Understanding the Hardness of Proving Formulas in Propositional Logic

Jakob Nordström

KTH Royal Institute of Technology
Stockholm, Sweden

Proof complexity workshop
Banff International Research Station, Canada
October 2–7, 2011

Joint work with Eli Ben-Sasson

A Fundamental Theoretical Problem. . .

Problem

Given a propositional logic formula F, is it true no matter how we assign values to its variables?

TAUTOLOGY: Fundamental problem in Theoretical Computer Science since Cook's NP-completeness paper (1971)

(And significance realized much earlier — cf. Gödel's letter 1956)

These days recognized as one of the main challenges for all of mathematics — one of the million dollar "Millennium Problems"

. . . with Huge Practical Implications

- All known algorithms run in exponential time in worst case
- But enormous progress on applied computer programs last 10-15 years
- These so-called SAT solvers are routinely deployed to solve large-scale real-world problems with millions of variables
- Used in e.g. hardware verification, software testing, software package management, artificial intelligence, cryptography, bioinformatics, and more
- But we also know small example formulas with only hundreds of variables that trip up even state-of-the-art SAT solvers

What Makes Formulas Hard or Easy?

- Best known algorithms based on simple DPLL method from 1960s (although with many clever optimizations)
- Corresponds to search algorithm for resolution proof system
- How can SAT solvers be so good in practice? And what explains whether a particular formula is tractable or too hard?
- Key bottlenecks for SAT solvers: time and memory
- What are the connections between these resources? Are they correlated? Are there trade-offs?
- This talk: What can proof complexity say about this? (For resolution and more general k-DNF resolution proof systems)

Outline

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

Some Notation and Terminology

- Literal a: variable x or its negation $\overline{x}$
- Clause $C = a_1 \vee \cdots \vee a_k$: disjunction of literals
- Term $T = a_1 \wedge \cdots \wedge a_k$: conjunction of literals
- CNF formula $F = C_1 \wedge \cdots \wedge C_m$: conjunction of clauses
  k-CNF formula: CNF formula with clauses of size $\leq k$
- DNF formula $D = T_1 \vee \cdots \vee T_m$: disjunction of terms
  k-DNF formula: DNF formula with terms of size $\leq k$
- All CNF formulas assumed to have clauses of size $\mathcal{O}(1)$ throughout this talk

k-DNF Resolution

- Prove that given CNF formula is unsatisfiable
- Proof operates with k-DNF formulas (standard resolution corresponds to 1-DNF formulas, i.e., disjunctive clauses)
- Proof is "presented on blackboard"
- Derivation steps:
  - Write down clauses of CNF formula being refuted (axiom clauses)
  - Infer new k-DNF formulas
  - Erase formulas that are not currently needed (to save space on blackboard)
- Proof ends when contradictory empty clause 0 derived

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \lor y$
3. $\overline{y} \lor z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$\boxed{x}$

Write down axiom 1: x

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

---

x

$\overline{y} \vee z$

Write down axiom 1: x

Write down axiom 3: $\overline{y} \vee z$

Example 2-DNF Resolution Refutation

Can write down axioms,
infer new formulas, and
erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

x
$\overline{y} \vee z$

Write down axiom 1: x
Write down axiom 3: $\overline{y} \vee z$
Combine x and $\overline{y} \vee z$
to get $(x \wedge \overline{y}) \vee z$

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$$\begin{array}{l} x \\ \overline{y} \vee z \\ (x \wedge \overline{y}) \vee z \end{array}$$

Write down axiom 1: x
Write down axiom 3: $\overline{y} \vee z$
Combine x and $\overline{y} \vee z$
to get $(x \wedge \overline{y}) \vee z$

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$$\begin{array}{|l|} \hline x \\ \overline{y} \vee z \\ (x \wedge \overline{y}) \vee z \\ \hline \end{array}$$

Write down axiom 1: x
Write down axiom 3: $\overline{y} \vee z$
Combine x and $\overline{y} \vee z$
to get $(x \wedge \overline{y}) \vee z$
Erase the line x

Example 2-DNF Resolution Refutation

Can write down axioms,
infer new formulas, and
erase used formulas

1. x
2. $\overline{x} \lor y$
3. $\overline{y} \lor z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$\overline{y} \lor z$
$(x \land \overline{y}) \lor z$

Write down axiom 1: x
Write down axiom 3: $\overline{y} \lor z$
Combine x and $\overline{y} \lor z$
to get $(x \land \overline{y}) \lor z$
Erase the line x

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$\overline{y} \vee z$
$(x \wedge \overline{y}) \vee z$

Write down axiom 3: $\overline{y} \vee z$
Combine x and $\overline{y} \vee z$
to get $(x \wedge \overline{y}) \vee z$
Erase the line x
Erase the line $\overline{y} \vee z$

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$(x \wedge \overline{y}) \vee z$

Write down axiom 3: $\overline{y} \vee z$
Combine x and $\overline{y} \vee z$
to get $(x \wedge \overline{y}) \vee z$
Erase the line x
Erase the line $\overline{y} \vee z$

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \lor y$
3. $\overline{y} \lor z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$$(x \land \overline{y}) \lor z$$
$$\overline{x} \lor y$$

Combine x and $\overline{y} \lor z$
to get $(x \land \overline{y}) \lor z$
Erase the line x
Erase the line $\overline{y} \lor z$
Write down axiom 2: $\overline{x} \lor y$

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$(x \wedge \overline{y}) \vee z$
$\overline{x} \vee y$

Erase the line x
Erase the line $\overline{y} \vee z$
Write down axiom 2: $\overline{x} \vee y$
Infer z from
$\overline{x} \vee y$ and $(x \wedge \overline{y}) \vee z$

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$(x \wedge \overline{y}) \vee z$
$\overline{x} \vee y$
z

Erase the line x
Erase the line $\overline{y} \vee z$
Write down axiom 2: $\overline{x} \vee y$
Infer z from
$\overline{x} \vee y$ and $(x \wedge \overline{y}) \vee z$

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \lor y$
3. $\overline{y} \lor z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$(x \land \overline{y}) \lor z$
$\overline{x} \lor y$
z

Erase the line $\overline{y} \lor z$
Write down axiom 2: $\overline{x} \lor y$
Infer z from
$\overline{x} \lor y$ and $(x \land \overline{y}) \lor z$
Erase the line $(x \land \overline{y}) \lor z$

Example 2-DNF Resolution Refutation

Can write down axioms,
infer new formulas, and
erase used formulas

1. x
2. $\overline{x} \lor y$
3. $\overline{y} \lor z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$\overline{x} \lor y$

z

Erase the line $\overline{y} \lor z$
Write down axiom 2: $\overline{x} \lor y$
Infer z from
$\overline{x} \lor y$ and $(x \land \overline{y}) \lor z$
Erase the line $(x \land \overline{y}) \lor z$

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$\overline{x} \vee y$
z

Write down axiom 2: $\overline{x} \vee y$
Infer z from
$\overline{x} \vee y$ and $(x \wedge \overline{y}) \vee z$
Erase the line $(x \wedge \overline{y}) \vee z$
Erase the line $\overline{x} \vee y$

Example 2-DNF Resolution Refutation

Can write down axioms,
infer new formulas, and
erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

---

z

Write down axiom 2: $\overline{x} \vee y$
Infer z from
$\overline{x} \vee y$ and $(x \wedge \overline{y}) \vee z$
Erase the line $(x \wedge \overline{y}) \vee z$
Erase the line $\overline{x} \vee y$

