Computer-Aided Reasoning for Software

Introduction

Emina Torlak
emina@cs.washington.edu
Today

What is this course about?

Course logistics

Review of propositional logic

A basic SAT solver!
Tools for building better software, more easily
Tools for building better software, more easily.
Tools for building better software, more easily

automatic verification, debugging & synthesis
Tools for building better software, more easily

```java
class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;

        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }

        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next; String data;
}
```

Is this list reversal procedure correct?
**Tools for building better software, more easily**

```java
class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;

        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }
        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next; String data;
}
```

Is this list reversal procedure correct?

Verification diagram showing the initial and final states of the list.
Tools for building better software, more easily

class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;

        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }
        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next; String data;
}
class List {
    Node head;
    
    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;
        
        near.next = far;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }
        
        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next; String data;
}
class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;

        near.next = ??;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }

        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next; String data;
}
class List {
    Node head;

    void reverse() {
        Node near = head;
        Node mid = near.next;
        Node far = mid.next;
        near.next = null;
        while (far != null) {
            mid.next = near;
            near = mid;
            mid = far;
            far = far.next;
        }
        mid.next = near;
        head = mid;
    }
}

class Node {
    Node next; String data;
}
By the end of this course, you’ll be able to build computer-aided tools for any domain!
By the end of this course, you’ll be able to build computer-aided tools for any domain!
logistics

Topics, structure, people
Course overview

program question

logic

automated reasoning engine

tool
Course overview

program question

verifier, synthesizer, fault localizer

logic

SAT, SMT, model finders & checkers
Fig. 1. Decision procedures can be rather complex... those that we consider in this book take formulas of different theories as input, possibly mix them (using the Nelson–Oppen procedure – see Chap. 10), decide their satisfiability ("YES" or "NO"), and, if yes, provide a satisfying assignment.

Which Theories? Which Algorithms?

A first-order theory can be considered "interesting", at least from a practical perspective, if it fulfills at least these two conditions:

1. The theory is expressive enough to model a real decision problem. Moreover, it is more expressive or more natural for the purpose of expressing some models in comparison with theories that are easier to decide.

Source: Drawing from “Decision Procedures” by Kroening & Strichman.
Course overview

program question

verifier, synthesizer, fault localizer

logic

SAT, SMT, model finders & checkers

study (part I)

Drawing from “Decision Procedures” by Kroening & Strichman
Course overview

**program**  **question**

**logic**

SAT, SMT, model finders & checkers

**verifier, synthesizer, fault localizer**

study (part I)

build! (part II)

Fig. 1. Decision procedures can be rather complex... those that we consider in this book take formulas of different theories as input, possibly mix them (using the Nelson–Oppen procedure – see Chap. 10), decide their satisfiability (“YES” or “NO”), and, if yes, provide a satisfying assignment.

Which Theories? Which Algorithms?

A first-order theory can be considered “interesting”, at least from a practical perspective, if it fulfills at least these two conditions:

1. The theory is expressive enough to model a real decision problem. Moreover, it is more expressive or more natural for the purpose of expressing some models in comparison with theories that are easier to decide.

Drawing from “Decision Procedures” by Kroening & Strichman
Grading

4 individual homework assignments (50%)
  • conceptual problems & proofs (TeX)
  • implementations (Racket)
  • may discuss problems with others but solutions must be your own

Course project (50%)
  • build a computer-aided reasoning tool for a domain of your choice
  • teams of 2-3 people
  • see the course web page for timeline, deliverables and other details

build! (part II)

study (part I)
Reading and references

Required readings posted on the course web page

- Complete each reading before the lecture for which it is assigned

Recommended text books

- Bradley & Manna, *The Calculus of Computation*
- Kroening & Strichman, *Decision Procedures*

Related courses

Advice for doing well in 507

Come to class (prepared)
  • Lecture notes are enough to teach from, but not enough to learn from

Participate
  • Ask and answer questions

Meet deadlines
  • Turn homework in on time
  • Start homework and project sooner than you think you need to
  • Follow instructions for submitting code (we have to be able to run it)
People

Emina Torlak
PLSE
CSE 596
Fridays 11-12

James Bornholt
PLSE
CSE 218
Wednesdays 11-12
People

instructor

Emina Torlak
PLSE
CSE 596
Fridays 11-12

TA

James Bornholt
PLSE
CSE 218
Wednesdays 11-12

students!

