Lifting Applied to Proof Complexity

Marc Vinyals

Technion
Haifa, Israel

Banff workshop on Proof Complexity

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. Compose to $F \circ g$.
3. Prove generic lifting theorem.
4. Lifted formula $F \circ g$ 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. Compose to $F \circ g$.
3. Prove generic lifting theorem.
4. Lifted formula $F \circ g$ hard in strong model/measure.

- Many results in proof complexity follow this pattern.

Results Using Lifting

- Separation of Tree-like Resolution & Cutting Planes vs Resolution
- Separation of Resolution Space vs Width
- Size-space trade-offs in Resolution & Cutting Planes
- Rank lower bounds for semialgebraic proof systems
- Size-space-precision trade-offs in Cutting Planes
- Separation of Regular Resolution vs Resolution
- Supercritical trade-offs
- Separation of Polynomial Calculus vs Sherali–Adams
- Lower bounds for Tree-like Res(Lin)
- Separation of Res(k) vs Res(k+1)
- ...

Warm-up: Resolution Size Lower Bound for Tseitin

Tseitin

- One variable per edge
- One constraint $\bigoplus_{e \ni v} x_e = \chi_v$ per vertex

Warm-up: Resolution Size Lower Bound for Tseitin

Tseitin

- One variable per edge
- One constraint $\bigoplus_{e \ni v} x_e = \chi_v$ per vertex

Plan

1. Prove width lower bound for Tseitin.
2. Lift to $\mathrm{Ts} \circ \oplus$.
3. Prove generic lifting theorem

Lemma

If $F \circ \oplus$ has a proof of size s
Then F has a proof of width $\mathrm{O}(\log s)$

4. Get exponential size lower bound for $\mathrm{Ts} \circ \oplus$.

Warm-up: Resolution Size Lower Bound for Tseitin

Tseitin

- One variable per edge
- One constraint $\bigoplus_{e \ni v} x_e = \chi_v$ per vertex

Plan

1. Prove width lower bound for Tseitin.
2. Lift to $\mathrm{Ts} \circ \oplus$.
3. Prove generic lifting theorem

Lemma

If $F \circ \oplus$ has a proof of size s
Then F has a proof of width $\mathrm{O}(\log s)$

4. Get exponential size lower bound for $\mathrm{Ts} \circ \oplus$.

Lifting a CNF Formula

- 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 a CNF Formula

- 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

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

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

Lifting a CNF Formula

- 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

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

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

Warm-up: Resolution Size Lower Bound for Tseitin

Tseitin

- One variable per edge
- One constraint $\bigoplus_{e \ni v} x_e = \chi_v$ per vertex

Plan

1. Prove width lower bound for Tseitin.
2. Lift to $\mathrm{Ts} \circ \oplus$.
3. Prove generic lifting theorem

Lemma

If $F \circ \oplus$ has a proof of size s
Then F has a proof of width $\mathrm{O}(\log s)$

4. Get exponential size lower bound for $\mathrm{Ts} \circ \oplus$.

Lifting Width to Size

Lemma

If $F \circ \oplus$ has a proof of size s
Then F has a proof of width $\mathrm{O}(\log s)$

Proof

- Let ρ be the following restriction.
  - For each original variable x, pick either x^1 or x^2 at random.
  - Set the picked variable to 0 or 1 at random.

Lifting Width to Size

Lemma

If $F \circ \oplus$ has a proof of size s
Then F has a proof of width $\mathrm{O}(\log s)$

Proof

- Let ρ be the following restriction.
  - For each original variable x, pick either x^1 or x^2 at random.
  - Set the picked variable to 0 or 1 at random.
- Assume π proof of $F \circ \oplus$ of length s.
- Then $\pi' = \pi\restriction_\rho$ proof of F (up to flipping literals).

Lifting Width to Size

Lemma

If $F \circ \oplus$ has a proof of size s
Then F has a proof of width $O(\log s)$

Proof

- Let ρ be the following restriction.
  - For each original variable x, pick either x^1 or x^2 at random.
  - Set the picked variable to 0 or 1 at random.
- Assume π proof of $F \circ \oplus$ of length s.
- Then $\pi' = \pi\restriction_\rho$ proof of F (up to flipping literals).
- Claim: some π' has width $O(\log s)$.
  - $\Pr[C \text{ survives}] \leq (3/4)^{w(C)}$.
  - By union bound $\Pr[\text{some wide } C \text{ survives}] \leq s \cdot (3/4)^{4 \log s} < 1$.

