How Limited Interaction Hinders Real Communication (and What it Means for Proof and Circuit Complexity)

Marc Vinyals

KTH Royal Institute of Technology
Stockholm, Sweden

joint work with Susanna F. de Rezende and Jakob Nordström

Proof Complexity Workshop
May 18, 2016, St. Petersburg, Russia

Cutting Planes

Work with inequalities

$$x \vee \overline{y} \quad \rightarrow \quad x + (1 - y) \geq 1 \quad \rightarrow \quad x - y \geq 0$$

Cutting Planes

Work with inequalities

$$x \vee \overline{y} \quad \to \quad x + (1 - y) \geq 1 \quad \to \quad x - y \geq 0$$

Rules

Variable axioms

$$\frac{}{x \geq 0} \qquad \frac{}{-x \geq -1}$$

Addition

$$\frac{\sum a_i x_i \geq a \qquad \sum b_i x_i \geq b}{\sum (a_i + b_i) x_i \geq a + b}$$

Division

$$\frac{\sum a_i x_i \geq a}{\sum (a_i / k) x_i \geq \lceil a/k \rceil}$$

Cutting Planes

Work with inequalities

$$x \vee \overline{y} \quad \to \quad x + (1 - y) \geq 1 \quad \to \quad x - y \geq 0$$

Rules

Variable axioms

$$\frac{}{x \geq 0} \qquad \frac{}{-x \geq -1}$$

Addition

$$\frac{\sum a_i x_i \geq a \qquad \sum b_i x_i \geq b}{\sum (a_i + b_i) x_i \geq a + b}$$

Division

$$\frac{\sum a_i x_i \geq a}{\sum (a_i / k) x_i \geq \lceil a/k \rceil}$$

Goal: derive $0 \geq 1$

Complexity Measures

Size # bits in proof

- Size $2^{O(N)}$ always possible.

Length # lines in proof

- Worst case $2^{\Omega(N^{\epsilon})}$. [Pudlák '97]

Complexity Measures

Size # bits in proof

- Size $2^{O(N)}$ always possible.

Length # lines in proof

- Worst case $2^{\Omega(N^{\epsilon})}$. [Pudlák '97]

Total space max # bits in memory at the same time

- Space $O(N^2)$ always possible; worst case $\Omega(N)$.

Line space max # lines in memory at the same time

- Space 5 always possible. [Galesi, Pudlák, Thapen '15]

Trade-offs

Question

Assume F has a proof in length L and another proof in space s.
Is there a proof in length $\mathrm{O}(L)$ and space $\mathrm{O}(s)$?

Trade-offs

Question

Assume F has a proof in length L and another proof in space s.
Is there a proof in length $O(L)$ and space $O(s)$?

No

Trade-offs

Question

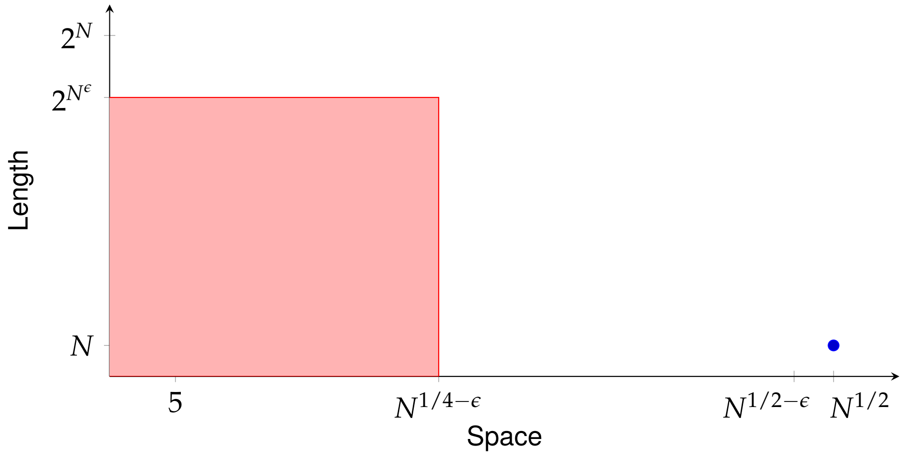
Assume F has a proof in length L and another proof in space s.
Is there a proof in length $\mathrm{O}(L)$ and space $\mathrm{O}(s)$?

