PROPOSITIONAL LOGIC

MATHEMATICAL LOGIC

- Logic is the foundation of computation.
- We will use logic for multiple purposes:
  - Describing specifications
  - Describing program executions
  - Mathematical guarantees of logic will translate to guarantees of program correctness
  - Decision procedures for logic will be used for verification.

PROPOSITIONAL LOGIC

Is $p \to q \to r \leftrightarrow (p \wedge q) \to r$ valid?

Is $p \wedge \bot \to \neg q \vee \top$ satisfiable?

SYNTAX

Atom	Truth Values - $\perp$: False, $\top$: True Propositional Variables - p,q,r…
Logical Connectives	$\wedge$: and, $\vee$: or, $\neg$: not, $\rightarrow$: implies, $\leftrightarrow$: if and only if(iff)
Literal	Atom or its negation
Formula	A literal or the application of logical connectives to formulae

SEMANTICS

Interpretation I

I : Set of Propositional Variables $\rightarrow \{ \bot , \top \}$

MODEL OF

Given an interpretation I and Formula F,

$I \models F$	F evaluates to $\top$ under I
$I \not\models F$	F evaluates to $\bot$ under I

SEMANTICS: INDUCTIVE DEFINITION

Base Case:

$I \models \top$	
$I \not\models \bot$	
$I \models p$	iff I(p)=$\top$
$I \not\models p$	iff I(p)=$\bot$

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 $I \not\models F_2$
Other cases ...	

EXAMPLE

$I = \{p : True, q : False\}$

$F = p \wedge q \rightarrow p \vee \neg q$

Is $I \vDash F$?

1. $I \nvDash q$
2. $I \nvDash p \wedge q$
3. $I \vDash p \wedge q \rightarrow p \vee \neg q$

PRECEDENCE OF LOGICAL CONNECTIVES

- We assume the following precedence from highest to lowest:
  - $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
  - Example: $\neg p \wedge q \rightarrow p \vee q \wedge r$ is the same as $((\neg p) \wedge q) \rightarrow (p \vee (q \wedge r))$.
- We assume that all logical connectives associate to the right.
  - Example: $p \rightarrow q \rightarrow r$ is the same as $p \rightarrow (q \rightarrow r)$
- Parenthesis can be used to change precedence or associativity.

SATISFIABILITY AND VALIDITY

- A formula F is satisfiable iff there exists an interpretation I such that $I \models F$.
- A formula F is valid iff for all interpretations I, $I \models F$.
- A formula F is valid iff $\neg F$ is unsatisfiable.
  - A Decision Procedure for satisfiability is therefore also a decision procedure for validity. How?

QUESTIONS

- A formula can either be SAT, UNSAT or VALID.
    - Does Validity ⇒ Satisfiability?
    - Does Satisfiability ⇒ Validity?
- Can a decision procedure for Validity be used as a decision procedure for Satisfiability?
    - F is satisfiable iff ¬F is not valid.
- Are the following formulae are sat, unsat or valid?
    - $p \land q \rightarrow p \lor q$
    - $p \lor q \rightarrow \neg p \lor \neg q$
    - $(p \rightarrow q \rightarrow r) \land (p \land q \land \neg r)$

MORE TERMINOLOGY

- Formulae F_1 and F_2 are equivalent (denoted by $F_1 \Leftrightarrow F_2$) when the formula $F_1 \leftrightarrow F_2$ is valid.
  - Example: $p \rightarrow q \Leftrightarrow \neg p \vee q$
  - Another definition: F_1 and F_2 are equivalent if for all interpretations I, $I \vDash F_1$ if and only if $I \vDash F_2$.
- Formula F_1 implies F_2 (denoted by $F_1 \Rightarrow F_2$) when the formula $F_1 \rightarrow F_2$ is valid.
  - Example: $(p \rightarrow q) \wedge p \Rightarrow q$
- Formulae F_1 and F_2 are equisatisfiable when F_1 is satisfiable if and only if F_2 is satisfiable.
  - Example: $p \wedge (q \vee r)$ and $q \vee r$ are equisatisfiable

MORE EXAMPLES

- Which of the following are true?
  - $\neg(F_1 \wedge F_2) \Leftrightarrow \neg F_1 \vee \neg F_2$
  - $(F_1 \leftrightarrow F_2) \wedge (F_2 \leftrightarrow F_3) \Rightarrow (F_1 \leftrightarrow F_3)$
  - $p \Leftrightarrow p \wedge q$
  - p and q are equisatisfiable.
- What is the simplest example of two formulae which are not equisatisfiable?

