Automated Program Verification and Testing
15414/15614 Fall 2016
Lecture 2:
Propositional Logic

Matt Fredrikson
mfredrik@cs.cmu.edu

October 17, 2016

Propositional Formulas: Syntax

$$\boxed{p \vee \neg q \rightarrow r}$$

An *atom* is an assertion that is either true or false

A *literal* is an atom or its negation

Propositional formulas are built from literals and *logical connectives*

More Syntax: Well-Formed Formulas

We obtain *well-formed formulas* using the grammar below:

$\langle \textit{atom} \rangle$ ::= $\top$ **(true)** | $\bot$ **(false)** | $P, Q, \ldots$ **(propositional variables)**

$\langle \textit{literal} \rangle$ ::= $\langle \textit{atom} \rangle$ | $\neg \langle \textit{atom} \rangle$ **(negation)**

$$
\begin{aligned}
\langle \textit{formula} \rangle ::= {} & \langle \textit{literal} \rangle \\
| {} & \neg \langle \textit{formula} \rangle && \textbf{(negation)} \\
| {} & \langle \textit{formula} \rangle \wedge \langle \textit{formula} \rangle && \textbf{(conjunction)} \\
| {} & \langle \textit{formula} \rangle \vee \langle \textit{formula} \rangle && \textbf{(disjunction)} \\
| {} & \langle \textit{formula} \rangle \rightarrow \langle \textit{formula} \rangle && \textbf{(implication)} \\
| {} & \langle \textit{formula} \rangle \leftrightarrow \langle \textit{formula} \rangle && \textbf{(equivalence)}
\end{aligned}
$$

Propositional Formulas: Semantics

Goal: Give meaning to propositional formulas

Assign Boolean truth values to (formula, interpretation) pairs

Formula F + **Interpretation** I = **Truth Value** (*true*, *false*)

Note: we often abbreviate *true* by 1 and *false* by 0

Interpretation

An interpretation I for propositional formula F maps every propositional variable appearing in F to a truth value, i.e.:

$$I = \{P \mapsto \textit{true}, Q \mapsto \textit{false}, R \mapsto \textit{false}, \ldots\}$$

Interpretations

Satisfying Interpretation

I is a *satisfying interpretation* of a propositional formula F if F is *true* under I. We denote this with the notation:

$$I \models F$$

Falsifying Interpretation

I is a *falsifying interpretation* of a propositional formula F if F is *false* under I. We denote this with the notation:

$$I \not\models F$$

Semantics: Inductive Definition

Define meaning of atoms first

Assuming these definitions, define each logical connective

Base Case:

$I \models \top$

$I \not\models \bot$

$I \models P$ iff $I[P]$ = *true*

$I \not\models P$ iff $I[P]$ = *false*

Inductive Case:

$I \models \neg F$ iff $I \not\models F$

$I \models F_1 \wedge F_2$ iff $I \models F_1$ and $I \models F_2$

$I \models F_1 \vee F_2$ 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 $I \not\models F_2$

What's with $\rightarrow$?

$$\boxed{I \models P \rightarrow Q \text{ iff } I \not\models P \text{ or } I \models Q}$$

If P is *false*, then $P \rightarrow Q$ is always *true*—can this be right?

P	Q	$P \rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

$(P \wedge Q) \rightarrow P$ should *always* be true

Two cases:

- $P \wedge Q$ is *true*: $I \models 1 \wedge 1 \rightarrow 1$
- $P \wedge Q$ is *false*:

$$I \models 1 \wedge 0 \rightarrow 1$$
$$I \models 0 \wedge 1 \rightarrow 0$$

$P \rightarrow Q$ should not always be equal to $Q \rightarrow P$

$$I \not\models 1 \rightarrow 0$$

Inductive Semantics: Example

$$\boxed{P \land Q \to P \lor \neg Q}$$

$I : \{P \mapsto \textit{true}, Q \mapsto \textit{false}\}$

	Step	Reason
1.	$I \models P$	$I[P]$ = *true*
2.	$I \not\models Q$	$I[Q]$ = *false*
3.	$I \models \neg Q$	*(2)* and $\neg$
4.	$I \not\models P \land Q$	*(2)* and $\land$
5.	$I \models P \land Q \to P \lor \neg Q$	*(4)* and $\to$

Which steps are unnecessary?

