# Understanding Space in Resolution: Optimal Lower Bounds and Exponential Trade-offs

Jakob Nordström
jakobn@mit.edu

Massachusetts Institute of Technology
Cambridge, Massachusetts, USA

Computational Complexity of Discrete Problems
Schloss Dagstuhl, Germany
September 14–19, 2008

*Joint work with Eli Ben-Sasson*

# Executive Summary of Talk

- Resolution: proof system for refuting CNF formulas
- Perhaps *the* most studied system in proof complexity
- Basis of current state-of-the-art SAT-solvers (winners in SAT 2007 competition: resolution + clause learning)
- Key resources: time and space
- What are the connections between these resources?
  Are time and space correlated?
  Are there time/space trade-offs?

# Outline

1. Resolution
   - Basics
   - Some Previous Work
   - Our Results
2. Outline of Proofs
   - Substitution Space Theorem
   - Pebble Games and Pebbling Contradictions
   - Putting the Pieces Together
3. Open Problems

# Some Notation and Terminology

- Literal $a$: variable $x$ or its negation $\overline{x}$
- Clause $C = a_1 \vee \ldots \vee a_k$: disjunction of literals
  At most $k$ literals: $k$-clause
- CNF formula $F = C_1 \wedge \ldots \wedge C_m$: conjunction of clauses
  $k$-CNF formula: CNF formula consisting of $k$-clauses
  (assume $k$ fixed)
- Refer to clauses of CNF formula as axioms
  (as opposed to derived clauses)

# Resolution Rule

Resolution rule:

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

## Observation

*If $F$ is a satisfiable CNF formula and $D$ is derived from clauses $C_1, C_2 \in F$ by the resolution rule, then $F \wedge D$ is satisfiable.*

Prove $F$ unsatisfiable by deriving the unsatisfiable empty clause 0 (the clause with no literals) from $F$ by resolution

# Resolution Rule

Resolution rule:

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

**Observation**

*If $F$ is a satisfiable CNF formula and $D$ is derived from clauses $C_1, C_2 \in F$ by the resolution rule, then $F \wedge D$ is satisfiable.*

Prove $F$ unsatisfiable by deriving the unsatisfiable empty clause 0 (the clause with no literals) from $F$ by resolution

# Resolution Rule

Resolution rule:

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

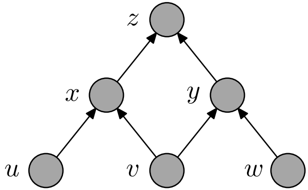
**Observation**

*If $F$ is a satisfiable CNF formula and $D$ is derived from clauses $C_1, C_2 \in F$ by the resolution rule, then $F \wedge D$ is satisfiable.*

Prove $F$ unsatisfiable by deriving the unsatisfiable empty clause 0 (the clause with no literals) from $F$ by resolution

# Example CNF Formula

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

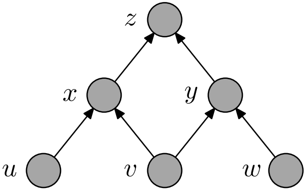



Defined in terms of directed acyclic graph (DAG):

- source vertices true
- truth propagates upwards
- but sink vertex is false

# Example CNF Formula

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

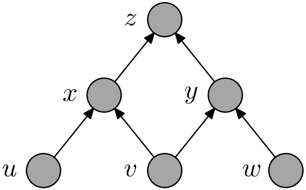



Defined in terms of directed acyclic graph (DAG):

- source vertices true
- truth propagates upwards
- but sink vertex is false

# Example CNF Formula

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

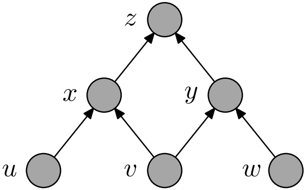



Defined in terms of directed acyclic graph (DAG):

- source vertices true
- truth propagates upwards
- but sink vertex is false

# Example CNF Formula

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$




Defined in terms of directed acyclic graph (DAG):

- source vertices true
- truth propagates upwards
- but sink vertex is false

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 0 |
| max # lines on board | 0 |
| max # literals on board | 0 |

Can write down axioms,
erase used clauses or
infer new clauses (but only from clauses currently on the board!)

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 1 |
| max # lines on board | 1 |
| max # literals on board | 1 |

$u$

Write down axiom 1: $u$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 2 |
| max # lines on board | 2 |
| max # literals on board | 2 |

$u$
$v$

Write down axiom 2: $v$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 3 |
| max # lines on board | 3 |
| max # literals on board | 5 |

$u$
$v$
$\overline{u} \lor \overline{v} \lor x$

Write down axiom 4: $\overline{u} \lor \overline{v} \lor x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 3 |
| max # lines on board | 3 |
| max # literals on board | 5 |

$u$
$v$
$\overline{u} \lor \overline{v} \lor x$

Infer $\overline{v} \lor x$ from $u$ and $\overline{u} \lor \overline{v} \lor x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 4 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$u$
$v$
$\overline{u} \lor \overline{v} \lor x$
$\overline{v} \lor x$

Infer $\overline{v} \lor x$ from $u$ and $\overline{u} \lor \overline{v} \lor x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 4 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$u$
$v$
$\overline{u} \vee \overline{v} \vee x$
$\overline{v} \vee x$

Erase clause $\overline{u} \vee \overline{v} \vee x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 4 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$u$
$v$
$\overline{v} \lor x$

Erase clause $\overline{u} \lor \overline{v} \lor x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 4 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$u$

$v$

$\overline{v} \lor x$

Erase clause $u$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 4 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$v$
$\overline{v} \lor x$

Erase clause $u$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 4 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$v$
$\overline{v} \lor x$

Infer $x$ from
$v$ and $\overline{v} \lor x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 5 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$v$
$\overline{v} \lor x$
$x$

Infer $x$ from
$v$ and $\overline{v} \lor x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 5 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$v$
$\overline{v} \lor x$
$x$

Erase clause $\overline{v} \lor x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 5 |
| max # lines on board | 4 |
| max # literals on board | 7 |

| |
|---|
| $v$ |
| $x$ |

Erase clause $\overline{v} \lor x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 5 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$v$
$x$

Erase clause $v$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 5 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$x$

Erase clause $v$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 6 |
| max # lines on board | 4 |
| max # literals on board | 7 |

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

Write down axiom 6: $\overline{x} \lor \overline{y} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 6 |
| max # lines on board | 4 |
| max # literals on board | 7 |

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

Infer $\overline{y} \lor z$ from $x$ and $\overline{x} \lor \overline{y} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 7 |
| max # lines on board | 4 |
| max # literals on board | 7 |

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

Infer $\overline{y} \lor z$ from
$x$ and $\overline{x} \lor \overline{y} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 7 |
| max # lines on board | 4 |
| max # literals on board | 7 |

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

Erase clause $\overline{x} \lor \overline{y} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 7 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$x$

$\overline{y} \lor z$

Erase clause $\overline{x} \lor \overline{y} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 7 |
| max # lines on board | 4 |
| max # literals on board | 7 |

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

Erase clause $x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 7 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$\overline{y} \lor z$

Erase clause $x$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 8 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor y$

Write down axiom 5: $\overline{v} \lor \overline{w} \lor y$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 8 |
| max # lines on board | 4 |
| max # literals on board | 7 |

$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor y$

Infer $\overline{v} \lor \overline{w} \lor z$ from
$\overline{y} \lor z$ and $\overline{v} \lor \overline{w} \lor y$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 9 |
| max # lines on board | 4 |
| max # literals on board | 8 |

$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor y$
$\overline{v} \lor \overline{w} \lor z$

Infer $\overline{v} \lor \overline{w} \lor z$ from $\overline{y} \lor z$ and $\overline{v} \lor \overline{w} \lor y$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 9 |
| max # lines on board | 4 |
| max # literals on board | 8 |

$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor y$
$\overline{v} \lor \overline{w} \lor z$

Erase clause $\overline{v} \lor \overline{w} \lor y$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 9 |
| max # lines on board | 4 |
| max # literals on board | 8 |