DECISION PROCEDURES FOR SATISFIABILITY AND VALIDITY

- Two methods
  - Truth Tables: Search for satisfying interpretation
  - Semantic Argument: Rule-based deductive approach
- Modern SAT solvers use combination of both approaches

TRUTH TABLES - EXAMPLE

$$p \wedge q \rightarrow p \vee \neg q$$

p	q	$\neg q$	$p \wedge q$	$p \vee \neg q$	$p \wedge q \rightarrow p \vee \neg q$
0	0	1	0	1	1
0	1	0	0	0	1
1	0	1	0	1	1
1	1	0	1	1	1

TRUTH TABLES - EXAMPLE

$p \wedge q \rightarrow p \vee \neg q$ is valid

p	q	$\neg q$	$p \wedge q$	$p \vee \neg q$	$p \wedge q \rightarrow p \vee \neg q$
0	0	1	0	1	1
0	1	0	0	0	1
1	0	1	0	1	1
1	1	0	1	1	1

SEMANTIC ARGUMENT METHOD

- Deductive approach for showing validity based on proof rules
- Main Idea: Proof by Contradiction.
  - Assume that a falsifying interpretation exists.
  - Use proof rules to deduce more facts.
  - Find contradictory facts.

PROOF RULES (NEGATION)

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

PROOF RULES (NEGATION)

PREMISE

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

PROOF RULES (NEGATION)

PREMISE

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

DEDUCTION

PROOF RULES (NEGATION)

PREMISE

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

DEDUCTION

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

PROOF RULES (CONJUNCTION)

$$\begin{array}{lll} I & \models & F \land G \\ \hline I & \models & F \\ I & \models & G \end{array}$$

PROOF RULES (CONJUNCTION)

$$\frac{I \models F \land G}{\begin{array}{l} I \models F \\ I \models G \end{array}}$$

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

PROOF RULES (CONJUNCTION)

$$\frac{I \models F \land G}{\begin{array}{l} I \models F \\ I \models G \end{array}}$$

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

BRANCHING:

Need to show a contradiction in every branch

PROOF RULES (DISJUNCTION)

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

$$\frac{I \not\models F \vee G}{\begin{array}{l} I \not\models F \\ I \not\models G \end{array}}$$

PROOF RULES (IMPLICATION)

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

$$\begin{array}{l} I \not\models F \to G \\ \hline I \models F \\ I \not\models G \end{array}$$

PROOF RULES (IFF)

$$\frac{I \models F \leftrightarrow G}{I \models F \land G \quad | \quad I \not\models F \lor G}$$

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

PROOF RULES (CONTRADICTION)

$$\begin{array}{rcl} I & \models & F \\ I & \not\models & F \\ \hline I & \models & \bot \end{array}$$

EXAMPLE

Prove that $p \wedge q \to p \vee \neg q$ is valid

EXAMPLE

Prove that $p \wedge q \rightarrow p \vee \neg q$ is valid

$$I \not\models p \wedge q \rightarrow p \vee \neg q$$

EXAMPLE

Prove that $p \land q \rightarrow p \lor \neg q$ is valid

$$\frac{I \not\models p \land q \rightarrow p \lor \neg q}{I \models p \land q \qquad I \not\models p \lor \neg q}$$

EXAMPLE

Prove that $p \wedge q \rightarrow p \vee \neg q$ is valid

$$\cfrac{I \not\models p \wedge q \rightarrow p \vee \neg q}{\cfrac{I \models p \wedge q}{\begin{array}{c} I \models p \\ I \models q \end{array}} \quad \cfrac{I \not\models p \vee \neg q}{\begin{array}{c} I \not\models p \\ I \not\models \neg q \end{array}}}$$

