$

$x_{31} \lor x_{21}$

$\overline{x_{11}} \lor x_{21}$

$\overline{x_{11}}$

$\cdots$

x_{11}

$\bot$

Cutting Planes

$x_{11} \vee x_{12}$	$x_{21} \vee x_{22}$	$x_{31} \vee x_{32}$
$\overline{x_{11}} \vee \overline{x_{21}}$	$\overline{x_{11}} \vee \overline{x_{31}}$	$\overline{x_{21}} \vee \overline{x_{31}}$
$\overline{x_{12}} \vee \overline{x_{22}}$	$\overline{x_{12}} \vee \overline{x_{32}}$	$\overline{x_{22}} \vee \overline{x_{32}}$

Cutting Planes

$$x_{11} + x_{12} \geq 1 \qquad x_{21} + x_{22} \geq 1 \qquad x_{31} + x_{32} \geq 1$$

$$\overline{x_{11}} + \overline{x_{21}} \geq 1 \qquad \overline{x_{11}} + \overline{x_{31}} \geq 1 \qquad \overline{x_{21}} + \overline{x_{31}} \geq 1$$

$$\overline{x_{12}} + \overline{x_{22}} \geq 1 \qquad \overline{x_{12}} + \overline{x_{32}} \geq 1 \qquad \overline{x_{22}} + \overline{x_{32}} \geq 1$$

Cutting Planes

$$
\begin{array}{rrr}
x_{11} + x_{12} \geq 1 & x_{21} + x_{22} \geq 1 & x_{31} + x_{32} \geq 1 \\
1 - x_{11} + 1 - x_{21} \geq 1 & 1 - x_{11} + 1 - x_{31} \geq 1 & 1 - x_{21} + 1 - x_{31} \geq 1 \\
1 - x_{12} + 1 - x_{22} \geq 1 & 1 - x_{12} + 1 - x_{32} \geq 1 & 1 - x_{22} + 1 - x_{32} \geq 1
\end{array}
$$

Cutting Planes

$$x_{11} + x_{12} \geq 1 \qquad x_{21} + x_{22} \geq 1 \qquad x_{31} + x_{32} \geq 1$$
$$-x_{11} - x_{21} \geq -1 \qquad -x_{11} - x_{31} \geq -1 \qquad -x_{21} - x_{31} \geq -1$$
$$-x_{12} - x_{22} \geq -1 \qquad -x_{12} - x_{32} \geq -1 \qquad -x_{22} - x_{32} \geq -1$$

Cutting Planes

$$x_{11} + x_{12} \geq 1 \qquad x_{21} + x_{22} \geq 1 \qquad x_{31} + x_{32} \geq 1$$

$$-x_{11} - x_{21} \geq -1 \qquad -x_{11} - x_{31} \geq -1 \qquad -x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} \geq -1 \qquad -x_{12} - x_{32} \geq -1 \qquad -x_{22} - x_{32} \geq -1$$

$$-2x_{11} - 2x_{21} - 2x_{31} \geq -3$$

Cutting Planes

$$x_{11} + x_{12} \geq 1 \qquad x_{21} + x_{22} \geq 1 \qquad x_{31} + x_{32} \geq 1$$
$$-x_{11} - x_{21} \geq -1 \qquad -x_{11} - x_{31} \geq -1 \qquad -x_{21} - x_{31} \geq -1$$
$$-x_{12} - x_{22} \geq -1 \qquad -x_{12} - x_{32} \geq -1 \qquad -x_{22} - x_{32} \geq -1$$

$$-2x_{11} - 2x_{21} - 2x_{31} \geq -3$$
$$-x_{11} - x_{21} - x_{31} \geq -3/2$$

Cutting Planes

$$x_{11} + x_{12} \geq 1 \qquad x_{21} + x_{22} \geq 1 \qquad x_{31} + x_{32} \geq 1$$
$$-x_{11} - x_{21} \geq -1 \qquad -x_{11} - x_{31} \geq -1 \qquad -x_{21} - x_{31} \geq -1$$
$$-x_{12} - x_{22} \geq -1 \qquad -x_{12} - x_{32} \geq -1 \qquad -x_{22} - x_{32} \geq -1$$

$$-2x_{11} - 2x_{21} - 2x_{31} \geq -3$$
$$-x_{11} - x_{21} - x_{31} \geq -3/2$$
$$-x_{11} - x_{21} - x_{31} \geq -1$$