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

$$\boxed{\begin{array}{l} z \\ \overline{z} \end{array}}$$

Infer z from
$\overline{x} \vee y$ and $(x \wedge \overline{y}) \vee z$
Erase the line $(x \wedge \overline{y}) \vee z$
Erase the line $\overline{x} \vee y$
Write down axiom 4: $\overline{z}$

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

---

z

$\overline{z}$

Erase the line $(x \wedge \overline{y}) \vee z$

Erase the line $\overline{x} \vee y$

Write down axiom 4: $\overline{z}$

Infer 0 from

$\overline{z}$ and z

Example 2-DNF Resolution Refutation

Can write down axioms, infer new formulas, and erase used formulas

1. x
2. $\overline{x} \vee y$
3. $\overline{y} \vee z$
4. $\overline{z}$

Rules:

- Infer new formulas only from formulas currently on board
- Only k-DNF formulas can appear on board (for $k = 2$)
- Details about derivation rules won't matter for us

---

z
$\overline{z}$
0

Erase the line $(x \wedge \overline{y}) \vee z$
Erase the line $\overline{x} \vee y$
Write down axiom 4: $\overline{z}$
Infer 0 from
$\overline{z}$ and z

Complexity Measures of Interest: Length and Space

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

Length

\# formulas written on blackboard counted with repetitions

Space

Somewhat less straightforward — several ways of measuring

$$x$$
$$\overline{y} \lor z$$
$$(x \land \overline{y}) \lor z$$

Formula space:	3
Total space:	6
Variable space:	3

Complexity Measures of Interest: Length and Space

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

Length

\# formulas written on blackboard counted with repetitions

Space

Somewhat less straightforward — several ways of measuring

$$x$$
$$\overline{y} \lor z$$
$$(x \land \overline{y}) \lor z$$

Formula space: 3
Total space: 6
Variable space: 3

Complexity Measures of Interest: Length and Space

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

Length

$\#$ formulas written on blackboard counted with repetitions

Space

Somewhat less straightforward — several ways of measuring

$$\begin{array}{l} x \\ \overline{y} \lor z \\ (x \land \overline{y}) \lor z \end{array}$$

Formula space:	3
Total space:	6
Variable space:	3

Complexity Measures of Interest: Length and Space

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

Length

formulas written on blackboard counted with repetitions

Space

Somewhat less straightforward — several ways of measuring

1. x
2. $\overline{y} \lor z$
3. $(x \land \overline{y}) \lor z$

Formula space: 3
Total space: 6
Variable space: 3

Complexity Measures of Interest: Length and Space

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

Length

\# formulas written on blackboard counted with repetitions

Space

Somewhat less straightforward — several ways of measuring

$$\boxed{\begin{array}{l} x^{1} \\ \overline{y}^{2} \vee z^{3} \\ (x^{4} \wedge \overline{y})^{5} \vee z^{6} \end{array}}$$

Formula space:	3
Total space:	6
Variable space:	3

Complexity Measures of Interest: Length and Space

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

Length

\# formulas written on blackboard counted with repetitions

Space

Somewhat less straightforward — several ways of measuring

$$\boxed{\begin{array}{l} x^{1} \\ \overline{y}^{2} \vee z^{3} \\ (x \wedge \overline{y}) \vee z \end{array}}$$

Formula space:	3
Total space:	6
Variable space:	3

Complexity Measures of Interest: Length and Space

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

Length

\# formulas written on blackboard counted with repetitions

Space

Somewhat less straightforward — several ways of measuring

$$\boxed{\begin{array}{l} x \\ \overline{y} \lor z \\ (x \land \overline{y}) \lor z \end{array}}$$

Formula space:	3
Total space:	6
Variable space:	3

Length and Space Bounds for Resolution

Let n = size of formula

Length: at most 2^n
Lower bound $\exp(\Omega(n))$ [Urquhart '87, Chvátal & Szemerédi '88]

Formula space (a.k.a. clause space): at most n
Lower bound $\Omega(n)$ [Torán '99, Alekhnovich et al. '00]

Total space: at most n^2
No better lower bound than $\Omega(n)$!?

[Sidenote: space bounds hold even for "magic algorithms" always making optimal choices — so might be much stronger in practice]

Comparing Length and Space

Some "rescaling" needed to get meaningful comparisons of length and space

- Length exponential in formula size in worst case
- Formula space at most linear
- So natural to compare space to logarithm of length

Length-Space Correlation for Resolution?

$\exists$ constant space refutation $\Rightarrow$ $\exists$ polynomial length refutation [Atserias & Dalmau '03]

For tree-like resolution: any polynomial length refutation can be carried out in logarithmic space [Esteban & Torán '99]

So essentially no trade-offs for tree-like resolution

Does short length imply small space for general resolution? Has been open — even no consensus on likely "right answer"

Length-Space Correlation for Resolution?

$\exists$ constant space refutation $\Rightarrow$ $\exists$ polynomial length refutation [Atserias & Dalmau '03]

For tree-like resolution: any polynomial length refutation can be carried out in logarithmic space [Esteban & Torán '99]

So essentially no trade-offs for tree-like resolution

Does short length imply small space for general resolution?
Has been open — even no consensus on likely "right answer"

Length-Space Correlation for Resolution?

$\exists$ constant space refutation $\Rightarrow$ $\exists$ polynomial length refutation [Atserias & Dalmau '03]

For tree-like resolution: any polynomial length refutation can be carried out in logarithmic space [Esteban & Torán '99]

So essentially no trade-offs for tree-like resolution

Does short length imply small space for general resolution?
Has been open — even no consensus on likely "right answer"

Length-Space Trade-offs for Resolution?

Nothing known about length-space trade-offs for resolution refutations in the general, unrestricted proof system

(Some trade-off results in restricted settings in [Ben-Sasson '02, Nordström '07])

Previous Work on k-DNF Resolution ($k \geq 2$)

Length: lower bound $\exp\bigl(\Omega\bigl(n^{1-o(1)}\bigr)\bigr)$ [Segerlind et al. '04, Alekhnovich '05]

Formula space: lower bound $\Omega(n)$ [Esteban et al. '02]

(Suppressing dependencies on k)

(k+1)-DNF resolution exponentially stronger than k-DNF resolution w.r.t. length [Segerlind et al. '04]

No hierarchy known w.r.t. space
Except for tree-like k-DNF resolution [Esteban et al. '02]
(But tree-like k-DNF weaker than standard resolution)

No trade-off results known

Previous Work on k-DNF Resolution ($k \geq 2$)

Length: lower bound $\exp\left(\Omega\left(n^{1-o(1)}\right)\right)$ [Segerlind et al. '04, Alekhnovich '05]

Formula space: lower bound $\Omega(n)$ [Esteban et al. '02]

(Suppressing dependencies on k)

(k+1)-DNF resolution exponentially stronger than k-DNF resolution w.r.t. length [Segerlind et al. '04]

No hierarchy known w.r.t. space
Except for tree-like k-DNF resolution [Esteban et al. '02]
(But tree-like k-DNF weaker than standard resolution)

No trade-off results known

Previous Work on k-DNF Resolution ($k \geq 2$)

Length: lower bound $\exp\bigl(\Omega\bigl(n^{1-o(1)}\bigr)\bigr)$ [Segerlind et al. '04, Alekhnovich '05]

Formula space: lower bound $\Omega\bigl(n\bigr)$ [Esteban et al. '02]

(Suppressing dependencies on k)

(k+1)-DNF resolution exponentially stronger than k-DNF resolution w.r.t. length [Segerlind et al. '04]

No hierarchy known w.r.t. space
Except for tree-like k-DNF resolution [Esteban et al. '02]
(But tree-like k-DNF weaker than standard resolution)