No

Previously studied for resolution and polynomial calculus

[Ben Sasson, Nordström '11] [Beame, Beck, Impagliazzo '12] [Beck, Nordström, Tang '13]

Trade-offs

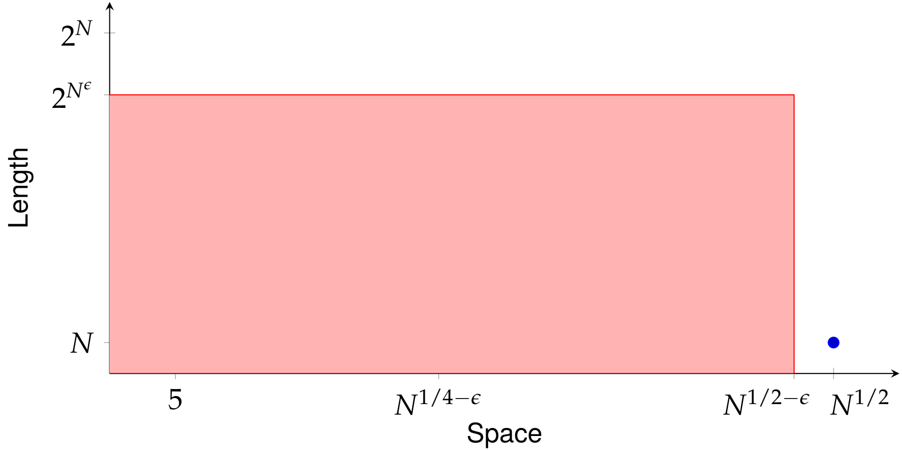


[Huynh, Nordström '12]

Can do length $O(N)$, space $N^{1/2}$.

But space $N^{1/4-\epsilon}$ requires size $\exp(N^{\epsilon-o(1)})$.

Trade-offs

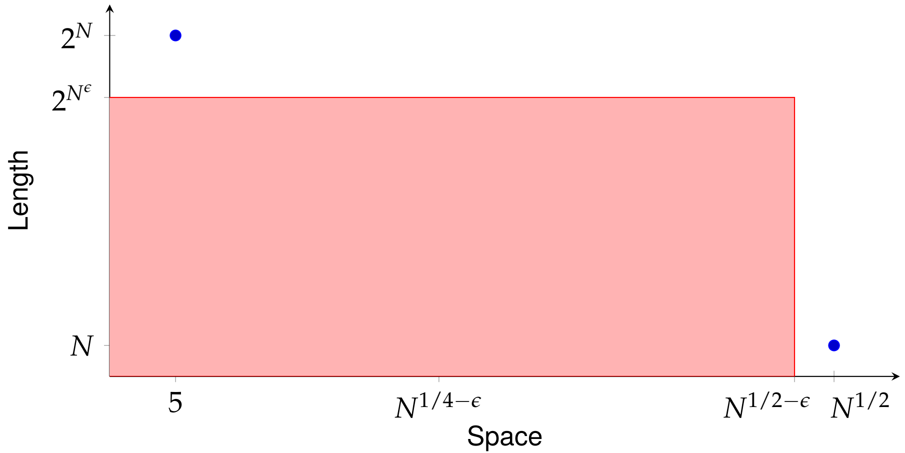


[Göös, Pitassi '14]

Can do length $N^{1+o(1)}$, space $N^{1/2+o(1)}$.

But space $N^{1/2-\epsilon}$ requires size $\exp(N^{\epsilon-o(1)})$.