Satisfiability & Validity

Satisfiable Formula

A formula F is satisfiable if and only if *there exists* an interpretation I such that $I \models F$.

Valid Formula

A formula F is valid if and only if *for all* interpretations I, it is the case that $I \models F$.

Note: Satisfiability and Validity are dual notions.

F is valid if and only if $\neg F$ is unsatisfiable

Proving Satisfiability & Validity

Note: duality lets us prove either property, translate into dual result

We'll assume we're proving validity

There are two basic approaches for proving these properties

Search

1. Enumerate all interpretations
2. Check that each is satisfying

Deduction

1. Define proof rules from the semantics
2. Apply rules to reach desired conclusion

Proof by Search: Truth Tables

$$F : P \wedge Q \rightarrow P \vee \neg Q$$

Goal: Determine whether F is valid.

P	Q	$P \wedge Q$	$P \vee \neg Q$	F
0	0	0	1	1
0	1	0	0	1
1	0	0	1	1
1	1	1	1	1

First, fill out the truth table.

F is valid $\Leftrightarrow$ all rows are *true*

F is unsat. $\Leftrightarrow$ all rows are *false*

F is valid

Proving Satisfiability & Validity

There are two basic approaches for proving these properties

Note: duality lets us prove either property, translate into dual result

Search

1. Enumerate all interpretations
2. Check that each is satisfying

Brute-force approach
Runtime: $2^{|\text{vars}|}$

Deduction

1. Define proof rules from the semantics
2. Apply rules to reach desired conclusion

Proof by Deduction: Semantic Argument

Several techniques for proving validity by deduction

We'll focus on the semantic argument method

1. Assume F is not valid: there exists I such that $I \not\models F$
2. Apply proof rules (more on this shortly)
3. **If**: no contradiction, no applicable rules, conclude that F is invalid
4. **If**: every branch reaches contradiction, conclude that F is valid

Semantic Argument: Proof Rules (Negation)

According to the semantics for negation:

- From $I \models \neg F$ we can deduce $I \not\models F$:

$$\frac{I \models \neg F}{I \not\models F}$$

- From $I \not\models \neg F$, deduce $I \models F$:

$$\frac{I \not\models \neg F}{I \models F}$$

Semantic Argument: Proof Rules (Conjunction)

According to the semantics for conjunction:

- From $I \models F \wedge G$:

$$\frac{I \models F \wedge G}{I \models F \qquad I \models G}$$

  Note that there are two simultaneous conclusions in this rule

- From $I \not\models F \wedge G$:

$$\frac{I \not\models F \wedge G}{I \not\models F \quad \mid \quad I \not\models G}$$

  The bar denotes “or”, so this introduces two cases into the proof

Semantic Argument: Proof Rules (Disjunction)

According to the semantics for disjunction:

- From $I \models F \vee G$:

$$\frac{I \models F \vee G}{I \models F \quad | \quad I \models G}$$

- From $I \not\models F \vee G$:

$$\frac{I \not\models F \vee G}{I \not\models F \qquad I \not\models G}$$

Semantic Argument: Proof Rules (Implication)

According to the semantics for implication:

- From $I \models F \rightarrow G$:

$$\frac{I \models F \rightarrow G}{I \not\models F \quad | \quad I \models G}$$

- From $I \not\models F \rightarrow G$:

$$\frac{I \not\models F \rightarrow G}{I \models F \quad I \not\models G}$$

Semantic Argument: Proof Rules (Equivalence)

According to the semantics for equivalence:

- From $I \models F \leftrightarrow G$:

$$\frac{I \models F \leftrightarrow G}{I \models F \wedge G \quad \mid \quad I \models \neg F \wedge \neg G}$$

