Propositional proof compression

Andreas Fellner

EMCL Workshop 2014, Vienna
18^{th}, 19^{th} February, 2014

A proof

$$
\begin{tikzcd}
 & \bar{a}, b & & a, b \\
\bar{a}, \bar{b} & & b \arrow[ul] \arrow[ur] & \\
 & \bar{a} \arrow[ul] \arrow[ur] & & a \\
 & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

Axioms

$\{\bar{a}, \bar{b}\}, \{\bar{a}, b\}, \{a, b\}, \{a\}$

A proof

$$
\begin{tikzcd}
 & \bar{a}, b & & a \\
\bar{a}, \bar{b} & & b \arrow[ul] \arrow[ur] & \\
 & \bar{a} \arrow[ul] \arrow[ur] & & \\
 & & \bot \arrow[ul] \arrow[uuur] &
\end{tikzcd}
$$

Axioms

$\{\bar{a}, \bar{b}\}, \{\bar{a}, b\}, \{a\}$

Another proof

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{a}, b & & \bar{b}, c \\
& \bar{a}, \bar{c} \arrow[ul] \arrow[ur] & & \bar{a}, c \arrow[ul] \arrow[ur] & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Axioms

$\{a\}, \{\bar{a}, b\}, \{\bar{b}, c\}, \{\bar{a}, \bar{b}, \bar{c}\}$

Another proof

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{b}, c & & \\
& \bar{a}, \bar{b} \arrow[ul] \arrow[ur] & & \bar{a}, b & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \perp \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Axioms

$\{a\}, \{\bar{a}, b\}, \{\bar{b}, c\}, \{\bar{a}, \bar{b}, \bar{c}\}$

Puropose

- Smaller proof libraries
- Faster proof checking
- Smaller unsat cores; better interpolants
- Easier combination of deductive system

Table of Contents

Processing proofs

Topological order

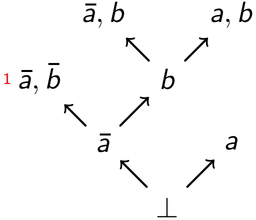
- Order proof nodes
- Premise before node

$$\begin{tikzcd}
 & \bar{a}, b & & a, b \\
\bar{a}, \bar{b} & & b \arrow[ul] \arrow[ur] & \\
 & \bar{a} \arrow[ul] \arrow[ur] & & a \\
 & & \perp \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Processing proofs

Topological order

- Order proof nodes
- Premise before node



$\bar{a}, \bar{b}$

Processing proofs

Topological order

- Order proof nodes
- Premise before node

$$
\begin{tikzcd}
 & {}^{2}\,\bar{a}, b & & a, b \\
{}^{1}\,\bar{a}, \bar{b} & & b \arrow[ul] \arrow[ur] & \\
 & \bar{a} \arrow[ul] \arrow[ur] & & a \\
 & & \perp \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

$\bar{a}, \bar{b} \quad \bar{a}, b$

Processing proofs

Topological order

- Order proof nodes
- Premise before node

$$
\begin{tikzcd}
 & {\scriptstyle 2}\ \bar{a}, b & & {\scriptstyle 3}\ a, b \\
{\scriptstyle 1}\ \bar{a}, \bar{b} & & b \arrow[ul] \arrow[ur] & \\
 & \bar{a} \arrow[ul] \arrow[ur] & & a \\
 & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

$\bar{a}, \bar{b} \quad \bar{a}, b \quad a, b$

Processing proofs

Topological order

- Order proof nodes
- Premise before node

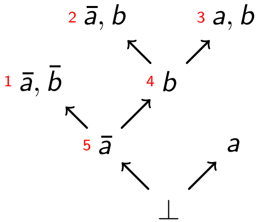
$$
\begin{tikzcd}
 & {\color{red}2}\ \bar{a}, b & & {\color{red}3}\ a, b \\
{\color{red}1}\ \bar{a}, \bar{b} & & {\color{red}4}\ b \arrow[ul] \arrow[ur] & \\
 & \bar{a} \arrow[ul] \arrow[ur] & & a \\
 & & \perp \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

$\bar{a}, \bar{b}$ $\quad \bar{a}, b$ $\quad a, b$ $\quad b$

Processing proofs

Topological order

- Order proof nodes
- Premise before node

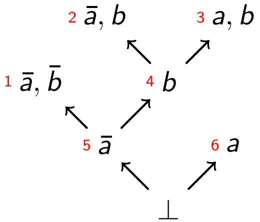


$\bar{a}, \bar{b}$ $\quad \bar{a}, b$ $\quad a, b$ $\quad b$ $\quad \bar{a}$

Processing proofs

Topological order

- Order proof nodes
- Premise before node

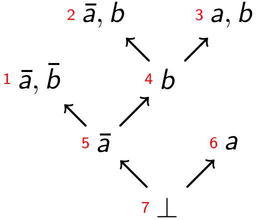


$\bar{a}, \bar{b} \quad \bar{a}, b \quad a, b \quad b \quad \bar{a} \quad a$

Processing proofs

Topological order

- Order proof nodes
- Premise before node

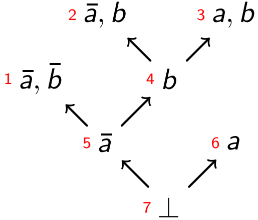


$\bar{a}, \bar{b} \quad \bar{a}, b \quad a, b \quad b \quad \bar{a} \quad a \quad \perp$

Processing proofs

Topological order

- Order proof nodes
- Premise before node



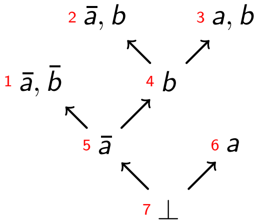
$\bar{a}, \bar{b}$ $\quad \bar{a}, b$ $\quad a, b$ $\quad b$ $\quad \bar{a}$ $\quad a$ $\quad \perp$

Top-Down $\longrightarrow$

Processing proofs

Topological order

- Order proof nodes
- Premise before node



$\bar{a}, \bar{b}$ $\quad \bar{a}, b$ $\quad a, b$ $\quad b$ $\quad \bar{a}$ $\quad a$ $\quad \bot$

Top-Down $\longrightarrow$

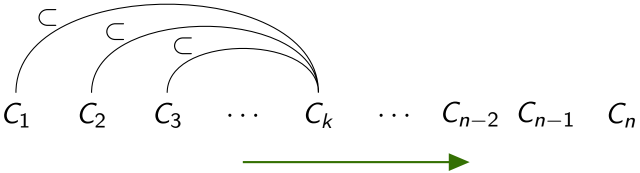
$\longleftarrow$ Bottom-Up

Subsumption for Proof Compression

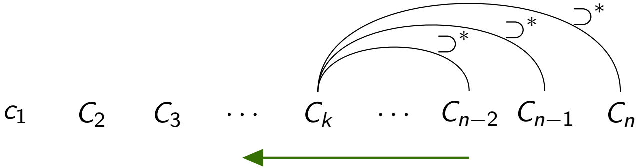
- Subsumption
  - C_1 subsumes C_2 iff $C_1 \subset C_2$
- Replace subsumed clauses by their subsumers
- Fix nodes with changed premises
  - Pivot in both premises $\rightarrow$ resolve premises
  - Pivot missing in a premise $\rightarrow$ use this premise

Top-Down and Bottom-Up Subsumption

Top-Down



Bottom-Up



$C \subset^* D$ iff $C \subset D$ and C is not an ancestor of D

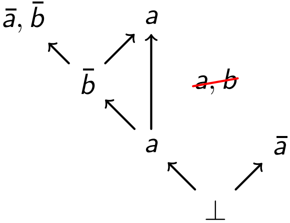
Top-Down Subsumption Example

$$
\begin{tikzcd}[column sep=small]
1\ \bar{a}, \bar{b} & & 2\ a & & \\
& 3\ \bar{b} \arrow[ul] \arrow[ur] & & 4\ a, b & \\
& & 5\ a \arrow[ul] \arrow[ur] & & 6\ \bar{a} \\
& & & 7\ \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