$\overline{y} \lor z$

$\overline{v} \lor \overline{w} \lor z$

Erase clause $\overline{v} \lor \overline{w} \lor y$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 9 |
| max # lines on board | 4 |
| max # literals on board | 8 |

$\overline{y} \lor z$

$\overline{v} \lor \overline{w} \lor z$

Erase clause $\overline{y} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 9 |
| max # lines on board | 4 |
| max # literals on board | 8 |

$\overline{v} \lor \overline{w} \lor z$

Erase clause $\overline{y} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 10 |
| max # lines on board | 4 |
| max # literals on board | 8 |

$\overline{v} \lor \overline{w} \lor z$

$v$

Write down axiom 2: $v$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 11 |
| max # lines on board | 4 |
| max # literals on board | 8 |

$\overline{v} \vee \overline{w} \vee z$
$v$
$w$

Write down axiom 3: $w$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 12 |
| max # lines on board | 4 |
| max # literals on board | 8 |

$\overline{v} \lor \overline{w} \lor z$
$v$
$w$
$\overline{z}$

Write down axiom 7: $\overline{z}$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 12 |
| max # lines on board | 4 |
| max # literals on board | 8 |

$\overline{v} \lor \overline{w} \lor z$
$v$
$w$
$\overline{z}$

Infer $\overline{w} \lor z$ from
$v$ and $\overline{v} \lor \overline{w} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 13 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$\overline{v} \lor \overline{w} \lor z$
$v$
$w$
$\overline{z}$
$\overline{w} \lor z$

Infer $\overline{w} \lor z$ from $v$ and $\overline{v} \lor \overline{w} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 13 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$\overline{v} \lor \overline{w} \lor z$
$v$
$w$
$\overline{z}$
$\overline{w} \lor z$

Erase clause $v$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 13 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$\overline{v} \lor \overline{w} \lor z$
$w$
$\overline{z}$
$\overline{w} \lor z$

Erase clause $v$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 13 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$\overline{v} \lor \overline{w} \lor z$
$w$
$\overline{z}$
$\overline{w} \lor z$

Erase clause $\overline{v} \lor \overline{w} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 13 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$w$
$\overline{z}$
$\overline{w} \lor z$

Erase clause $\overline{v} \lor \overline{w} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 13 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$w$
$\overline{z}$
$\overline{w} \vee z$

Infer $z$ from
$w$ and $\overline{w} \vee z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 14 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$w$
$\overline{z}$
$\overline{w} \lor z$
$z$

Infer $z$ from
$w$ and $\overline{w} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| **Blackboard bookkeeping** | |
|---|---|
| total # clauses on board | 14 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$w$
$\overline{z}$
$\overline{w} \lor z$
$z$

Erase clause $w$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 14 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$\overline{z}$
$\overline{w} \lor z$
$z$

Erase clause $w$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 14 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$\overline{z}$
$\overline{w} \lor z$
$z$

Erase clause $\overline{w} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 14 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$\overline{z}$

$z$

Erase clause $\overline{w} \lor z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 14 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$\overline{z}$

$z$

Infer 0 from
$\overline{z}$ and $z$

# Example Resolution Refutation

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

| Blackboard bookkeeping | |
|---|---|
| total # clauses on board | 15 |
| max # lines on board | 5 |
| max # literals on board | 8 |

$\overline{z}$
$z$
0

Infer 0 from
$\overline{z}$ and $z$

# Definition of Length and Space

- Length $L(\pi)$ of refutation $\pi : F \vdash 0$
  total # clauses in all of $\pi$
  (in our example 15)
- (Clause) Space $Sp(\pi)$ of refutation $\pi : F \vdash 0$
  max # clauses on blackboard simultaneously
  (in our example 5)
- Variable space $VarSp(\pi)$ of refutation $\pi : F \vdash 0$
  max # literals on blackboard simultaneously
  (in our example 8)

# Length and Space of Refuting $F$

- Length of refuting $F$ is

$$L(F \vdash 0) = \min_{\pi : F \vdash 0} \{ L(\pi) \}$$

- Clause space of refuting $F$ is

$$Sp(F \vdash 0) = \min_{\pi : F \vdash 0} \{ Sp(\pi) \}$$

- Variable space of refuting $F$ is

$$VarSp(F \vdash 0) = \min_{\pi : F \vdash 0} \{ VarSp(\pi) \}$$

# Why Should We Care About These Measures?

- Length: Lower bound on time for proof search algorithm
- Space: Lower bound on memory for proof search algorithm

Can also give ideas for proof search heuristics

# Which Space Measure Should We Care About?

Which space measure is “the right one”?

Potentially long discussion. . .

Short answer: Clause space more studied but both are interesting

Technical aside: When comparing different measures, for simplicity consider only $k$-CNF formulas (during this talk)

# Which Space Measure Should We Care About?

Which space measure is “the right one”?

Potentially long discussion. . .

Short answer: Clause space more studied but both are interesting

Technical aside: When comparing different measures, for simplicity consider only $k$-CNF formulas (during this talk)

# Upper and Lower Bounds on Length

Easy upper bound: $L(F \vdash 0) \leq 2^{(\#\text{ variables in } F + 1)}$

**Theorem (Haken 1985)**

*Polynomial-size CNF formula family with (weakly) exponential lower bound on refutation length (pigeonhole principle)*

Later improved to truly exponential lower bounds for different formula families ([Urquhart 1987, Chvátal & Szemerédi 1988] and others)

But resolution used widely in practice anyway
Amenable to proof search because of its simplicity

# Upper and Lower Bounds on Length

Easy upper bound: $L(F \vdash 0) \leq 2^{(\#\text{ variables in } F + 1)}$

**Theorem (Haken 1985)**

*Polynomial-size CNF formula family with (weakly) exponential lower bound on refutation length (pigeonhole principle)*

Later improved to truly exponential lower bounds for different formula families ([Urquhart 1987, Chvátal & Szemerédi 1988] and others)

But resolution used widely in practice anyway
Amenable to proof search because of its simplicity

# Upper and Lower Bounds on Length

Easy upper bound: $L(F \vdash 0) \leq 2^{(\#\text{ variables in } F + 1)}$

**Theorem (Haken 1985)**

*Polynomial-size CNF formula family with (weakly) exponential lower bound on refutation length (pigeonhole principle)*

Later improved to truly exponential lower bounds for different formula families ([Urquhart 1987, Chvátal & Szemerédi 1988] and others)

But resolution used widely in practice anyway
Amenable to proof search because of its simplicity

# Upper and Lower Bounds on Space

Easy upper bound on clause space: $Sp(F \vdash 0) \leq$ size of $F$, or more precisely $\leq \min(\#\text{ variables in } F, \#\text{ clauses in } F) + \mathcal{O}(1)$

**Theorem (Torán 1999, Alekhnovich et al. 2000)**

*There are polynomial-size CNF formula families matching this upper bound on clause space up to multiplicative constants*

Easy bound on variable space: $VarSp(F \vdash 0) \leq (\text{size of } F)^2$

No matching lower bound known! Not even superlinear bound

# Upper and Lower Bounds on Space

Easy upper bound on clause space: $Sp(F \vdash 0) \leq$ size of $F$, or more precisely $\leq \min(\#\text{ variables in } F, \#\text{ clauses in } F) + \mathcal{O}(1)$

**Theorem (Torán 1999, Alekhnovich et al. 2000)**

*There are polynomial-size CNF formula families matching this upper bound on clause space up to multiplicative constants*

Easy bound on variable space: $VarSp(F \vdash 0) \leq (\text{size of } F)^2$

No matching lower bound known! Not even superlinear bound

# Upper and Lower Bounds on Space

Easy upper bound on clause space: $Sp(F \vdash 0) \leq$ size of $F$, or more precisely $\leq \min(\#\text{ variables in } F, \#\text{ clauses in } F) + \mathcal{O}(1)$

**Theorem (Torán 1999, Alekhnovich et al. 2000)**

*There are polynomial-size CNF formula families matching this upper bound on clause space up to multiplicative constants*

Easy bound on variable space: $VarSp(F \vdash 0) \leq (\text{size of } F)^2$

No matching lower bound known! Not even superlinear bound

# Upper and Lower Bounds on Space

Easy upper bound on clause space: $Sp(F \vdash 0) \leq$ size of $F$, or more precisely $\leq \min(\#\text{ variables in } F, \#\text{ clauses in } F) + \mathcal{O}(1)$

**Theorem (Torán 1999, Alekhnovich et al. 2000)**

*There are polynomial-size CNF formula families matching this upper bound on clause space up to multiplicative constants*

Easy bound on variable space: $VarSp(F \vdash 0) \leq (\text{size of } F)^2$

No matching lower bound known! Not even superlinear bound

# Are Short Proofs Simple?

Does the length of refuting a formula tell us anything about the space?