No trade-off results known

Our results 1: An Optimal Length-Space Separation

Length and space in resolution are "completely uncorrelated"

Theorem (Ben-Sasson & Nordström, FOCS '08)

There are k-CNF formula families of size $\mathcal{O}(n)$ with

- *refutation length $\mathcal{O}(n)$ requiring*
- *formula space $\Omega(n/\log n)$.*

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

Our Results 2: Length-Space Trade-offs

We prove collection of length-space trade-offs

Results hold for

- resolution (essentially tight analysis)
- k-DNF resolution, $k \geq 2$ (with slightly worse parameters)

Different trade-offs covering (almost) whole range of space from constant to linear

Simple, explicit formulas

Example 1: Robust Trade-offs for Small Space

Theorem (Ben-Sasson & Nordström, ICS '11)

For any $\omega(1)$ function and any fixed K there exist explicit CNF formulas of size $\mathcal{O}(n)$

- *refutable in resolution in total space $\omega(1)$*
- *refutable in resolution in length $\mathcal{O}(n)$ and total space $\approx \sqrt[3]{n}$*
- *any resolution refutation in formula space $\ll \sqrt[3]{n}$ requires superpolynomial length*
- *any k-DNF resolution refutation, $k \leq K$, in formula space $\ll n^{1/3(k+1)}$ requires superpolynomial length*

Example 1: Robust Trade-offs for Small Space

Theorem (Ben-Sasson & Nordström, ICS '11)

For any $\omega(1)$ function and any fixed K there exist explicit CNF formulas of size $\mathcal{O}(n)$

- *refutable in resolution in total space $\omega(1)$*
- *refutable in resolution in length $\mathcal{O}(n)$ and total space $\approx \sqrt[3]{n}$*
- *any resolution refutation in formula space $\ll \sqrt[3]{n}$ requires superpolynomial length*
- *any k-DNF resolution refutation, $k \leq K$, in formula space $\ll n^{1/3(k+1)}$ requires superpolynomial length*

Example 1: Robust Trade-offs for Small Space

Theorem (Ben-Sasson & Nordström, ICS '11)

For any $\omega(1)$ function and any fixed K there exist explicit CNF formulas of size $\mathcal{O}(n)$

- *refutable in resolution in total space $\omega(1)$*
- *refutable in resolution in length $\mathcal{O}(n)$ and total space $\approx \sqrt[3]{n}$*
- *any resolution refutation in formula space $\ll \sqrt[3]{n}$ requires superpolynomial length*
- *any k-DNF resolution refutation, $k \leq K$, in formula space $\ll n^{1/3(k+1)}$ requires superpolynomial length*

Example 1: Robust Trade-offs for Small Space

Theorem (Ben-Sasson & Nordström, ICS '11)

For any $\omega(1)$ function and any fixed K there exist explicit CNF formulas of size $\mathcal{O}(n)$

- *refutable in resolution in total space $\omega(1)$*
- *refutable in resolution in length $\mathcal{O}(n)$ and total space $\approx \sqrt[3]{n}$*
- *any resolution refutation in formula space $\ll \sqrt[3]{n}$ requires superpolynomial length*
- *any k-DNF resolution refutation, $k \leq K$, in formula space $\ll n^{1/3(k+1)}$ requires superpolynomial length*

Example 1: Robust Trade-offs for Small Space

Theorem (Ben-Sasson & Nordström, ICS '11)

For any $\omega(1)$ function and any fixed K there exist explicit CNF formulas of size $\mathcal{O}(n)$

- *refutable in resolution in total space $\omega(1)$*
- *refutable in resolution in length $\mathcal{O}(n)$ and total space $\approx \sqrt[3]{n}$*
- *any resolution refutation in formula space $\ll \sqrt[3]{n}$ requires superpolynomial length*
- *any k-DNF resolution refutation, $k \leq K$, in formula space $\ll n^{1/3(k+1)}$ requires superpolynomial length*

Some Quick Technical Remarks

Upper bounds hold for

- total space (# literals) — larger measure
- standard syntactic rules

Lower bounds hold for

- formula space (# lines) — smaller measure
- semantic rules — exponentially stronger than syntactic

Space definition reminder

$$\boxed{\begin{array}{l} x \\ \overline{y} \vee z \\ (x \wedge \overline{y}) \vee z \end{array}}$$

Formula space: 3
Total space: 6
Variable space: 3

Our Results 3: Space Hierarchy for k-DNF Resolution

We also separate k-DNF resolution from $(k+1)$-DNF resolution w.r.t. formula space

Theorem (Ben-Sasson & Nordström, ICS '11)

For any constant k there are explicit CNF formulas of size $\mathcal{O}(n)$

- *refutable in $(k+1)$-DNF resolution in formula space $\mathcal{O}(1)$ but such that*
- *any k-DNF resolution refutation requires formula space $\Omega\left(\sqrt[k+1]{n/\log n}\right)$*

Rest of This Talk

- Study old combinatorial game from the 70s and 80s
- Prove new theorem about amplification of space hardness via variable substitution
- Combine the two

How to Get a Handle on Time-Space Relations?

Want to find formulas that

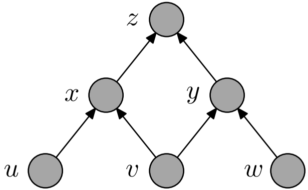
- can be quickly refuted but require large space
- have space-efficient refutations requiring much time

Such time-space trade-off questions well-studied for pebble games modelling calculations described by DAGs ([Cook & Sethi '76] 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

