Hardness Escalation in Proof Complexity via Composition

Marc Vinyals

KTH Royal Institute of Technology
Stockholm, Sweden

China Theory Week
July 18 2017, Shanghai, China

Proof Complexity

Setup

Prove CNF formula unsatisfiable.

Present proof on board.

- Write down axiom clauses
- Infer new clauses
$$\frac{C \vee x \qquad D \vee \overline{x}}{C \vee D}$$
- Erase clauses to save space

Goal: derive empty clause $\perp$

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

Proof Complexity

Setup

Prove CNF formula unsatisfiable.

Present proof on board.

- Write down axiom clauses
- Infer new clauses
$$\frac{C \lor x \qquad D \lor \overline{x}}{C \lor D}$$
- Erase clauses to save space

Goal: derive empty clause $\perp$

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

$$\boxed{x \lor y}$$

Proof Complexity

Setup

Prove CNF formula unsatisfiable.

Present proof on board.

- Write down axiom clauses
- Infer new clauses
  $$\frac{C \vee x \qquad D \vee \overline{x}}{C \vee D}$$
- Erase clauses to save space

Goal: derive empty clause $\perp$

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

$x \vee y$

$\overline{x} \vee y$

Proof Complexity

Setup

Prove CNF formula unsatisfiable.

Present proof on board.

- Write down axiom clauses
- Infer new clauses
$$\frac{C \lor x \qquad D \lor \overline{x}}{C \lor D}$$
- Erase clauses to save space

Goal: derive empty clause $\perp$

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

$$x \lor y$$
$$\overline{x} \lor y$$
$$y$$

Proof Complexity

Setup

Prove CNF formula unsatisfiable.

Present proof on board.

- Write down axiom clauses
- Infer new clauses
$$\frac{C \lor x \qquad D \lor \overline{x}}{C \lor D}$$
- Erase clauses to save space

Goal: derive empty clause $\perp$

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

$$\cancel{x \lor y}$$
$$\overline{x} \lor y$$
$$y$$

Proof Complexity

Setup

Prove CNF formula unsatisfiable.

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

Present proof on board.

- Write down axiom clauses
- Infer new clauses

$$\frac{C \vee x \qquad D \vee \overline{x}}{C \vee D}$$

- Erase clauses to save space

$$\cancel{\overline{x} \vee y}$$
$$y$$

Goal: derive empty clause $\perp$

Proof Complexity

Setup

Prove CNF formula unsatisfiable.

Present proof on board.

- Write down axiom clauses
- Infer new clauses
$$\frac{C \vee x \qquad D \vee \overline{x}}{C \vee D}$$
- Erase clauses to save space

Goal: derive empty clause $\perp$

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

$$\boxed{\begin{array}{c} y \\ \overline{y} \end{array}}$$

Proof Complexity

Setup

Prove CNF formula unsatisfiable.

Present proof on board.

- Write down axiom clauses
- Infer new clauses

$$\frac{C \lor x \qquad D \lor \overline{x}}{C \lor D}$$

- Erase clauses to save space

Goal: derive empty clause $\perp$

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

$$\boxed{\begin{array}{c} y \\ \overline{y} \\ \perp \end{array}}$$

Proof Complexity

Setup

Prove CNF formula unsatisfiable.

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

Present proof on board.

- Write down axiom clauses
- Infer new clauses
$$\frac{C \vee x \qquad D \vee \overline{x}}{C \vee D}$$
- Erase clauses to save space

$$\boxed{\begin{array}{c} y \\ \overline{y} \\ \perp \end{array}}$$

Goal: derive empty clause $\perp$

Questions

- How much time will this take? (Length)
- How large is the blackboard? (Space)

Complexity Measures

Length

$x \lor y$	$x \lor y$	$x \lor y$	$\cancel{x \lor y}$	y	y
	$\overline{x} \lor y$	$\overline{x} \lor y$	$\overline{x} \lor y$	$\overline{y}$	$\overline{y}$
		y	y		$\perp$
1	2	3		4	5

Length of a proof: # Lines
Length of refuting a formula: Min over all proofs
Worst case $\mathrm{O}(2^N)$, matching $\exp(\Omega(N))$.