Warm-up: Resolution Size Lower Bound for Tseitin

Tseitin

- One variable per edge
- One constraint $\bigoplus_{e \ni v} x_e = \chi_v$ per vertex

Plan

1. Prove width lower bound for Tseitin.
2. Lift to $\mathrm{Ts} \circ \oplus$.
3. Prove generic lifting theorem

Lemma

If $F \circ \oplus$ has a proof of size s
Then F has a proof of width $\mathrm{O}(\log s)$

4. Get exponential size lower bound for $\mathrm{Ts} \circ \oplus$.

Warm-up: Resolution Size Lower Bound for Tseitin

Tseitin

- One variable per edge
- One constraint $\bigoplus_{e \ni v} x_e = \chi_v$ per vertex

Plan

1. Prove width lower bound for Tseitin.
2. Lift to $\mathrm{Ts} \circ \oplus$.
3. Prove generic lifting theorem

Lemma

If $F \circ \oplus$ has a proof of size s
Then F has a proof of width $\mathrm{O}(\log s)$

4. Get exponential size lower bound for $\mathrm{Ts} \circ \oplus$.

Communication

Lifting

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

Plan

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

- Many results in proof complexity follow this pattern.

Lifting via Communication Complexity

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

Plan

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

- Many results in proof complexity follow this pattern.

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

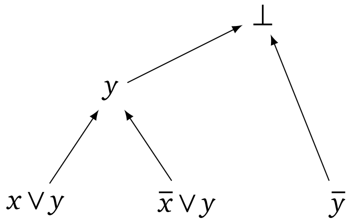
Example

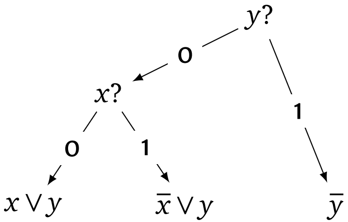
Given $F = \{x \vee y,\ \overline{x} \vee y,\ \overline{y}\}$

Input $x = 0,\ y = 1$

Output $\overline{y}$

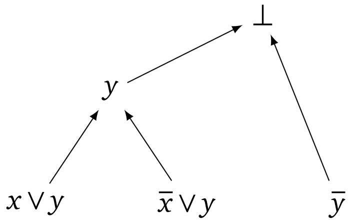
Proofs as Search Problems

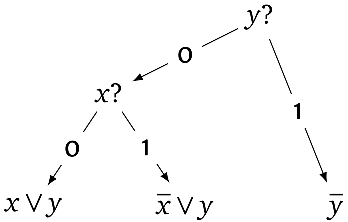




- Small proof $\implies$ small decision tree.

Proofs as Search Problems





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

Deterministic Communication

Alice

Bob

x $f(x,y)$? y

- Two parties compute $f(x,y)$
- Alice knows $x \in X$, Bob knows $y \in Y$

Deterministic Communication

Alice $\xrightarrow{\quad m_1(x) \quad}$ Bob

$\xleftarrow{\quad m_2(y, m_1) \quad}$

$\xrightarrow{\quad m_3(x, m_1, m_2) \quad}$

$\xleftarrow{\quad m_4(y, m_1, m_2, m_3) \quad}$

x $\qquad f(x,y)? \qquad$ y

- Two parties compute $f(x,y)$
- Alice knows $x \in X$, Bob knows $y \in Y$
- Communicate alternately

Deterministic Communication

Alice $\xrightarrow{\quad m_1(x) \quad}$ Bob

$\xleftarrow{\quad m_2(y, m_1) \quad}$

$\xrightarrow{\quad m_3(x, m_1, m_2) \quad}$

$\xleftarrow{\quad m_4(y, m_1, m_2, m_3) \quad}$

x $\qquad f(x,y)?$ $\qquad y$

- Two parties compute $f(x,y)$
- Alice knows $x \in X$, Bob knows $y \in Y$
- Communicate alternately
- Unlimited computing power (deterministic)
- Cost = # bits sent in worst case

Deterministic Communication

Alice

x

$6 \mid x+y$?