Cutting Planes

$$x_{11} + x_{12} \geq 1 \qquad x_{21} + x_{22} \geq 1 \qquad x_{31} + x_{32} \geq 1$$

$$-x_{11} - x_{21} \geq -1 \qquad -x_{11} - x_{31} \geq -1 \qquad -x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} \geq -1 \qquad -x_{12} - x_{32} \geq -1 \qquad -x_{22} - x_{32} \geq -1$$

$$-2x_{11} - 2x_{21} - 2x_{31} \geq -3$$

$$-x_{11} - x_{21} - x_{31} \geq -3/2$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

Cutting Planes

$$x_{11} + x_{12} \geq 1 \qquad x_{21} + x_{22} \geq 1 \qquad x_{31} + x_{32} \geq 1$$

$$-x_{11} - x_{21} \geq -1 \qquad -x_{11} - x_{31} \geq -1 \qquad -x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} \geq -1 \qquad -x_{12} - x_{32} \geq -1 \qquad -x_{22} - x_{32} \geq -1$$

$$-2x_{11} - 2x_{21} - 2x_{31} \geq -3$$

$$-x_{11} - x_{21} - x_{31} \geq -3/2$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

$$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$$

Cutting Planes

$$x_{11} + x_{12} \geq 1 \qquad x_{21} + x_{22} \geq 1 \qquad x_{31} + x_{32} \geq 1$$

$$-x_{11} - x_{21} \geq -1 \qquad -x_{11} - x_{31} \geq -1 \qquad -x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} \geq -1 \qquad -x_{12} - x_{32} \geq -1 \qquad -x_{22} - x_{32} \geq -1$$

$$-2x_{11} - 2x_{21} - 2x_{31} \geq -3$$

$$-x_{11} - x_{21} - x_{31} \geq -3/2$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

$$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$$

$$x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} \geq 3$$

Cutting Planes

$$x_{11} + x_{12} \geq 1 \qquad x_{21} + x_{22} \geq 1 \qquad x_{31} + x_{32} \geq 1$$
$$-x_{11} - x_{21} \geq -1 \qquad -x_{11} - x_{31} \geq -1 \qquad -x_{21} - x_{31} \geq -1$$
$$-x_{12} - x_{22} \geq -1 \qquad -x_{12} - x_{32} \geq -1 \qquad -x_{22} - x_{32} \geq -1$$

$$\begin{aligned}
-2x_{11} - 2x_{21} - 2x_{31} &\geq -3 \\
-x_{11} - x_{21} - x_{31} &\geq -3/2 \\
-x_{11} - x_{21} - x_{31} &\geq -1 \\
-x_{12} - x_{22} - x_{32} &\geq -1 \\
-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} &\geq -2 \\
x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} &\geq 3 \\
0 &\geq 1
\end{aligned}$$