- Does short length imply small space?
- Or are there formulas with short, easy refutations that must require large space?

For restricted form of so called tree-like resolution
$Sp(F \vdash 0) \leq \log L(F \vdash 0) + \mathcal{O}(1)$ [Esteban & Torán 1999]

General case has remained open, with no consensus on what the “right answer” should be

Results in [Nordström 2006, Nordström & Håstad 2008] can be interpreted as giving a clue but do not rule anything out

# Are Short Proofs Simple?

Does the length of refuting a formula tell us anything about the space?

- Does short length imply small space?
- Or are there formulas with short, easy refutations that must require large space?

For restricted form of so called tree-like resolution
$Sp(F \vdash 0) \leq \log L(F \vdash 0) + \mathcal{O}(1)$ [Esteban & Torán 1999]

General case has remained open, with no consensus on what the “right answer” should be

Results in [Nordström 2006, Nordström & Håstad 2008] can be interpreted as giving a clue but do not rule anything out

# Are Short Proofs Simple?

Does the length of refuting a formula tell us anything about the space?

- Does short length imply small space?
- Or are there formulas with short, easy refutations that must require large space?

For restricted form of so called tree-like resolution
$Sp(F \vdash 0) \leq \log L(F \vdash 0) + \mathcal{O}(1)$ [Esteban & Torán 1999]

General case has remained open, with no consensus on what the "right answer" should be

Results in [Nordström 2006, Nordström & Håstad 2008] can be interpreted as giving a clue but do not rule anything out

# Are Simple Proofs Short?

Formulas refutable in small space are refutable in short length—easy corollary of [Atserias & Dalmau 2003]

- But can space-efficient proofs always be carried out quickly?
- Or are there length-space trade-offs in resolution?

Some restricted trade-off results in [Ben-Sasson 2002, Hertel & Pitassi 2007, Nordström 2007]

Again not much known in the general case

# Are Simple Proofs Short?

Formulas refutable in small space are refutable in short length—easy corollary of [Atserias & Dalmau 2003]

- But can space-efficient proofs always be carried out quickly?
- Or are there length-space trade-offs in resolution?

Some restricted trade-off results in [Ben-Sasson 2002, Hertel & Pitassi 2007, Nordström 2007]

Again not much known in the general case

# What Trade-off Parameters Are of Interest?

- For what values of refutation space?
  Constant? Sublinear? Linear? Superlinear?
- How robust?
  Given minimal refutation space $S$, how much larger space is needed to get short length?
- How dramatic?
  Polynomial? Superpolynomial? Exponential?
- How explicit?
  Just a threshold, or is the whole trade-off curve known?

# What Trade-off Parameters Are of Interest?

- For what values of refutation space?
  Constant? Sublinear? Linear? Superlinear?
- How robust?
  Given minimal refutation space $S$, how much larger space is needed to get short length?
- How dramatic?
  Polynomial? Superpolynomial? Exponential?
- How explicit?
  Just a threshold, or is the whole trade-off curve known?

# What Trade-off Parameters Are of Interest?

- For what values of refutation space?
  Constant? Sublinear? Linear? Superlinear?
- How robust?
  Given minimal refutation space $S$, how much larger space is needed to get short length?
- How dramatic?
  Polynomial? Superpolynomial? Exponential?
- How explicit?
  Just a threshold, or is the whole trade-off curve known?

# What Trade-off Parameters Are of Interest?

- For what values of refutation space?
  Constant? Sublinear? Linear? Superlinear?
- How robust?
  Given minimal refutation space $S$, how much larger space is needed to get short length?
- How dramatic?
  Polynomial? Superpolynomial? Exponential?
- How explicit?
  Just a threshold, or is the whole trade-off curve known?

# Short Proofs May Be Spacious

Length and clause space are "completely uncorrelated"

**Theorem**

*There are k-CNF formulas* $\{F_n\}_{n=1}^{\infty}$ *of size* $\mathcal{O}(n)$ *with*

- *refutation length* $L(F_n \vdash 0) = \mathcal{O}(n)$ *and*
- *refutation clause space* $Sp(F_n \vdash 0) = \Omega(n/\log n)$.

Optimal separation—given length $n$, always possible to achieve space $\mathcal{O}(n/\log n)$

# Simple Proofs Can Be (Very) Long

## Theorem

*There are k-CNF formulas* $\{F_n\}_{n=1}^{\infty}$ *of size* $\mathcal{O}(n)$ *refutable in linear length* $L(F_n \vdash 0) = \mathcal{O}(n)$ *such that*

1. $Sp(F_n \vdash 0) = \mathcal{O}(1)$ *but* $L(\pi) = \Omega\left((n/Sp(\pi))^2\right)$ *for any refutation* $\pi$
2. $Sp(F_n \vdash 0) = \omega(1)$ *but for space* $\lesssim \sqrt[3]{n}$ *superpolynomial length is needed*
3. $Sp(F_n \vdash 0) = \mathcal{O}(\log^2 n)$ *but all the way up to space* $\mathcal{O}(n/\log n)$*, length* $n^{\Omega(\log \log n)}$ *is needed*
4. $Sp(F_n \vdash 0)$ *up to* $\mathcal{O}(n/\log n)$ *but even getting within multiplicative factor requires exponential length*

NB! Results hold for both space flavours

# Simple Proofs Can Be (Very) Long

## Theorem

*There are k-CNF formulas* $\{F_n\}_{n=1}^{\infty}$ *of size* $\mathcal{O}(n)$ *refutable in linear length* $L(F_n \vdash 0) = \mathcal{O}(n)$ *such that*

1. $Sp(F_n \vdash 0) = \mathcal{O}(1)$ *but* $L(\pi) = \Omega\big((n/Sp(\pi))^2\big)$ *for any refutation* $\pi$
2. $Sp(F_n \vdash 0) = \omega(1)$ *but for space* $\lesssim \sqrt[3]{n}$ *superpolynomial length is needed*
3. $Sp(F_n \vdash 0) = \mathcal{O}(\log^2 n)$ *but all the way up to space* $\mathcal{O}(n/\log n)$*, length* $n^{\Omega(\log \log n)}$ *is needed*
4. $Sp(F_n \vdash 0)$ *up to* $\mathcal{O}(n/\log n)$ *but even getting within multiplicative factor requires exponential length*

NB! Results hold for both space flavours

# Simple Proofs Can Be (Very) Long

**Theorem**

*There are k-CNF formulas* $\{F_n\}_{n=1}^{\infty}$ *of size* $\mathcal{O}(n)$ *refutable in linear length* $L(F_n \vdash 0) = \mathcal{O}(n)$ *such that*

1. $Sp(F_n \vdash 0) = \mathcal{O}(1)$ *but* $L(\pi) = \Omega\big((n/Sp(\pi))^2\big)$ *for any refutation* $\pi$
2. $Sp(F_n \vdash 0) = \omega(1)$ *but for space* $\lesssim \sqrt[3]{n}$ *superpolynomial length is needed*
3. $Sp(F_n \vdash 0) = \mathcal{O}(\log^2 n)$ *but all the way up to space* $\mathcal{O}(n/\log n)$*, length* $n^{\Omega(\log \log n)}$ *is needed*
4. $Sp(F_n \vdash 0)$ *up to* $\mathcal{O}(n/\log n)$ *but even getting within multiplicative factor requires exponential length*