- From $I \not\models F \leftrightarrow G$:

$$\frac{I \not\models F \leftrightarrow G}{I \models F \wedge \neg G \quad \mid \quad I \models \neg F \wedge G}$$

Semantic Argument: Proof Rules

$$\frac{I \models \neg F}{I \not\models F} \qquad \frac{I \not\models \neg F}{I \models F}$$

$$\frac{I \models F \wedge G}{I \models F \qquad I \models G} \qquad \frac{I \not\models F \wedge G}{I \not\models F \quad | \quad I \not\models G}$$

$$\frac{I \models F \vee G}{I \models F \quad | \quad I \models G} \qquad \frac{I \not\models F \vee G}{I \not\models F \qquad I \not\models G} \qquad \frac{I \models F \rightarrow G}{I \not\models F \quad | \quad I \models G}$$

$$\frac{I \not\models F \rightarrow G}{I \models F \qquad I \not\models G} \qquad \frac{I \models F \leftrightarrow G}{I \models F \wedge G \quad | \quad I \models \neg F \wedge \neg G}$$

$$\frac{I \not\models F \leftrightarrow G}{I \models F \wedge \neg G \quad | \quad I \models \neg F \wedge G}$$

Semantic Argument: Example

$$\boxed{F : P \wedge Q}$$

1	$I \not\models P \wedge Q$	(assumption)
2	$I \not\models P$	(1 and $\wedge$, case a)
3	$I \not\models Q$	(1 and $\wedge$, case b)

$$\frac{I \models \neg F}{I \not\models F} \qquad \frac{I \not\models \neg F}{I \models F}$$

$$\frac{I \models F \wedge G}{I \models F \qquad I \models G}$$

$$\frac{I \not\models F \wedge G}{I \not\models F \quad | \quad I \not\models G}$$

No more rules to apply, no contradiction

Therefore, F is invalid, and I is a falsifying interpretation

Semantic Argument: Example

$$F : P \wedge Q \rightarrow P \vee \neg Q$$

1	$I \not\models F$	(assum.)
2	$I \models P \wedge Q$	(1 and $\rightarrow$)
3	$I \not\models P \vee \neg Q$	(1 and $\rightarrow$)
4	$I \models P$	(2 and $\wedge$)
5	$I \not\models P$	(3 and $\vee$)
6	$\perp$	(4 and 5)

$$\frac{I \models \neg F}{I \not\models F} \qquad \frac{I \not\models \neg F}{I \models F} \qquad \frac{I \models F \wedge G}{I \models F \quad I \models G}$$

$$\frac{I \not\models F \wedge G}{I \not\models F \quad | \quad I \not\models G} \qquad \frac{I \models F \vee G}{I \models F \quad | \quad I \models G}$$

$$\frac{I \not\models F \vee G}{I \not\models F \quad I \not\models G} \qquad \frac{I \models F \rightarrow G}{I \not\models F \quad | \quad I \models G}$$

$$\frac{I \not\models F \rightarrow G}{I \models F \quad I \not\models G}$$

Found a contradiction, so F is valid

Semantic Judgements

Equivalence of Formulas

Propositional formulas F_1 and F_2 are *equivalent*, written $F_1 \Leftrightarrow F_2$, if and only if the propositional formula $F_1 \leftrightarrow F_2$ is valid.

Implication

Propositional formula F_1 *implies* F_2, written $F_1 \Rightarrow F_2$, if and only if the propositional formula $F_1 \rightarrow F_2$ is valid.

Important: $F_1 \Leftrightarrow F_2$ and $F_1 \Rightarrow F_2$ are *not* propositional formulas.

Equivalence and implication let us relate the semantics of formulas

We can decide these judgements by solving for validity, and thus, satisfiability.

Normal Forms

Normal Form

A *normal form* of a logic:

- Restricts the syntax of formulas
- Has equivalent representation for any formula in the logic

Think of an intermediate representation for logic...