A Few Proof Systems

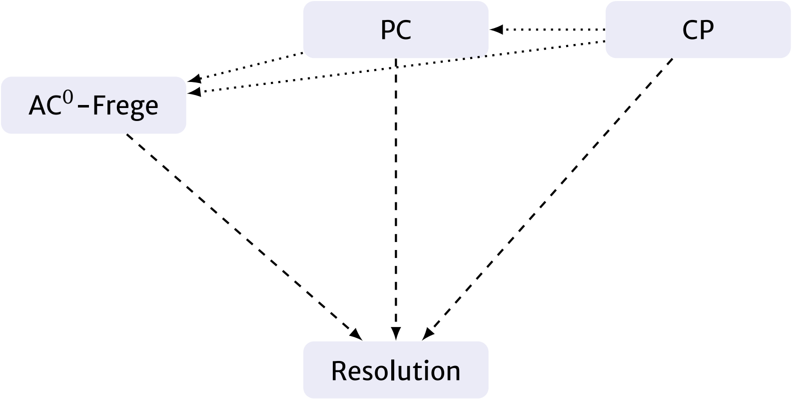
Resolution
Lines are clauses

Polynomial Calculus
Lines are polynomials

Cutting Planes
Lines are linear inequalities

Bounded Depth Frege
Lines are AC^0 circuits

Family Picture



$A \longrightarrow B$: A simulates B (with only polynomial loss)
$A \cdots\blacktriangleright B$: B cannot simulate A (separation)
$A - - \blacktriangleright B$: simulation+separation
$A \blacktriangleleft\cdots\blacktriangleright B$: incomparable

Lifting

Lifting

- Proving lower bounds is hard.
- Let us prove easier lower bounds.

Lifting

- Proving lower bounds is hard.
- Let us prove easier lower bounds.

Plan

1. Prove formula F hard in weak model/measure.
2. Lift to $F \circ g$.
3. Prove generic lifting theorem.
4. Lifted problem hard in strong model/measure.

Lifting

- Proving lower bounds is hard.
- Let us prove easier lower bounds.

Plan

1. Prove formula F hard in weak model/measure.
2. Lift to $F \circ g$.
3. Prove generic lifting theorem.
4. Lifted problem hard in strong model/measure.

- Many results in proof complexity follow this pattern.

Lifting

- Proving lower bounds is hard.
- Let us prove easier lower bounds.

Plan

1. Prove formula F hard in weak model/measure.
2. Lift to $F \circ g$.
3. Prove generic lifting theorem.
4. Lifted problem hard in communication complexity.
5. Lifted problem has no short proofs.

- Many results in proof complexity follow this pattern.
- This talk: communication complexity techniques.

Lifting in Proof Complexity

- Have formula F with variables $x_1, \ldots, x_n$.
- Replace variable x_i with gadget $g(x_i^1, \ldots, x_i^k)$.

Lifting in Proof Complexity

- Have formula F with variables $x_1, \ldots, x_n$.
- Replace variable x_i with gadget $g(x_i^1, \ldots, x_i^k)$.

Example

$$F \quad = \quad \{x \vee y,\ \overline{x} \vee y,\ \overline{y}\}$$

$$F \circ \oplus \quad = \quad \{x^1 \oplus x^2 \vee y^1 \oplus y^2,\ \overline{x^1 \oplus x^2} \vee y^1 \oplus y^2,\ \overline{y^1 \oplus y^2}\}$$

Lifting in Proof Complexity

- Have formula F with variables $x_1, \dots, x_n$.
- Replace variable x_i with gadget $g(x_i^1, \dots, x_i^k)$.

Example

$$F = \{x \vee y,\ \overline{x} \vee y,\ \overline{y}\}$$

$$\begin{aligned}
F \circ \oplus &= \{x^1 \oplus x^2 \vee y^1 \oplus y^2,\ \overline{x^1 \oplus x^2} \vee y^1 \oplus y^2,\ \overline{y^1 \oplus y^2}\} \\
&= x^1 \vee x^2 \vee y^1 \vee y^2,\ x^1 \vee x^2 \vee \overline{y^1} \vee \overline{y^2}, \\
&\quad \overline{x^1} \vee \overline{x^2} \vee y^1 \vee y^2,\ \overline{x^1} \vee \overline{x^2} \vee \overline{y^1} \vee \overline{y^2}, \\
&\quad \dots \\
&\quad y_1 \vee \overline{y_2},\ \overline{y_1} \vee y_2
\end{aligned}$$