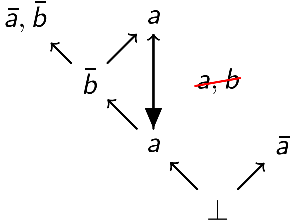
Top-Down Subsumption Example

$$
\begin{tikzcd}[column sep=small]
\bar{a}, \bar{b} & & a & & \\
& \bar{b} \arrow[ul] \arrow[ur] & & a, b & \\
& & a \arrow[ul] \arrow[ur] & & \bar{a} \\
& & & \perp \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

Top-Down Subsumption Example



Top-Down Subsumption Example



Top-Down Subsumption Example

$$\begin{tikzcd} a & & \bar{a} \\ & \perp \arrow[ul] \arrow[ur] & \end{tikzcd}$$

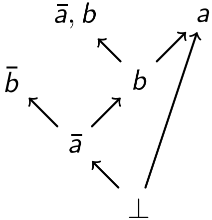
Bottom-Up Subsumption Example

$$
\begin{tikzcd}
 & {\scriptstyle 2}\ \bar{a}, b & & {\scriptstyle 3}\ a, b \\
{\scriptstyle 1}\ \bar{b} & & {\scriptstyle 4}\ b \arrow[ul] \arrow[ur] & \\
 & {\scriptstyle 5}\ \bar{a} \arrow[ul] \arrow[ur] & & {\scriptstyle 6}\ a \\
 & & {\scriptstyle 7}\ \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

Bottom-Up Subsumption Example

$$\begin{tikzcd}
 & \bar{a}, b & & a, b \\
\bar{b} & & b \arrow[ul] \arrow[ur] & \\
 & \bar{a} \arrow[ul] \arrow[ur] & & a \\
 & & \perp \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

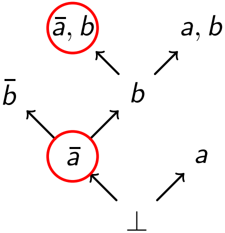
Bottom-Up Subsumption Example



Bottom-Up Subsumption Example

$$
\begin{tikzcd}
 & 2\ \bar{a}, b & & 3\ a, b \\
1\ \bar{b} & & 4\ b \arrow[ul] \arrow[ur] & \\
 & 5\ \bar{a} \arrow[ul] \arrow[ur] & & 6\ a \\
 & & 7\ \perp \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

Bottom-Up Subsumption Example



Bottom-Up Subsumption Example

$$
\begin{tikzcd}
 & & & a, b \\
\bar{b} & & b \arrow[ur] \arrow[dl, bend right] & \\
 & \bar{a} \arrow[ul] \arrow[ur] & & a \\
 & & \perp \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

LowerUnivalents

Definition (Valent literal)

In a proof ψ, a literal ℓ is *valent* for the subproof φ iff $\bar{\ell}$ belongs to the conclusion of $\psi \setminus (\varphi)$ but not to the conclusion of ψ.

Definition (Univalent subproof)

A subproof φ with conclusion Γ is *univalent* w.r.t. a set Δ of literals iff φ has exactly one valent literal ℓ, $\ell \notin \Delta$ and $\Gamma \subseteq \Delta \cup \{\ell\}$. ℓ is called the *univalent literal* of φ w.r.t. Δ.

Idea

- Δ are negated univalent literals
- Delete univalent subproofs
- Reinsert in order of deletion

LowerUnivalents Example

$$\Delta = \emptyset$$

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{a}, b & & \bar{b}, c \\
& \bar{a}, \bar{c} \arrow[ul] \arrow[ur] & & \bar{a}, c \arrow[ul] \arrow[ur] & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \bot \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

LowerUnivalents Example

$$\Delta = \{\bar{a}\}$$

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{a}, b & & \bar{b}, c \\
& \bar{a}, \bar{c} \arrow[ul] \arrow[ur] & & \bar{a}, c \arrow[ul] \arrow[ur] & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \perp \arrow[ul] \arrow[ur, dashed] &
\end{tikzcd}$$

LowerUnivalents Example

$$\Delta = \{\bar{a}, \bar{b}\}$$

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{a}, b & & \bar{b}, c \\
& \bar{a}, \bar{c} \arrow[ul] \arrow[ur, dashed] & & \bar{a}, c \arrow[ul, dashed] \arrow[ur] & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \perp \arrow[ul] \arrow[ur, dashed] &
\end{tikzcd}$$

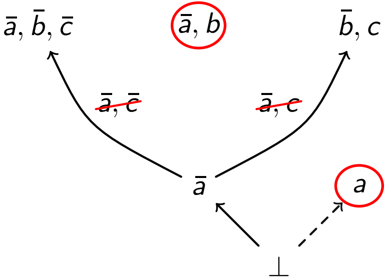
LowerUnivalents Example

$$\Delta = \{\bar{a}, \bar{b}\}$$

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{a}, b & & \bar{b}, c \\
& \cancel{\bar{a}, \bar{c}} & & \bar{a}, c \arrow[ul, dashed] \arrow[ur] & \\
& & \bar{a} \arrow[ur] \arrow[uull, bend left] & & a \\
& & & \bot \arrow[ul] \arrow[ur, dashed] &
\end{tikzcd}$$

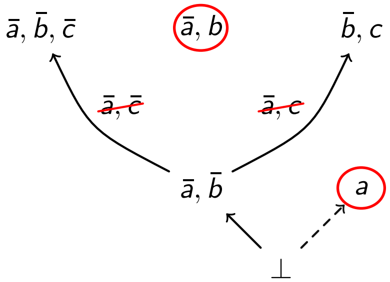
LowerUnivalents Example

$$\Delta = \{\bar{a}, \bar{b}\}$$



LowerUnivalents Example

$$\Delta = \{\bar{a}, \bar{b}\}$$



LowerUnivalents Example

$$\Delta = \{\bar{a}, \bar{b}\}$$

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{a}, b & & \bar{b}, c \\
& \cancel{\bar{a}, \bar{c}} & & \cancel{\bar{a}, c} & \\
& & \bar{a}, \bar{b} \arrow[uull] \arrow[uurr] & & a \\
& & & \cancel{\perp} &
\end{tikzcd}$$

LowerUnivalents Example

$$\Delta = \{\bar{a}, \bar{b}\}$$

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{b}, c & & \\
& \bar{a}, \bar{b} \arrow[ul] \arrow[ur] & & \bar{a}, b & \\
& & & & a
\end{tikzcd}$$

LowerUnivalents Example

$$\Delta = \{\bar{a}, \bar{b}\}$$

$$\begin{tikzcd}[column sep=small]
\bar{a}, \bar{b}, \bar{c} & & \bar{b}, c & & \\
& \bar{a}, \bar{b} \arrow[ul] \arrow[ur] & & \bar{a}, b & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a
\end{tikzcd}$$

LowerUnivalents Example

$$\Delta = \{\bar{a}, \bar{b}\}$$

$$\begin{tikzcd}
\bar{a}, \bar{b}, \bar{c} & & \bar{b}, c & & \\
& \bar{a}, \bar{b} \arrow[ul] \arrow[ur] & & \bar{a}, b & \\
& & \bar{a} \arrow[ul] \arrow[ur] & & a \\
& & & \perp \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Outline

Space Compression

Space measure

- Maximal amount of nodes that have to be kept in memory at once when checking the proof

Deletion information

- Extra lines in proof output
- Example: y is the last child of x
  - Read and check node x

    ...
  - Read and check node y
  - Delete node x

    ...

