LAST LECTURE

- What/Why/How of Verification
- A Brief History of Verification
- Course Logistics

COURSE STRUCTURE

CONSTRAINT SOLVERS

- Propositional Logic, SAT solving, DPLL
- First-Order Logic, SMT
- First-Order Theories

↓

DEDUCTIVE VERIFICATION

- Operational Semantics
- Strongest Post-condition, Weakest Pre-condition
- Hoare Logic

↓

MODEL CHECKING AND OTHER VERIFICATION TECHNIQUES

- Predicate Abstraction, CEGAR
- Abstract Interpretation
- Property-directed Reachability
- …

LOGIC

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

PROPOSITIONAL LOGIC

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

$$p \wedge \bot \to \neg q \vee \top$$

Atom	Truth Values - $\bot$: False, $\top$: True Propositional Variables - p,q,r…
Logical Connectives	$\wedge$: and, $\vee$: or, $\neg$: not, $\to$: 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 : Propositional Variables → Truth Values

MODEL OF

Given an interpretation I and Formula F,

$I \models F$	F evaluates to True under I
$I \not\models F$	F evaluates to False under I

SEMANTICS: INDUCTIVE DEFINITION

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 $I \not\models F_2$

EXAMPLE

$I = \{p : True, q : False\}$ $\quad$ $F = p \wedge q \rightarrow p \vee \neg q$

Does $I \models F$?

1. $I \models p$
2. $I \not\models q$
3. $I \not\models p \wedge q$
4. $I \models p \wedge q \rightarrow p \vee \neg q$

SATISFIABILITY AND VALIDITY

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

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.
- Which of the following formulae are sat, unsat or valid?
  - $p \wedge q \rightarrow p \vee q$
  - $p \vee q \rightarrow \neg p \vee \neg q$
  - $(p \rightarrow q \rightarrow r) \wedge (p \wedge q \wedge \neg r)$

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: $p \rightarrow q \Leftrightarrow \neg p \vee q$
- 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)

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

PREMISE

DEDUCTION

PROOF RULES (NEGATION)

PREMISE

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

DEDUCTION

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

PROOF RULES (CONJUNCTION)

$$\begin{array}{lcl} I & \models & F \wedge G \\ \hline I & \models & F \\ I & \models & G \end{array}$$

PROOF RULES (CONJUNCTION)

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

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

PROOF RULES (CONJUNCTION)

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

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

BRANCHING

PROOF RULES (DISJUNCTION)

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

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

PROOF RULES (IMPLICATION)

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

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

PROOF RULES (IFF)

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

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

PROOF RULES (CONTRADICTION)

$$\frac{\begin{array}{rcl} I & \models & F \\ I & \not\models & F \end{array}}{\begin{array}{rcl} I & \models & \perp \end{array}}$$

EXAMPLE

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

$$\frac{I \not\models p \wedge q \rightarrow p \vee \neg q}{I \models p \wedge q \qquad I \not\models p \vee \neg q}$$

EXAMPLE

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

$$\dfrac{I \nvDash p \land q \rightarrow p \lor \neg q}{I \vDash p \land q \qquad I \nvDash p \lor \neg q}$$

$$\dfrac{I \vDash p \land q}{\begin{array}{c} I \vDash p \\ I \vDash q \end{array}} \qquad \dfrac{I \nvDash p \lor \neg q}{\begin{array}{c} I \nvDash p \\ I \nvDash \neg q \end{array}}$$

EXAMPLE

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

$$\dfrac{I \not\models p \land q \rightarrow p \lor \neg q}{\dfrac{I \models p \land q}{\begin{matrix} \boxed{I \models p} \\ I \models q \end{matrix}} \qquad \dfrac{I \not\models p \lor \neg q}{\begin{matrix} \boxed{I \not\models p} \\ I \not\models \neg q \end{matrix}}}$$

CONTRADICTION

EXAMPLE WITH BRANCHING

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

EXAMPLE WITH BRANCHING

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

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

EXAMPLE WITH BRANCHING

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

$$\dfrac{I \not\models (p \rightarrow q \wedge p) \rightarrow q}{I \models (p \rightarrow q \wedge p) \qquad I \not\models q}$$

EXAMPLE WITH BRANCHING

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

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

EXAMPLE WITH BRANCHING

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

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

EXAMPLE WITH BRANCHING

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

$$I \nvDash (p \rightarrow q \land p) \rightarrow q$$

$$I \vDash (p \rightarrow q \land p) \qquad I \nvDash q$$

$$I \vDash (p \rightarrow q) \qquad \boxed{I \vDash p}$$

$$\boxed{I \nvDash p} \;\Big|\; I \vDash q$$

CONTRADICTION

EXAMPLE WITH BRANCHING

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

$$\dfrac{I \not\models (p \rightarrow q \wedge p) \rightarrow q}{\dfrac{I \models (p \rightarrow q \wedge p)}{\dfrac{I \models (p \rightarrow q)}{I \not\models p \;\mid\; \boxed{I \models q}} \quad I \models p} \quad \boxed{I \not\models q}}$$

CONTRADICTION

Each branch should lead to a contradiction