NB! Results hold for both space flavours

# Simple Proofs Can Be (Very) Long

## Theorem

*There are k-CNF formulas* $\{F_n\}_{n=1}^{\infty}$ *of size* $\mathcal{O}(n)$ *refutable in linear length* $L(F_n \vdash 0) = \mathcal{O}(n)$ *such that*

1. $Sp(F_n \vdash 0) = \mathcal{O}(1)$ *but* $L(\pi) = \Omega\big((n/Sp(\pi))^2\big)$ *for any refutation* $\pi$
2. $Sp(F_n \vdash 0) = \omega(1)$ *but for space* $\lesssim \sqrt[3]{n}$ *superpolynomial length is needed*
3. $Sp(F_n \vdash 0) = \mathcal{O}\big(\log^2 n\big)$ *but all the way up to space* $\mathcal{O}(n/\log n)$, *length* $n^{\Omega(\log\log n)}$ *is needed*
4. $Sp(F_n \vdash 0)$ *up to* $\mathcal{O}(n/\log n)$ *but even getting within multiplicative factor requires exponential length*

NB! Results hold for both space flavours

# Simple Proofs Can Be (Very) Long

## Theorem

*There are k-CNF formulas* $\{F_n\}_{n=1}^{\infty}$ *of size* $\mathcal{O}(n)$ *refutable in linear length* $L(F_n \vdash 0) = \mathcal{O}(n)$ *such that*

1. $Sp(F_n \vdash 0) = \mathcal{O}(1)$ *but* $L(\pi) = \Omega\big((n/Sp(\pi))^2\big)$ *for any refutation* $\pi$
2. $Sp(F_n \vdash 0) = \omega(1)$ *but for space* $\lesssim \sqrt[3]{n}$ *superpolynomial length is needed*
3. $Sp(F_n \vdash 0) = \mathcal{O}(\log^2 n)$ *but all the way up to space* $\mathcal{O}(n/\log n)$*, length* $n^{\Omega(\log \log n)}$ *is needed*
4. $Sp(F_n \vdash 0)$ *up to* $\mathcal{O}(n/\log n)$ *but even getting within multiplicative factor requires exponential length*

NB! Results hold for both space flavours

# Simple Proofs Can Be (Very) Long

## Theorem

*There are k-CNF formulas* $\{F_n\}_{n=1}^{\infty}$ *of size* $\mathcal{O}(n)$ *refutable in linear length* $L(F_n \vdash 0) = \mathcal{O}(n)$ *such that*

1. $Sp(F_n \vdash 0) = \mathcal{O}(1)$ *but* $L(\pi) = \Omega\big((n/Sp(\pi))^2\big)$ *for any refutation* $\pi$
2. $Sp(F_n \vdash 0) = \omega(1)$ *but for space* $\lesssim \sqrt[3]{n}$ *superpolynomial length is needed*
3. $Sp(F_n \vdash 0) = \mathcal{O}\big(\log^2 n\big)$ *but all the way up to space* $\mathcal{O}(n/\log n)$*, length* $n^{\Omega(\log\log n)}$ *is needed*
4. $Sp(F_n \vdash 0)$ *up to* $\mathcal{O}(n/\log n)$ *but even getting within multiplicative factor requires exponential length*

NB! Results hold for both space flavours

# Any Practical Implications?

Yes and no

Space measures memory consumption for clause learning algorithms but space $\leq$ formula size—practical applications usually will have much more memory available than that

But maybe lower bounds on space can give clue about hardness anyway

(Sabharwal et al. 2003) exhibits formulas with very short refutations that state-of-the-art SAT-solver cannot find

Same kind of formulas that we have been studying

# Any Practical Implications?

Yes and no

Space measures memory consumption for clause learning algorithms but space $\leq$ formula size—practical applications usually will have much more memory available than that

But maybe lower bounds on space can give clue about hardness anyway

(Sabharwal et al. 2003) exhibits formulas with very short refutations that state-of-the-art SAT-solver cannot find

Same kind of formulas that we have been studying

# Rest of This Talk

- Prove new theorem about variable substitution and proof space
- Study old combinatorial game from the 1970s
- Combine the two

# Key Idea: Variable Substitution

Substitute $x_1 \oplus x_2$ for every variable $x$ in formula. Example:

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

$$\Downarrow$$

$$(x_1 \oplus x_2) \vee \neg(y_1 \oplus y_2)$$

$$\Downarrow$$

$$\begin{aligned} & (x_1 \vee x_2 \vee y_1 \vee \overline{y}_2) \\ \wedge\ & (x_1 \vee x_2 \vee \overline{y}_1 \vee y_2) \\ \wedge\ & (\overline{x}_1 \vee \overline{x}_2 \vee y_1 \vee \overline{y}_2) \\ \wedge\ & (\overline{x}_1 \vee \overline{x}_2 \vee \overline{y}_1 \vee y_2) \end{aligned}$$

# Key Technical Result: Substitution Space Theorem

## Theorem

*For any CNF formula $F$, let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for $x$, written in CNF in canonical way. Then any refutation $\pi$ of $F[\oplus]$ can be transformed into refutation $\pi'$ of $F$ such that*

- *Length of $\pi \geq$ length of $\pi'$ (sort of but not quite—actually # axiom downloads in $\pi \geq$ # axiom downloads in $\pi'$)*
- *Clause space of $\pi \geq$ maximal # variables mentioned simultaneously in $\pi'$*

(Full statement is slightly more general)

# Key Technical Result: Substitution Space Theorem

## Theorem

*For any CNF formula $F$, let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for $x$, written in CNF in canonical way. Then any refutation $\pi$ of $F[\oplus]$ can be transformed into refutation $\pi'$ of $F$ such that*

- *Length of $\pi \geq$ length of $\pi'$ (sort of but not quite—actually # axiom downloads in $\pi \geq$ # axiom downloads in $\pi'$)*
- *Clause space of $\pi \geq$ maximal # variables mentioned simultaneously in $\pi'$*

(Full statement is slightly more general)

# Key Technical Result: Substitution Space Theorem

## Theorem

*For any CNF formula $F$, let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for $x$, written in CNF in canonical way. Then any refutation $\pi$ of $F[\oplus]$ can be transformed into refutation $\pi'$ of $F$ such that*

- *Length of $\pi \geq$ length of $\pi'$ (sort of but not quite—actually # axiom downloads in $\pi \geq$ # axiom downloads in $\pi'$)*
- *Clause space of $\pi \geq$ maximal # variables mentioned simultaneously in $\pi'$*

(Full statement is slightly more general)

# Key Technical Result: Substitution Space Theorem

**Theorem**

*For any CNF formula $F$, let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for $x$, written in CNF in canonical way. Then any refutation $\pi$ of $F[\oplus]$ can be transformed into refutation $\pi'$ of $F$ such that*

- *Length of $\pi \geq$ length of $\pi'$ (sort of but not quite—actually # axiom downloads in $\pi \geq$ # axiom downloads in $\pi'$)*
- *Clause space of $\pi \geq$ maximal # variables mentioned simultaneously in $\pi'$*

(Full statement is slightly more general)

# Sketch of Proof of Substitution Space Theorem

Given refutation $\pi$ of $F[\oplus]$, make "shadow refutation" $\pi'$ of $F$

| **XOR formula** $F[\oplus]$ | **Original formula** $F$ |
|---|---|
| If XOR blackboard implies e.g. $(x_1 \oplus x_2) \vee \neg(y_1 \oplus y_2)$... | write $x \vee \overline{y}$ on shadow blackboard |
| For consecutive XOR blackboard configurations... | can get between corresponding shadow blackboards by legal derivation steps |
| ... axiom download made on XOR blackboard | Axiom download on shadow blackboard only when... |
| ... is at most # clauses on XOR blackboard | # variables mentioned on shadow blackboard... |