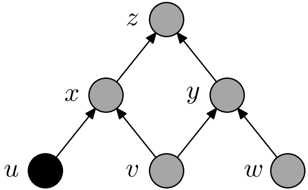


# moves	0
Current # pebbles	0
Max # pebbles so far	0

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

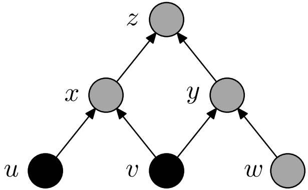


# moves	1
Current # pebbles	1
Max # pebbles so far	1

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

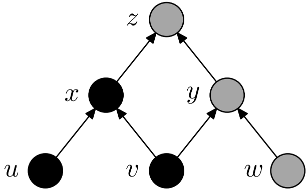


# moves	2
Current # pebbles	2
Max # pebbles so far	2

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

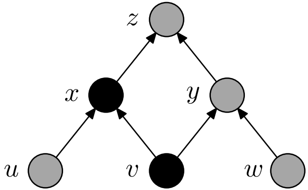


# moves	3
Current # pebbles	3
Max # pebbles so far	3

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

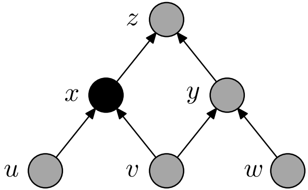


# moves	4
Current # pebbles	2
Max # pebbles so far	3

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

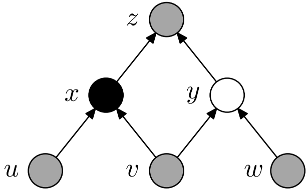


# moves	5
Current # pebbles	1
Max # pebbles so far	3

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

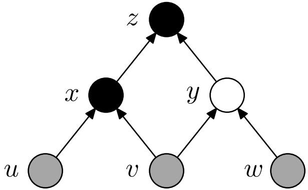


# moves	6
Current # pebbles	2
Max # pebbles so far	3

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

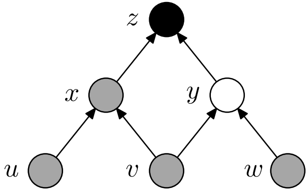


# moves	7
Current # pebbles	3
Max # pebbles so far	3

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

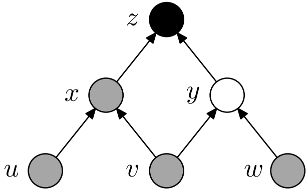


# moves	8
Current # pebbles	2
Max # pebbles so far	3

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

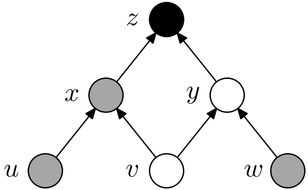


# moves	8
Current # pebbles	2
Max # pebbles so far	3

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

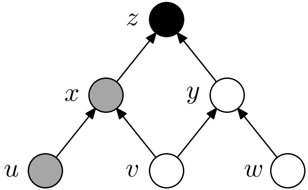


# moves	9
Current # pebbles	3
Max # pebbles so far	3

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

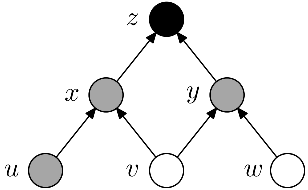


# moves	10
Current # pebbles	4
Max # pebbles so far	4

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

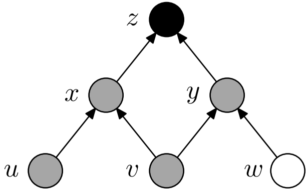


# moves	11
Current # pebbles	3
Max # pebbles so far	4

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G

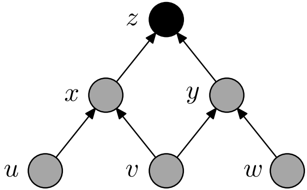


# moves	12
Current # pebbles	2
Max # pebbles so far	4

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

The Black-White Pebble Game

Goal: get single black pebble on sink vertex of G



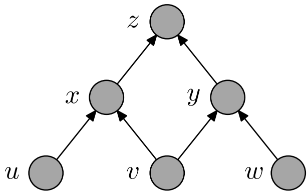
# moves	13
Current # pebbles	1
Max # pebbles so far	4

1. Can place black pebble on (empty) vertex v if all predecessors (vertices with edges to v) 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 if all predecessors have pebbles

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

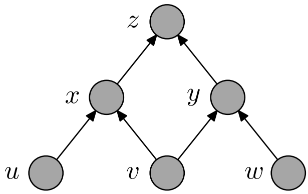
Studied by [Bonet et al. '98, Raz & McKenzie '99, Ben-Sasson & Wigderson '99] and others

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



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

Studied by [Bonet et al. '98, Raz & McKenzie '99, Ben-Sasson & Wigderson '99] 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 $\Leftrightarrow$ computed results
- white pebbles $\Leftrightarrow$ guesses needing to be verified

"Know z assuming v, w"

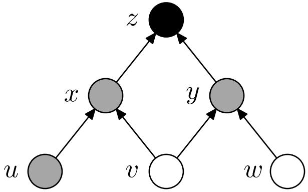
Corresponds to $(v \wedge w) \rightarrow z$, i.e., blackboard clause $\boxed{\overline{v} \vee \overline{w} \vee z}$

So translate clauses to pebbles by:
unnegated variable $\Rightarrow$ black pebble
negated variable $\Rightarrow$ white pebble

Interpreting Refutations as Black-White Pebblings

Black-white pebbling models non-deterministic computation

- black pebbles $\Leftrightarrow$ computed results
- white pebbles $\Leftrightarrow$ guesses needing to be verified



"Know z assuming v, w"

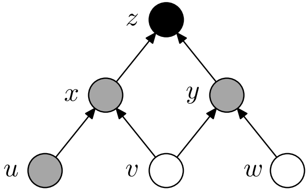
Corresponds to $(v \wedge w) \rightarrow z$, i.e., blackboard clause $\boxed{\overline{v} \vee \overline{w} \vee z}$

So translate clauses to pebbles by:
unnegated variable $\Rightarrow$ black pebble
negated variable $\Rightarrow$ white pebble

Interpreting Refutations as Black-White Pebblings

Black-white pebbling models non-deterministic computation

- black pebbles $\Leftrightarrow$ computed results
- white pebbles $\Leftrightarrow$ guesses needing to be verified



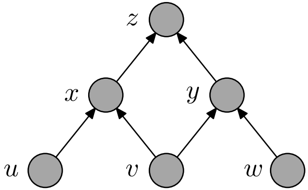
"Know z assuming v, w"

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:
unegated variable $\Rightarrow$ black pebble
negated variable $\Rightarrow$ white pebble

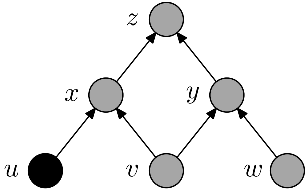
Example of Refutation-Pebbling Correspondence

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

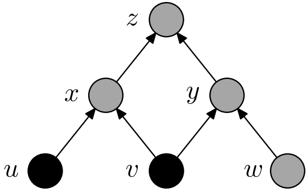


u

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

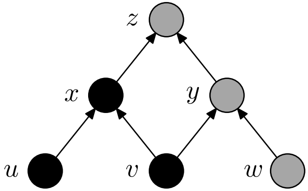
v

Write down axiom 1: u

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

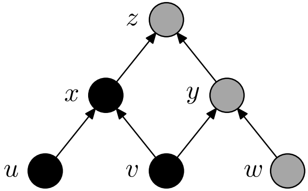
v

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

Write down axiom 1: u
Write down axiom 2: v
Write down axiom 4: $\overline{u} \lor \overline{v} \lor x$

Example of Refutation-Pebbling Correspondence

1. u
2. v
3. w
4. $\overline{u} \lor \overline{v} \lor x$
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 1: u

Write down axiom 2: v

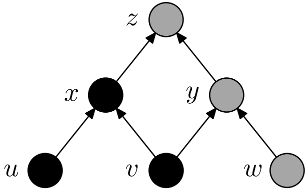
Write down axiom 4: $\overline{u} \lor \overline{v} \lor x$

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

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

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. $\overline{z}$



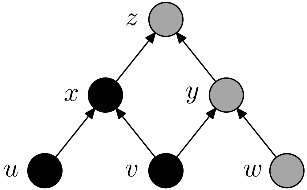
---

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

Write down axiom 1: u
Write down axiom 2: v
Write down axiom 4: $\overline{u} \lor \overline{v} \lor x$
Infer $\overline{v} \lor x$ from
u and $\overline{u} \lor \overline{v} \lor x$

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. $\overline{z}$



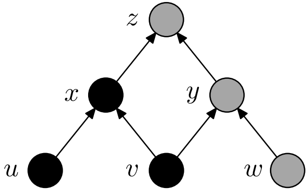
---

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

Write down axiom 2: v
Write down axiom 4: $\overline{u} \lor \overline{v} \lor x$
Infer $\overline{v} \lor x$ from
u and $\overline{u} \lor \overline{v} \lor x$
Erase the 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

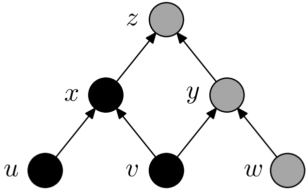
v

$\overline{v} \lor x$

Write down axiom 2: v
Write down axiom 4: $\overline{u} \lor \overline{v} \lor x$
Infer $\overline{v} \lor x$ from
u and $\overline{u} \lor \overline{v} \lor x$
Erase the 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. $\overline{z}$