Complexity Measures

Line Space

[Esteban, Torán '99] [Alekhnovich, Ben Sasson, Razborov, Wigderson '00]

$x \lor y$	$x \lor y$	$x \lor y$	$\cancel{x \lor y}$	y	y
	$\overline{x} \lor y$	$\overline{x} \lor y$	$\overline{x} \lor y$	$\overline{y}$	$\overline{y}$
		y	y		$\bot$
1	2	3	2	2	3

Line Space of a proof: Max lines in configuration (whiteboard)
Line Space of refuting a formula: Min over all proofs
Worst case $N + O(1)$, matching $\Omega(N)$.

Proof Systems

Resolution

- Logic reasoning
- Very well understood

Proof Systems

Resolution

- Logic reasoning
- Very well understood

Polynomial calculus

- Algebraic reasoning
- Reasonably understood

Proof Systems

Resolution

- Logic reasoning
- Very well understood

Polynomial calculus

- Algebraic reasoning
- Reasonably understood

Cutting planes

- Pseudoboolean reasoning
- Not well understood

Proof Systems

Resolution

- Logic reasoning
- Very well understood

Polynomial calculus

- Algebraic reasoning
- Reasonably understood

Cutting planes

- Pseudoboolean reasoning
- Not well understood

Sums of squares

- Semidefinite programming
- Not well understood

Composition

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

Composition

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

Would not it be nice if...?

1. Have original problem.
2. Prove hard in weak model/measure.
3. Compose.
4. Composed problem hard in strong model/measure.

Composition in Proof Complexity

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

Composition 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

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

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

Composition 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

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

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

Resolution Space

- Width: Size of largest clause in proof.
- Theorem: Width $\leq$ Space. [Atserias, Dalmau '02]

Problem:

Formulas with small width but large space.

Resolution Space

- Width: Size of largest clause in proof.
- Theorem: Width $\leq$ Space. [Atserias, Dalmau '02]

Problem:
Formulas with small width but large space.

Theorem [Ben Sasson, Nordström '11]

$\mathrm{LinSp}(F \circ \oplus) = \Omega(\mathrm{VarSp}(F))$

Strong measure: Line Space.
Weak measure: Variable Space. Max variables in configuration.
Composition: XOR

Polynomial Calculus Space

Problem:

Formulas with small degree but large space.

Polynomial Calculus Space

Problem:

Formulas with small degree but large space.

Theorem [Filmus, Lauria, Mikša, Nordström, V '13]

$$\mathrm{MonSp}(F \circ \oplus) = \Omega(\mathrm{Width}(F))$$

Strong measure: Monomial Space. Max monomials in configuration.
Weak measure: Width in resolution proof.
Composition: XOR

Sum of Squares Length

Problem:

Formulas that require large length.

Sum of Squares Length

Problem:

Formulas that require large length.

Theorem [Göös, Pitassi '14]

$\mathrm{Rank}(F \circ \textsc{ver}) = \Omega(\mathrm{Depth}(F))$

Strong measure: Tree-like length.

Weak measure: Queries in decision tree.

Composition: Versatile gadget.

Falsified Clause Search Problem

- Given: CNF formula F
- Input: Assignment to variables $\alpha : x \mapsto \{0,1\}^n$
- Task: Find clause $C \in F$ falsified by assignment α

Sum of Squares Length

Problem:

Formulas that require large length.

Theorem [Göös, Pitassi '14]

$$\mathrm{Rank}(F \circ \textsc{ver}) = \Omega(\mathrm{Depth}(F))$$

Strong measure: Tree-like length.

Weak measure: Queries in decision tree.

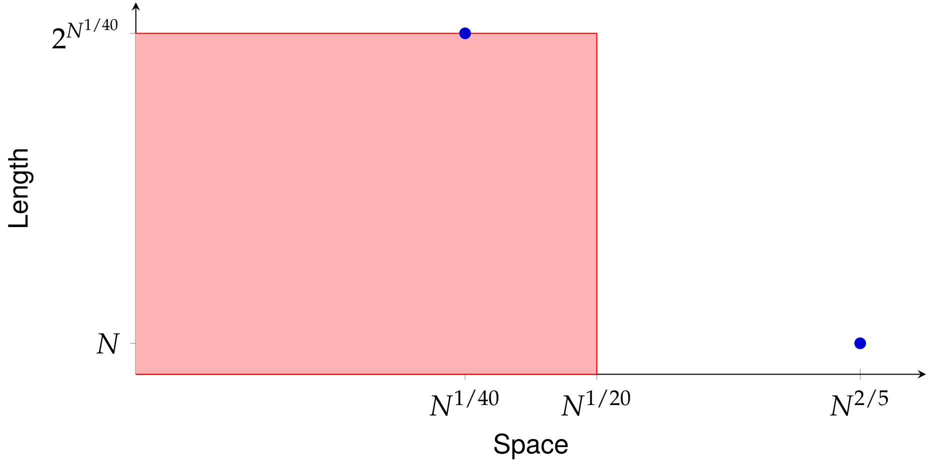
Composition: Versatile gadget.