# Sketch of Proof of Substitution Space Theorem

Given refutation $\pi$ of $F[\oplus]$, make "shadow refutation" $\pi'$ of $F$

| **XOR formula** $F[\oplus]$ | **Original formula** $F$ |
|---|---|
| If XOR blackboard implies e.g. $(x_1 \oplus x_2) \lor \neg(y_1 \oplus y_2)\ldots$ | write $x \lor \overline{y}$ on shadow blackboard |
| For consecutive XOR blackboard configurations… | can get between corresponding shadow blackboards by legal derivation steps |
| … axiom download made on XOR blackboard | Axiom download on shadow blackboard only when… |
| … is at most # clauses on XOR blackboard | # variables mentioned on shadow blackboard… |

# Sketch of Proof of Substitution Space Theorem

Given refutation $\pi$ of $F[\oplus]$, make "shadow refutation" $\pi'$ of $F$

| **XOR formula $F[\oplus]$** | **Original formula $F$** |
|---|---|
| If XOR blackboard implies e.g. $(x_1 \oplus x_2) \lor \neg(y_1 \oplus y_2)\ldots$ | write $x \lor \overline{y}$ on shadow blackboard |
| For consecutive XOR blackboard configurations… | can get between corresponding shadow blackboards by legal derivation steps |
| … axiom download made on XOR blackboard | Axiom download on shadow blackboard only when… |
| … is at most # clauses on XOR blackboard | # variables mentioned on shadow blackboard… |

# Sketch of Proof of Substitution Space Theorem

Given refutation $\pi$ of $F[\oplus]$, make "shadow refutation" $\pi'$ of $F$

| **XOR formula $F[\oplus]$** | **Original formula $F$** |
|---|---|
| If XOR blackboard implies e.g. $(x_1 \oplus x_2) \lor \neg(y_1 \oplus y_2)$... | write $x \lor \overline{y}$ on shadow blackboard |
| For consecutive XOR blackboard configurations... | can get between corresponding shadow blackboards by legal derivation steps |
| ... axiom download made on XOR blackboard | Axiom download on shadow blackboard only when... |
| ... is at most # clauses on XOR blackboard | # variables mentioned on shadow blackboard... |

# Sketch of Proof of Substitution Space Theorem

Given refutation $\pi$ of $F[\oplus]$, make "shadow refutation" $\pi'$ of $F$

| **XOR formula** $F[\oplus]$ | **Original formula** $F$ |
|---|---|
| If XOR blackboard implies e.g. $(x_1 \oplus x_2) \vee \neg(y_1 \oplus y_2)\ldots$ | write $x \vee \overline{y}$ on shadow blackboard |
| For consecutive XOR blackboard configurations… | can get between corresponding shadow blackboards by legal derivation steps |
| … axiom download made on XOR blackboard | Axiom download on shadow blackboard only when… |
| … is at most # clauses on XOR blackboard | # variables mentioned on shadow blackboard… |

# Sketch of Proof of Substitution Space Theorem

Given refutation $\pi$ of $F[\oplus]$, make "shadow refutation" $\pi'$ of $F$

| **XOR formula** $F[\oplus]$ | **Original formula** $F$ |
|---|---|
| If XOR blackboard implies e.g. $(x_1 \oplus x_2) \vee \neg(y_1 \oplus y_2)$... | write $x \vee \overline{y}$ on shadow blackboard |
| For consecutive XOR blackboard configurations... | can get between corresponding shadow blackboards by legal derivation steps |
| ... axiom download made on XOR blackboard | Axiom download on shadow blackboard only when... |
| ... is at most # clauses on XOR blackboard | # variables mentioned on shadow blackboard... |

# Sketch of Proof of Substitution Space Theorem

Given refutation $\pi$ of $F[\oplus]$, make "shadow refutation" $\pi'$ of $F$

| **XOR formula** $F[\oplus]$ | **Original formula** $F$ |
|---|---|
| If XOR blackboard implies e.g. $(x_1 \oplus x_2) \vee \neg(y_1 \oplus y_2)$... | write $x \vee \overline{y}$ on shadow blackboard |
| For consecutive XOR blackboard configurations... | can get between corresponding shadow blackboards by legal derivation steps |
| ... axiom download made on XOR blackboard | Axiom download on shadow blackboard only when... |
| ... is at most # clauses on XOR blackboard | # variables mentioned on shadow blackboard... |

# Sketch of Proof of Substitution Space Theorem

Given refutation $\pi$ of $F[\oplus]$, make "shadow refutation" $\pi'$ of $F$

| **XOR formula $F[\oplus]$** | **Original formula $F$** |
|---|---|
| If XOR blackboard implies e.g. $(x_1 \oplus x_2) \vee \neg(y_1 \oplus y_2)\ldots$ | write $x \vee \overline{y}$ on shadow blackboard |
| For consecutive XOR blackboard configurations... | can get between corresponding shadow blackboards by legal derivation steps |
| ... axiom download made on XOR blackboard | Axiom download on shadow blackboard only when... |
| ... is at most # clauses on XOR blackboard | # variables mentioned on shadow blackboard... |

# Sketch of Proof of Substitution Space Theorem

Given refutation $\pi$ of $F[\oplus]$, make "shadow refutation" $\pi'$ of $F$

| **XOR formula** $F[\oplus]$ | **Original formula** $F$ |
|---|---|
| If XOR blackboard implies e.g. $(x_1 \oplus x_2) \vee \neg(y_1 \oplus y_2)\ldots$ | write $x \vee \overline{y}$ on shadow blackboard |
| For consecutive XOR blackboard configurations... | can get between corresponding shadow blackboards by legal derivation steps |
| ... axiom download made on XOR blackboard | Axiom download on shadow blackboard only when... |
| ... is at most # clauses on XOR blackboard | # variables mentioned on shadow blackboard... |

# How to Get a Handle on Length-Space Relations?

Want to find formulas that

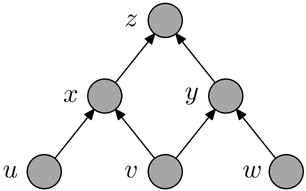
- can be quickly refuted but require large space
- have space-efficient refutations requiring much time

Such time-space trade-off questions well-studied for pebble games modelling calculations described by DAGs ([Cook & Sethi 1976] and many others)

- Time needed for calculation: # pebbling moves
- Space needed for calculation: max # pebbles required

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

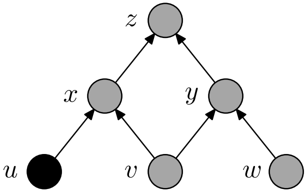



| Number of pebbles | |
|---|---|
| Current | 0 |
| Max so far | 0 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

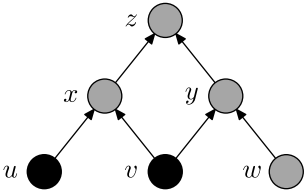



| Number of pebbles | |
|---|---|
| Current | 1 |
| Max so far | 1 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of *G*

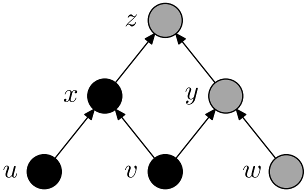



| Number of pebbles | |
|---|---|
| Current | 2 |
| Max so far | 2 |

1. Can place black pebble on (empty) vertex *v* if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from *v* if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

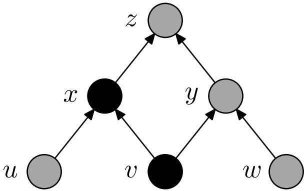



| Number of pebbles | |
|---|---|
| Current | 3 |
| Max so far | 3 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

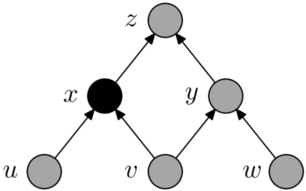



| Number of pebbles | |
|---|---|
| Current | 2 |
| Max so far | 3 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

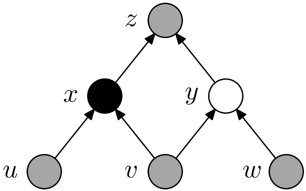



| Number of pebbles | |
|---|---|
| Current | 1 |
| Max so far | 3 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

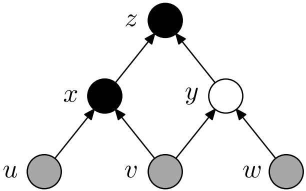



| Number of pebbles | |
|---|---|
| Current | 2 |
| Max so far | 3 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