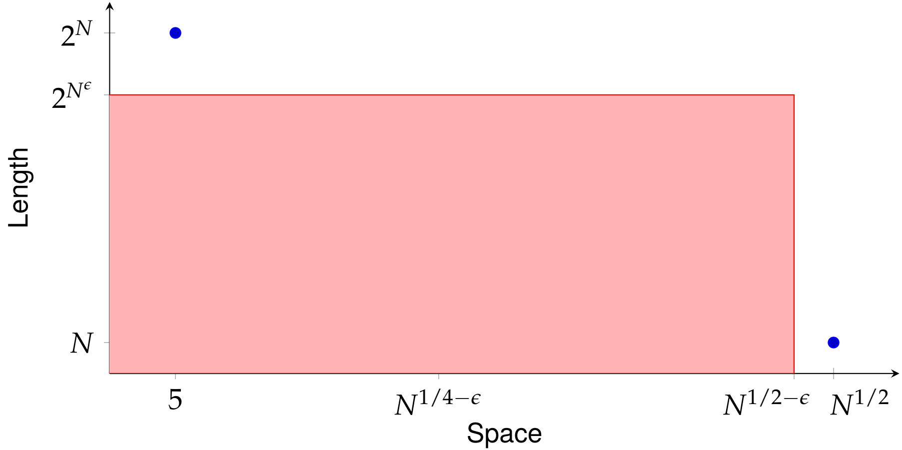
Trade-offs



[Galesi, Pudlák, Thapen '15]

Can do length 2^N, space 5.

Trade-offs



[Galesi, Pudlák, Thapen '15]

Can do length 2^N, space 5.

But exponential coefficients and quadratic total space.

Trade-offs

Question

Assume F has a proof in small total space with polynomial coefficients. Are there still trade-offs?

Trade-offs

Question

Assume F has a proof in small total space with polynomial coefficients. Are there still trade-offs?

Cannot answer with previous techniques (provably)

Trade-offs

Question

Assume F has a proof in small total space with polynomial coefficients. Are there still trade-offs?

Cannot answer with previous techniques (provably)

This talk:

Yes

Main Result

Theorem

There is a family of 6-CNF formulas with

- *short proofs: size $\mathrm{O}(N)$, total space $\mathrm{O}(N^{2/5})$;*

Main Result

Theorem

There is a family of 6-CNF formulas with

- *short proofs: size $\mathrm{O}(N)$, total space $\mathrm{O}(N^{2/5})$;*
- *small space proofs: total space $\mathrm{O}(N^{1/40})$, size $2^{\mathrm{O}(N^{1/40})}$;*

Main Result

Theorem

There is a family of 6-CNF formulas with

- *short proofs: size* $\mathrm{O}(N)$, *total space* $\mathrm{O}(N^{2/5})$;
- *small space proofs: total space* $\mathrm{O}(N^{1/40})$, *size* $2^{\mathrm{O}(N^{1/40})}$;
- *but line space* $N^{1/20-\epsilon}$ *requires length* $\exp(\Omega(N^{1/40}))$.

Main Result

Theorem

There is a family of 6-CNF formulas with

- *short proofs: size $O(N)$, total space $O(N^{2/5})$;*
- *small space proofs: total space $O(N^{1/40})$, size $2^{O(N^{1/40})}$;*
- *but line space $N^{1/20-\epsilon}$ requires length $\exp(\Omega(N^{1/40}))$.*

- Upper bounds with constant coefficients, counting all bits.
- Lower bound with unbounded coefficients, only counting lines.
- Lower bound for semantic cutting planes.

Main Result

Theorem

There is a family of 6-CNF formulas with

- *short proofs: size* $\mathrm{O}(N)$, *total space* $\mathrm{O}(N^{2/5})$*;*
- *small space proofs: total space* $\mathrm{O}(N^{1/40})$, *size* $2^{\mathrm{O}(N^{1/40})}$*;*
- *but line space* $N^{1/20-\epsilon}$ *requires length* $\exp(\Omega(N^{1/40}))$*.*

- Upper bounds with constant coefficients, counting all bits.
- Lower bound with unbounded coefficients, only counting lines.
- Lower bound for semantic cutting planes.