Your name
Research area
Let’s get started! A review of propositional logic

• Syntax
• Semantics
• Satisfiability and validity
• Proof methods
• Semantic judgments
• Normal forms (NNF, DNF, CNF)
Syntax of propositional logic

\[(\neg p \land T) \lor (q \rightarrow \bot)\]
Syntax of propositional logic

Atom

truth symbols: \( \top \) (“true”), \( \bot \) (“false”)

propositional variables: \( p, q, r, \ldots \)
Syntax of propositional logic

Atom

truth symbols: \( \top \) ("true"), \( \bot \) ("false")
propositional variables: \( p, q, r, \ldots \)

Literal

an atom \( \alpha \) or its negation \( \neg \alpha \)
Syntax of propositional logic

Atom

truth symbols: \( \top \) ("true"), \( \bot \) ("false")
propositional variables: \( p, q, r, \ldots \)

Literal

an atom \( \alpha \) or its negation \( \neg \alpha \)

Formula

a literal or the application of a logical connective to formulas \( F, F_1, F_2 \):

\[ \neg F \] 
\[ F_1 \land F_2 \] 
\[ F_1 \lor F_2 \] 
\[ F_1 \rightarrow F_2 \] 
\[ F_1 \leftrightarrow F_2 \]

"not" (negation)
"and" (conjunction)
"or" (disjunction)
"implies" (implication)
"if and only if" (iff)
An **interpretation** $I$ for a propositional formula $F$ maps every variable in $F$ to a truth value:

$$I : \{ p \mapsto \text{true}, q \mapsto \text{false}, \ldots \}$$
Semantics of propositional logic: interpretations

An **interpretation** $I$ for a propositional formula $F$ maps every variable in $F$ to a truth value:

$$I : \{ p \mapsto \text{true}, q \mapsto \text{false}, \ldots \}$$

$I$ is a **satisfying interpretation** of $F$, written as $I \models F$, if $F$ evaluates to true under $I$.

$I$ is a **falsifying interpretation** of $F$, written as $I \not\models F$, if $F$ evaluates to false under $I$. 
Semantics of propositional logic: definition

Base cases:

- \( I \models \top \)
- \( I \not\models \bot \)
- \( I \models p \) iff \( I[p] = \text{true} \)
- \( I \not\models p \) iff \( I[p] = \text{false} \)
Semantics of propositional logic: definition

Base cases:

- $I \models \top$
- $I \not\models \bot$
- $I \models p \iff I[p] = \text{true}$
- $I \not\models p \iff I[p] = \text{false}$

Inductive cases:
Semantics of propositional logic: definition

**Base cases:**

- $I \models \top$
- $I \not\models \bot$
- $I \models p$ iff $I[p] = \text{true}$
- $I \not\models p$ iff $I[p] = \text{false}$

**Inductive cases:**

- $I \models \neg F$ iff $I \not\models F$
Semantics of propositional logic: definition

**Base cases:**

- $I \models \top$
- $I \not\models \bot$
- $I \models p \iff I[p] = \text{true}$
- $I \not\models p \iff I[p] = \text{false}$

**Inductive cases:**

- $I \models \neg F \iff I \not\models F$
- $I \models F_1 \land F_2 \iff I \models F_1$ and $I \models F_2$
Semantics of propositional logic: definition

**Base cases:**

- $I \models \top$
- $I \not\models \bot$
- $I \models p$ iff $I[p] = \text{true}$
- $I \not\models p$ iff $I[p] = \text{false}$

**Inductive cases:**

- $I \models \neg F$ iff $I \not\models F$
- $I \models F_1 \wedge F_2$ iff $I \models F_1$ and $I \models F_2$
- $I \models F_1 \lor F_2$ iff $I \models F_1$ or $I \models F_2$
- $I \models F_1 \rightarrow F_2$ iff $I \not\models F_1$ or $I \models F_2$
- $I \models F_1 \leftrightarrow F_2$ iff $I \models F_1$ and $I \models F_2$, or $I \not\models F_1$ and $I \not\models F_2$
Semantics of propositional logic: example

\[ F: (p \land q) \rightarrow (p \lor \neg q) \]
\[ I: \{ p \mapsto \text{true}, q \mapsto \text{false} \} \]
Semantics of propositional logic: example

\[ F: \quad (p \wedge q) \rightarrow (p \lor \neg q) \]
\[ I: \quad \{p \leftrightarrow \text{true}, q \leftrightarrow \text{false}\} \]
\[ I \models F \]
Satisfiability & validity of propositional formulas

$F$ is **satisfiable** iff $I \models F$ for some $I$.

