L03: Inference & Proofs

- Objectives
  - Rules of Inference
    - Rules of Inference for Propositional Logic
    - Rules of Inference for Predicate Logic
  - Basic Proof Techniques
    - Some Terminology
    - Direct Proof
    - Proof by Contraposition
    - Proof by Contradiction

- Reading

  Kenneth Rosen: Section 1.6, 1.8

Rules of Inference

- Proofs in mathematics are valid arguments that establish the truth of mathematical statements.
  - By an **argument**, we mean a sequence of statements that end with a conclusion.
  - By **valid**, we mean that the conclusion, or final statement of the argument, must follow from the truth of the preceding statements, or **premises**, of the argument.
  - That is, an argument is valid if and only if it is impossible for all the premises to be true and the conclusion to be false.
- To deduce new statements from statements we already have, we use **rules of inference** which are templates for constructing valid arguments.
- Rules of inference are our basic tools for establishing the truth of statements.

Outline

- **Rules of Inference**
  - **Rules of Inference for Propositional Logic**
  - Rules of Inference for Predicate Logic
- **Basic Proof Technique**
  - Some Terminology
  - Direct Proof
  - Proof by Contraposition
  - Proof by Contradiction

Argument

- **Definition**

  An **argument** in propositional logic is a sequence of propositions.

  All but the final proposition in the argument are called **premises** or **hypotheses** and the final proposition is called the **conclusion**.

- **Definition**

  An argument is **valid** if the truth of all its premises implies that the conclusion is true.

Rules of Inference for Propositional Logic

- **Remark**

  An argument with premises p_1, p_2, … , p_n and conclusion q is valid when $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ is a tautology.

  Using a truth table to show the validity of an argument form can be very tedious.

  This process can be simplified significantly by using rules of inference.

Rules of Inference for Propositional Logic

Rules of Inference for Propositional Logic		
Rule of inference	**Tautology**	**Name**
$\begin{array}{rl} & p \\ & p \to q \\ \hline \therefore & q \end{array}$	$[p \wedge (p \to q)] \to q$	Modus ponens
$\begin{array}{rl} & \neg q \\ & p \to q \\ \hline \therefore & \neg p \end{array}$	$[\neg q \wedge (p \to q)] \to \neg p$	Modus tollens
$\begin{array}{rl} & p \to q \\ & q \to r \\ \hline \therefore & p \to r \end{array}$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Hypothetical syllogism
$\begin{array}{rl} & p \vee q \\ & \neg p \\ \hline \therefore & q \end{array}$	$[(p \vee q) \wedge \neg p] \to q$	Disjunctive syllogism

Rules of Inference for Propositional Logic (cont'd)

Rules of Inference for Propositional Logic		
Rule of inference	**Tautology**	**Name**
$\begin{array}{rl} & p \\ \hline \therefore & p \lor q \end{array}$	$p \to (p \lor q)$	Addition
$\begin{array}{rl} & p \land q \\ \hline \therefore & p \end{array}$	$(p \land q) \to p$	Simplification
$\begin{array}{rl} & p \\ & q \\ \hline \therefore & p \land q \end{array}$	$[(p) \land (q)] \to (p \land q)$	Conjunction
$\begin{array}{rl} & p \lor q \\ & \neg p \lor r \\ \hline \therefore & q \lor r \end{array}$	$[(p \lor q) \land (\neg p \lor r)] \to (q \lor r)$	Resolution

Examples

- **Example**

  Show that the hypotheses "it is not snowing or Jasmine is skiing" and "it is snowing or Bart is playing hockey" imply that "Jasmine is skiing or Bart is playing hockey".
- s: it is snowing
- k: Jasmine is skiing
- h: Bart is playing hockey
- **Solution**

$$\begin{array}{l} \neg s \lor k \\ s \lor h \\ \hline \therefore\ k \lor h \end{array}$$

(by resolution)

Example

- **Example**

  Show that the hypotheses $(p \wedge q) \vee r$ and $r \rightarrow s$ imply the conclusion $p \vee s$.