Interesting scenario

- Proof checker has much less memory than proof producer

Black Pebbling Game

A pebble is a small stone

Rules

- If all premises of a node p are pebbled, p may be pebbled
- Nodes can be unpebbled at any time
- Each node can be pebbled only once

Goal

- Pebble some node v

Pebbling problem

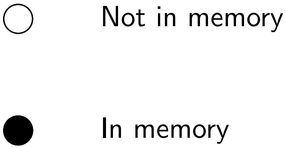
- For a given DAG and a node v, can v be pebbled using no more than n pebbles in total?
- PSPACE-complete (John R. Gilbert et al., 1980)

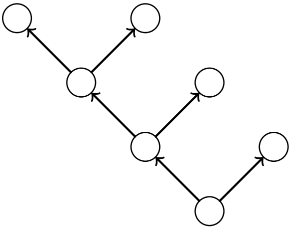
Pebbling Game Example

$$
\begin{tikzcd}[column sep=small]
\bar{a}, \bar{b} & & a & & \\
& \bar{b} \arrow[ul] \arrow[ur] & & a, b & \\
& & a \arrow[ul] \arrow[ur] & & \bar{a} \\
& & & \perp \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

Pebbling Game Example

Maximum pebbles used: 0



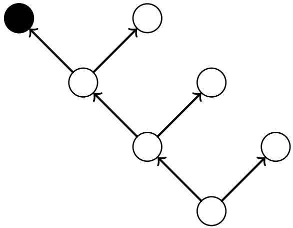


Pebbling Game Example

Maximum pebbles used: 1

Not in memory

In memory

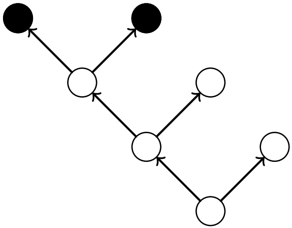


Pebbling Game Example

Maximum pebbles used: 2

Not in memory

In memory

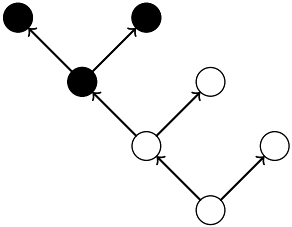


Pebbling Game Example

Maximum pebbles used: 3

Not in memory

In memory

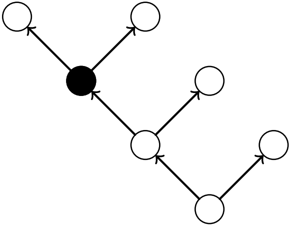


Pebbling Game Example

Maximum pebbles used: 3

○ Not in memory

● In memory

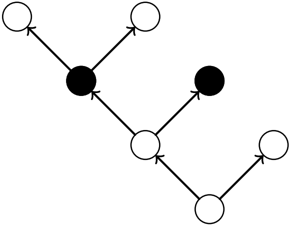


Pebbling Game Example