Falsified Clause Search Problem

Given CNF formula F

Input Assignment to variables $\alpha : x \mapsto \{0,1\}^n$

Output Clause $C \in F$ falsified by assignment α

Falsified Clause Search Problem

Given CNF formula F

Input Assignment to variables $\alpha : x \mapsto \{0,1\}^n$

Output Clause $C \in F$ falsified by assignment α

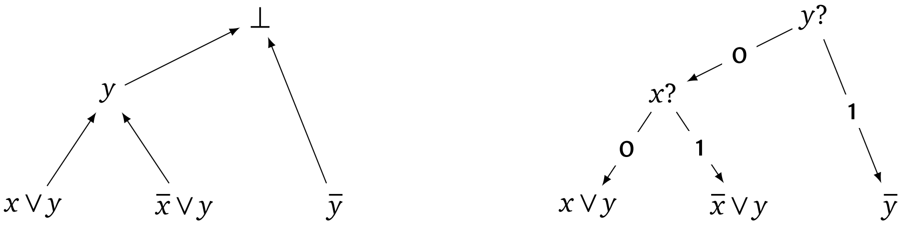
Example

Given $F = \{x \vee y,\ \overline{x} \vee y,\ \overline{y}\}$

Input $x = 0,\ y = 1$

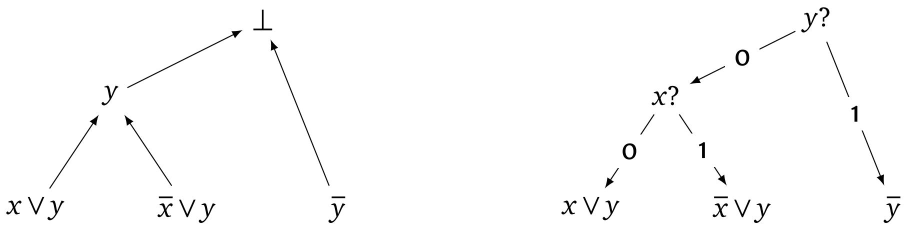
Output $\overline{y}$

Proofs as Search Problems



- Small proof $\implies$ small decision tree.

Proofs as Search Problems



- Small proof $\implies$ small decision tree.
- But proofs cannot be balanced, we only get depth lower bounds.
- Use communication complexity.

Examples

Resolution vs Cutting Planes

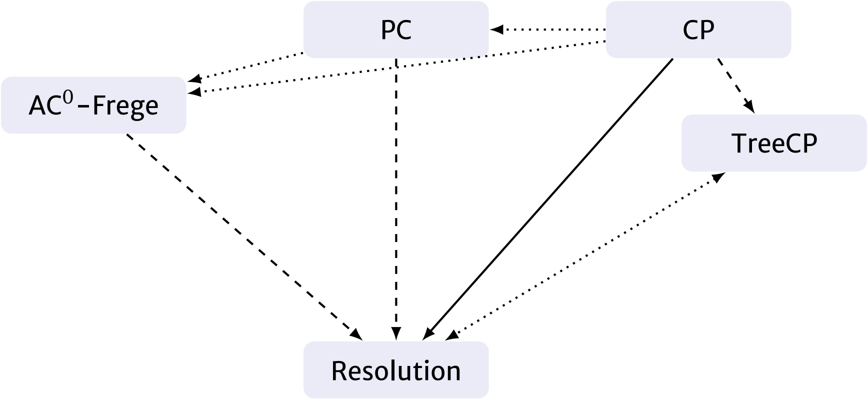
[Bonet, Esteban, Galesi, Johannsen '98]

Theorem

There exists a formula family F_n such that

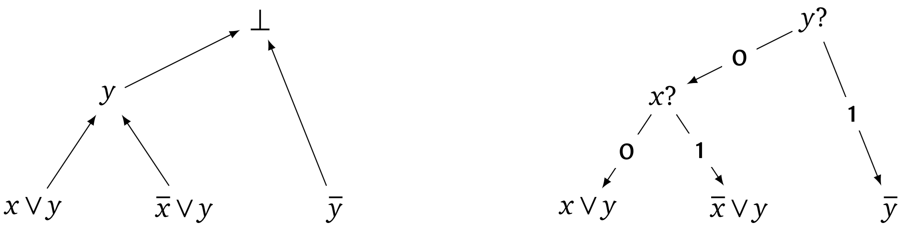
- F_n *has resolution proofs of length* $\mathrm{poly}(n)$
- *But every tree-like CP proof must have length* $\exp(\Omega(n))$

Family Picture



$A \longrightarrow B$: A simulates B (with only polynomial loss)
$A \cdots\rightarrow B$: B cannot simulate A (separation)
$A \dashrightarrow B$: simulation+separation
$A \leftarrow\cdots\rightarrow B$: incomparable

Proofs as Search Problems



- Small proof $\implies$ small decision tree.
- But proofs cannot be balanced, we only get depth lower bounds.
- Use communication complexity.