Cutting Planes Trade-Offs

Problem:

Formulas with small length and space, but not at the same time.

Cutting Planes Trade-Offs



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

Cutting Planes Trade-Offs

Problem:

Formulas with small length and space, but not at the same time.

Cutting Planes Trade-Offs

Problem:

Formulas with small length and space, but not at the same time.

Theorem [de Rezende, Nordström, V '16]

F needs q queries with r rounds. Then
$F \circ \textsc{ind}$ needs space q/r with length 2^r.

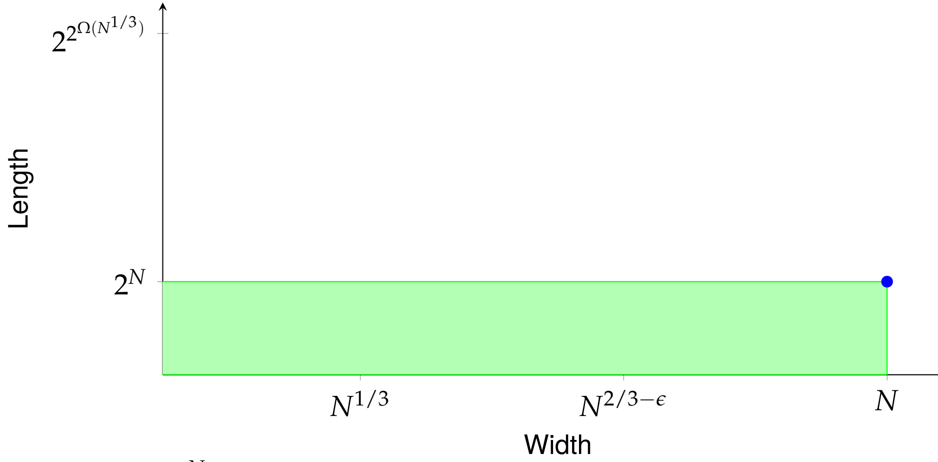
Strong measure: (Length, Line Space).
Weak measure: (Queries, Rounds).
Composition: Indexing.

Supercritical Trade-Offs in Tree-like Resolution

Problem:

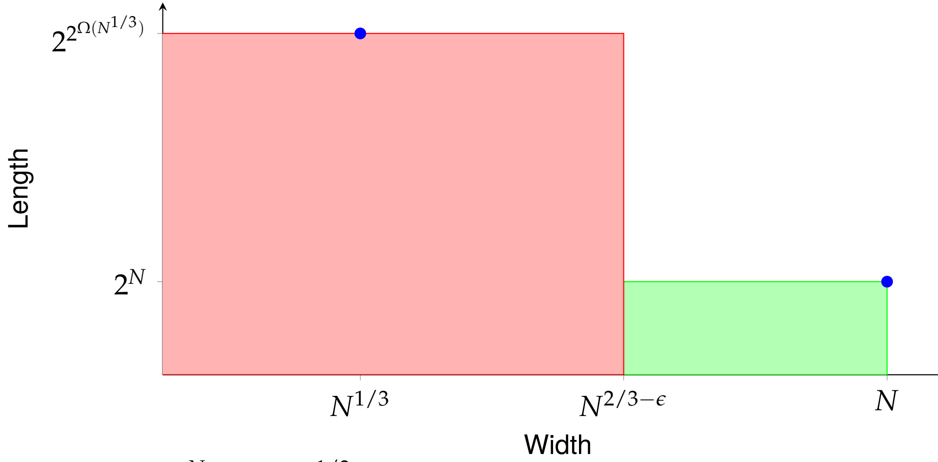
Trade-offs outside worst-case region

Supercritical Trade-Offs



Can do length 2^N, width N.

Supercritical Trade-Offs



Can do length 2^N, width $N^{1/3}$.