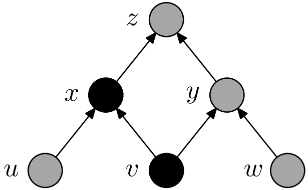
---

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

Write down axiom 4: $\overline{u} \lor \overline{v} \lor x$
Infer $\overline{v} \lor x$ from
u and $\overline{u} \lor \overline{v} \lor x$
Erase the clause $\overline{u} \lor \overline{v} \lor x$
Erase the 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

$\overline{v} \lor x$

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

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

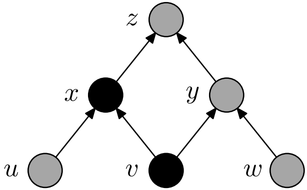
u and $\overline{u} \lor \overline{v} \lor x$

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

Erase the 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. $\overline{z}$



---

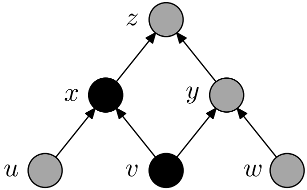
v

$\overline{v} \lor x$

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

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

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

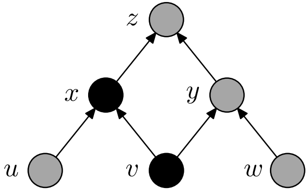
Erase the clause u

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

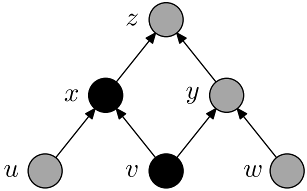
$\overline{v} \lor x$

x

Erase the clause $\overline{u} \lor \overline{v} \lor x$
Erase the clause u
Infer x from
v and $\overline{v} \lor x$
Erase the 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. $\overline{z}$

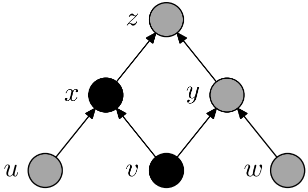


v
x

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

Infer x from

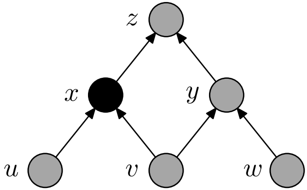
v and $\overline{v} \lor x$

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

Erase the 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. $\overline{z}$



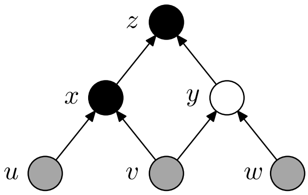
---

x

Erase the clause u
Infer x from
v and $\overline{v} \lor x$
Erase the clause $\overline{v} \lor x$
Erase the 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. $\overline{z}$



---

x

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

Infer x from

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

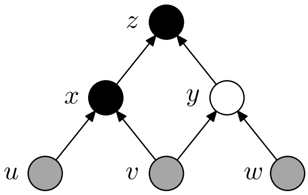
Erase the clause $\overline{v} \vee x$

Erase the clause v

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

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. $\overline{z}$



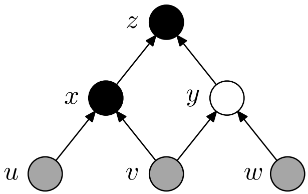
---

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

Erase the clause $\overline{v} \lor x$
Erase the clause v
Write down axiom 6: $\overline{x} \lor \overline{y} \lor z$
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. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$



---

x

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

$\overline{y} \lor z$

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

Erase the clause v

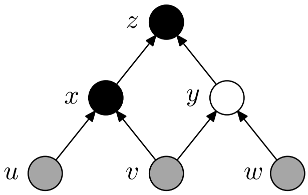
Write down axiom 6: $\overline{x} \lor \overline{y} \lor z$

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



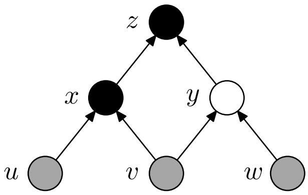
---

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

Erase the clause v
Write down axiom 6: $\overline{x} \lor \overline{y} \lor z$
Infer $\overline{y} \lor z$ from
x and $\overline{x} \lor \overline{y} \lor z$
Erase the clause $\overline{x} \lor \overline{y} \lor z$

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. $\overline{z}$



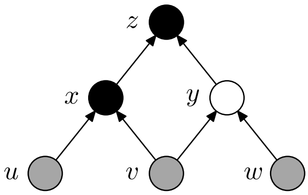
---

x
$\overline{y} \lor z$

Erase the clause v
Write down axiom 6: $\overline{x} \lor \overline{y} \lor z$
Infer $\overline{y} \lor z$ from
x and $\overline{x} \lor \overline{y} \lor z$
Erase the clause $\overline{x} \lor \overline{y} \lor z$

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. $\overline{z}$



x

$\overline{y} \lor z$

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

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

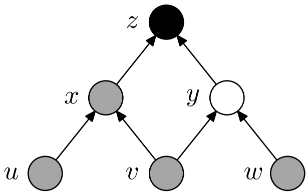
x and $\overline{x} \lor \overline{y} \lor z$

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

Erase the 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. $\overline{z}$

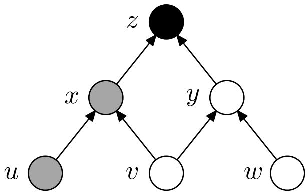


$\overline{y} \lor z$

Write down axiom 6: $\overline{x} \lor \overline{y} \lor z$
Infer $\overline{y} \lor z$ from
x and $\overline{x} \lor \overline{y} \lor z$
Erase the clause $\overline{x} \lor \overline{y} \lor z$
Erase the clause 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. $\overline{z}$

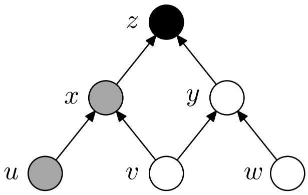


$\overline{y} \vee z$
$\overline{v} \vee \overline{w} \vee y$

Infer $\overline{y} \vee z$ from
x and $\overline{x} \vee \overline{y} \vee z$
Erase the clause $\overline{x} \vee \overline{y} \vee z$
Erase the clause x
Write down axiom 5: $\overline{v} \vee \overline{w} \vee y$

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. $\overline{z}$



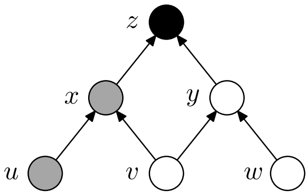
$\overline{y} \lor z$

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

Erase the clause $\overline{x} \lor \overline{y} \lor z$
Erase the clause x
Write down axiom 5: $\overline{v} \lor \overline{w} \lor y$
Infer $\overline{v} \lor \overline{w} \lor z$ from
$\overline{y} \lor z$ and $\overline{v} \lor \overline{w} \lor y$

Example 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. $\overline{z}$

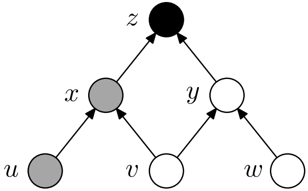


$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor y$
$\overline{v} \lor \overline{w} \lor z$

Erase the clause $\overline{x} \lor \overline{y} \lor z$
Erase the clause x
Write down axiom 5: $\overline{v} \lor \overline{w} \lor y$
Infer $\overline{v} \lor \overline{w} \lor z$ from
$\overline{y} \lor z$ and $\overline{v} \lor \overline{w} \lor y$

Example 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. $\overline{z}$

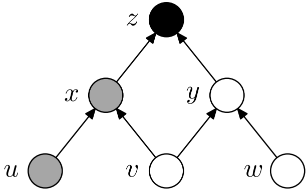


$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor y$
$\overline{v} \lor \overline{w} \lor z$