- Holds for resolution and polynomial calculus proof systems.

Spin-off

Exponential separation of the monotone-AC hierarchy

Theorem

There is a monotone Boolean function with

- *small monotone circuits: size* $\mathrm{O}(n)$, *depth* $\log^i(n)$, *fan-in* $n^{4/5}$
- *but monotone circuits of depth* $\mathrm{O}(\log^{i-1} n)$ *require size* $\exp(\Omega(n^\epsilon))$.

Superpolynomial separation known [Raz, McKenzie '97]

Devious Plan

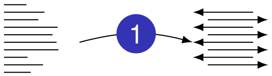
Assume refutation in length L and space s

Devious Plan

Assume refutation in length L and space s

$\downarrow$

1. Communication protocol for falsified clause search problem

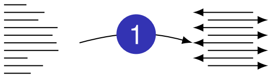


Devious Plan

Assume refutation in length L and space s

$\downarrow$

1. Communication protocol for Search(F)



Devious Plan

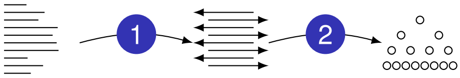
Assume refutation in length L and space s

$\downarrow$

1. Communication protocol for Search(F)

$\downarrow$

2. Parallel decision tree for Search(F)



Devious Plan

Assume refutation in length L and space s

$\downarrow$

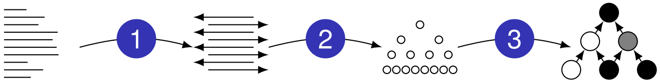
1. Communication protocol for Search(F)

$\downarrow$

2. Parallel decision tree for Search(F)

$\downarrow$

3. Strategy for Dymond–Tompa pebble game



Devious Plan

Assume refutation in length L and space s

$\downarrow$

1. Communication protocol for Search(F)

$\downarrow$

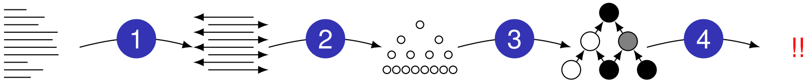
2. Parallel decision tree for Search(F)

$\downarrow$

3. Strategy for Dymond–Tompa pebble game

$\downarrow$

4. Construct graph with trade-offs



Devious Plan ❶: Proof $\rightarrow$ Protocol

Refutation in length L, space s $\rightarrow$
Protocol for Search(F) in $\log L$ rounds, communication $s \log L$

- Inspired by [Beame, Pitassi, Segerlind '05] [Beame, Huynh, Pitassi '10], explicit in [Huynh, Nordström '12].
- Key twists:
  - Real communication model
  - Measure number of rounds