$F$ is **valid** iff $I \models F$ for all $I$. 
Satisfiability & validity of propositional formulas

\[ F \text{ is } \textbf{satisfiable} \text{ iff } I \vDash F \text{ for some } I. \]

\[ F \text{ is } \textbf{valid} \text{ iff } I \vDash F \text{ for all } I. \]

**Duality** of satisfiability and validity:

\[ F \text{ is valid iff } \neg F \text{ is unsatisfiable.} \]
Satisfiability & validity of propositional formulas

\[ F \text{ is satisfiable iff } I \models F \text{ for some } I. \]

\[ F \text{ is valid iff } I \models F \text{ for all } I. \]

**Duality** of satisfiability and validity:

\[ F \text{ is valid iff } \neg F \text{ is unsatisfiable.} \]

If we have a procedure for checking satisfiability, then we can also check validity of propositional formulas, and vice versa.
Techniques for deciding satisfiability & validity

- Search
- Deduction

SAT solver
Enumerate all interpretations (i.e., build a truth table), and check that they satisfy the formula.

Techniques for deciding satisfiability & validity

Search

Enumerate all interpretations (i.e., build a truth table), and check that they satisfy the formula.

Deduction

SAT solver
Enumerate all interpretations (i.e., build a truth table), and check that they satisfy the formula.

Assume the formula is invalid, apply proof rules, and check for contradiction in every branch of the proof tree.
Proof by search (truth tables)

F: \((p \land q) \rightarrow (p \lor \neg q)\)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>(p \land q)</th>
<th>(\neg q)</th>
<th>(p \lor \neg q)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Proof by search (truth tables)

F: \((p \land q) \rightarrow (p \lor \neg q)\)

<table>
<thead>
<tr>
<th>(p)</th>
<th>(q)</th>
<th>(p \land q)</th>
<th>(\neg q)</th>
<th>(p \lor \neg q)</th>
<th>(F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Proof by deduction (semantic arguments)

Example proof rules:

\[
\begin{align*}
I \models \neg F & \quad \quad & I \models F_1 \land F_2 \\
I \not\models F & \quad\quad & I \models F_1 \\
& \quad\quad & I \models F_2 \\
I \not\models \neg F & \quad\quad & I \not\models F_1 \land F_2 \\
I \models F & \quad\quad & I \not\models F_1 \quad I \not\models F_2
\end{align*}
\]
Proof by deduction (semantic arguments)

Example proof rules:

\[
\begin{align*}
I & \models \neg F & I & \models F_1 \land F_2 \\
& I \nmid F & I & \models F_1 \\
& & I & \models F_2 \\
I & \nmid \neg F & I & \nmid F_1 \land F_2 \\
& I & \nmid F_1 & I & \nmid F_2
\end{align*}
\]

\[F: \ p \land \neg q\]
Proof by deduction (semantic arguments)

Example proof rules:

\[ \frac{I \models \neg F}{I \not\models F} \quad \frac{I \models F_1 \land F_2}{I \models F_1} \quad \frac{I \models F_2}{I \not\models F_1 \land F_2} \quad \frac{I \not\models \neg F}{I \models F} \quad \frac{I \not\models F_1}{I \models F_2} \quad \frac{I \models F_1 \land F_2}{I \not\models F_1 \land F_2} \]

\[F: \ p \land \neg q\]

1. \(I \not\models p \land \neg q\) (assumption)
Proof by deduction (semantic arguments)

Example proof rules:

\[
\begin{align*}
I \not\models \neg F & \\
\therefore I \not\models F
\end{align*}
\]

\[
\begin{align*}
I \models F_1 \land F_2 & \\
I \models F_1 & \\
I \models F_2
\end{align*}
\]

\[
\begin{align*}
I \not\models \neg F & \\
\therefore I \not\models F
\end{align*}
\]

\[
\begin{align*}
I \not\models F_1 \land F_2 & \\
I \not\models F_1 & \\
I \not\models F_2
\end{align*}
\]

\[
F: \quad p \land \neg q
\]

1. \(I \not\models p \land \neg q\) (assumption)

a. \(I \not\models p\) (1, \(\land\))
Proof by deduction (semantic arguments)