EXAMPLE

Prove that $p \land q \to p \lor \neg q$ is valid

$$\dfrac{I \not\models p \land q \to p \lor \neg q}{\dfrac{I \models p \land q}{\begin{array}{c}\boxed{I \models p} \\ I \models q\end{array}} \qquad \dfrac{I \not\models p \lor \neg q}{\begin{array}{c}\boxed{I \not\models p} \\ I \not\models \neg q\end{array}}}$$

CONTRADICTION

EXAMPLE WITH BRANCHING

Prove that $(p \rightarrow q) \wedge p \rightarrow q$ is valid

EXAMPLE WITH BRANCHING

Prove that $(p \rightarrow q) \land p \rightarrow q$ is valid

$$I \not\models (p \rightarrow q) \land p \rightarrow q$$

EXAMPLE WITH BRANCHING

Prove that $(p \to q) \land p \to q$ is valid

$$\frac{I \not\models (p \to q) \land p \to q}{I \models (p \to q \land p) \qquad I \not\models q}$$

EXAMPLE WITH BRANCHING

Prove that $(p \rightarrow q) \land p \rightarrow q$ is valid

$$\frac{I \not\models (p \rightarrow q) \land p \rightarrow q}{\dfrac{I \models (p \rightarrow q \land p)}{I \models (p \rightarrow q) \quad I \models p} \quad I \not\models q}$$

EXAMPLE WITH BRANCHING

Prove that $(p \to q) \land p \to q$ is valid

$$\dfrac{I \not\models (p \to q) \land p \to q}{I \models (p \to q \land p) \qquad I \not\models q}$$

$$\dfrac{I \models (p \to q \land p)}{I \models (p \to q) \qquad I \models p}$$

$$\dfrac{I \models (p \to q)}{I \not\models p \quad \mid \quad I \models q}$$

EXAMPLE WITH BRANCHING

Prove that $(p \to q) \land p \to q$ is valid

$$\dfrac{I \not\models (p \to q) \land p \to q}{\dfrac{I \models (p \to q \land p)}{\dfrac{I \models (p \to q)}{\boxed{I \not\models p} \;\Big|\; I \models q} \quad \boxed{I \models p}} \quad I \not\models q}$$

CONTRADICTION

EXAMPLE WITH BRANCHING

Prove that $(p \to q) \land p \to q$ is valid

$$I \not\models (p \to q) \land p \to q$$

$$I \models (p \to q \land p) \qquad \boxed{I \not\models q}$$

$$I \models (p \to q) \qquad I \models p$$

$$I \not\models p \;\Big|\; \boxed{I \models q}$$

CONTRADICTION

Each branch should lead to a contradiction

ANNOUNCEMENTS

- Lectures slides and recorded video lectures are available on the course webpage.
- Chapter 1 of the BM book is uploaded on the course moodle page.
    - Please try Exercises 1.1-1.5.

QUESTIONS

- Is the semantic argument method complete?
- Can we use the semantic argument method for satisfiability?
- What is the time complexity of the semantic argument method?

DECISION PROCEDURES FOR SAT

- We will go through the DPLL algorithm.
  - Davis-Putnam-Logemann-Loveland Algorithm
  - Combines truth table and deductive approaches
  - Requires formulae in Conjunctive Normal Form (CNF)
  - Forms the basis of modern SAT solvers

NORMAL FORMS

- A Normal Form of a formula F is another equivalent formula F′ which obeys some syntactic restrictions.
- Three important normal forms:
  - Negation Normal Form (NNF): Should use only $\neg$, $\wedge$, $\vee$ as the logical connectives, and $\neg$ should only be applied to literals
  - Disjunctive Normal Form (DNF): Should be a disjunction of conjunction of literals
  - Conjunctive Normal Form (CNF): Should be a conjunction of disjunction of literals

CONJUNCTIVE NORMAL FORM

- A conjunction of disjunction of literals

$$\bigwedge_i \bigvee_j \ell_{i,j} \quad \text{for literals } \ell_{i,j}$$

- Each inner disjunct is also called a clause
- Is every formula in CNF also in NNF?