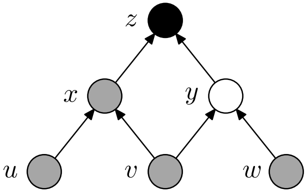



| Number of pebbles | |
|---|---|
| Current | 3 |
| Max so far | 3 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

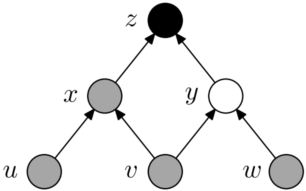



| Number of pebbles | |
|---|---|
| Current | 2 |
| Max so far | 3 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

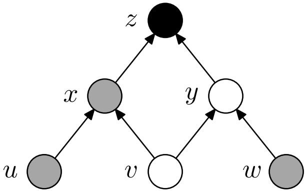



| Number of pebbles | |
|---|---|
| Current | 2 |
| Max so far | 3 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

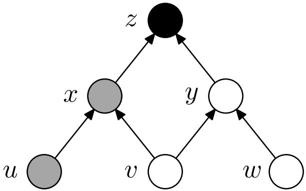



| Number of pebbles | |
|---|---|
| Current | 3 |
| Max so far | 3 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

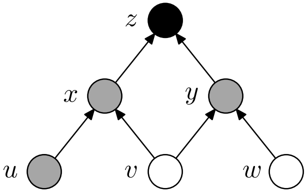



| Number of pebbles | |
|---|---|
| Current | 4 |
| Max so far | 4 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

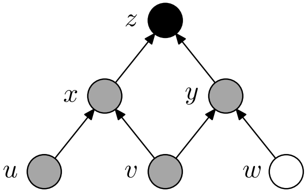



| Number of pebbles | |
|---|---|
| Current | 3 |
| Max so far | 4 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$

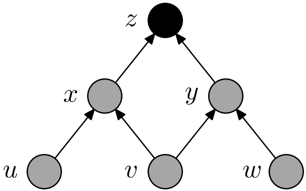



| Number of pebbles | |
|---|---|
| Current | 2 |
| Max so far | 4 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

# The Black-White Pebble Game

Goal: get single black pebble on sink vertex of $G$




| Number of pebbles | |
|---|---|
| Current | 1 |
| Max so far | 4 |

1. Can place black pebble on (empty) vertex $v$ if all immediate predecessors have pebbles on them
2. Can always remove black pebble from vertex
3. Can always place white pebble on (empty) vertex
4. Can remove white pebble from $v$ if all immediate predecessors have pebbles on them

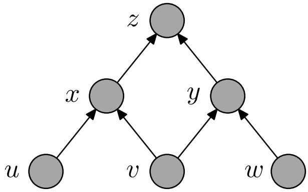
# Pebbling Price

- Cost of pebbling:
  max # pebbles simultaneously in $G$
  (in our example 4)
- Black-white pebbling price $\mathit{BW\text{-}Peb}(G)$ of DAG $G$:
  minimal cost of any pebbling
- Black pebbling price $\mathit{Peb}(G)$ of DAG $G$:
  minimal cost of any pebbling using black pebbles only
- Black pebbling price at most square of black-white pebbling price but known to coincide within multiplicative factor for many DAGs

# Pebbling Contradiction

CNF formula encoding pebble game on DAG $G$

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$




- sources are true
- truth propagates upwards
- but sink is false

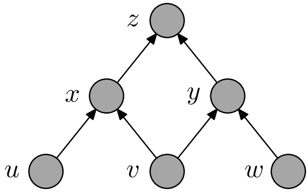
Studied by [Bonet et al. 1998, Raz & McKenzie 1999, Ben-Sasson & Wigderson 1999] and others

Our hope is that pebbling properties of DAG somehow carry over to resolution refutations of pebbling contradictions

# Pebbling Contradiction

CNF formula encoding pebble game on DAG $G$

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$




- sources are true
- truth propagates upwards
- but sink is false

Studied by [Bonet et al. 1998, Raz & McKenzie 1999, Ben-Sasson & Wigderson 1999] and others

Our hope is that pebbling properties of DAG somehow carry over to resolution refutations of pebbling contradictions

# Interpreting Refutations as Black-White Pebblings

Black-white pebbling models non-deterministic computation

- black pebbles ⇔ computed results
- white pebbles ⇔ guesses needing to be verified



"Know $z$ assuming $v$, $w$"

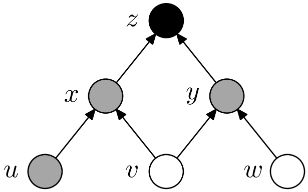
Corresponds to $(v \wedge w) \rightarrow z$, i.e., blackboard clause $\overline{v} \vee \overline{w} \vee z$

So translate clauses to pebbles by:
unnegated variable ⇒ black pebble
negated variable ⇒ white pebble

# Interpreting Refutations as Black-White Pebblings

Black-white pebbling models non-deterministic computation

- black pebbles ⇔ computed results
- white pebbles ⇔ guesses needing to be verified




"Know $z$ assuming $v$, $w$"

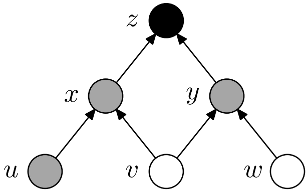
Corresponds to $(v \wedge w) \rightarrow z$, i.e., blackboard clause $\boxed{\overline{v} \vee \overline{w} \vee z}$

So translate clauses to pebbles by:
unnegated variable ⇒ black pebble
negated variable ⇒ white pebble

# Interpreting Refutations as Black-White Pebblings

Black-white pebbling models non-deterministic computation

- black pebbles ⇔ computed results
- white pebbles ⇔ guesses needing to be verified



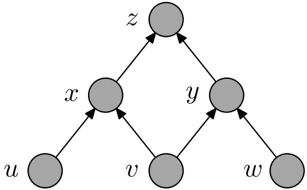

"Know $z$ assuming $v$, $w$"

Corresponds to $(v \land w) \rightarrow z$, i.e., blackboard clause $\overline{v} \lor \overline{w} \lor z$

So translate clauses to pebbles by:
unegated variable ⇒ black pebble
negated variable ⇒ white pebble

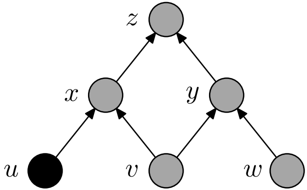
# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$



# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

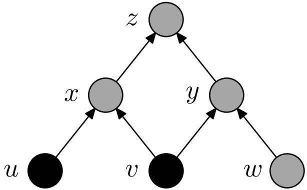



$u$

Write down axiom 1: $u$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

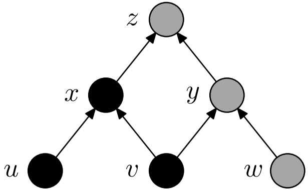



$u$
$v$

Write down axiom 2: $v$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

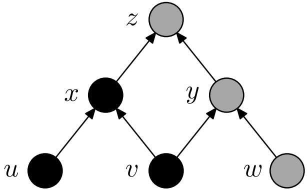



$u$
$v$
$\overline{u} \lor \overline{v} \lor x$

Write down axiom 4: $\overline{u} \lor \overline{v} \lor x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

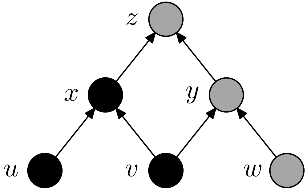



$u$
$v$
$\overline{u} \vee \overline{v} \vee x$

Infer $\overline{v} \vee x$ from
$u$ and $\overline{u} \vee \overline{v} \vee x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

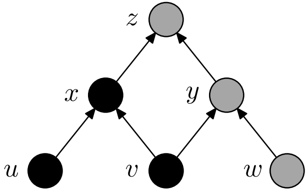



$u$
$v$
$\overline{u} \vee \overline{v} \vee x$
$\overline{v} \vee x$

Infer $\overline{v} \vee x$ from $u$ and $\overline{u} \vee \overline{v} \vee x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