Bob

y

Deterministic Communication

Alice $\xrightarrow{\quad x \pmod 2 \quad}$ Bob

x $\qquad 6 \mid x+y?$ $\qquad y$

Deterministic Communication

Alice $\xrightarrow{\quad x \pmod 2 \quad}$ Bob

$\xleftarrow{\quad \text{No / Maybe, } y \pmod 3 \quad}$

x $\qquad 6 \mid x + y?$ $\qquad y$

Deterministic Communication

Alice $\xrightarrow{\quad x \pmod 2 \quad}$ Bob

$\xleftarrow{\quad \text{No / Maybe, } y \pmod 3 \quad}$

$\xrightarrow{\quad \text{Yes / No} \quad}$

x

$6 \mid x+y?$

y

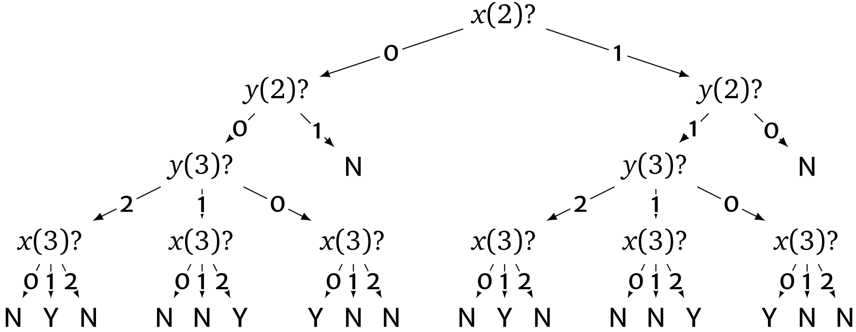
Deterministic Communication

Alice —— $x \pmod{2}$ ——→ Bob

←—— No / Maybe, $y \pmod{3}$ ——

—— Yes / No ——→

x $\quad 6 \mid x+y?$ $\quad y$



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* $\exp(\Omega(n))$

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 $\xrightarrow{\quad -1 \quad}$ 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 $\xleftarrow{\quad 0 \quad}$ 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

$$0 \geq 1$$

$$\boxed{\begin{aligned} &-x_{11} - x_{21} - x_{31} \\ &-x_{12} - x_{22} - x_{32} \geq -2 \end{aligned}}$$

$$\begin{aligned} &x_{11} + x_{21} + x_{31} \\ &+x_{12} + x_{22} + x_{32} \geq 3 \end{aligned}$$

$$\begin{aligned} &-x_{11} - x_{21} \\ &-x_{31} \geq -1 \end{aligned}$$

$$\begin{aligned} &-x_{12} - x_{22} \\ &-x_{32} \geq -1 \end{aligned}$$

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 $\xrightarrow{\quad 0 \quad}$ 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 $\xleftarrow{\quad 1 \quad}$ 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

$$0 \geq 1$$

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

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

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

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

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

$$0 \geq 1$$

$$\begin{aligned} -x_{11} - x_{21} - x_{31} \\ -x_{12} - x_{22} - x_{32} \geq -2 \end{aligned} \qquad \begin{aligned} x_{11} + x_{21} + x_{31} \\ +x_{12} + x_{22} + x_{32} \geq 3 \end{aligned}$$

$$\begin{aligned} -x_{11} - x_{21} \\ -x_{31} \geq -1 \end{aligned} \qquad \begin{aligned} -x_{12} - x_{22} \\ -x_{32} \geq -1 \end{aligned}$$

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.

Alice $\xrightarrow{e^{\pi}}$ Oracle $\xleftarrow{\pi^{e}}$ Bob

x

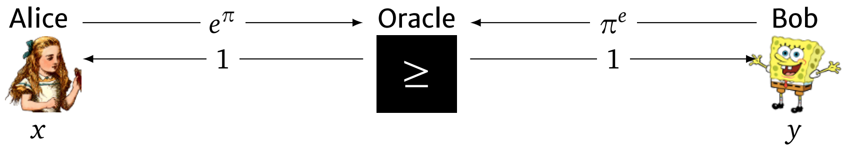
$\boxed{\geq}$

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

Lifting With a GT Oracle

Theorem

If $f \circ \mathrm{IND}$ has a GT-protocol of depth d
Then f has a decision tree of depth $\mathrm{O}(d/\log n)$

$$\begin{aligned} \mathrm{IND}\colon [n] \times \{0,1\}^n &\to \{0,1\} \\ (x,y) &\mapsto y_x \end{aligned}$$

Lifting With a GT Oracle

Theorem

If $f \circ \mathrm{IND}$ has a GT-protocol of depth d
Then f has a decision tree of depth $\mathrm{O}(d/\log n)$

$$\mathrm{IND} : [n] \times \{0,1\}^n \to \{0,1\}$$
$$(x,y) \mapsto y_x$$

Separation follows from Pebbling formula with Indexing.