Tree-like CP to Communication

$$0 \geq 1$$

$$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$$

$$x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} \geq 3$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

Alice

$$x_{11} = 0, x_{22} = 1, x_{31} = 0$$

Bob

$$x_{12} = 1, x_{21} = 0, x_{32} = 1$$

Tree-like CP to Communication

$$0 \geq 1$$

$$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$$

$$x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} \geq 3$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

Alice

$$x_{11} = 0, x_{22} = 1, x_{31} = 0$$

Bob

$$x_{12} = 1, x_{21} = 0, x_{32} = 1$$

- Alice sends sum of her variables; Bob evaluates inequality.

Tree-like CP to Communication

$$0 \geq 1$$

$$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$$

$$x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} \geq 3$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

Alice —— -1 ——→ Bob

$x_{11} = 0, x_{22} = 1, x_{31} = 0$

$x_{12} = 1, x_{21} = 0, x_{32} = 1$

- Alice sends sum of her variables; Bob evaluates inequality.

Tree-like CP to Communication

$0 \geq 1$

$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$

$x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} \geq 3$

$-x_{11} - x_{21} - x_{31} \geq -1$

$-x_{12} - x_{22} - x_{32} \geq -1$

Alice ← 0 — Bob

$x_{11} = 0, x_{22} = 1, x_{31} = 0$

$x_{12} = 1, x_{21} = 0, x_{32} = 1$

- Alice sends sum of her variables; Bob evaluates inequality.

Tree-like CP to Communication

$$0 \geq 1$$

$$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$$

$$x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} \geq 3$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

Alice

$x_{11} = 0, x_{22} = 1, x_{31} = 0$

Bob

$x_{12} = 1, x_{21} = 0, x_{32} = 1$

- Alice sends sum of her variables; Bob evaluates inequality.

Tree-like CP to Communication

$$0 \geq 1$$

$$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$$

$$x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} \geq 3$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

Alice —— 0 ——→ Bob

$x_{11} = 0, x_{22} = 1, x_{31} = 0$

$x_{12} = 1, x_{21} = 0, x_{32} = 1$

- Alice sends sum of her variables; Bob evaluates inequality.

Tree-like CP to Communication

$$0 \geq 1$$

$$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$$

$$x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} \geq 3$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

Alice ← 1 — Bob

$x_{11} = 0, x_{22} = 1, x_{31} = 0$

$x_{12} = 1, x_{21} = 0, x_{32} = 1$

- Alice sends sum of her variables; Bob evaluates inequality.

Tree-like CP to Communication

$$0 \geq 1$$

$$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$$

$$x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} \geq 3$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

Alice

$x_{11} = 0, x_{22} = 1, x_{31} = 0$

Bob

$x_{12} = 1, x_{21} = 0, x_{32} = 1$

- Alice sends sum of her variables; Bob evaluates inequality.

Tree-like CP to Communication

$$0 \geq 1$$

$$-x_{11} - x_{21} - x_{31} - x_{12} - x_{22} - x_{32} \geq -2$$

$$x_{11} + x_{21} + x_{31} + x_{12} + x_{22} + x_{32} \geq 3$$

$$-x_{11} - x_{21} - x_{31} \geq -1$$

$$-x_{12} - x_{22} - x_{32} \geq -1$$

Alice

$$x_{11} = 0, x_{22} = 1, x_{31} = 0$$

Bob

$$x_{12} = 1, x_{21} = 0, x_{32} = 1$$

- Alice sends sum of her variables; Bob evaluates inequality.
- Ok if small coefficients, in general solve GT.