Erase the clause x
Write down axiom 5: $\overline{v} \lor \overline{w} \lor y$
Infer $\overline{v} \lor \overline{w} \lor z$ from
$\overline{y} \lor z$ and $\overline{v} \lor \overline{w} \lor y$
Erase the 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. $\overline{z}$

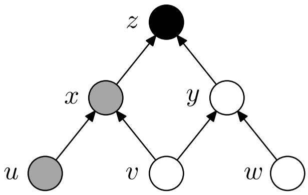


$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor z$

Erase the clause x
Write down axiom 5: $\overline{v} \lor \overline{w} \lor y$
Infer $\overline{v} \lor \overline{w} \lor z$ from
$\overline{y} \lor z$ and $\overline{v} \lor \overline{w} \lor y$
Erase the 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. $\overline{z}$

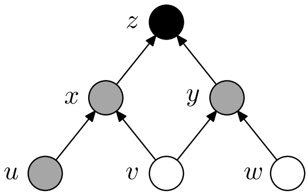


$\overline{y} \lor z$
$\overline{v} \lor \overline{w} \lor z$

Write down axiom 5: $\overline{v} \lor \overline{w} \lor y$
Infer $\overline{v} \lor \overline{w} \lor z$ from
$\overline{y} \lor z$ and $\overline{v} \lor \overline{w} \lor y$
Erase the clause $\overline{v} \lor \overline{w} \lor y$
Erase the 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. $\overline{z}$

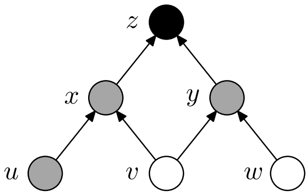


$\overline{v} \lor \overline{w} \lor z$

Write down axiom 5: $\overline{v} \lor \overline{w} \lor y$
Infer $\overline{v} \lor \overline{w} \lor z$ from
$\overline{y} \lor z$ and $\overline{v} \lor \overline{w} \lor y$
Erase the clause $\overline{v} \lor \overline{w} \lor y$
Erase the clause $\overline{y} \lor z$

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. $\overline{z}$



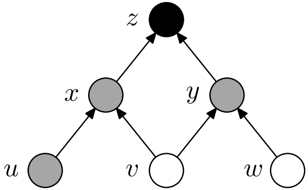
$\overline{v} \vee \overline{w} \vee z$

v

Infer $\overline{v} \vee \overline{w} \vee z$ from
$\overline{y} \vee z$ and $\overline{v} \vee \overline{w} \vee y$
Erase the clause $\overline{v} \vee \overline{w} \vee y$
Erase the clause $\overline{y} \vee z$
Write down axiom 2: 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. $\overline{z}$



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

v

w

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

Erase the clause $\overline{v} \vee \overline{w} \vee y$

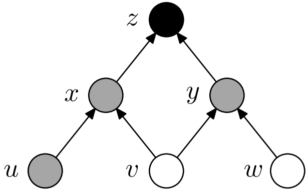
Erase the clause $\overline{y} \vee z$

Write down axiom 2: v

Write down axiom 3: w

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

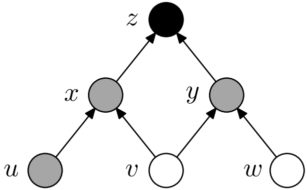
w

$\overline{z}$

Erase the clause $\overline{v} \vee \overline{w} \vee y$
Erase the clause $\overline{y} \vee z$
Write down axiom 2: v
Write down axiom 3: w
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

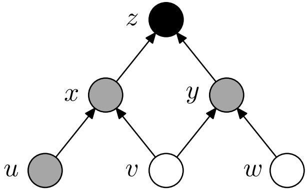
w

$\overline{z}$

Write down axiom 2: v
Write down axiom 3: w
Write down axiom 7: $\overline{z}$
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. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

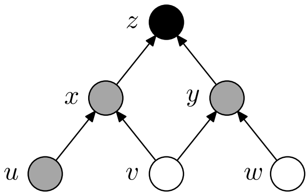


$\overline{v} \lor \overline{w} \lor z$
v
w
$\overline{z}$
$\overline{w} \lor z$

Write down axiom 2: v
Write down axiom 3: w
Write down axiom 7: $\overline{z}$
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. $\overline{u} \lor \overline{v} \lor x$
5. $\overline{v} \lor \overline{w} \lor y$
6. $\overline{x} \lor \overline{y} \lor z$
7. $\overline{z}$

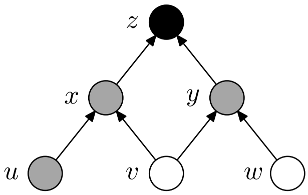


$\overline{v} \lor \overline{w} \lor z$
v
w
$\overline{z}$
$\overline{w} \lor z$

Write down axiom 3: w
Write down axiom 7: $\overline{z}$
Infer $\overline{w} \lor z$ from
v and $\overline{v} \lor \overline{w} \lor z$
Erase the 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. $\overline{z}$

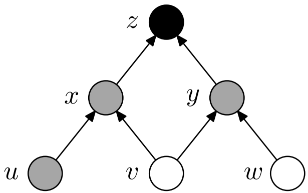


$\overline{v} \vee \overline{w} \vee z$
w
$\overline{z}$
$\overline{w} \vee z$

Write down axiom 3: w
Write down axiom 7: $\overline{z}$
Infer $\overline{w} \vee z$ from
v and $\overline{v} \vee \overline{w} \vee z$
Erase the 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. $\overline{z}$

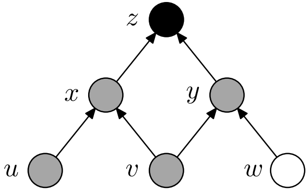


$\overline{v} \lor \overline{w} \lor z$
w
$\overline{z}$
$\overline{w} \lor z$

Write down axiom 7: $\overline{z}$
Infer $\overline{w} \lor z$ from
v and $\overline{v} \lor \overline{w} \lor z$
Erase the clause v
Erase the 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

$\overline{z}$

$\overline{w} \lor z$

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

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

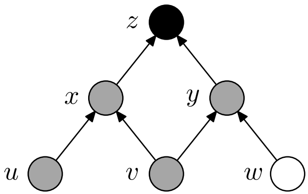
v and $\overline{v} \lor \overline{w} \lor z$

Erase the clause v

Erase the 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

$\overline{z}$

$\overline{w} \lor z$

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

Erase the clause v

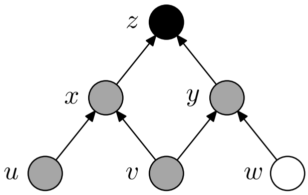
Erase the clause $\overline{v} \lor \overline{w} \lor z$

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

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

Erase the clause v

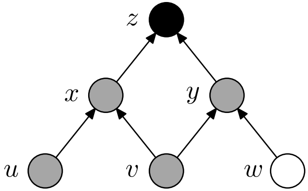
Erase the clause $\overline{v} \lor \overline{w} \lor z$

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. $\overline{z}$



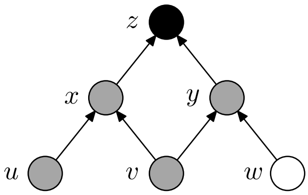
---

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

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

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. $\overline{z}$



$\overline{z}$

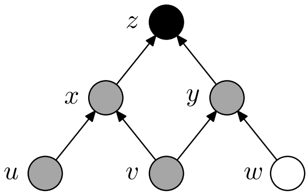
$\overline{w} \vee z$

z

Erase the clause v
Erase the clause $\overline{v} \vee \overline{w} \vee z$
Infer z from
w and $\overline{w} \vee z$
Erase the 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 the clause $\overline{v} \lor \overline{w} \lor z$