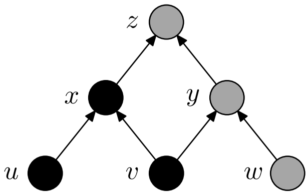



$u$
$v$
$\overline{u} \lor \overline{v} \lor x$
$\overline{v} \lor x$

Erase clause $\overline{u} \lor \overline{v} \lor x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

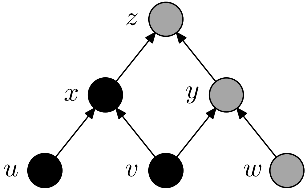



$u$
$v$
$\overline{v} \lor x$

Erase clause $\overline{u} \lor \overline{v} \lor x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

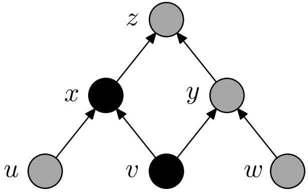



$u$
$v$
$\overline{v} \lor x$

Erase clause $u$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

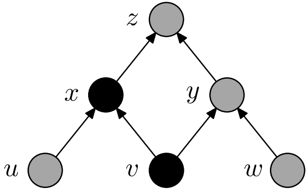



$v$
$\overline{v} \lor x$

Erase clause $u$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

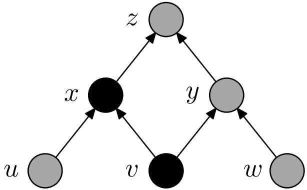



$v$
$\overline{v} \lor x$

Infer $x$ from $v$ and $\overline{v} \lor x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

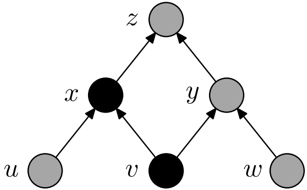



$v$
$\overline{v} \lor x$
$x$

Infer $x$ from
$v$ and $\overline{v} \lor x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

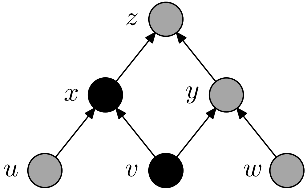



$v$
$\overline{v} \vee x$
$x$

Erase clause $\overline{v} \vee x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

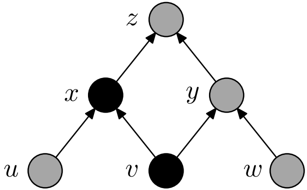



$v$
$x$

Erase clause $\overline{v} \lor x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

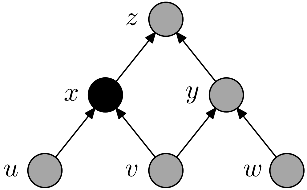


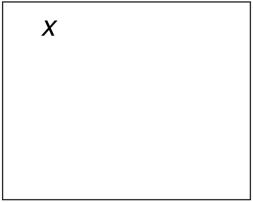

$v$
$x$

Erase clause $v$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

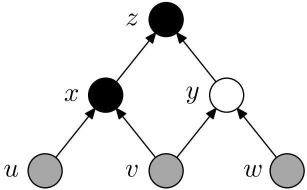



Erase clause $v$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

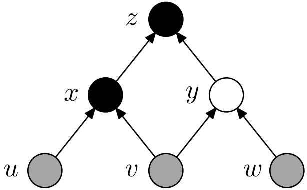



$x$
$\overline{x} \lor \overline{y} \lor z$

Write down axiom 6: $\overline{x} \lor \overline{y} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

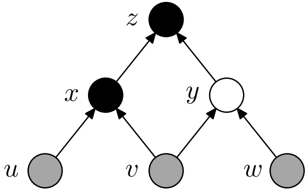



$x$
$\overline{x} \vee \overline{y} \vee z$

Infer $\overline{y} \vee z$ from $x$ and $\overline{x} \vee \overline{y} \vee z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

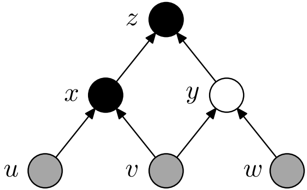



$x$
$\overline{x} \lor \overline{y} \lor z$
$\overline{y} \lor z$

Infer $\overline{y} \lor z$ from $x$ and $\overline{x} \lor \overline{y} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

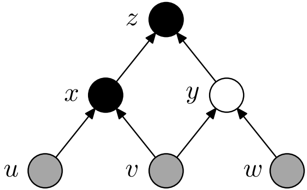



$x$
$\overline{x} \vee \overline{y} \vee z$
$\overline{y} \vee z$

Erase clause $\overline{x} \vee \overline{y} \vee z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

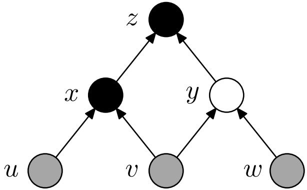



$x$
$\overline{y} \lor z$

Erase clause $\overline{x} \lor \overline{y} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

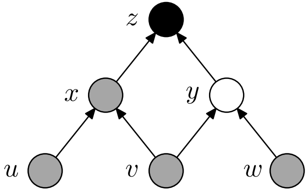



$x$
$\overline{y} \vee z$

Erase clause $x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

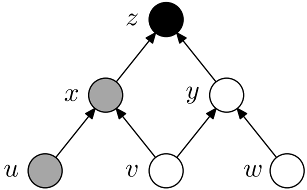



$\overline{y} \lor z$

Erase clause $x$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

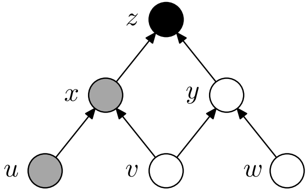



$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor y$

Write down axiom 5: $\overline{v} \lor \overline{w} \lor y$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$



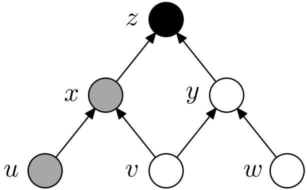

$\overline{y} \vee z$

$\overline{v} \vee \overline{w} \vee y$

Infer $\overline{v} \vee \overline{w} \vee z$ from $\overline{y} \vee z$ and $\overline{v} \vee \overline{w} \vee y$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

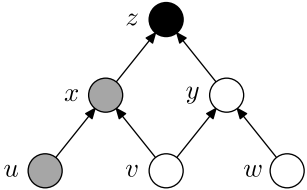



$\overline{y} \vee z$
$\overline{v} \vee \overline{w} \vee y$
$\overline{v} \vee \overline{w} \vee z$

Infer $\overline{v} \vee \overline{w} \vee z$ from $\overline{y} \vee z$ and $\overline{v} \vee \overline{w} \vee y$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

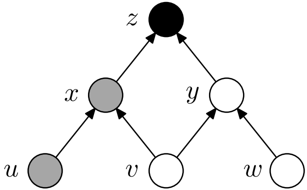



$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor y$
$\overline{v} \lor \overline{w} \lor z$

Erase clause $\overline{v} \lor \overline{w} \lor y$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

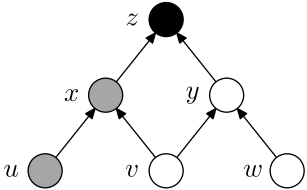



$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor z$

Erase clause $\overline{v} \lor \overline{w} \lor y$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

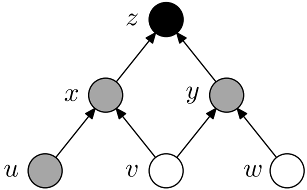



$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor z$

Erase clause $\overline{y} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

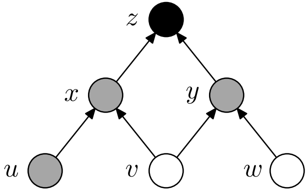



$\overline{v} \lor \overline{w} \lor z$

Erase clause $\overline{y} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

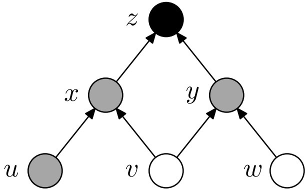



$\overline{v} \lor \overline{w} \lor z$
$v$

Write down axiom 2: $v$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

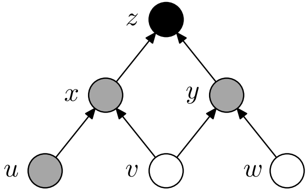



$\overline{v} \lor \overline{w} \lor z$
$v$
$w$

Write down axiom 3: $w$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

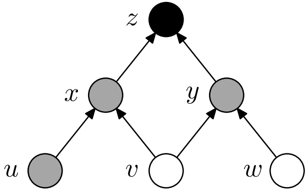



$\overline{v} \lor \overline{w} \lor z$
$v$
$w$
$\overline{z}$

Write down axiom 7: $\overline{z}$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