Communication with a GT Oracle

- Want a lifting theorem for a model of communication where GT is easy.
- e.g. Randomized
- or Deterministic with a GT oracle.

Communication with a GT Oracle

- Want a lifting theorem for a model of communication where GT is easy.
- e.g. Randomized
- or Deterministic with a GT oracle.

Alice

x

Oracle

$\geq$

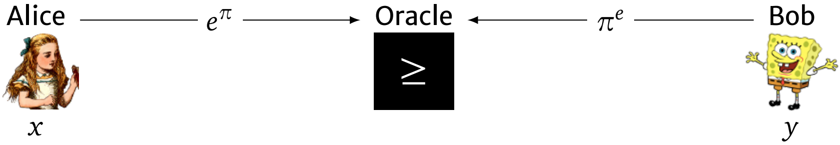
Bob

y

- Send $f(x)$, $g(y)$ to oracle
- Both parties see answer
- Cost number of calls

Communication with a GT Oracle

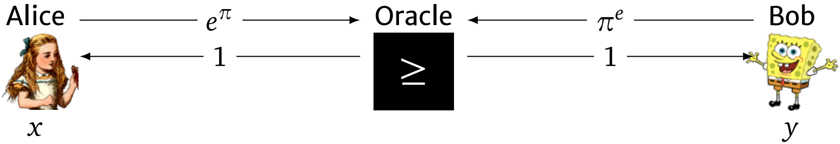
- Want a lifting theorem for a model of communication where GT is easy.
- e.g. Randomized
- or Deterministic with a GT oracle.



- Send $f(x)$, $g(y)$ to oracle
- Both parties see answer
- Cost number of calls

Communication with a GT Oracle

- Want a lifting theorem for a model of communication where GT is easy.
- e.g. Randomized
- or Deterministic with a GT oracle.



- Send $f(x)$, $g(y)$ to oracle
- Both parties see answer
- Cost number of calls

Lifting With a GT Oracle

Theorem

$$\mathsf{P}_{\mathrm{cc}}^{\mathsf{GT}}(f \circ \mathrm{IND}) = \Omega(\mathsf{P}_{\mathrm{dt}}(f) \cdot \log n)$$

Lifting With a GT Oracle

Theorem

$\mathsf{P}_{\mathrm{cc}}^{\mathsf{GT}}(f \circ \mathrm{IND}) = \Omega(\mathsf{P}_{\mathrm{dt}}(f) \cdot \log n)$

Proof

- Essentially like Arkadev's talk.

Lifting With a GT Oracle

Theorem

$\mathsf{P}_{\mathrm{cc}}^{\mathsf{GT}}(f \circ \mathrm{IND}) = \Omega(\mathsf{P}_{\mathrm{dt}}(f) \cdot \log n)$

Proof

- Essentially like Arkadev's talk. Recall:
- One bit of communication partitions inputs into two rectangles.
- At least one is large.

Lifting With a GT Oracle

Theorem

$\mathsf{P}_{\mathrm{cc}}^{\mathsf{GT}}(f \circ \mathrm{IND}) = \Omega(\mathsf{P}_{\mathrm{dt}}(f) \cdot \log n)$

Proof

- Essentially like Arkadev's talk. Recall:
- One bit of communication partitions inputs into two rectangles.
- At least one is large.
- Now partition inputs into two triangles.
- At least one contains a large rectangle.