Real Communication

Introduced by [Krajíček '98] to study cutting planes

- Compare real numbers at cost 1

Alice

$\geq$

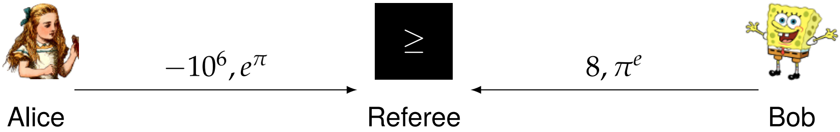
Referee

Bob

Real Communication

Introduced by [Krajíček '98] to study cutting planes

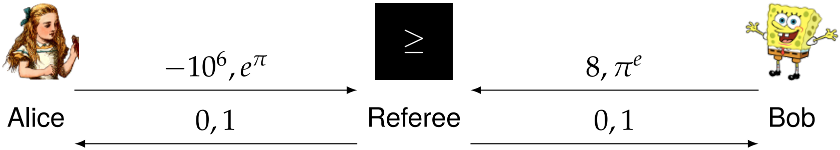
- Compare real numbers at cost 1



Real Communication

Introduced by [Krajíček ’98] to study cutting planes

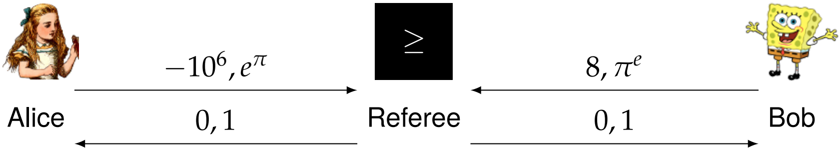
- Compare real numbers at cost 1



Real Communication

Introduced by [Krajíček ’98] to study cutting planes

- Compare real numbers at cost 1



- Simulates deterministic communication (Alice sends m, Bob sends $1/2$)
- Stronger than deterministic communication (EQ)

Devious Plan 1: Proof $\rightarrow$ Protocol

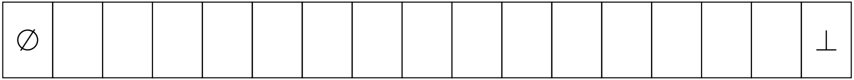
Falsified clause search on CNF $F(x, y)$

- Alice $\leftarrow$ assignment to x variables
- Bob $\leftarrow$ assignment to y variables
- Task: Find falsified clause

Devious Plan 1: Proof $\rightarrow$ Protocol

Falsified clause search on CNF $F(x, y)$

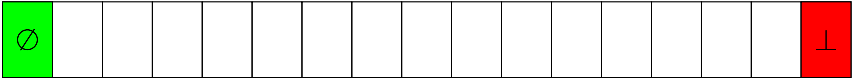
- Alice $\leftarrow$ assignment to x variables
- Bob $\leftarrow$ assignment to y variables
- Task: Find falsified clause



Devious Plan 1: Proof $\to$ Protocol

Falsified clause search on CNF $F(x, y)$

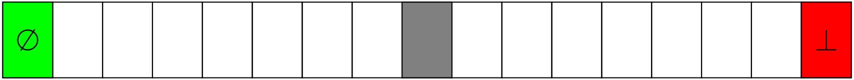
- Alice $\leftarrow$ assignment to x variables
- Bob $\leftarrow$ assignment to y variables
- Task: Find falsified clause



Devious Plan 1: Proof → Protocol

Falsified clause search on CNF $F(x, y)$

- Alice ← assignment to x variables
- Bob ← assignment to y variables
- Task: Find falsified clause

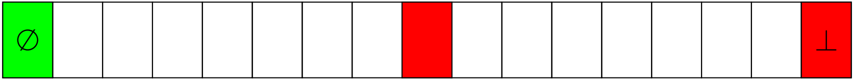


- Alice evaluates $\sum a_i x_i - a$ in s inequalities
- Bob evaluates $-\sum a_i y_i$ in s inequalities
- $\alpha(\mathbb{C}) = 1$ iff Referee answers $111\ldots1$

Devious Plan 1: Proof $\to$ Protocol

Falsified clause search on CNF $F(x,y)$

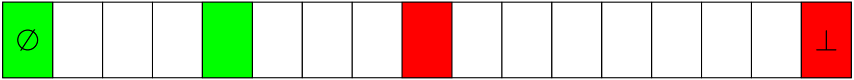
- Alice $\leftarrow$ assignment to x variables
- Bob $\leftarrow$ assignment to y variables
- Task: Find falsified clause



Devious Plan 1: Proof $\to$ Protocol

Falsified clause search on CNF $F(x, y)$

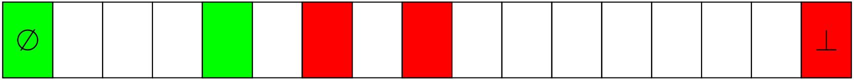
- Alice $\leftarrow$ assignment to x variables
- Bob $\leftarrow$ assignment to y variables
- Task: Find falsified clause