Infer z from

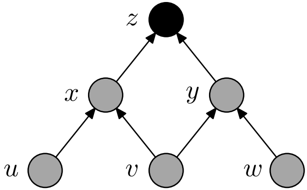
w and $\overline{w} \lor z$

Erase the clause w

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

Infer z from

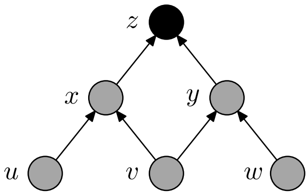
w and $\overline{w} \lor z$

Erase the clause w

Erase the 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. $\overline{z}$



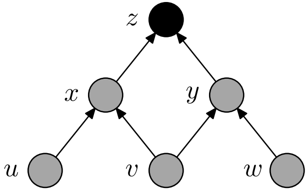
$\overline{z}$

z

w and $\overline{w} \lor z$
Erase the clause w
Erase the clause $\overline{w} \lor z$
Infer 0 from
$\overline{z}$ and 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

0

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

Erase the clause w

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

Infer 0 from

$\overline{z}$ and z

Formal Refutation-Pebbling Correspondence

Theorem (Ben-Sasson '02)

Any refutation translates into black-white pebbling with

- *# moves ≤ refutation length*
- *# pebbles ≤ variable space*

Observation (Ben-Sasson et al. '00)

Any black-pebbles-only pebbling translates into refutation with

- *refutation length ≤ # moves*
- *total space ≤ # pebbles*

Unfortunately pebbling contradictions are extremely easy w.r.t. formula space! — not what we want

Formal Refutation-Pebbling Correspondence

Theorem (Ben-Sasson '02)

Any refutation translates into black-white pebbling with

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

Observation (Ben-Sasson et al. '00)

Any black-pebbles-only pebbling translates into refutation with

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

Unfortunately pebbling contradictions are extremely easy w.r.t. formula space! — not what we want

Formal Refutation-Pebbling Correspondence

Theorem (Ben-Sasson '02)

Any refutation translates into black-white pebbling with

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

Observation (Ben-Sasson et al. '00)

Any black-pebbles-only pebbling translates into refutation with

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

Unfortunately pebbling contradictions are extremely easy w.r.t. formula space! — not what we want

Key Idea: Variable Substitution

Make formula harder by substituting $x_1 \oplus x_2$ for every variable x (also works for other Boolean functions with "right" properties):

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

$$\Downarrow$$

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

$$\Downarrow$$

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

Key Technical Result: Substitution Theorem

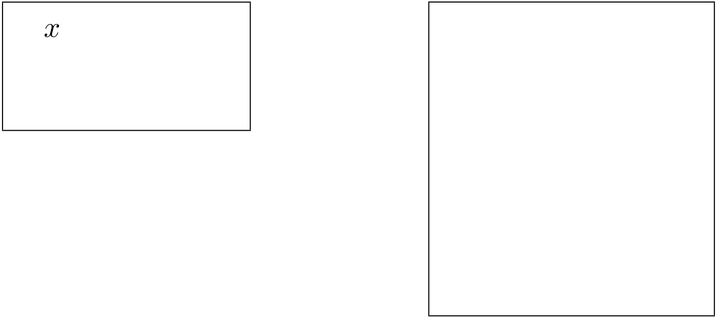
Let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for x

Obvious approach for $F[\oplus]$: mimic refutation of F

Key Technical Result: Substitution Theorem

Let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for x

Obvious approach for $F[\oplus]$: mimic refutation of F



Key Technical Result: Substitution Theorem

Let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for x

Obvious approach for $F[\oplus]$: mimic refutation of F

x

$\overline{x} \lor y$

Key Technical Result: Substitution Theorem

Let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for x

Obvious approach for $F[\oplus]$: mimic refutation of F

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

Key Technical Result: Substitution Theorem

Let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for x

Obvious approach for $F[\oplus]$: mimic refutation of F

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

$x_1 \lor x_2$
$\overline{x}_1 \lor \overline{x}_2$

Key Technical Result: Substitution Theorem

Let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for x

Obvious approach for $F[\oplus]$: mimic refutation of F

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

$x_1 \lor x_2$
$\overline{x}_1 \lor \overline{x}_2$
$x_1 \lor \overline{x}_2 \lor y_1 \lor y_2$
$x_1 \lor \overline{x}_2 \lor \overline{y}_1 \lor \overline{y}_2$
$\overline{x}_1 \lor x_2 \lor y_1 \lor y_2$
$\overline{x}_1 \lor x_2 \lor \overline{y}_1 \lor \overline{y}_2$

Key Technical Result: Substitution Theorem

Let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for x

Obvious approach for $F[\oplus]$: mimic refutation of F

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

$x_1 \vee x_2$
$\overline{x}_1 \vee \overline{x}_2$
$x_1 \vee \overline{x}_2 \vee y_1 \vee y_2$
$x_1 \vee \overline{x}_2 \vee \overline{y}_1 \vee \overline{y}_2$
$\overline{x}_1 \vee x_2 \vee y_1 \vee y_2$
$\overline{x}_1 \vee x_2 \vee \overline{y}_1 \vee \overline{y}_2$
$y_1 \vee y_2$
$\overline{y}_1 \vee \overline{y}_2$

Key Technical Result: Substitution Theorem

Let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for x

Obvious approach for $F[\oplus]$: mimic refutation of F

$$\begin{array}{l} x \\ \overline{x} \lor y \\ y \end{array}$$

$$\begin{array}{l} x_1 \lor x_2 \\ \overline{x}_1 \lor \overline{x}_2 \\ x_1 \lor \overline{x}_2 \lor y_1 \lor y_2 \\ x_1 \lor \overline{x}_2 \lor \overline{y}_1 \lor \overline{y}_2 \\ \overline{x}_1 \lor x_2 \lor y_1 \lor y_2 \\ \overline{x}_1 \lor x_2 \lor \overline{y}_1 \lor \overline{y}_2 \\ y_1 \lor y_2 \\ \overline{y}_1 \lor \overline{y}_2 \end{array}$$

For such refutation of $F[\oplus]$:

- length $\geq$ length for F
- formula space $\geq$ variable space for F

Key Technical Result: Substitution Theorem

Let $F[\oplus]$ denote formula with XOR $x_1 \oplus x_2$ substituted for x

Obvious approach for $F[\oplus]$: mimic refutation of F

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

$x_1 \lor x_2$
$\overline{x}_1 \lor \overline{x}_2$
$x_1 \lor \overline{x}_2 \lor y_1 \lor y_2$
$x_1 \lor \overline{x}_2 \lor \overline{y}_1 \lor \overline{y}_2$
$\overline{x}_1 \lor x_2 \lor y_1 \lor y_2$
$\overline{x}_1 \lor x_2 \lor \overline{y}_1 \lor \overline{y}_2$
$y_1 \lor y_2$
$\overline{y}_1 \lor \overline{y}_2$

For such refutation of $F[\oplus]$:

- length $\geq$ length for F
- formula space $\geq$ variable space for F

Prove that this is (sort of) best one can do for $F[\oplus]$!