CNF CONVERSION

- We can use distribution of $\vee$ over $\wedge$ to obtain formula in CNF
  - $F_1 \vee (F_2 \wedge F_3) \Leftrightarrow (F_1 \vee F_2) \wedge (F_1 \vee F_3)$
  - Causes exponential blowup.
- Tseitin's transformation algorithm can be used to obtain an equisatisfiable CNF formula linear in size
  - BM Chapter 1

TRUTH TABLE BASED METHOD

Decision Procedure for Satisfiability:
Returns true if F is SAT, false if F is UNSAT

```
SAT(F){
   if (F = ⊤) return true;
   if (F = ⊥) return false;
   Choose a variable p in F;
   return SAT(F[⊤/p]) ∨ SAT(F[⊥/p]);
}
```

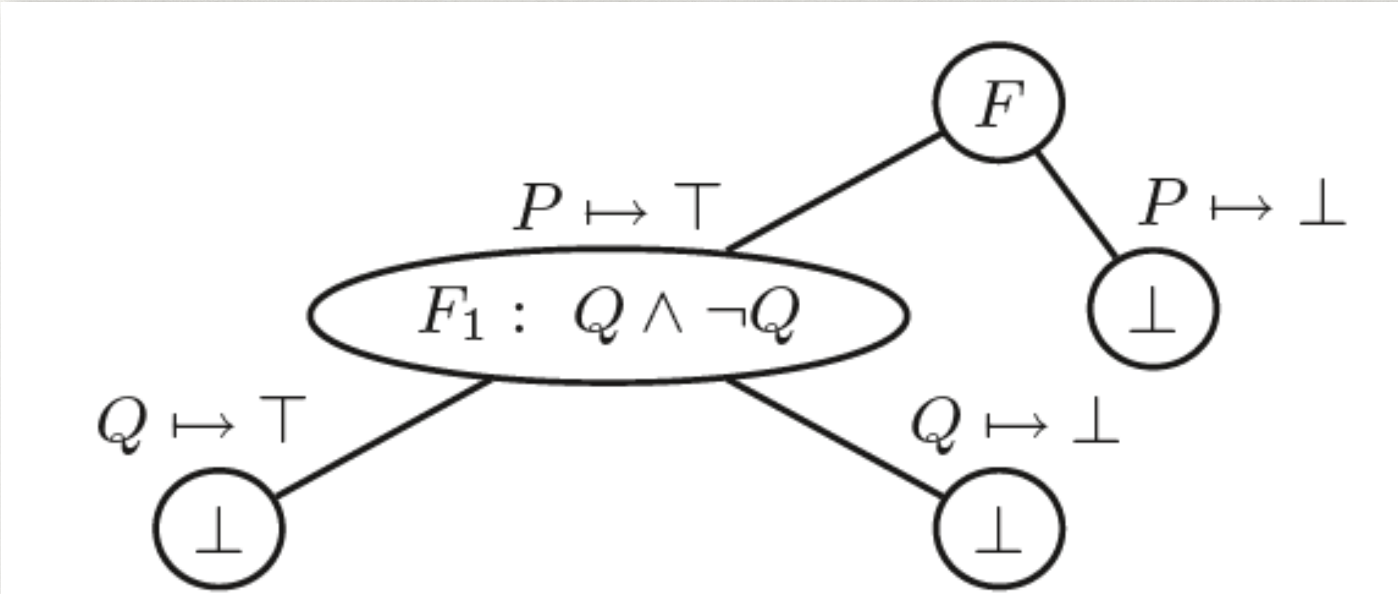
F[G/P] : G REPLACES EVERY OCCURRENCE OF P IN F, THEN SIMPLIFY

SIMPLIFICATION

- Following equivalences can be used to simplify:
  - $F \wedge \bot \Leftrightarrow \bot$
  - $F \wedge \top \Leftrightarrow F$
  - $F \vee \bot \Leftrightarrow F$
  - $F \vee \top \Leftrightarrow \top$

EXAMPLE

- SAT($(P \to Q) \land P \land \neg Q$)
- $F = (\neg P \lor Q) \land P \land \neg Q$
- $F[\top / P] \triangleq (\bot \lor Q) \land \top \land \neg Q \equiv Q \land \neg Q$



SIMPLIFICATION MAY SAVE BRANCHING ON SOME OCCASIONS