Example proof rules:

\[
\frac{I \models \neg F}{I \not\models F} \quad \frac{I \models F_1 \land F_2}{I \models F_1} \quad \frac{I \models F_2}{I \not\models F_1 \land F_2} \\
\frac{I \not\models \neg F}{I \models F} \quad \frac{I \not\models F_1 \land F_2}{I \not\models F_1} \quad \frac{I \not\models F_2}{I \not\models F_1 \land F_2}
\]

\[F: \ p \land \neg q\]

1. \(I \not\models p \land \neg q\) \hspace{1cm} \text{(assumption)}
   
a. \(I \not\models p\) \hspace{1cm} \text{(1, \land)}
   
b. \(I \not\models \neg q\) \hspace{1cm} \text{(1, \land)}
Proof by deduction (semantic arguments)

Example proof rules:

\[
\begin{align*}
I & \not \models F \\
\hline
I & \not \models F
\end{align*}
\]

\[
\begin{align*}
I & \not \models F_1 \land F_2 \\
\hline
I & \not \models F_1 \\
I & \not \models F_2
\end{align*}
\]

\[
\begin{align*}
I & \not \models \neg F \\
\hline
I & \models F
\end{align*}
\]

\[
\begin{align*}
I & \not \models \neg F_1 \land F_2 \\
\hline
I & \not \models F_1 \\
I & \not \models F_2
\end{align*}
\]

\[
F: \quad p \land \neg q
\]

1. \( I \not \models p \land \neg q \)  \hspace{1cm} \text{(assumption)}
   
   a. \( I \not \models p \)  \hspace{1cm} (1, \land)
   
   b. \( I \not \models \neg q \)  \hspace{1cm} (1, \land)
   
   i. \( I \models q \)  \hspace{1cm} (1b, \neg)
Proof by deduction (semantic arguments)

Example proof rules:

\[
\begin{align*}
I \models \neg F & \quad I \models F_1 \land F_2 \\
\hline
I \not\models F & \quad I \models F_1 \quad I \models F_2
\end{align*}
\]

\[
\begin{align*}
I \not\models \neg F & \quad I \not\models F_1 \land F_2 \\
\hline
I \models F & \quad I \not\models F_1 \quad I \not\models F_2
\end{align*}
\]

\[F: \quad p \land \neg q\]

1. \(I \not\models p \land \neg q\)  \quad (assumption)
   a. \(I \not\models p\)  \quad (1, \land)
   b. \(I \not\models \neg q\)  \quad (1, \land)
   i. \(I \models q\)  \quad (1b, \neg)

Invalid; \(I\) is a falsifying interpretation.
Semantic judgements

Formulas $F_1$ and $F_2$ are **equivalent**, written $F_1 \iff F_2$, iff $F_1 \iff F_2$ is valid.

Formula $F_1$ **implies** $F_2$, written $F_1 \implies F_2$, iff $F_1 \rightarrow F_2$ is valid.

$F_1 \iff F_2$ and $F_1 \implies F_2$ are not propositional formulas (not part of syntax). They are properties of formulas, just like validity or satisfiability.
Semantic judgements

Formulas $F_1$ and $F_2$ are **equivalent**, written $F_1 \iff F_2$, iff $F_1 \leftrightarrow F_2$ is valid.

Formula $F_1$ **implies** $F_2$, written $F_1 \implies F_2$, iff $F_1 \rightarrow F_2$ is valid.

If we have a procedure for checking satisfiability, then we can also check for equivalence and implication of propositional formulas.
Semantic judgements

Formulas $F_1$ and $F_2$ are **equivalent**, written $F_1 \iff F_2$, iff $F_1 \leftrightarrow F_2$ is valid.

Formula $F_1$ **implies** $F_2$, written $F_1 \implies F_2$, iff $F_1 \rightarrow F_2$ is valid.

If we have a procedure for checking satisfiability, then we can also check for equivalence and implication of propositional formulas.

Why do we care?
Getting ready for SAT solving with normal forms

A normal form for a logic is a syntactic restriction such that every formula in the logic has an equivalent formula in the normal form.
Getting ready for SAT solving with normal forms

A normal form for a logic is a syntactic restriction such that every formula in the logic has an equivalent formula in the normal form.

Assembly language for a logic.
Getting ready for SAT solving with normal forms

A **normal form** for a logic is a syntactic restriction such that every formula in the logic has an equivalent formula in the normal form.

Assembly language for a logic.