Polynomial Calculus vs Cutting Planes

[Garg, Göös, Kamath, Sokolov ’18; Göös, Kamath, Robere, Sokolov ’19]

Theorem

There exists a formula family F_n such that

- F_n *has polynomial calculus proof of length* $\mathrm{poly}(n)$
- *But every CP proof must have length* $\exp(\Omega(n))$

Polynomial Calculus vs Cutting Planes

[Garg, Göös, Kamath, Sokolov '18; Göös, Kamath, Robere, Sokolov '19]

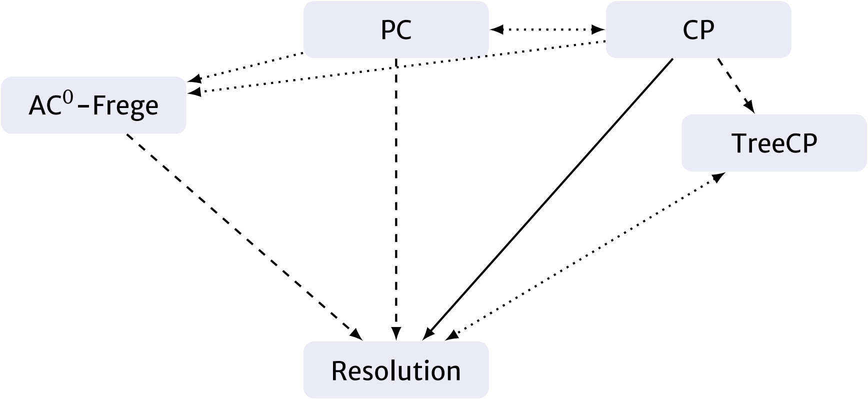
Theorem

There exists a formula family F_n such that

- *F_n has polynomial calculus proof of length* $\mathrm{poly}(n)$
- *But every CP proof must have length* $\exp(\Omega(n))$

- Uses "DAG-like" lifting
- More after tea!

Family Picture



$A \longrightarrow B$: A simulates B (with only polynomial loss)
$A \cdots\blacktriangleright B$: B cannot simulate A (separation)
$A - - \blacktriangleright B$: simulation+separation
$A \blacktriangleleft\cdots\blacktriangleright B$: incomparable

Coefficients in Cutting Planes

- Every Boolean function that can be represented with a linear inequality has a representation with coefficients of size $O(n!)$.

  [Muroga, Toda, Takasu '61]

- And this is tight.

  [Håstad '94]

Coefficients in Cutting Planes

- Every Boolean function that can be represented with a linear inequality has a representation with coefficients of size $O(n!)$.
  [Muroga, Toda, Takasu '61]
- And this is tight.
  [Håstad '94]

- Every formula that has a CP proof of length L has a proof of similar length and coefficients of size $O(2^L)$.
  [Buss, Clote '96]
- Is this needed?

Coefficients in Cutting Planes

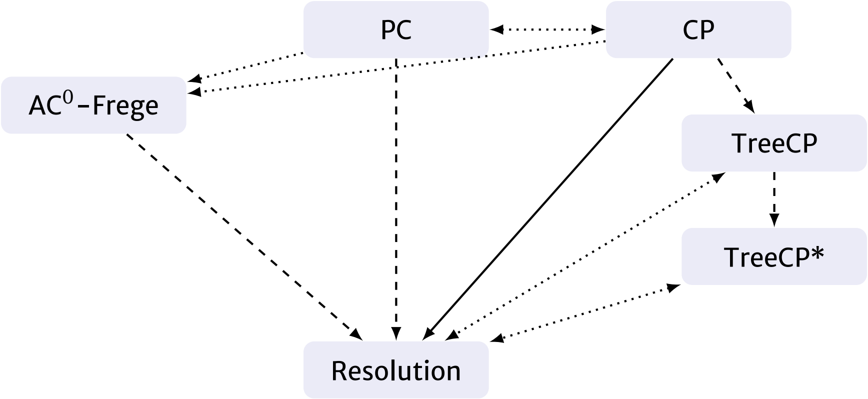
[de Rezende, Meir, Nordström, Pitassi, Robere, V]

Theorem

There exists a formula family F_n such that

- F_n *has tree-like CP proofs of length* $L = \mathrm{poly}(n)$
- F_n *has tree-like CP proofs with coefficient size* $c = \mathrm{O}(1)$
- *But every tree-like CP proof must have* $\log L \cdot c = \Omega(n)$

Family Picture



$A \longrightarrow B$: A simulates B (with only polynomial loss)
$A \cdots\blacktriangleright B$: B cannot simulate A (separation)
$A - - \blacktriangleright B$: simulation+separation
$A \blacktriangleleft\cdots\blacktriangleright B$: incomparable

How to Use Large Coefficients

How to encode $x_1 = y_1, \ldots, x_n = y_n$?