Three major propositional normal forms

Negation (NNF)	**Disjunctive (DNF)**	**Conjunctive (CNF)**
$\wedge, \vee, \neg$ $\neg$ only on literals	Disjunction of conjunctions	Conjunction of disjunctions

Negation Normal Form (NNF)

Apply equivalences to convert to NNF:

$$
\begin{aligned}
\neg\neg F &\Leftrightarrow F \\
\neg\top &\Leftrightarrow \bot \\
\neg\bot &\Leftrightarrow \top \\
\neg(F_1 \wedge F_2) &\Leftrightarrow \neg F_1 \vee \neg F_2 \\
\neg(F_1 \vee F_2) &\Leftrightarrow \neg F_1 \wedge \neg F_2 \\
F_1 \rightarrow F_2 &\Leftrightarrow \neg F_1 \vee F_2
\end{aligned}
$$

$$
\begin{aligned}
\langle \textit{atom} \rangle &::= \top \mid \bot \mid P, Q, \ldots \\
\langle \textit{literal} \rangle &::= \langle \textit{atom} \rangle \mid \neg \langle \textit{atom} \rangle \\
\langle \textit{formula} \rangle &::= \langle \textit{literal} \rangle \\
&\quad \mid \langle \textit{formula} \rangle \wedge \langle \textit{formula} \rangle \\
&\quad \mid \langle \textit{formula} \rangle \vee \langle \textit{formula} \rangle
\end{aligned}
$$

NNF Conversion

$$\boxed{\neg(P \to \neg(P \wedge Q))}$$

1. $\neg(P \to \neg(P \wedge Q))$
2. $\neg(\neg P \vee \neg(P \wedge Q))$
3. $\neg\neg P \wedge (P \wedge Q)$
4. $P \wedge P \wedge Q$

$$\begin{aligned}
\neg\neg F &\Leftrightarrow F \\
\neg\top &\Leftrightarrow \bot \\
\neg\bot &\Leftrightarrow \top \\
\neg(F_1 \wedge F_2) &\Leftrightarrow \neg F_1 \vee \neg F_2 \\
\neg(F_1 \vee F_2) &\Leftrightarrow \neg F_1 \wedge \neg F_2 \\
F_1 \to F_2 &\Leftrightarrow \neg F_1 \vee F_2
\end{aligned}$$

Disjunctive Normal Form (DNF)

Take the form:

$$\bigvee_i \bigwedge_j P_{ij}$$

To convert to DNF:

1. Convert to NNF
2. Distribute $\wedge$ over $\vee$

Distributive equivalences:

$$F_1 \wedge (F_2 \vee F_3) \Leftrightarrow (F_1 \wedge F_2) \vee (F_1 \wedge F_3)$$
$$(F_1 \vee F_2) \wedge F_3 \Leftrightarrow (F_1 \wedge F_3) \vee (F_2 \wedge F_3)$$

$\langle \textit{atom} \rangle$ ::= $\top \mid \bot \mid P, Q, \ldots$

$\langle \textit{literal} \rangle$ ::= $\langle \textit{atom} \rangle \mid \neg \langle \textit{atom} \rangle$

$\langle \textit{clause} \rangle$ ::= $\langle \textit{literal} \rangle$
$\mid \langle \textit{literal} \rangle \wedge \langle \textit{clause} \rangle$

$\langle \textit{formula} \rangle$ ::= $\langle \textit{clause} \rangle$
$\mid \langle \textit{clause} \rangle \vee \langle \textit{formula} \rangle$

Converting to DNF: Example

$$\boxed{(F_1 \vee F_2) \wedge (\neg F_3 \rightarrow F_4)}$$

1. $(F_1 \vee F_2) \wedge (\neg F_3 \rightarrow F_4)$
2. $(F_1 \vee F_2) \wedge (\neg\neg F_3 \vee F_4)$
3. $(F_1 \vee F_2) \wedge (F_3 \vee F_4)$
4. $(F_1 \vee F_2) \wedge (F_3 \vee F_4)$
5. $(F_1 \wedge (F_3 \vee F_4)) \vee (F_2 \wedge (F_3 \vee F_4))$
6. $(F_1 \wedge F_3) \vee (F_1 \wedge F_4) \vee (F_2 \wedge F_3) \vee (F_2 \wedge F_4)$

Deciding SAT for DNF formulas is trivial

But! May cause exponential blowup in formula size.