Maximum pebbles used: 3

Not in memory

In memory

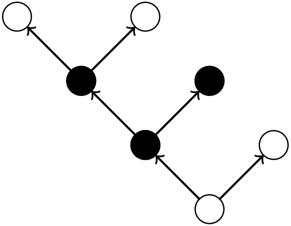


Pebbling Game Example

Maximum pebbles used: 3

 Not in memory

 In memory

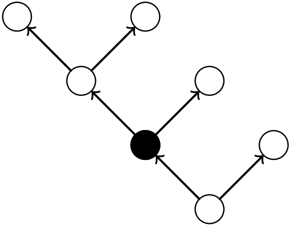


Pebbling Game Example

Maximum pebbles used: 3

Not in memory

In memory

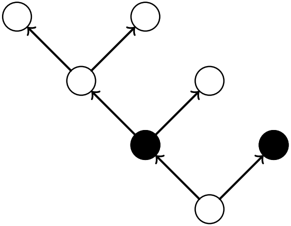


Pebbling Game Example

Maximum pebbles used: 3

Not in memory

In memory

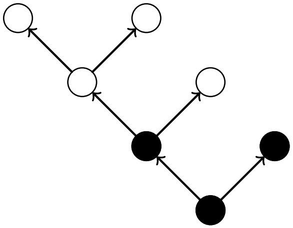


Pebbling Game Example

Maximum pebbles used: 3

Not in memory

In memory



Greedy Pebbling

Topological Order + Deletion Information

- Correspond to a strategy for the pebbling game

Top-Down

- Select node out of all pebbleable nodes
- Corresponds to playing the game

Bottom-Up

- Recursively queue up premises

Heuristics

Top-Down Pebbling

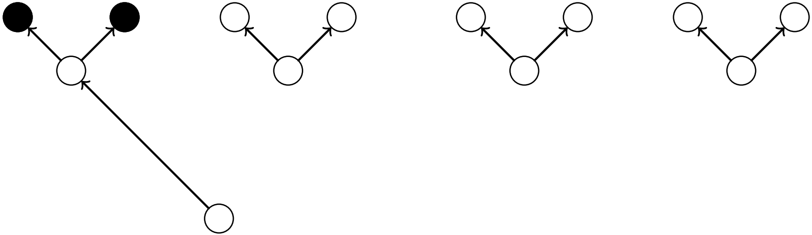
Maximum pebbles used: 0

Top-Down Pebbling

Maximum pebbles used: 1

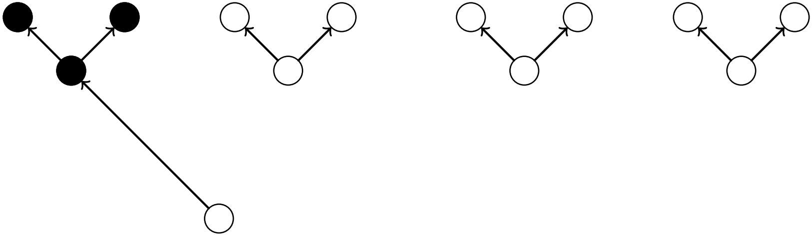
Top-Down Pebbling

Maximum pebbles used: 2



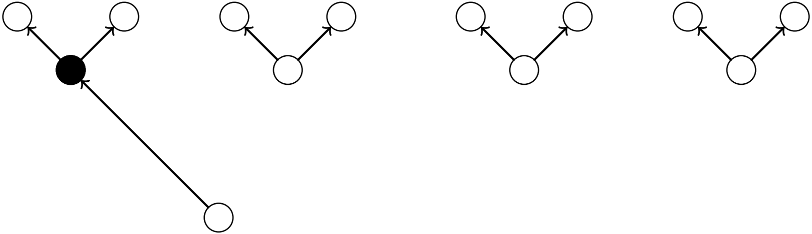
Top-Down Pebbling

Maximum pebbles used: 3



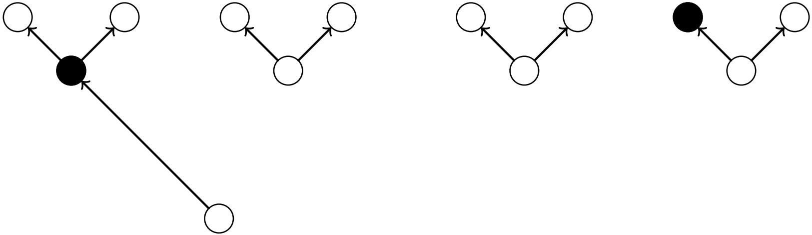
Top-Down Pebbling

Maximum pebbles used: 3



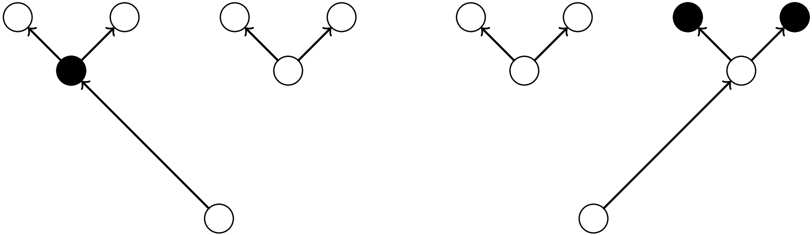
Top-Down Pebbling

Maximum pebbles used: 3



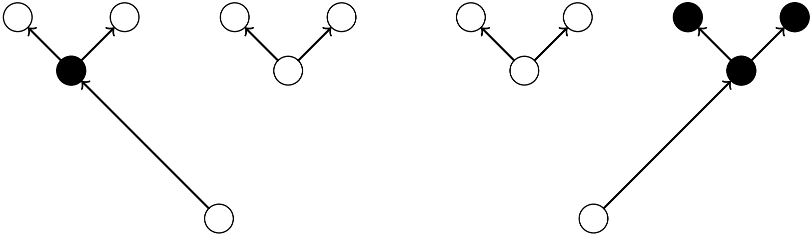
Top-Down Pebbling

Maximum pebbles used: 3



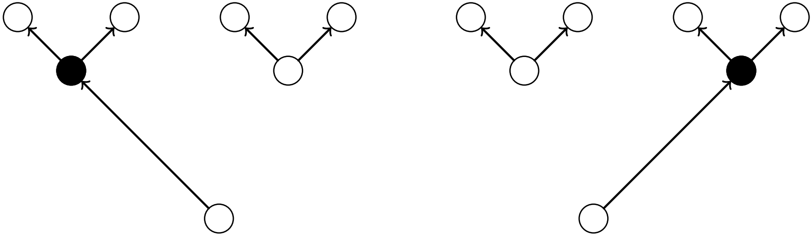