Devious Plan ①: Proof $\to$ Protocol

Falsified clause search on CNF $F(x, y)$

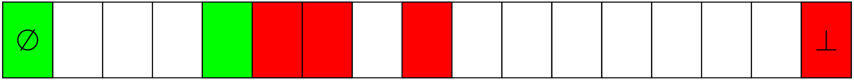
- Alice $\leftarrow$ assignment to x variables
- Bob $\leftarrow$ assignment to y variables
- Task: Find falsified clause



Devious Plan 1: Proof $\to$ Protocol

Falsified clause search on CNF $F(x, y)$

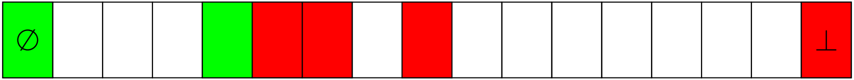
- Alice $\leftarrow$ assignment to x variables
- Bob $\leftarrow$ assignment to y variables
- Task: Find falsified clause



Devious Plan 1: Proof $\rightarrow$ Protocol

Falsified clause search on CNF $F(x, y)$

- Alice $\leftarrow$ assignment to x variables
- Bob $\leftarrow$ assignment to y variables
- Task: Find falsified clause

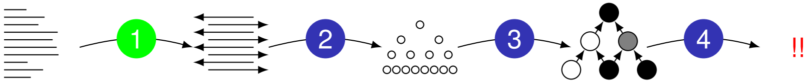


- $\alpha(\mathbb{C}) = 1 \quad \alpha(\mathbb{C} \cup \{A\}) = 0 \quad \Rightarrow \quad \alpha(A) = 0$
- $\log L$ rounds, communication $s \log L$

Devious Plan

Assume refutation in length L and space s

1. Communication protocol for Search(F) in $\log L$ rounds and communication $s \log L$
2. Parallel decision tree for Search(F)
3. Strategy for Dymond–Tompa pebble game
4. Construct graph with trade-offs



Devious Plan 2: Protocol $\to$ Decision Tree

Protocol for Lift(S) in r rounds, communication c $\to$
Parallel decision tree for S of depth r, c queries

Lifted Problem

- Function $f(z_1, \dots, z_n)$
- Alice $\leftarrow n$ indices $x_1, \dots, x_n$
- Bob $\leftarrow n$ arrays $y_1, \dots, y_n$

$z_1 = y_1[5] = 1$

x_1
5

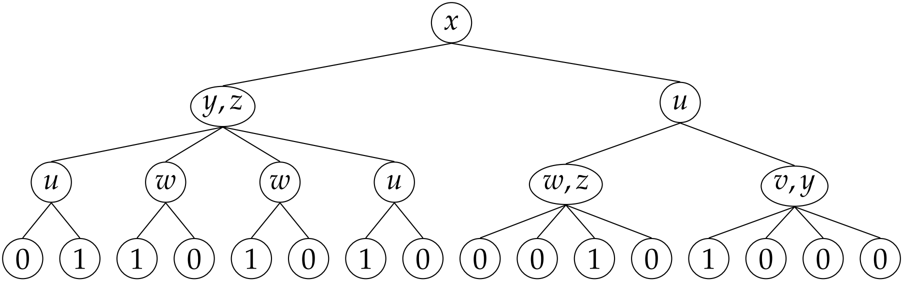
0	0	1	0	0	1	1	1

y_1

- Lifted function $\text{Lift}(f)(x, y) = f(y_1[x_1], \dots, y_n[x_n])$

Parallel Decision Trees

Decision tree with many queries per node [Valiant ’75]



Depth Longest branch

Queries # queries in a branch

Devious Plan ❷: Protocol $\rightarrow$ Decision Tree

Protocol for Lift(S) in r rounds, communication c $\rightarrow$
Parallel decision tree for S of depth r, c queries

Devious Plan 2: Protocol $\leftarrow$ Decision Tree

Protocol for Lift(S) in r rounds, communication c $\leftarrow$
Parallel decision tree for S of depth r, c queries