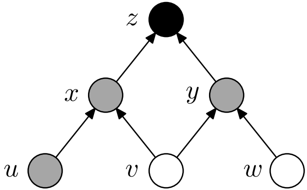



$\overline{v} \lor \overline{w} \lor z$
$v$
$w$
$\overline{z}$

Infer $\overline{w} \lor z$ from $v$ and $\overline{v} \lor \overline{w} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

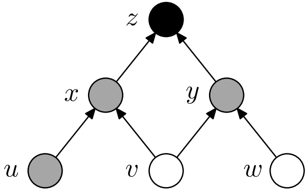



$\overline{v} \vee \overline{w} \vee z$
$v$
$w$
$\overline{z}$
$\overline{w} \vee z$

Infer $\overline{w} \vee z$ from $v$ and $\overline{v} \vee \overline{w} \vee z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

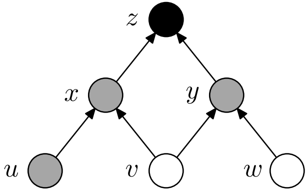



$\overline{v} \lor \overline{w} \lor z$
$v$
$w$
$\overline{z}$
$\overline{w} \lor z$

Erase clause $v$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

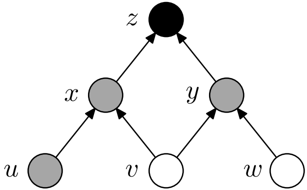



$\overline{v} \vee \overline{w} \vee z$
$w$
$\overline{z}$
$\overline{w} \vee z$

Erase clause $v$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

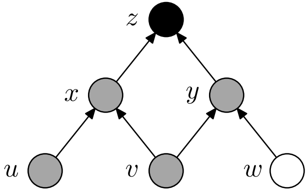



$\overline{v} \lor \overline{w} \lor z$
$w$
$\overline{z}$
$\overline{w} \lor z$

Erase clause $\overline{v} \lor \overline{w} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

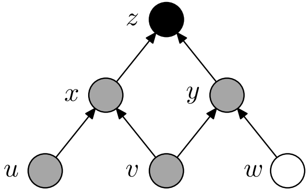



$w$
$\overline{z}$
$\overline{w} \lor z$

Erase clause $\overline{v} \lor \overline{w} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

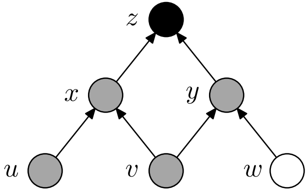



$w$
$\overline{z}$
$\overline{w} \lor z$

Infer $z$ from $w$ and $\overline{w} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

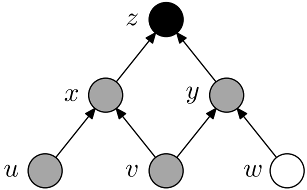



$w$
$\overline{z}$
$\overline{w} \lor z$
$z$

Infer $z$ from
$w$ and $\overline{w} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

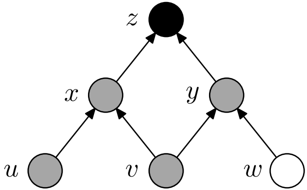



$w$
$\overline{z}$
$\overline{w} \lor z$
$z$

Erase clause $w$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

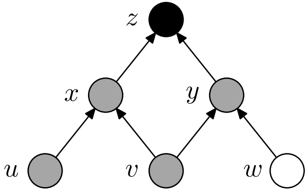



$\overline{z}$
$\overline{w} \lor z$
$z$

Erase clause $w$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

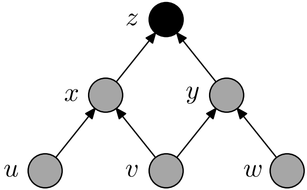



$\overline{z}$
$\overline{w} \lor z$
$z$

Erase clause $\overline{w} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

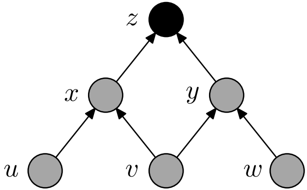



$\overline{z}$
$z$

Erase clause $\overline{w} \lor z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$

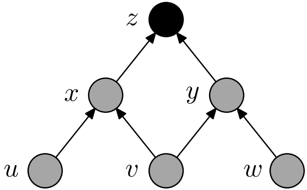



$\overline{z}$
$z$

Infer 0 from
$\overline{z}$ and $z$

# Example of Refutation-Pebbling Correspondence

1. $u$
2. $v$
3. $w$
4. $\overline{u} \vee \overline{v} \vee x$
5. $\overline{v} \vee \overline{w} \vee y$
6. $\overline{x} \vee \overline{y} \vee z$
7. $\overline{z}$




$\overline{z}$
$z$
0

Infer 0 from
$\overline{z}$ and $z$

# Formal Refutation-Pebbling Correspondence

**Theorem (Ben-Sasson 2002)**

*Any refutation translates into black-white pebbling with*

- *# moves $\leq$ refutation length*
- *# pebbles $\leq$ max # simultaneous variable occurrences*

**Theorem (Ben-Sasson et al. 2000)**

*Any black-only pebbling translates into refutation with*

- *refutation length $\leq$ # moves*
- *variable space $\leq$ # pebbles*

# Formal Refutation-Pebbling Correspondence

**Theorem (Ben-Sasson 2002)**

*Any refutation translates into black-white pebbling with*

- *# moves $\leq$ refutation length*
- *# pebbles $\leq$ max # simultaneous variable occurrences*

**Theorem (Ben-Sasson et al. 2000)**

*Any black-only pebbling translates into refutation with*

- *refutation length $\leq$ # moves*
- *variable space $\leq$ # pebbles*

# Then Along Comes the Substitution Space Theorem

Applying the Substitution Space Theorem

- lifts lower bound from variable occurrences to clause space
- maintains upper bound in terms of variable space

Get our results by

- using known pebbling results from literature of 70s and 80s
- proving a couple of new pebbling results
- to get tight trade-offs, showing that resolution proofs can sometimes do better than black-only pebblings

# Then Along Comes the Substitution Space Theorem

Applying the Substitution Space Theorem

- lifts lower bound from variable occurrences to clause space
- maintains upper bound in terms of variable space

Get our results by

- using known pebbling results from literature of 70s and 80s
- proving a couple of new pebbling results
- to get tight trade-offs, showing that resolution proofs can sometimes do better than black-only pebblings

# Lower Bounds on Variable Space?

**Open Question**

*Are there polynomial-size k-CNF formulas with variable refutation space* $\mathit{VarSp}(F \vdash 0) = \Omega\big((\mathit{size\ of\ } F)^2\big)$ *?*

Answer conjectured to be “yes” by (Alekhnovich et al. 2000)

Or can we at least prove a superlinear lower bound on variable space?

# Stronger Length-Space Trade-offs?

**Open Question**

*Are there superpolynomial trade-offs for formulas refutable in constant space?*

**Open Question**

*Are there formulas with trade-offs in the range space $>$ formula size? Or can every proof be carried out in at most linear space?*

Pebbling formulas cannot answer these questions—always refutable in linear time and linear space simultaneously

# Empirical Results?

**Open Question**

*Do our trade-off phenomena show up in real life for state-of-the-art SAT-solvers run on pebbling contradictions?*

(Possibly with some modifications to make easy proof somewhat harder to discover)

Or are pebbling formulas of all flavours always easy in practice?

# Summing up

- Optimal length-space separation in resolution
- Strong length-space trade-offs for wide range of parameters
- Many remaining open questions about space in resolution

Thank you for your attention!