Top-Down Pebbling

Maximum pebbles used: 4



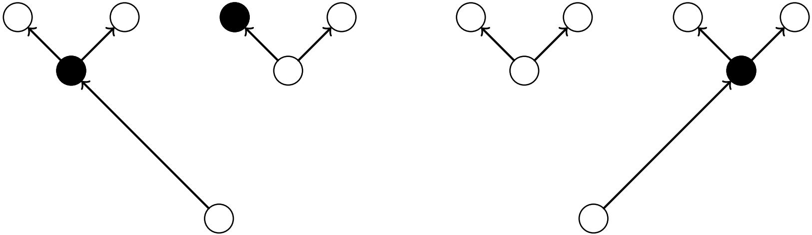
Top-Down Pebbling

Maximum pebbles used: 4



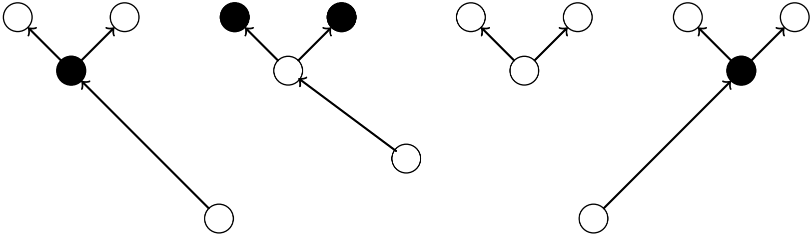
Top-Down Pebbling

Maximum pebbles used: 4



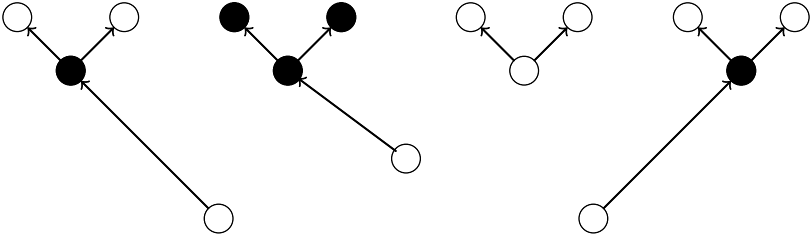
Top-Down Pebbling

Maximum pebbles used: 4



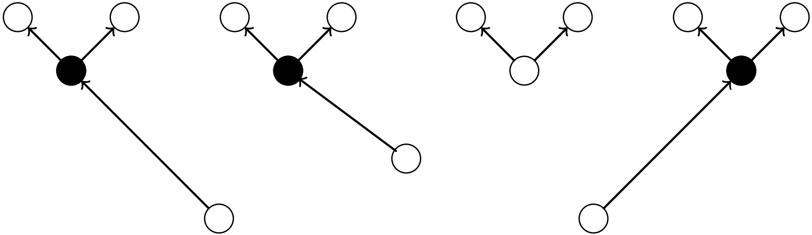
Top-Down Pebbling

Maximum pebbles used: 5



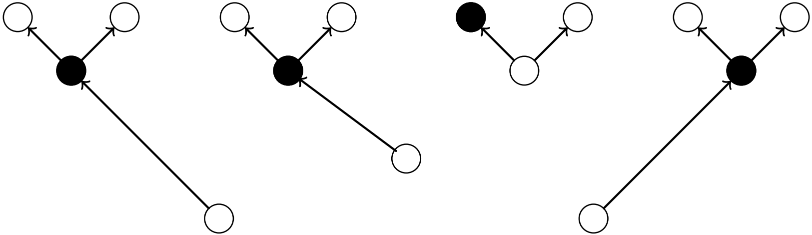
Top-Down Pebbling

Maximum pebbles used: 5



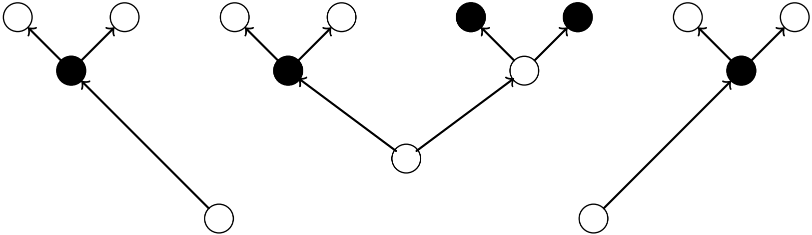
Top-Down Pebbling

Maximum pebbles used: 5



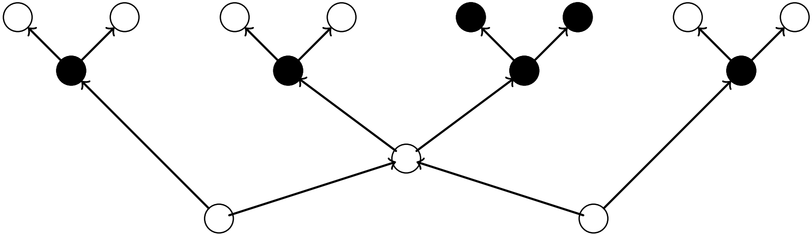
Top-Down Pebbling

Maximum pebbles used: 5



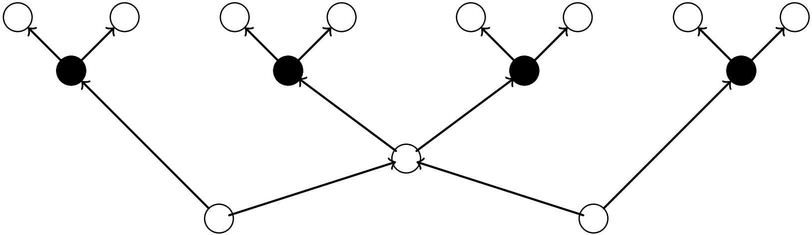
Top-Down Pebbling

Maximum pebbles used: 6



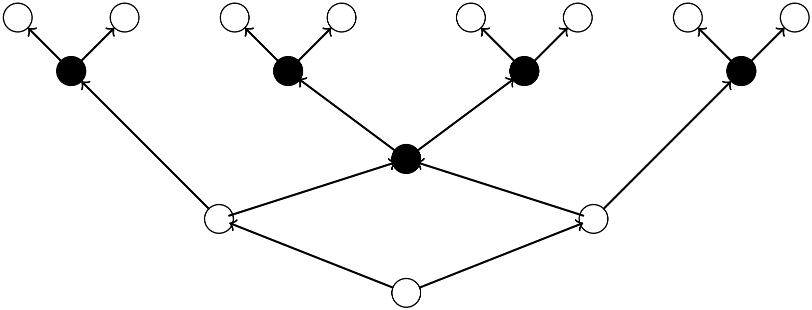
Top-Down Pebbling

Maximum pebbles used: 6



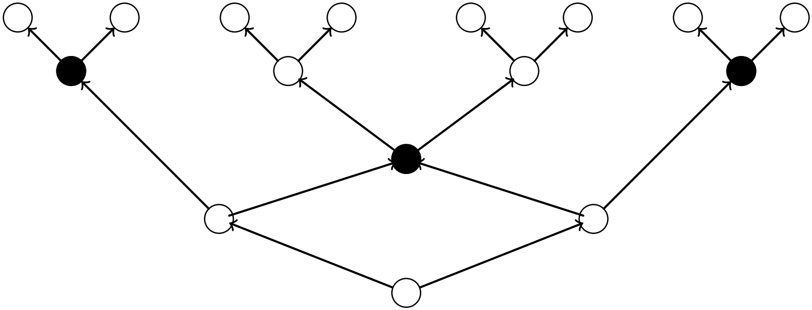
Top-Down Pebbling

Maximum pebbles used: 6



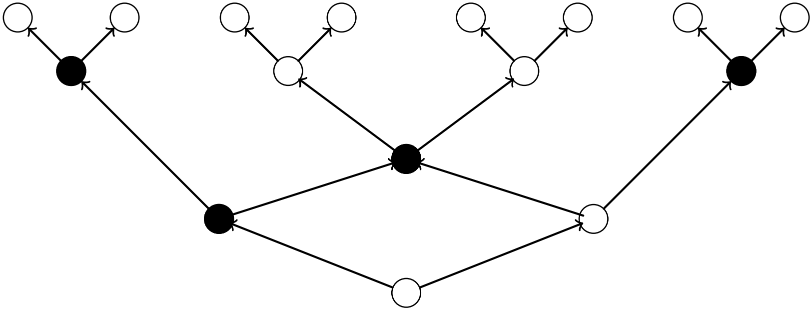
Top-Down Pebbling

Maximum pebbles used: 6



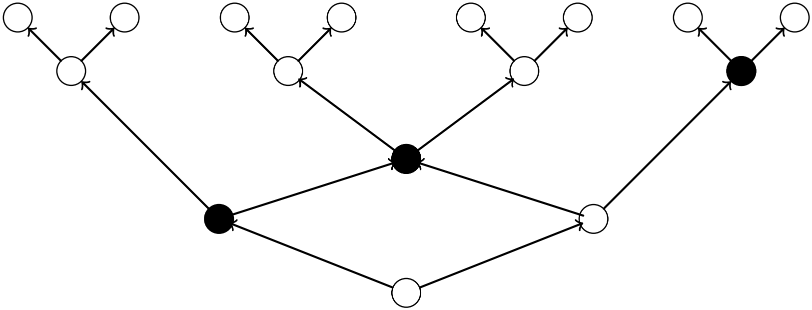
Top-Down Pebbling

Maximum pebbles used: 6



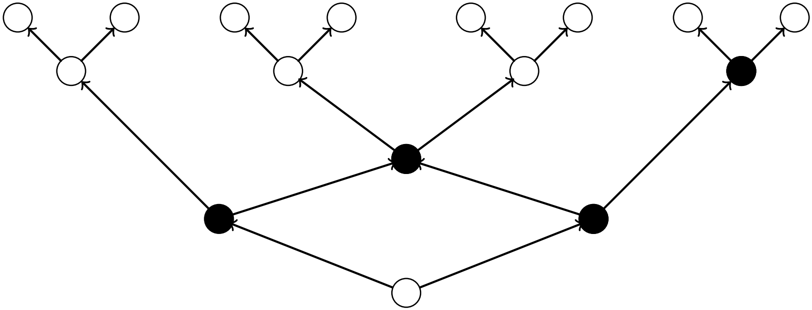
Top-Down Pebbling

Maximum pebbles used: 6



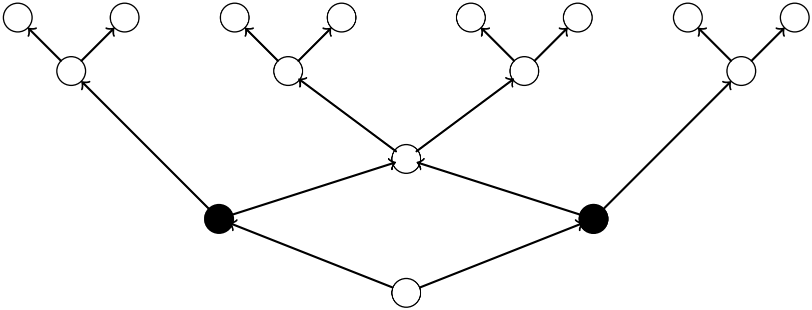
Top-Down Pebbling

Maximum pebbles used: 6



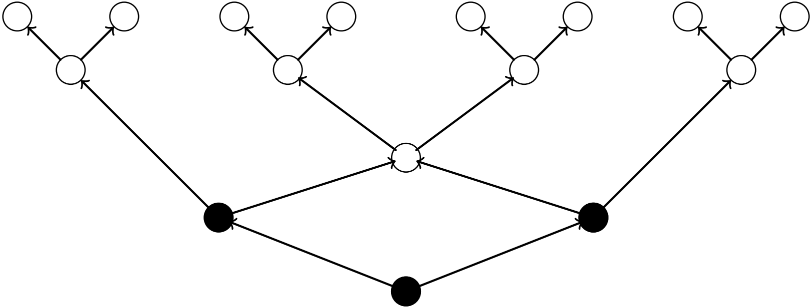
Top-Down Pebbling

Maximum pebbles used: 6



