

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 $p \rightarrow q \rightarrow r \leftrightarrow (p \wedge q) \rightarrow r$ valid?

Is $p \wedge \perp \rightarrow \neg q \vee \top$ satisfiable?

SYNTAX

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

Atom

Truth Values - \perp : False, \top : True

Propositional Variables - p, q, r, \dots

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

$I : \text{Propositional Variables} \rightarrow \text{Truth Values}$

Given an interpretation I and Formula F,

MODEL
OF

$I \models F$

F evaluates to True under I

$I \not\models F$

F evaluates to False under I

SEMANTICS: INDUCTIVE DEFINITION

Base Case:

$$I \models \top$$

$$I \not\models \perp$$

$$I \models p$$

$$I \not\models p$$

iff $I[p]=\text{true}$

iff $I[p]=\text{false}$

Inductive Case:

$$I \models \neg F$$

$$I \models F_1 \wedge F_2$$

$$I \models F_1 \vee F_2$$

$$I \models F_1 \rightarrow F_2$$

$$I \models F_1 \leftrightarrow F_2$$

iff $I \not\models F$

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

iff $I \models F_1$ or $I \models F_2$

iff $I \not\models F_1$ or $I \models F_2$

iff $I \models F_1$ and $I \models F_2$, or $I \not\models F_1$ and $I \not\models F_2$

EXAMPLE

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

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

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 $I \models F$.
- 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

QUESTIONS

- A formula can either be sat, unsat or valid.
 - Does Validity \Rightarrow Satisfiability?
 - Does Satisfiability \Rightarrow Validity?
- Can a decision procedure for Validity be used as a decision procedure for Satisfiability?
 - F is satisfiable iff $\neg F$ 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 |

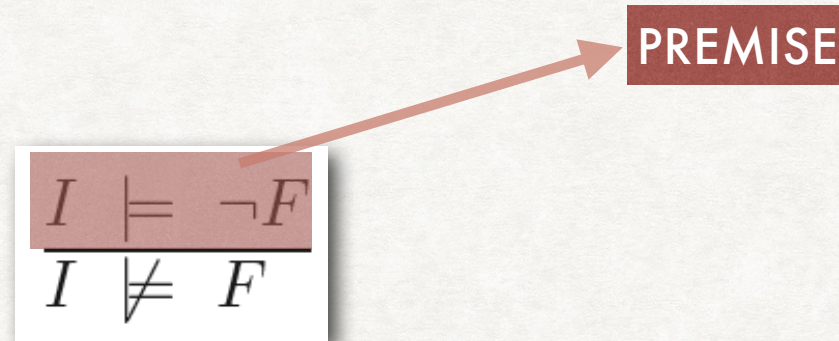
SEMANTIC ARGUMENT METHOD

- 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)

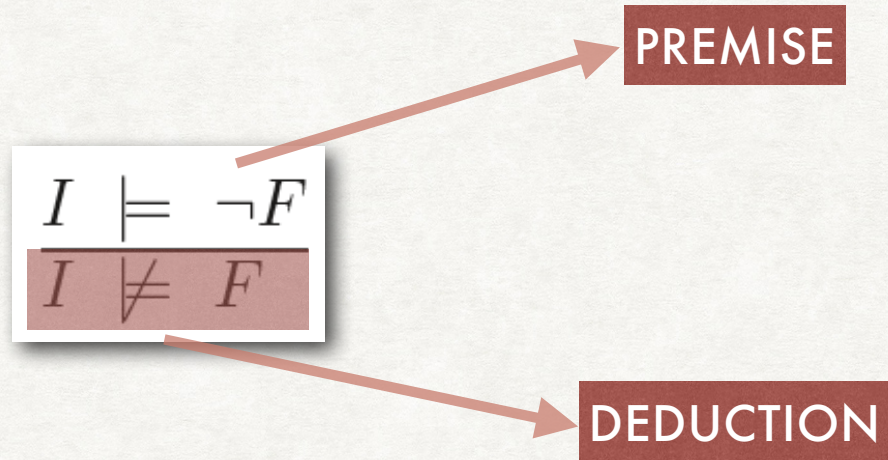


The diagram illustrates a logical rule for negation. It features a central box divided into two horizontal sections. The top section is shaded dark red and contains the expression $I \models \neg F$. The bottom section is white and contains the expression $I \not\models F$. A horizontal line separates these two sections. To the right of the top section, there is a dark red rectangular box containing the word "PREMISE" in white capital letters. A red arrow points from the top-right corner of the main box to the left side of the "PREMISE" box.