But width $N^{2/3-\epsilon}$ requires length $2^{2^{\Omega(N^{1/3})}}$.

Supercritical Trade-Offs in Tree-like Resolution

Problem:

Trade-offs outside worst-case region

Supercritical Trade-Offs in Tree-like Resolution

Problem:
Trade-offs outside worst-case region

Theorem [Razborov '16]

π proof of $F \circ_R \oplus$. Then
$\mathrm{Len}(\pi) = \exp(\Omega(\mathrm{Depth}(F)/\mathrm{Width}(\pi)))$

Strong measure: (Length, Width).
Weak measure: Depth.
Composition: XOR with reusing.

Cutting Planes Trade-Offs

Theorem [de Rezende, Nordström, V '16]

F needs q queries with r rounds. Then
$F \circ \textsc{ind}$ needs space q/r with length 2^r.

Cutting Planes Trade-Offs

Theorem [de Rezende, Nordström, V '16]

F needs q queries with r rounds. Then
$F \circ \textsc{ind}$ needs space q/r with length 2^r.

Let us build F.

- Can be solved in few queries.
- Can be solved in few rounds.
- But not both.

Pebbling Formulas

- Sources are true

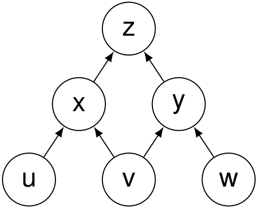
$$u$$
$$v$$
$$w$$

- Truth propagates

$$(u \land v) \to x$$
$$(v \land w) \to y$$
$$(x \land y) \to z$$

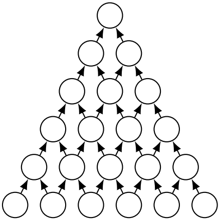
- Sink is false

$$\overline{z}$$



Dymond–Tompa Game

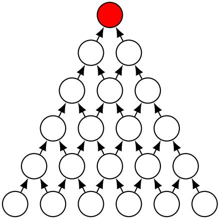
2-player pebble game on a DAG [Dymond, Tompa '85]



Dymond–Tompa Game

2-player pebble game on a DAG [Dymond, Tompa '85]

- Start with a challenged pebble on the sink

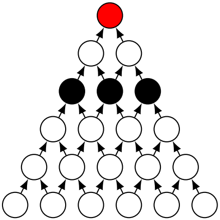


Rounds	0
Pebbles	1

Dymond–Tompa Game

2-player pebble game on a DAG [Dymond, Tompa '85]

- Start with a challenged pebble on the sink
- Each round:
  - Pebbler adds some pebbles



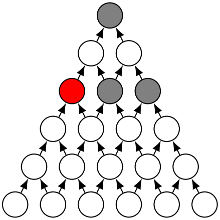
Rounds 1

Pebbles 4

Dymond–Tompa Game

2-player pebble game on a DAG [Dymond, Tompa '85]

- Start with a challenged pebble on the sink
- Each round:
  - Pebbler adds some pebbles
  - Challenger may challenge one new pebble



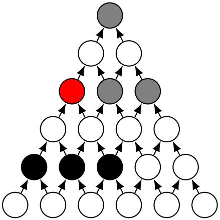
Rounds 1

Pebbles 4

Dymond–Tompa Game

2-player pebble game on a DAG [Dymond, Tompa '85]

- Start with a challenged pebble on the sink
- Each round:
  - Pebbler adds some pebbles
  - Challenger may challenge one new pebble



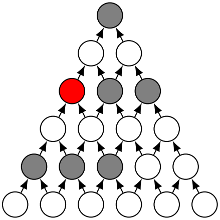
Rounds 2

Pebbles 7

Dymond–Tompa Game

2-player pebble game on a DAG [Dymond, Tompa '85]

- Start with a challenged pebble on the sink
- Each round:
  - Pebbler adds some pebbles
  - Challenger may challenge one new pebble



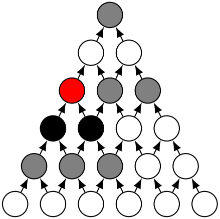
Rounds 2

Pebbles 7

Dymond–Tompa Game

2-player pebble game on a DAG [Dymond, Tompa '85]

- Start with a challenged pebble on the sink
- Each round:
  - Pebbler adds some pebbles
  - Challenger may challenge one new pebble