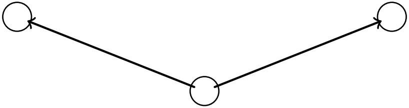
Top-Down Pebbling

Maximum pebbles used: 6



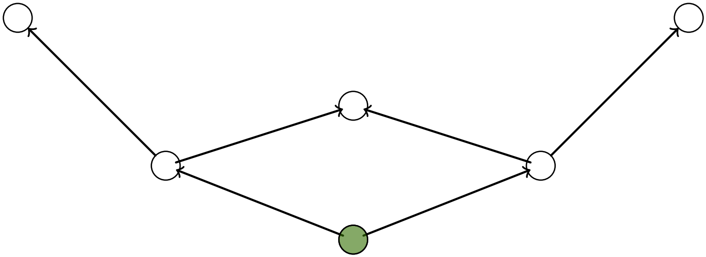
Bottom-up Pebbling

Maximum pebbles used: 0



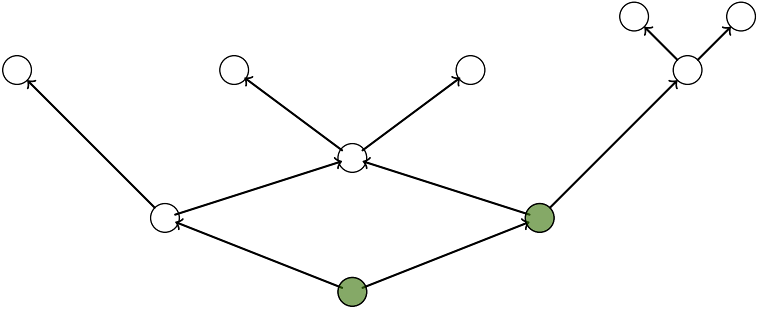
Bottom-up Pebbling

Maximum pebbles used: 0



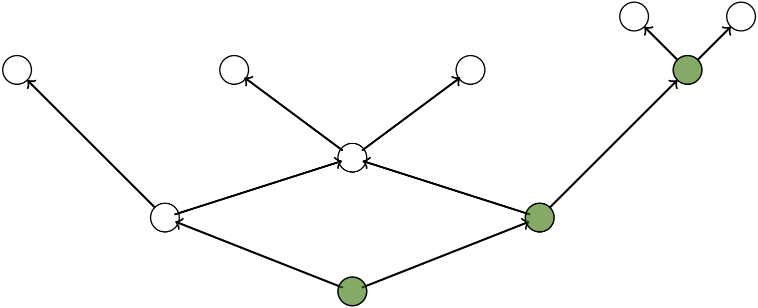
Bottom-up Pebbling

Maximum pebbles used: 0



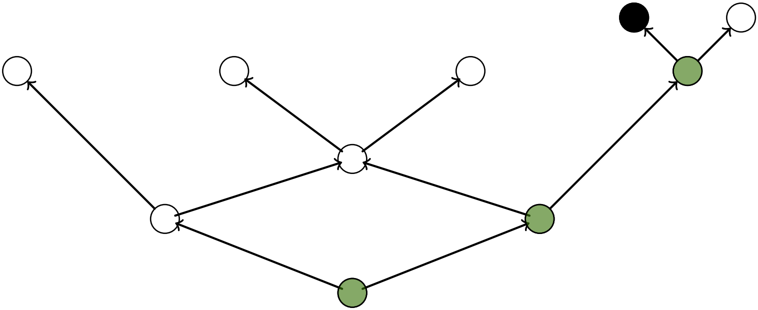
Bottom-up Pebbling

Maximum pebbles used: 0



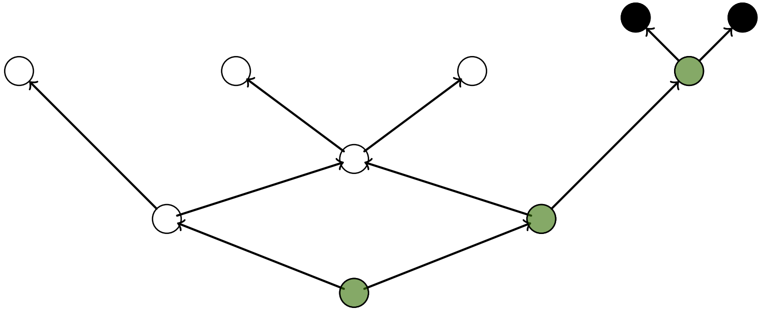
Bottom-up Pebbling

Maximum pebbles used: 1



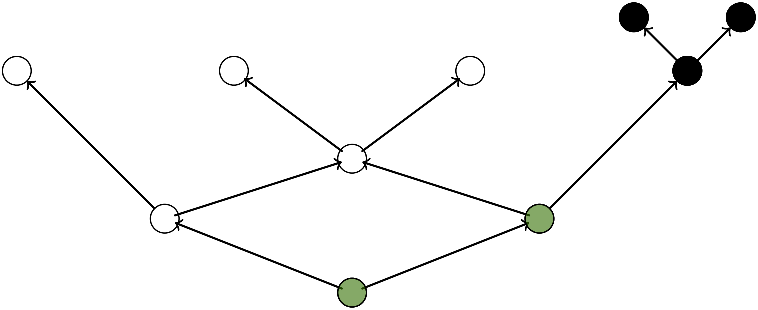
Bottom-up Pebbling

Maximum pebbles used: 2



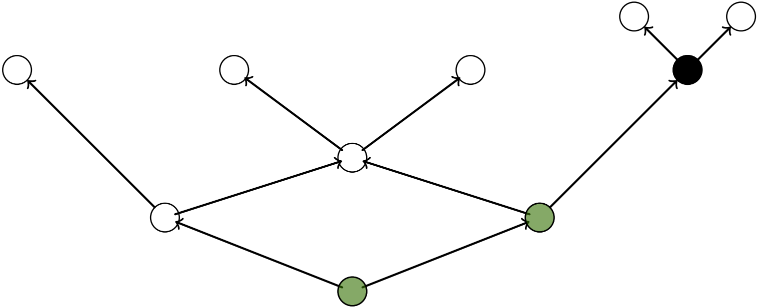
Bottom-up Pebbling

Maximum pebbles used: 3



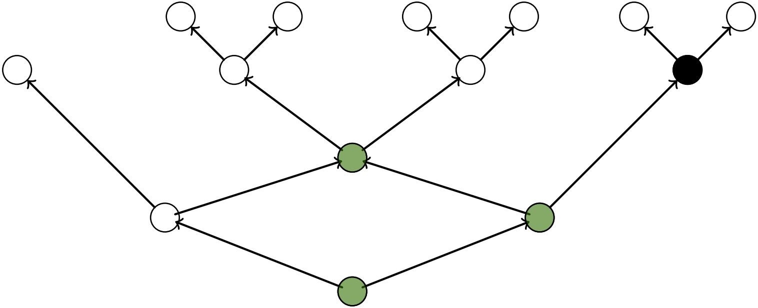
Bottom-up Pebbling

Maximum pebbles used: 3



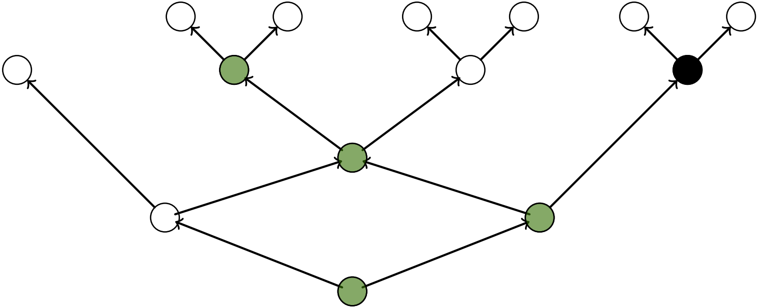
Bottom-up Pebbling

Maximum pebbles used: 3



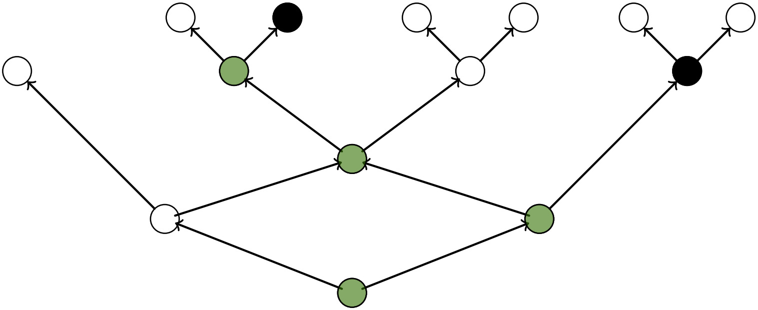
Bottom-up Pebbling

Maximum pebbles used: 3



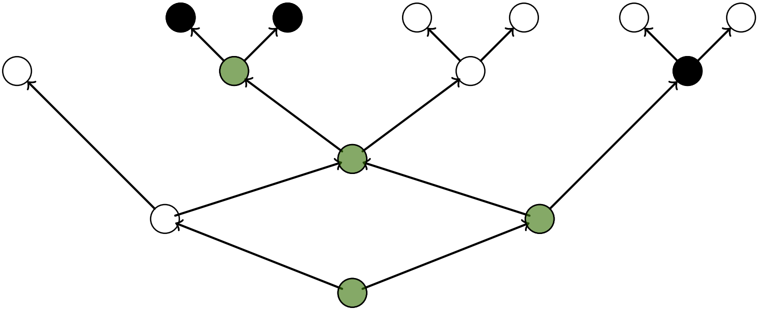
Bottom-up Pebbling

Maximum pebbles used: 3



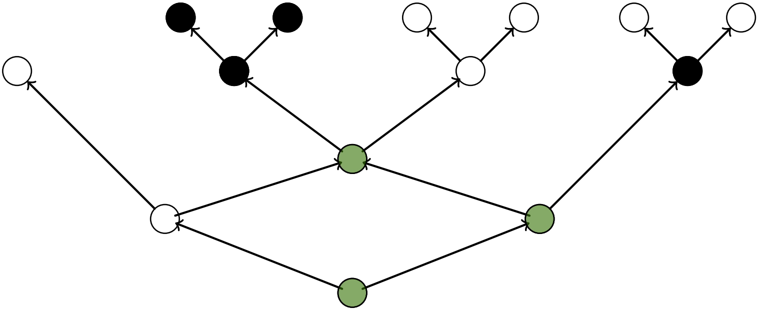
Bottom-up Pebbling

Maximum pebbles used: 3



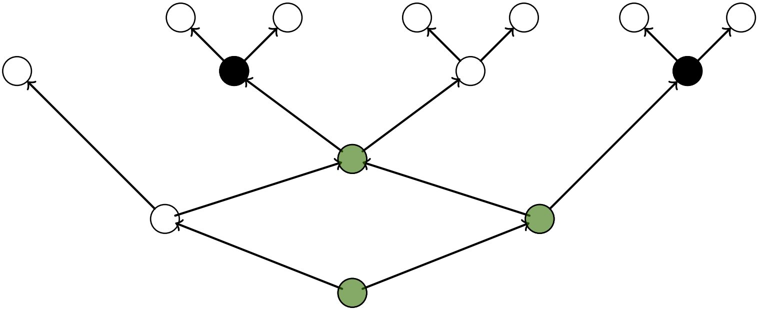
Bottom-up Pebbling

Maximum pebbles used: 4



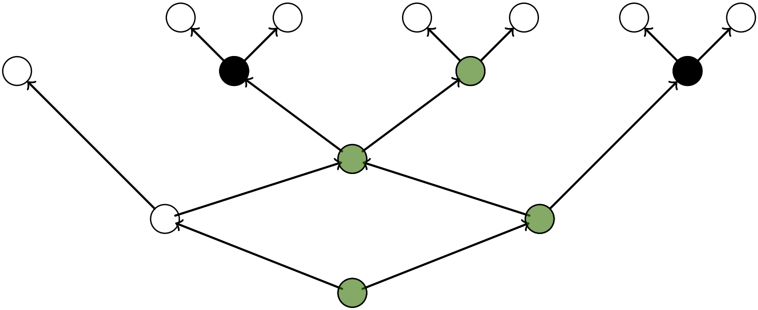
Bottom-up Pebbling

Maximum pebbles used: 4



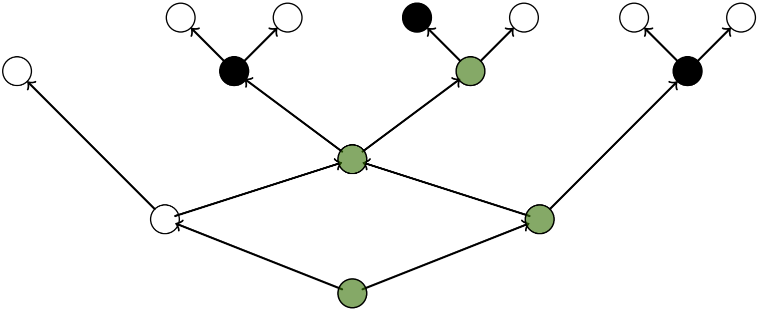
Bottom-up Pebbling