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]

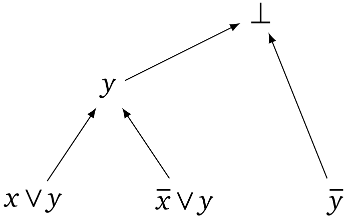
Theorem

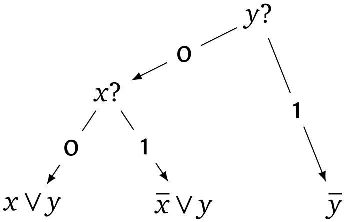
There exists a formula family F_n such that

- *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
- Need "DAG-like" protocols and decision trees

DAG-like Protocols





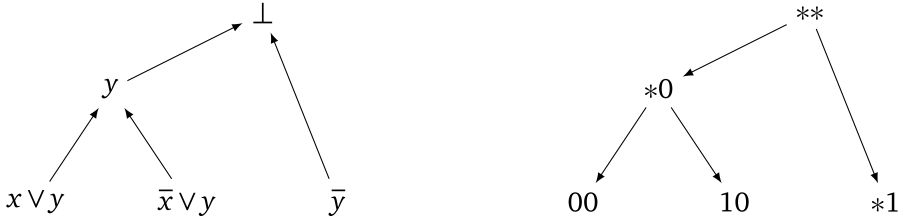
DAG-like Protocols

Dual of a proof:
Replace each line by set of assignments falsifying it; reverse arrows.

$$
\begin{tikzcd}
 & & & \bot & \\
 & y \arrow[urr] & & & \\
x \lor y \arrow[ur] & & \bar{x} \lor y \arrow[ul] & & \bar{y} \arrow[uul]
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
 & & & ** \arrow[dll] \arrow[ddr] & \\
 & *0 \arrow[dl] \arrow[dr] & & & \\
00 & & 10 & & *1
\end{tikzcd}
$$

DAG-like Protocols

Dual of a proof:
Replace each line by set of assignments falsifying it; reverse arrows.



Properties

- Each set has the same shape (resolution: subcube; CP: halfspace).
- Start with complete set (contradiction).
- Each point goes to at least one child (soundness).

Communication-friendly shapes: rectangles, triangles.

Decision DAGs

- Subcube-shaped DAG-like protocols
- Equiv. decision trees where we can forget variables

Decision DAGs

- Subcube-shaped DAG-like protocols
- Equiv. decision trees where we can forget variables

Width of a decision-DAG:
Largest co-dimension of a subcube (largest width of a clause)

Decision DAGs

- Subcube-shaped DAG-like protocols
- Equiv. decision trees where we can forget variables
- Equiv. Atserias–Dalmau game

Width of a decision-DAG:
Largest co-dimension of a subcube (largest width of a clause)

Decision DAGs

- Subcube-shaped DAG-like protocols
- Equiv. decision trees where we can forget variables
- Equiv. Atserias–Dalmau game

Width of a decision-DAG:
Largest co-dimension of a subcube (largest width of a clause)

Example: Fork has width 2
Fork: find a 1 followed by a 0; promise $x_1 = 1$ and $x_n = 0$

Decision DAGs

- Subcube-shaped DAG-like protocols
- Equiv. decision trees where we can forget variables
- Equiv. Atserias–Dalmau game

Width of a decision-DAG:
Largest co-dimension of a subcube (largest width of a clause)

Example: Fork has width 2
Fork: find a 1 followed by a 0; promise $x_1 = 1$ and $x_n = 0$

Non-example: Branching program for parity
Shapes are not subcubes

DAG-like Lifting

Theorem

If $f \circ \mathrm{IND}$ has a {rectangle,triangle}-DAG of size s
Then f has a decision-DAG of width $\mathrm{O}(\log s)$

DAG-like Lifting

Theorem

If $f \circ \mathrm{IND}$ has a {rectangle,triangle}-DAG of size s
Then f has a decision-DAG of width $\mathrm{O}(\log s)$

Separation follows from Tseitin formula with Indexing.

Discussion

Pros

- Modular proofs
- Connections to other areas

Cons

- Artificial formulas
- Lose grip on proof

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?
- More gadgets?

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 $z = g(x, y)$.