How to Use Large Coefficients

How to encode $x_1 = y_1, \ldots, x_n = y_n$?

- $2n$ inequalities

$$x_1 \geq y_1$$
$$y_1 \geq x_1$$
$$\ldots$$
$$x_n \geq y_n$$
$$y_n \geq x_n$$

How to Use Large Coefficients

How to encode $x_1 = y_1, \dots, x_n = y_n$?

- $2n$ inequalities

$$x_1 \geq y_1$$
$$y_1 \geq x_1$$
$$\dots$$
$$x_n \geq y_n$$
$$y_n \geq x_n$$

How to Use Large Coefficients

How to encode $x_1 = y_1, \dots, x_n = y_n$?

- $2n$ inequalities

$$\begin{aligned} x_1 &\geq y_1 \\ y_1 &\geq x_1 \\ &\dots \\ x_n &\geq y_n \\ y_n &\geq x_n \end{aligned}$$

- 1 equality

$$x_1 + 2x_2 + \cdots + 2^{n-1}x_n = y_1 + 2y_2 + \cdots 2^{n-1}y_n$$

How to Use Large Coefficients

How to encode $x_1 = y_1, \ldots, x_n = y_n$?

- $2n$ inequalities

$$x_1 \geq y_1$$
$$y_1 \geq x_1$$
$$\ldots$$
$$x_n \geq y_n$$
$$y_n \geq x_n$$

- 2 inequalities

$$x_1 + 2x_2 + \cdots + 2^{n-1}x_n \geq y_1 + 2y_2 + \cdots 2^{n-1}y_n$$
$$y_1 + 2y_2 + \cdots + 2^{n-1}y_n \geq x_1 + 2x_2 + \cdots 2^{n-1}x_n$$

Lifting with Equality Gadget

Theorem

$\mathsf{P}_{cc}(\mathrm{Search}(F \circ g)) \geq \deg_{\mathrm{Nss}}(F)$
for all gadgets g *such that* $\mathrm{rank}(g) \geq n/\deg_{\mathrm{Nss}}(F)$.

Nullstellensatz degree $\deg_{\mathrm{Nss}}(F)$:

- Interpret F as polynomials $\{f_i\}$.
- Pick polynomials g_i such that

$$\sum_i f_i g_i = 1$$

with minimal $\max_i \deg(f_i g_i)$.

Wishlist

- DAG-like lifting for intersections of triangles?

Wishlist

- DAG-like lifting for intersections of triangles?

- Multi-party lifting?

Wishlist

- DAG-like lifting for intersections of triangles?
- Multi-party lifting?
- Simulation version of lifting with equality gadget?

Wishlist

- DAG-like lifting for intersections of triangles?
- Multi-party lifting?
- Simulation version of lifting with equality gadget?
  - Round-aware lifting with equality?
  - DAG-like lifting with equality?

Take Home

- Have a new lifting theorem?
- Chances are it implies something for proof complexity!

Take Home

- Have a new lifting theorem?
- Chances are it implies something for proof complexity!

Thanks!

Technical Detail

- Proof for $F \circ g \implies$ protocol for $\mathrm{Search}(F \circ g)$.
- But lower bound for $\mathrm{Search}(F) \circ g$.

Technical Detail

- Proof for $F \circ g \implies$ protocol for $\mathrm{Search}(F \circ g)$.
- But lower bound for $\mathrm{Search}(F) \circ g$.

- Not a problem:
  protocol for $\mathrm{Search}(F \circ g) \implies$ protocol for $\mathrm{Search}(F) \circ g$.
  - On input (x,y) obtain clause D falsified by (x,y).
  - $D \in \mathrm{CNF}(C \circ g)$ with $C \in F$.
  - Answer C falsified by $z = g(x,y)$.