Conjunctive Normal Form (CNF)

Take the form:

$$\bigwedge_i \bigvee_j P_{ij}$$

To convert to CNF:

1. Convert to NNF
2. Distribute $\vee$ over $\wedge$

Will we run into the same problem as DNF?

Deciding SAT for CNF is not trivial

But most solvers take this as input...

$\langle \textit{atom} \rangle$ ::= $\top \mid \bot \mid P, Q, \ldots$

$\langle \textit{literal} \rangle$ ::= $\langle \textit{atom} \rangle \mid \neg \langle \textit{atom} \rangle$

$\langle \textit{clause} \rangle$ ::= $\langle \textit{literal} \rangle$
$\mid \langle \textit{literal} \rangle \vee \langle \textit{clause} \rangle$

$\langle \textit{formula} \rangle$ ::= $\langle \textit{clause} \rangle$
$\mid \langle \textit{clause} \rangle \wedge \langle \textit{formula} \rangle$

Equisatisfiability

Equisatisfiability

Formulas F and G are *equisatisfiable* when F is satisfiable if and only if G is satisfiable.

If F and G are equisatisfiable, are they equivalent?

Example:

- $F \vee G$
- $(F \vee H) \wedge (G \vee \neg H)$

$I = \{F \mapsto 1, G \mapsto 0, H \mapsto 1\}$

Equisatisfiability is weaker than equivalence

Idea: Find a short equisatisfiable CNF to give to SAT solver

Tseitin's Tranformation

Key Idea: Insert new variables to represent subformulas

- Introduce a new *representative* variable P_G for every subformula G of the original formula F
  - E.g., for $F = G_1 \wedge G_2$, we have representatives P_{G_1}, P_{G_2}.
- For each subformula $G = G_1 \circ G_2$, assert: $P_G \leftrightarrow P_{G_1} \circ P_{G_2}$
- Convert each $P_G \leftrightarrow P_{G_1} \circ P_{G_2}$ to CNF
- Finally, construct the top-level CNF:

$$P_F \wedge \bigwedge_{G=(G_1 \circ G_2) \in S_F} \text{CNF}(P_G \leftrightarrow P_{G_1} \circ P_{G_2})$$

Tseitin's Tranformation: By Example

$$\boxed{P \to (Q \wedge R)}$$

1. Introduce a fresh variable for every non-atomic subformula
2. Convert each equivalence into CNF
3. Assert the conjunction of T_1 and the CNF-converted equivalences

$$\begin{aligned} T_1 &\leftrightarrow P \to T_2 \\ T_2 &\leftrightarrow Q \wedge R \end{aligned}$$

$$\begin{aligned} F_1 &: (T_1 \vee P) \wedge (T_1 \vee \neg T_2) \wedge (\neg T_1 \vee \neg P \vee T_2) \\ F_2 &: (\neg T_2 \vee Q) \wedge (\neg T_2 \vee R) \wedge (T_2 \vee \neg Q \vee \neg R) \end{aligned}$$

$$T_1 \wedge F_1 \wedge F_2$$

Tseitin's Tranformation: Formula Size

$$P_F \wedge \bigwedge_{G=(G_1 \circ G_2) \in S_F} \text{CNF}(P_G \leftrightarrow P_{G_1} \circ P_{G_2})$$

- Each $P_G \leftrightarrow P_{G_1} \circ P_{G_2}$ contains at most three variables and two connectives
- Each term in the big conjunction has constant-bounded CNF representation size
- $|S_F|$ is bounded by the number of connectives in F
- Thus, the transformation causes a linear increase in formula size

First Homework

- Goes out today
  - Shorter assignment
  - Reason about validity, normal forms, modeling computations
- Due next Thursday (Sept. 8) before class starts
- Available on course webpage and Blackboard
- Hand in using Blackboard
  - We're working on a better system for future assignments...
- For next class, finish reading chapter 1 of Bradley & Manna.