Maximum pebbles used: 4



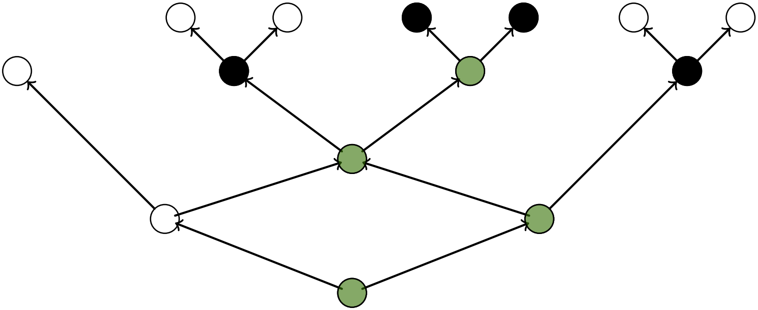
Bottom-up Pebbling

Maximum pebbles used: 4



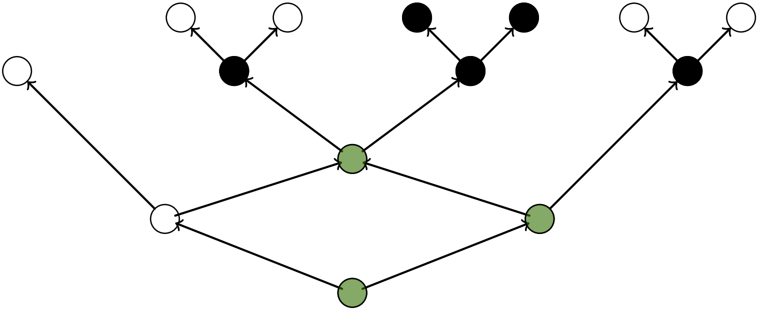
Bottom-up Pebbling

Maximum pebbles used: 4



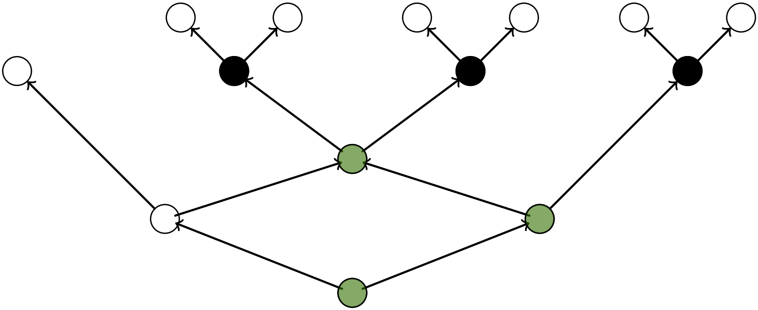
Bottom-up Pebbling

Maximum pebbles used: 5



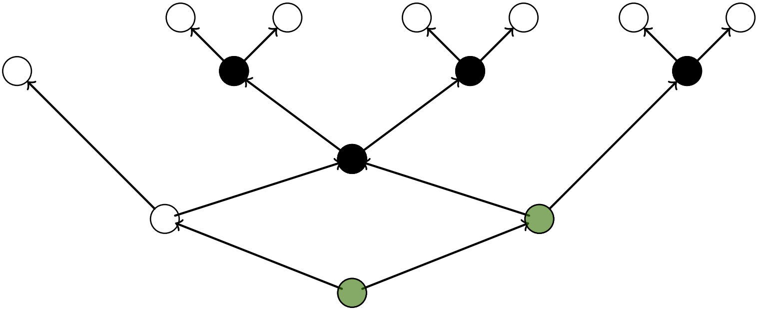
Bottom-up Pebbling

Maximum pebbles used: 5



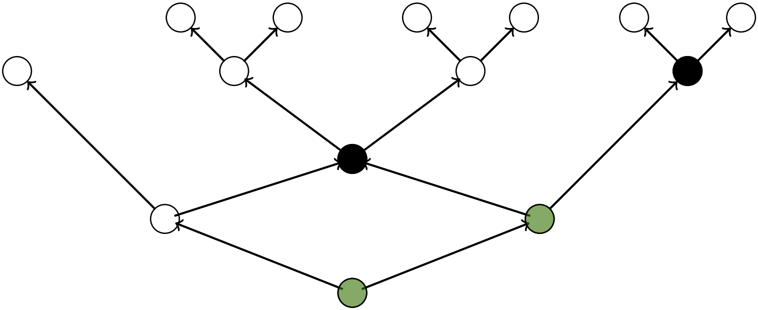
Bottom-up Pebbling

Maximum pebbles used: 5



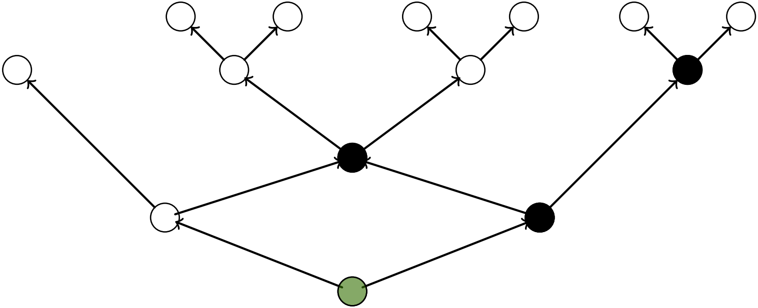
Bottom-up Pebbling

Maximum pebbles used: 5



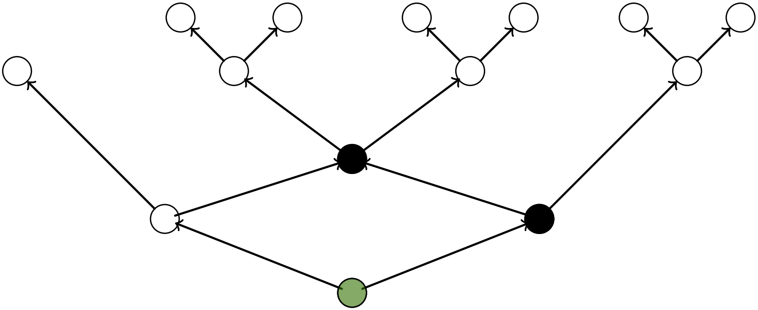
Bottom-up Pebbling

Maximum pebbles used: 5



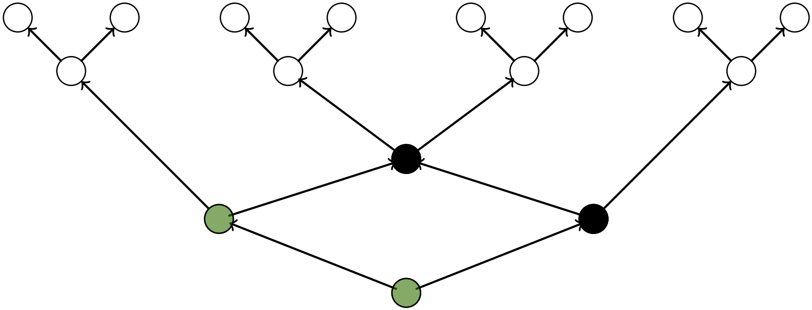
Bottom-up Pebbling

Maximum pebbles used: 5



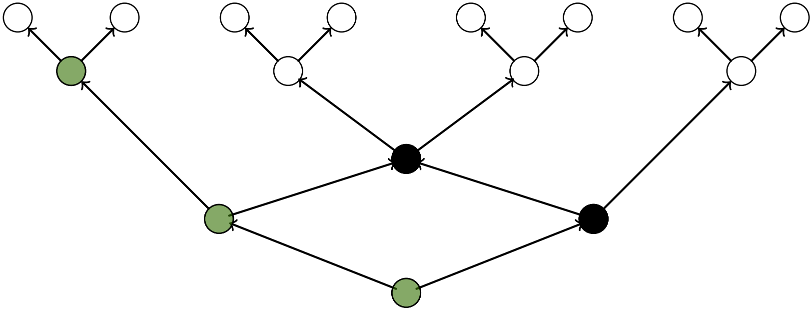
Bottom-up Pebbling

Maximum pebbles used: 5



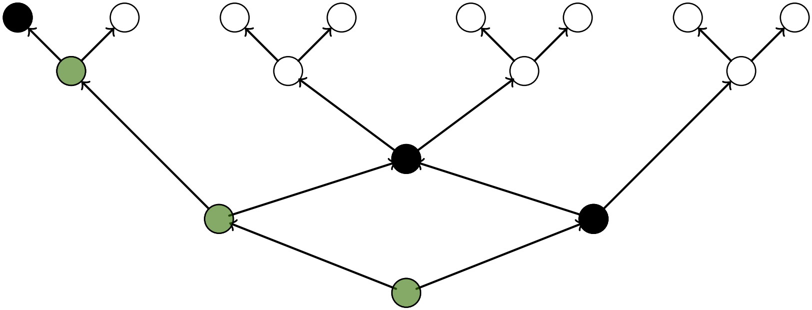
Bottom-up Pebbling

Maximum pebbles used: 5



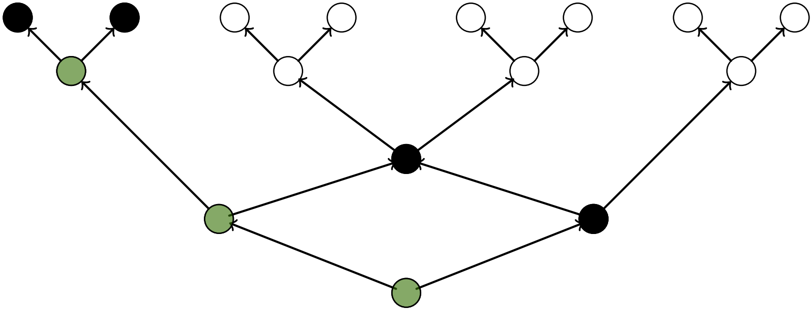
Bottom-up Pebbling

Maximum pebbles used: 5



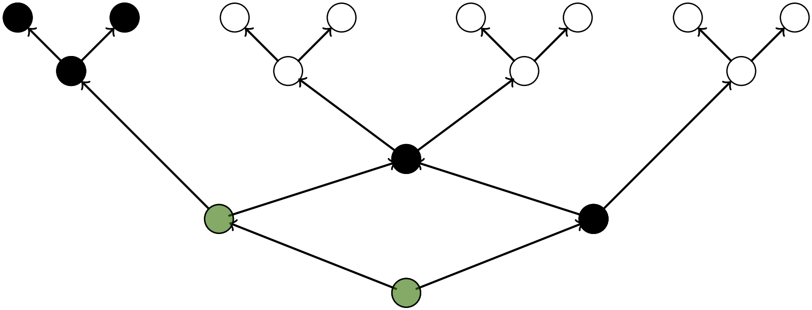
Bottom-up Pebbling

Maximum pebbles used: 5



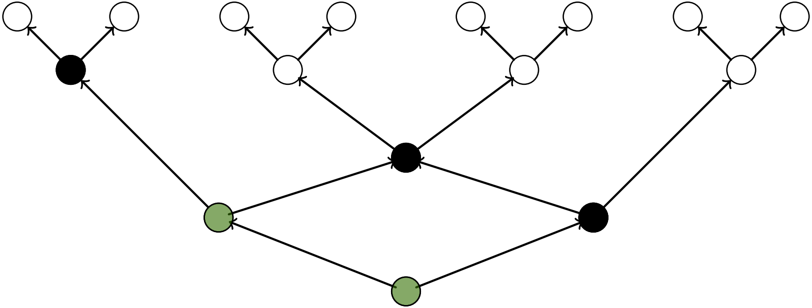
Bottom-up Pebbling

Maximum pebbles used: 5



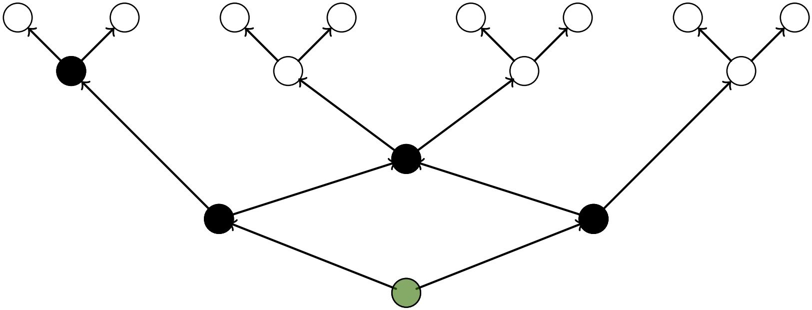
Bottom-up Pebbling

Maximum pebbles used: 5



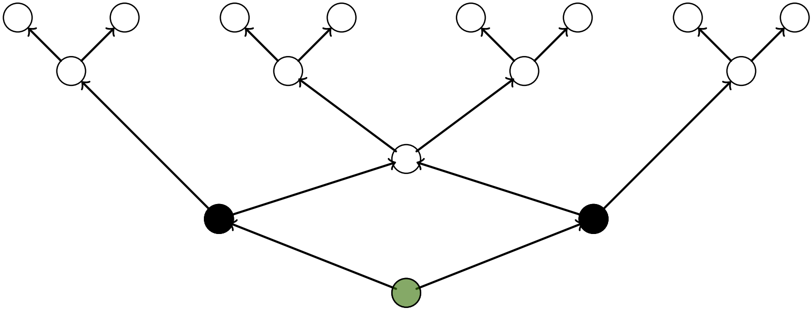
Bottom-up Pebbling

Maximum pebbles used: 5