Communication

Decision tree

Query $\{z_3, z_{28}\}$

Devious Plan 2: Protocol $\leftarrow$ Decision Tree

Protocol for Lift(S) in r rounds, communication c $\leftarrow$
Parallel decision tree for S of depth r, c queries

Communication

Alice sends x_3, x_{28}
Bob sends $y_3[x_3], y_{28}[x_{28}]$

Decision tree

Query $\{z_3, z_{28}\}$

Devious Plan ❷: Protocol $\to$ Decision Tree

Protocol for Lift(S) in r rounds, communication c $\to$
Parallel decision tree for S of depth r, c queries

Communication

Alice sends $x_1 + x_2 + \cdots + x_n$

Decision tree

Devious Plan ❷: Protocol $\rightarrow$ Decision Tree

Protocol for Lift(S) in r rounds, communication c $\rightarrow$
Parallel decision tree for S of depth r, c queries

Communication
Alice sends $x_1 + x_2 + \cdots + x_n$

Decision tree
???

Devious Plan 2: Protocol $\rightarrow$ Decision Tree

Protocol for Lift(S) in r rounds, communication c $\rightarrow$
Parallel decision tree for S of depth r, c queries

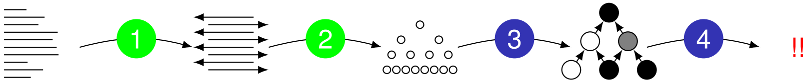
- Main technical result (Simulation Theorem)
  - Technique from [Raz, McKenzie '97]
  - Adapted to real communication in [Bonet, Esteban, Galesi, Johannsen '98]
  - Connection to decision trees made explicit in [Göös, Pitassi, Watson '15]
- Our contribution
  - Introduce rounds
  - Adapt to real communication preserving rounds

Devious Plan

Assume refutation of lifted formula in length L and space s

1. Communication protocol for Lift$($Search$(F))$ in $\log L$ rounds and communication $s \log L$
2. Parallel decision tree for Search(F) of depth $\log L$ and $s \log L$ queries
3. Strategy for Dymond–Tompa pebble game

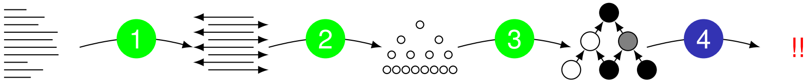
4. Construct graph with trade-offs



Devious Plan

Assume refutation of lifted pebbling formula in length L and space s

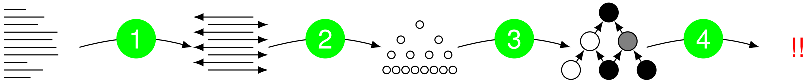
1. Communication protocol for Lift(Search(F)) in $\log L$ rounds and communication $s \log L$
2. Parallel decision tree for Search(F) of depth $\log L$ and $s \log L$ queries
3. Strategy for Dymond–Tompa pebble game for $\log L$ rounds and $s \log L$ pebbles [Chan '13]
4. Construct graph with trade-offs



Devious Plan

Assume refutation of lifted pebbling formula in length L and space s

1. Communication protocol for Lift$($Search$(F))$ in $\log L$ rounds and communication $s \log L$
2. Parallel decision tree for Search(F) of depth $\log L$ and $s \log L$ queries
3. Strategy for Dymond–Tompa pebble game for $\log L$ rounds and $s \log L$ pebbles
4. Construct graph where such strategy does not exist



Take Home

Remarks

- Strong size-space trade-offs for cutting planes
- Hold for resolution, polynomial calculus, cutting planes
- Key to measure rounds

Take Home

Remarks

- Strong size-space trade-offs for cutting planes
- Hold for resolution, polynomial calculus, cutting planes
- Key to measure rounds

Open problems

- Smaller lift size
- Stronger models of communication

Take Home

Remarks

- Strong size-space trade-offs for cutting planes
- Hold for resolution, polynomial calculus, cutting planes
- Key to measure rounds

Open problems

- Smaller lift size
- Stronger models of communication

Thanks!