Sketch of Proof of Substitution Theorem

Given refutation of $F[\oplus]$, extract "shadow refutation" of F

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

Sketch of Proof of Substitution Theorem

Given refutation of $F[\oplus]$, extract "shadow refutation" of F

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

Sketch of Proof of Substitution Theorem

Given refutation of $F[\oplus]$, extract "shadow refutation" of F

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

Sketch of Proof of Substitution Theorem

Given refutation of $F[\oplus]$, extract "shadow refutation" of F

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

Sketch of Proof of Substitution Theorem

Given refutation of $F[\oplus]$, extract "shadow refutation" of F

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

Sketch of Proof of Substitution Theorem

Given refutation of $F[\oplus]$, extract "shadow refutation" of F

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

Sketch of Proof of Substitution Theorem

Given refutation of $F[\oplus]$, extract "shadow refutation" of F

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

Sketch of Proof of Substitution Theorem

Given refutation of $F[\oplus]$, extract "shadow refutation" of F

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

Sketch of Proof of Substitution Theorem

Given refutation of $F[\oplus]$, extract "shadow refutation" of F

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

Pieces Together: Substitution + Pebbling Formulas

Making variable substitutions in pebbling formulas

- lifts lower bound from variable space to formula space
- maintains upper bound in terms of total space and length

Substitution with XOR over $k+1$ variables works against k-DNF resolution

Get our results by

- using known pebbling results from literature of 70s and 80s
- proving a couple of new pebbling results [Nordström '10]
- to get tight trade-offs, showing that resolution can sometimes do better than black-only pebbling [Nordström '10]

Pieces Together: Substitution + Pebbling Formulas

Making variable substitutions in pebbling formulas

- lifts lower bound from variable space to formula space
- maintains upper bound in terms of total space and length

Substitution with XOR over $k+1$ variables works against k-DNF resolution

Get our results by

- using known pebbling results from literature of 70s and 80s
- proving a couple of new pebbling results [Nordström '10]
- to get tight trade-offs, showing that resolution can sometimes do better than black-only pebbling [Nordström '10]

Pieces Together: Substitution + Pebbling Formulas

Making variable substitutions in pebbling formulas

- lifts lower bound from variable space to formula space
- maintains upper bound in terms of total space and length

Substitution with XOR over $k+1$ variables works against k-DNF resolution

Get our results by

- using known pebbling results from literature of 70s and 80s
- proving a couple of new pebbling results [Nordström '10]
- to get tight trade-offs, showing that resolution can sometimes do better than black-only pebbling [Nordström '10]

Lower Bounds on Total Space?

Open Question

Are there polynomial-size k-CNF formulas with total refutation space $\Omega\big((\text{size of } F)^2\big)$? in resolution

Answer conjectured to be "yes" by [Alekhnovich et al. 2000]

Or can one at least prove a superlinear lower bound measured in # variables?

Stronger Length-Space Trade-offs than from Pebbling?

Open Question

Are there superpolynomial trade-offs in resolution 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 — can impossibly have such strong trade-offs

Expecting to hear some exciting news on 2nd question later today!

Stronger Length-Space Trade-offs than from Pebbling?

Open Question

Are there superpolynomial trade-offs in resolution 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 — can impossibly have such strong trade-offs

Expecting to hear some exciting news on 2nd question later today!

Trade-offs for Stronger Proof Systems?

Recall key technical theorem: amplify space lower bounds through variable substitution

Almost completely oblivious to which proof system is being studied

Extended to strictly stronger k-DNF resolution proof systems — maybe can be made to work for other stronger systems as well?

Open Question

Can the Substitution Theorem be proven for, say, Cutting Planes or Polynomial Calculus (with/without Resolution), thus yielding time-space trade-offs for these proof systems as well?

Trade-offs for Stronger Proof Systems?

Recall key technical theorem: amplify space lower bounds through variable substitution

Almost completely oblivious to which proof system is being studied

Extended to strictly stronger k-DNF resolution proof systems — maybe can be made to work for other stronger systems as well?

Open Question

Can the Substitution Theorem be proven for, say, Cutting Planes or Polynomial Calculus (with/without Resolution), thus yielding time-space trade-offs for these proof systems as well?

Some Related Very Recent Developments

Theorem (Huynh & Nordström, Sep '11)

There are k-CNF formulas refutable in resolution in length $\mathcal{O}(n)$ such that any

- *PCR refutation in length L and monomial space s has*

$$s \log L = \Omega\left(\sqrt[4]{n/\log n}\right)$$

- *Cutting Planes refutation in length L and line space s has*

$$s \log L = \Omega\left(\sqrt[6]{n/\log^{13} n}\right)$$

Doesn't use substitution theorem, but lifting + communication complexity à la [Beame, Huynh & Pitassi '10]

Some Related Very Recent Developments

Theorem (Huynh & Nordström, Sep '11)

There are k-CNF formulas refutable in resolution in length $\mathcal{O}(n)$ such that any

- *PCR refutation in length L and monomial space s has*

$$s \log L = \Omega\left(\sqrt[4]{n/\log n}\right)$$

- *Cutting Planes refutation in length L and line space s has*

$$s \log L = \Omega\left(\sqrt[6]{n/\log^{13} n}\right)$$

Doesn't use substitution theorem, but lifting + communication complexity à la [Beame, Huynh & Pitassi '10]

Some Related Very Recent Developments

Theorem (Huynh & Nordström, Sep '11)

There are k-CNF formulas refutable in resolution in length $\mathcal{O}(n)$ such that any

- *PCR refutation in length L and monomial space s has*

$$s \log L = \Omega\left(\sqrt[4]{n/\log n}\right)$$

- *Cutting Planes refutation in length L and line space s has*

$$s \log L = \Omega\left(\sqrt[6]{n/\log^{13} n}\right)$$

Doesn't use substitution theorem, but lifting + communication complexity à la [Beame, Huynh & Pitassi '10]

Some Related Very Recent Developments

Theorem (Huynh & Nordström, Sep '11)

There are k-CNF formulas refutable in resolution in length $\mathcal{O}(n)$ such that any

- *PCR refutation in length L and monomial space s has*

$$s \log L = \Omega\left(\sqrt[4]{n/\log n}\right)$$

- *Cutting Planes refutation in length L and line space s has*

$$s \log L = \Omega\left(\sqrt[6]{n/\log^{13} n}\right)$$

Doesn't use substitution theorem, but lifting + communication complexity à la [Beame, Huynh & Pitassi '10]

Is Tractability Captured by Space Complexity?

Open Question

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

That is, does space complexity capture hardness?

Space suggested as hardness measure in [Ansótegui et al.'08]

Preliminary experiments seem to indicate that pebbling formulas might actually be hard for SAT solvers

Note that pebbling formulas are always extremely easy with respect to length, so hardness in practice would be intriguing

Is Tractability Captured by Space Complexity?

Open Question

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

That is, does space complexity capture hardness?

Space suggested as hardness measure in [Ansótegui et al.'08]

Preliminary experiments seem to indicate that pebbling formulas might actually be hard for SAT solvers

Note that pebbling formulas are always extremely easy with respect to length, so hardness in practice would be intriguing

Is Tractability Captured by Space Complexity?

Open Question

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

That is, does space complexity capture hardness?

Space suggested as hardness measure in [Ansótegui et al.'08]

Preliminary experiments seem to indicate that pebbling formulas might actually be hard for SAT solvers

Note that pebbling formulas are always extremely easy with respect to length, so hardness in practice would be intriguing

Take-Home Message

- Modern SAT solvers, although based on old and simple DPLL method, can be enormously successful in practice
- Key issue is to minimize time and memory consumption
- However, our results suggest strong time-space trade-offs that should make this impossible
- Many remaining open questions about space in proof complexity
- Main open practical question: is tractability captured by space complexity?

Advertisment

I'm hiring!

- 2 PhD students
- 1 postdoc
- Starting date autumn 2012
- More info soon at `www.csc.kth.se/~jakobn`

Advertisment

I'm hiring!

- 2 PhD students
- 1 postdoc
- Starting date autumn 2012
- More info soon at `www.csc.kth.se/~jakobn`

Thank you for your attention!