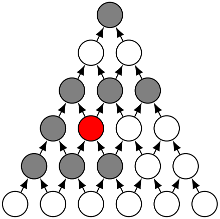
Rounds 3

Pebbles 9

Dymond–Tompa Game

2-player pebble game on a DAG [Dymond, Tompa '85]

- Start with a challenged pebble on the sink
- Each round:
  - Pebbler adds some pebbles
  - Challenger may challenge one new pebble
- Ends when challenged pebble is surrounded



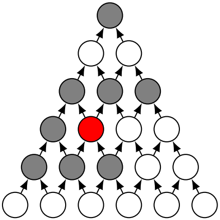
Rounds 3

Pebbles 9

Dymond–Tompa Game

2-player pebble game on a DAG [Dymond, Tompa '85]

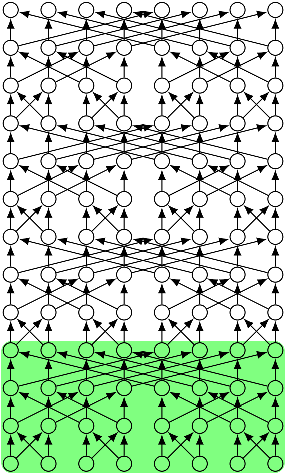
- Start with a challenged pebble on the sink
- Each round:
  - Pebbler adds some pebbles
  - Challenger may challenge one new pebble
- Ends when challenged pebble is surrounded
- Equivalent to decision tree on pebbling formula



Rounds	3
Pebbles	9

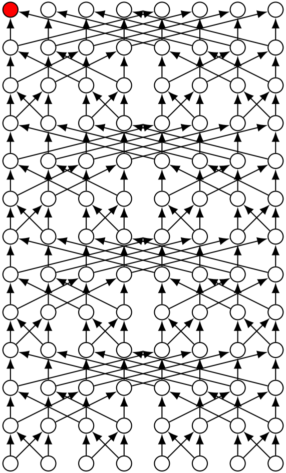
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs



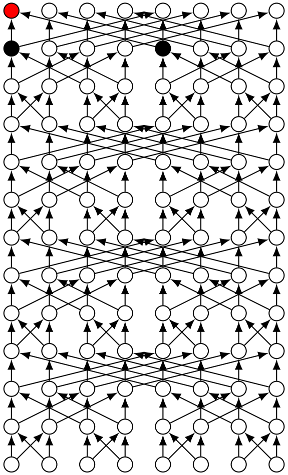
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds



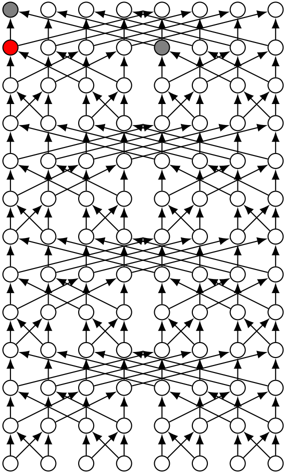
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds



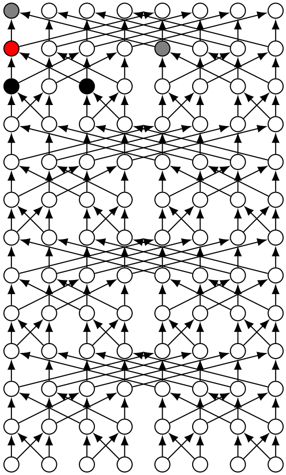
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds



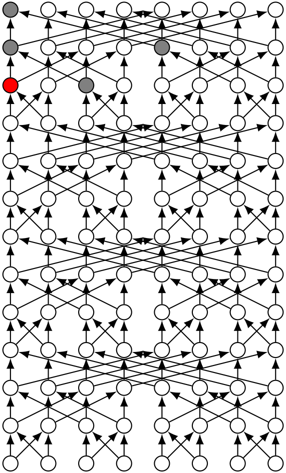
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds



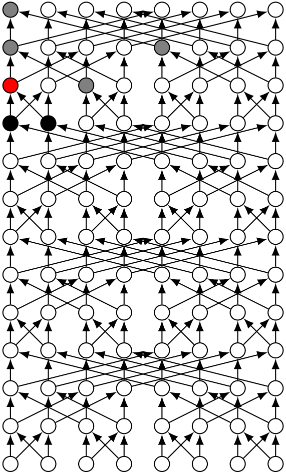
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds



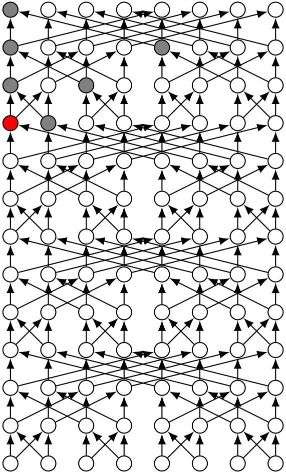
Trade-off for Dymond–Tompa

- Stack of $r + 1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds



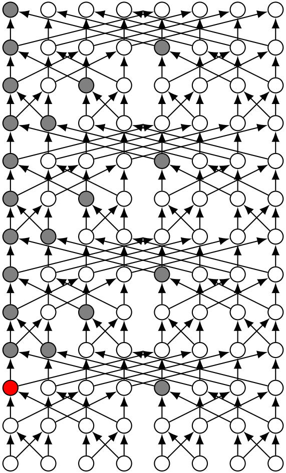
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r\log n$ pebbles in $r\log n$ rounds



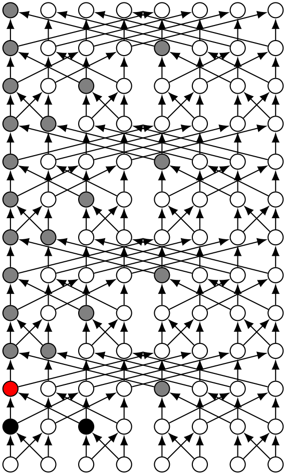
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds



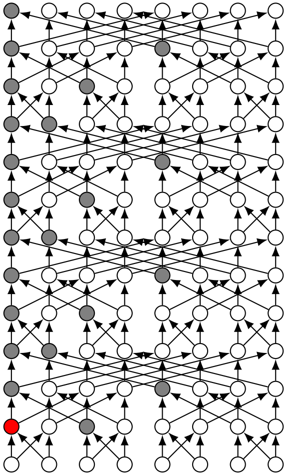
Trade-off for Dymond–Tompa

- Stack of $r + 1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds



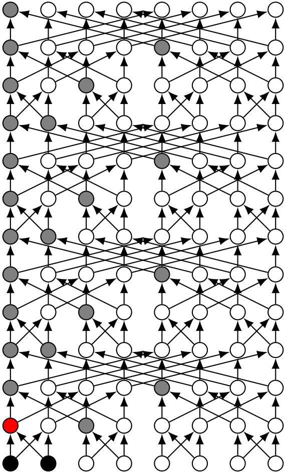
Trade-off for Dymond–Tompa

- Stack of $r + 1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds



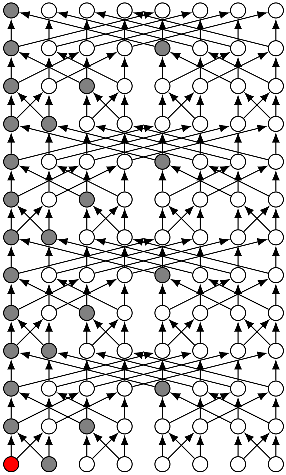
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds



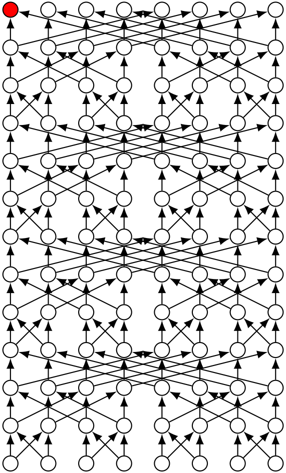
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r\log n$ pebbles in $r\log n$ rounds



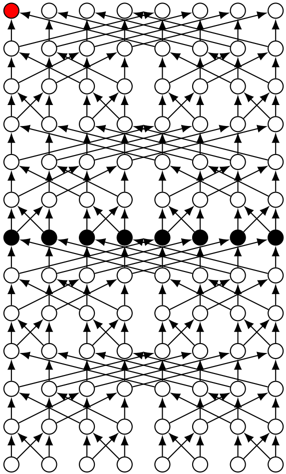
Trade-off for Dymond–Tompa

- Stack of $r + 1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds



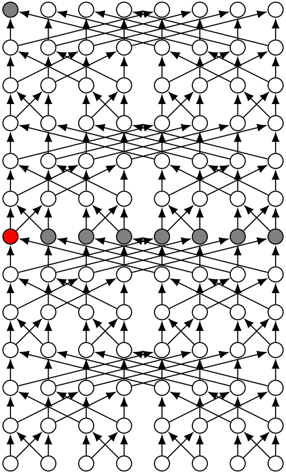
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds