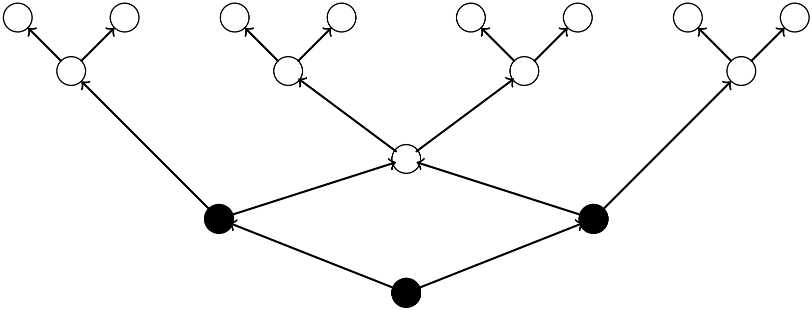
Bottom-up Pebbling

Maximum pebbles used: 5



Bottom-up Pebbling

Maximum pebbles used: 5



Outline

Skeptik

Proof compression tool

- First order logic framework
- Many propositional proof compression algorithms implemented

Developed at

- TU Wien
- Bruno Woltzenlogel Paleo
- Joseph Boudou

Scala

- Functional extension of Java

Check out at

- https://github.com/Paradoxika/Skeptik

Implemented algorithms

- DAGification
- EliminateTautologies
- RecycleUnits
- RecyclePivots
  - RecyclePivotsWithIntersection
- ReduceAndReconstruct
- LowerUnits
- LowerUnivalents
- Split
  - CottonSplit
  - MultiSplit
  - RecursiveSplit
- Subsumption algorithms
- Pebbling algorithms

My project

Google Summer of Code

- Three month coding project
- Paid by Google
- Subsumption, RecursiveSplit, Pebbling

EMCL Project

- Paper about Pebbling

This years GSoC

- Extend algorithms to First Order Logic
- http://www.iue.tuwien.ac.at/cse/index.php/gsoc/2014/ideas/153-skeptik.html
- Registration deadline: 21st March

Conclusion

Motivation

- Smaller proof libraries
- Faster proof checking
- Smaller unsat cores; better interpolants
- Easier combination of deductive system

Length compression

- Many different algorithms

Space compression

- Bottom-Up better than Top-Down
- Find better heuristics

Thank you for your attention !

Questions ?