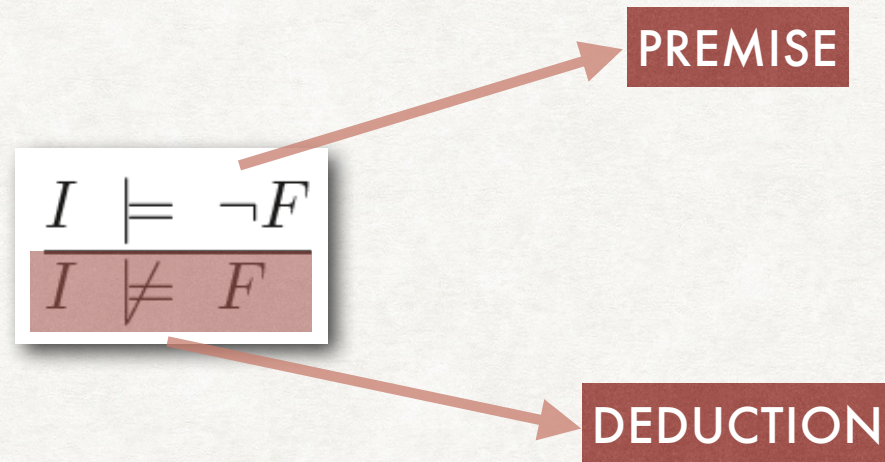
$$\frac{I \models \neg F}{I \not\models F}$$

PREMISE

PROOF RULES (NEGATION)



PROOF RULES (NEGATION)



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

PROOF RULES (CONJUNCTION)

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

PROOF RULES (CONJUNCTION)

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

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

PROOF RULES (CONJUNCTION)

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

$$\frac{I \not\models F \wedge G}{\begin{array}{l} I \not\models F \quad | \quad I \not\models G \end{array}}$$

BRANCHING



PROOF RULES (DISJUNCTION)

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

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

PROOF RULES (IMPLICATION)

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

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

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)

$$\frac{I \models F \quad I \not\models F}{I \models \perp}$$

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

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

EXAMPLE

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

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

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

$$I \models p$$

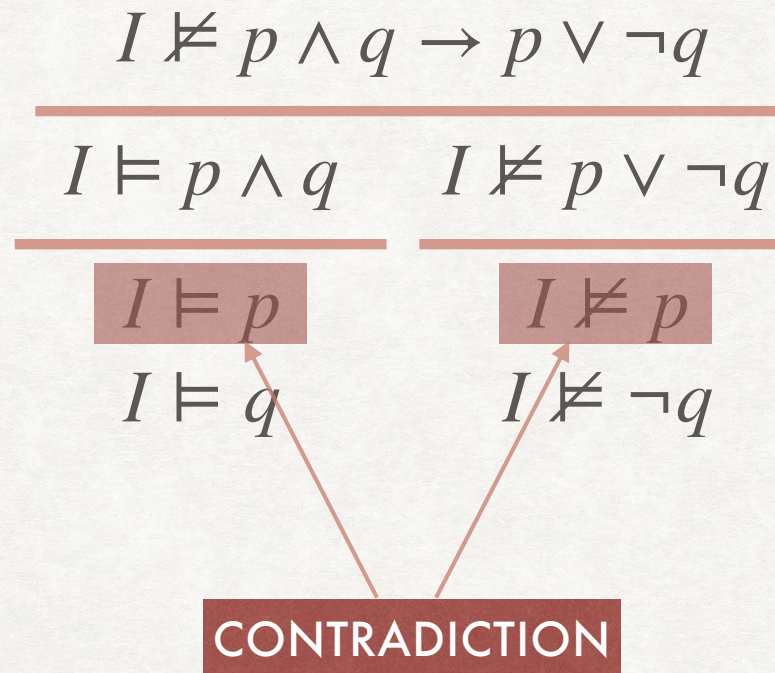
$$I \not\models p$$

$$I \models q$$

$$I \not\models \neg q$$

EXAMPLE

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



EXAMPLE WITH BRANCHING

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

EXAMPLE WITH BRANCHING

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

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

EXAMPLE WITH BRANCHING

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

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

$$I \models (p \rightarrow q \wedge p) \quad I \not\models q$$

EXAMPLE WITH BRANCHING

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

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

$$I \models (p \rightarrow q \wedge p) \quad I \not\models q$$

$$I \models (p \rightarrow q) \quad I \models p$$

EXAMPLE WITH BRANCHING

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

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

$$I \models (p \rightarrow q \wedge p) \quad I \not\models q$$

$$I \models (p \rightarrow q) \quad I \models p$$

$$I \not\models p \quad | \quad I \models q$$

EXAMPLE WITH BRANCHING

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

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

$$I \models (p \rightarrow q \wedge p) \quad I \not\models q$$

$$I \models (p \rightarrow q) \quad I \models p$$

$$I \not\models p \quad I \models q$$

CONTRADICTION

EXAMPLE WITH BRANCHING

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

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

$$I \models (p \rightarrow q \wedge p) \quad I \not\models q$$

$$I \models (p \rightarrow q) \quad I \models p$$

$$I \not\models p \quad I \models q$$

CONTRADICTION

Each branch should lead to a contradiction