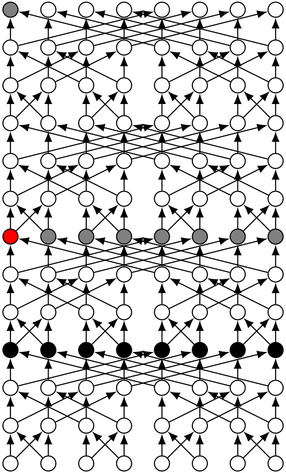
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r\log n$ pebbles in $r\log n$ rounds
- Or $n\log(r\log n)$ pebbles in $\log(r\log n)$ rounds



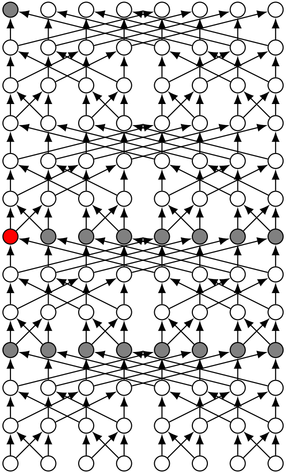
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r\log n$ pebbles in $r\log n$ rounds
- Or $n\log(r\log n)$ pebbles in $\log(r\log n)$ rounds



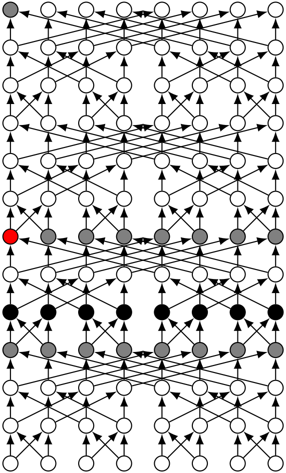
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds



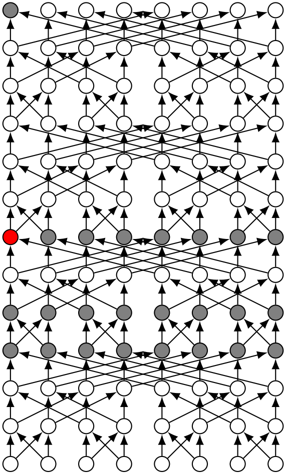
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds



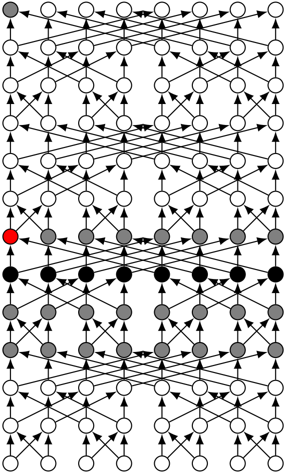
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds



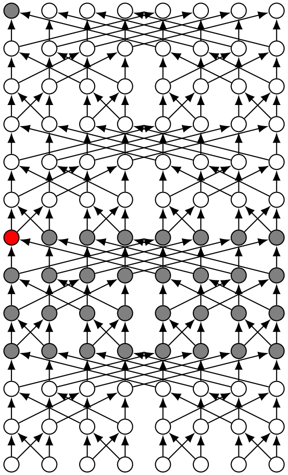
Trade-off for Dymond–Tompa

- Stack of $r + 1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds



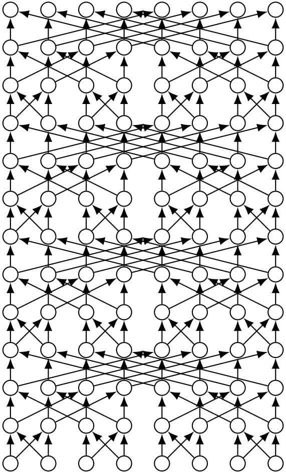
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds



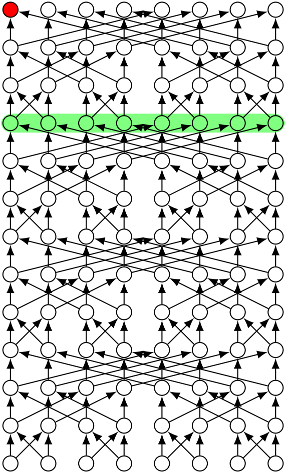
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds
- But r rounds require $n/4$ pebbles



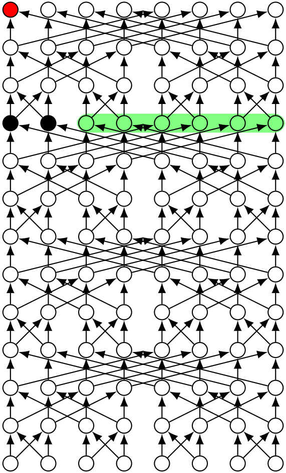
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds
- But r rounds require $n/4$ pebbles
  - Challenger does nothing...
    - ...if reachable from $n/2$ vertices $\log n$ rows below.



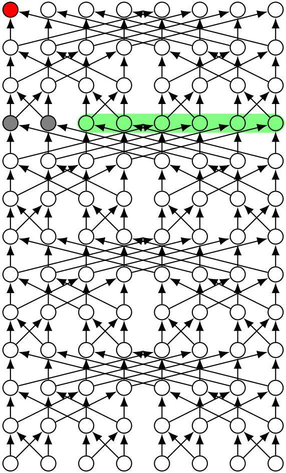
Trade-off for Dymond–Tompa

- Stack of $r + 1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds
- But r rounds require $n/4$ pebbles
  - Challenger does nothing...
    - ...if reachable from $n/2$ vertices $\log n$ rows below.



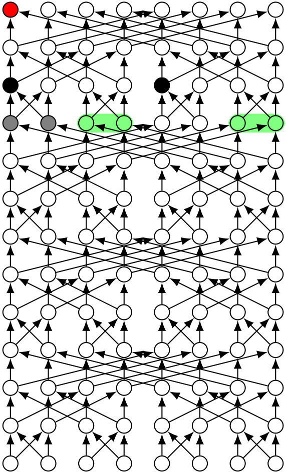
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r\log n$ pebbles in $r\log n$ rounds
- Or $n\log(r\log n)$ pebbles in $\log(r\log n)$ rounds
- But r rounds require $n/4$ pebbles
  - Challenger does nothing...
    - ...if reachable from $n/2$ vertices $\log n$ rows below.



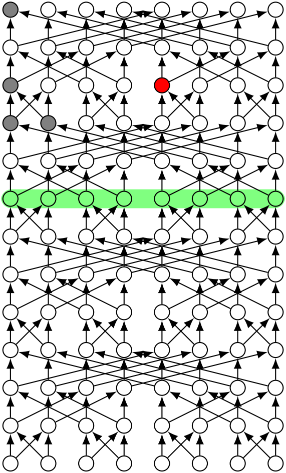
Trade-off for Dymond–Tompa

- Stack of $r+1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds
- But r rounds require $n/4$ pebbles
  - Challenger does nothing...
    - ...if reachable from $n/2$ vertices $\log n$ rows below.
  - Otherwise jump to vertex that
    - can reach current vertex, and
    - reachable from $n/2$ vertices $\log n$ rows below.



Trade-off for Dymond–Tompa

- Stack of $r + 1$ butterfly graphs
- Can do $2r \log n$ pebbles in $r \log n$ rounds
- Or $n \log(r \log n)$ pebbles in $\log(r \log n)$ rounds
- But r rounds require $n/4$ pebbles
  - Challenger does nothing...
    - ...if reachable from $n/2$ vertices $\log n$ rows below.
  - Otherwise jump to vertex that
    - can reach current vertex, and
    - reachable from $n/2$ vertices $\log n$ rows below.



Take Home

Remarks

- Composition is a very powerful technique
  - Proving lower bounds is hard.
  - Let us prove easier lower bounds.

Take Home

Remarks

- Composition is a very powerful technique
  - Proving lower bounds is hard.
  - Let us prove easier lower bounds.

Open problems

- More applications
- Smaller gadgets
  - Even identity?

Take Home

Remarks

- Composition is a very powerful technique
  - Proving lower bounds is hard.
  - Let us prove easier lower bounds.

Open problems

- More applications
- Smaller gadgets
  - Even identity?

Thanks!