Three important normal forms for propositional logic:
- Negation Normal Form (NNF)
- Disjunctive Normal Form (DNF)
- Conjunctive Normal Form (CNF)
Negation Normal Form (NNF)

Atom := Variable | \( T \) | \( \bot \)
Literal := Atom | \( \neg \)Atom
Formula := Literal | Formula op Formula
op := \( \land \) | \( \lor \)
Negation Normal Form (NNF)

Atom := Variable | $\top$ | $\bot$
Literal := Atom | $\neg$Atom
Formula := Literal | Formula op Formula
op := $\land$ | $\lor$

- The only allowed connectives are $\land$, $\lor$, and $\neg$.
- $\neg$ can appear only in literals.
Negation Normal Form (NNF)

Atom := Variable | ⊤ | ⊥
Literal := Atom | ¬Atom
Formula := Literal | Formula op Formula
op := ∧ | ∨

• The only allowed connectives are ∧, ∨, and ¬.
• ¬ can appear only in literals.

Conversion to NNF performed using DeMorgan’s Laws:
¬(F ∧ G) ⇔ ¬F ∨ ¬G
¬(F ∨ G) ⇔ ¬F ∧ ¬G
Disjunctive Normal Form (DNF)

Atom := Variable | ⊤ | ⊥
Literal := Atom | ¬Atom
Formula := Clause ∨ Formula
Clause := Literal | Literal ∧ Clauses
Disjunctive Normal Form (DNF)

Atom := Variable | ⊤ | ⊥
Literal := Atom | ¬Atom
Formula := Clause ∨ Formula
Clause := Literal | Literal ∧ Clauses

• Disjunction of conjunction of literals.
Disjunctive Normal Form (DNF)

Atom := Variable | T | ⊥
Literal := Atom | ¬Atom
Formula := Clause ∨ Formula
Clause := Literal | Literal ∧ Clauses

To convert to DNF, convert to NNF and distribute ∧ over ∨:

(F ∧ (G ∨ H)) ⇔ (F ∧ G) ∨ (F ∧ H)
((G ∨ H) ∧ F) ⇔ (G ∧ F) ∨ (H ∧ F)

• Disjunction of conjunction of literals.
Disjunctive Normal Form (DNF)

Atom := Variable | $\top$ | $\bot$
Literal := Atom | $\neg$Atom
Formula := Clause $\lor$ Formula
Clause := Literal | Literal $\land$ Clauses

• Disjunction of conjunction of literals.
• Deciding satisfiability of a DNF formula is trivial.

To convert to DNF, convert to NNF and distribute $\land$ over $\lor$:

\[(F \land (G \lor H)) \iff (F \land G) \lor (F \land H)\]
\[((G \lor H) \land F) \iff (G \land F) \lor (H \land F)\]
Disjunctive Normal Form (DNF)

Atom := Variable | T | F
Literal := Atom | ¬Atom
Formula := Clause ∨ Formula
Clause := Literal | Literal ∧ Clauses

• Disjunction of conjunction of literals.
• Deciding satisfiability of a DNF formula is trivial.
• Why not SAT solve by conversion to DNF?

To convert to DNF, convert to NNF and distribute ∧ over ∨:

(F ∧ (G ∨ H)) ⇔ (F ∧ G) ∨ (F ∧ H)
((G ∨ H) ∧ F) ⇔ (G ∧ F) ∨ (H ∧ F)
Conjunctive Normal Form (CNF)

Atom := Variable | T | ⊥
Literal := Atom | ¬Atom
Formula := Clause ∧ Formula
Clause := Literal | Literal ∨ Clauses

• Conjunction of disjunction of literals.
• Deciding the satisfiability of a CNF formula is hard.
• SAT solvers use CNF as their input language.

To convert to CNF, convert to NNF and distribute ∨ over ∧

(F ∨ (G ∧ H)) ⇔ (F ∨ G) ∧ (F ∨ H)

((G ∧ H) ∨ F) ⇔ (G ∨ F) ∧ (H ∨ F)
Conjunctive Normal Form (CNF)

Atom := Variable | ⊤ | ⊥
Literal := Atom | ¬ Atom
Formula := Clause ∧ Formula
Clause := Literal | Literal ∨ Clauses

• Conjunction of disjunction of literals.
• Deciding the satisfiability of a CNF formula is hard.
• SAT solvers use CNF as their input language.

Why CNF? Doesn't the conversion explode just as badly as DNF?

To convert to CNF, convert to NNF and distribute ∨ over ∧
(F ∨ (G ∧ H)) ⇔ (F ∨ G) ∧ (F ∨ H)
((G ∧ H) ∨ F) ⇔ (G ∨ F) ∧ (H ∨ F)
Equisatisfiability and Tseitin’s transformation
Equisatisfiability and Tseitin’s transformation

Formulas F and G are equisatisfiable if they are both satisfiable or they are both unsatisfiable.
Equisatisfiability and Tseitin’s transformation

Formulas $F$ and $G$ are **equisatisfiable** if they are both satisfiable or they are both unsatisfiable.

**Tseitin’s transformation** converts a propositional formula $F$ into an equisatisfiable CNF formula that is **linear** in the size of $F$. 
Equisatisfiability and Tseitin’s transformation

Formulas $F$ and $G$ are **equisatisfiable** if they are both satisfiable or they are both unsatisfiable.

**Tseitin’s transformation** converts a propositional formula $F$ into an equisatisfiable CNF formula that is **linear** in the size of $F$.

**Key idea:** introduce **auxiliary variables** to represent the output of subformulas, and constrain those variables using CNF clauses.
Equisatisfiability and Tseitin’s transformation

Formulas $F$ and $G$ are **equisatisfiable** if they are both satisfiable or they are both unsatisfiable.

**Tseitin’s transformation** converts a propositional formula $F$ into an equisatisfiable CNF formula that is **linear** in the size of $F$.

Key idea: introduce **auxiliary variables** to represent the output of subformulas, and constrain those variables using CNF clauses.
Equisatisfiability and Tseitin’s transformation

Formulas F and G are **equisatisfiable** if they are both satisfiable or they are both unsatisfiable.

**Tseitin’s transformation** converts a propositional formula F into an equisatisfiable CNF formula that is **linear** in the size of F.

Key idea: introduce **auxiliary variables** to represent the output of subformulas, and constrain those variables using CNF clauses.

\[
\begin{align*}
x &\rightarrow (y \land z) \\
a1 &\iff (x \rightarrow a2) \\
a2 &\iff (y \land z)
\end{align*}
\]
Equisatisfiability and Tseitin’s transformation

Formulas $F$ and $G$ are equisatisfiable if they are both satisfiable or they are both unsatisfiable.

Tseitin’s transformation converts a propositional formula $F$ into an equisatisfiable CNF formula that is linear in the size of $F$.

Key idea: introduce auxiliary variables to represent the output of subformulas, and constrain those variables using CNF clauses.
Equisatisfiability and Tseitin’s transformation

Formulas F and G are **equisatisfiable** if they are both satisfiable or they are both unsatisfiable.

**Tseitin’s transformation** converts a propositional formula F into an equisatisfiable CNF formula that is **linear** in the size of F.

Key idea: introduce **auxiliary variables** to represent the output of subformulas, and constrain those variables using CNF clauses.

\[
\begin{align*}
x &\rightarrow (y \land z) \\
a1 &
\iff \\
\neg a1 &\lor \neg x \lor a2 \\
(x \land \neg a2) &\lor a1 \\
a2 &\iff (y \land z)
\end{align*}
\]
Formulas $F$ and $G$ are equisatisfiable if they are both satisfiable or they are both unsatisfiable.

Tseitin’s transformation converts a propositional formula $F$ into an equisatisfiable CNF formula that is linear in the size of $F$.

Key idea: introduce auxiliary variables to represent the output of subformulas, and constrain those variables using CNF clauses.
A basic SAT solver!
// Returns true if the CNF formula F is satisfiable; otherwise returns false.

DPLL(F)
    G ← BCP(F)
    if G = ⊤ then return true
    if G = ⊥ then return false
    p ← choose(vars(G))
    return DPLL(G{p ↦ ⊤}) ||
            DPLL(G{p ↦ ⊥})
// Returns true if the CNF formula F is satisfiable; otherwise returns false.

DPLL(F)
  G ← BCP(F)
  if G = ⊤ then return true
  if G = ⊥ then return false
  p ← choose(vars(G))
  return DPLL(G{p ↦ ⊤}) || DPLL(G{p ↦ ⊥})

Boolean constraint propagation applies unit resolution until fixed point:

\[
\begin{align*}
\text{lit} & \quad \text{clause}[\text{lit}] \\
\top & \\
\text{lit} & \quad \text{clause}[\neg\text{lit}] \\
\bot &
\end{align*}
\]
Summary

Today

• Course overview & logistics
• Review of propositional logic
• A basic SAT solver

Next Lecture

• A modern SAT solver
• Read Chapter 1 of Bradley & Manna