- **Solution**

1. $(p \wedge q) \vee r$	Premise
2. $r \rightarrow s$	Premise
3. $\neg r \vee s$	2, equivalence
4. $(p \wedge q) \vee s$	1,3 resolution
5. $(p \vee s) \wedge (q \vee s)$	4, equivalence
6. $p \vee s$	5, simplification

Example

- Show that the following premises lead to the conclusion.
- Propositions
  - p: "it is sunny this afternoon."
  - q: "it is colder than yesterday."
  - r: "we will go swimming."
  - s: "we will take a canoe trip."
  - t: "we will be home by sunset"
- Premises:
  - "it is not sunny this afternoon and it is colder than yesterday"
    $\neg p \wedge q$
  - "we will go swimming only if it is sunny"
    $r \rightarrow p$
  - "if we do not go swimming, then we will take a canoe trip"
    $\neg r \rightarrow s$
  - "if we take a canoe trip, then we will be home by sunset"
    $s \rightarrow t$
- Conclusion: t: "we will be home by sunset".

Example (cont)

1. $\neg p \wedge q$ Premise
2. $\neg p$ 1, Simplification
3. $r \rightarrow p$ Premise
4. $\neg r$ 2,3 Modus tollens
5. $\neg r \rightarrow s$ Premise
6. s Modus ponens
7. $s \rightarrow t$ Premise
8. t Modus ponens

- **Remark:** We could have used a truth table to show that whenever each of the four premises is true, the conclusion is also true. However, because we are working with five propositional variables p, q, r, s, and t, such a truth table would have $2^5 = 32$ rows.

Outline

- **Rules of Inference**
  - Rules of Inference for Propositional Logic
  - **Rules of Inference for Predicate Logic**
- **Basic Proof Technique**
  - Some Terminology
  - Direct Proof
  - Proof by Contraposition
  - Proof by Contradiction

Rules of Inference for Predicate Logic

Rules of Inference for Predicate Logic	
Rule of inference	**Name**
$\forall x\, P(x)$ $\therefore\ P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore\ \forall x\, P(x)$	Universal generalization
$\exists x\, P(x)$ $\therefore\ P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore\ \exists x\, P(x)$	Existential generalization

Examples

- Show that the premises "everyone in this discrete mathematics class has taken a course in computer science" and "Joseph is a student in this class" imply the conclusion "Joseph has taken a course in computer science", using the following predicates.
  - $P(x)$: x is a student in the discrete mathematics class
  - $C(x)$: x has taken a course in computer science
- **Solution**

1. $\forall x\, (P(x) \rightarrow C(x))$	Premise
2. $P(Joseph) \rightarrow C(Joseph)$	Universal instantiation
3. $P(Joseph)$	Premise
4. $C(Joseph)$	2,3 Modus ponens

Example

- **Example**
  Assume that "for all positive integers *n*, if *n* is greater than 4, then n^2 is less than 2^n" is true. Use universal modus ponens to show that $100^2 < 2^{100}$

Example

- Show that the premises “a student in this class has not read the textbook” and “everyone in this class passed the course” imply the conclusion “someone who passed the course has not read the textbook”.
- Predicates:
  - $P(x)$: x is a student in this class
  - $R(x)$: x has read the textbook
  - $U(x)$: x passed the course

Solution

1. $\exists x\,(P(x) \wedge \neg R(x))$	Premise
2. $P(a) \wedge \neg R(a)$ for some a	1, Existential instantiation
3. $P(a)$	2, Simplification
4. $\neg R(a)$	2, Simplification
5. $\forall x\,(P(x) \rightarrow U(x))$	Premise
6. $P(a) \rightarrow U(a)$	*5,* Universal instantiation
7. $U(a)$	3,6, Modus ponens
8. $U(a) \wedge \neg R(a)$	4,7, Conjunction
9. $\exists x\,(U(x) \wedge \neg R(x))$	8, Existential generalization

Outline

- Rules of Inference
  - Rules of Inference for Propositional Logic
  - Rules of Inference for Predicate Logic
- Basic Proof Techniques
  - **Some Terminology**
  - Direct Proof
  - Proof by Contraposition
  - Proof by Contradiction

Some Terminology

- **Definition:** A **theorem** is a statement that can be shown to be true.
- **Definition:** An **axiom** is a statement that is assumed to be true.
- **Definition:** A less important theorem that is helpful in the proof of other theorems is called a **lemma**.
- **Definition:** A **proof** is a valid argument that establishes the truth of a theorem. The statements used in a proof can include axioms, premises of the theorem, and previously proved theorems or lemmas. Using these ingredients and rules of inference, the final step of the proof establishes the truth of the statement being proved.

Some Terminology

- **Definition**

  A **corollary** is a theorem that can be established directly from a theorem that has been proved.

- **Definition**

  A **conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

- **Remark**

  When a proof of a conjecture is found, the conjecture becomes a theorem. However, many conjectures are eventually found to be false.

Outline

- **Rules of Inference**
  - Rules of Inference for Propositional Logic
  - Rules of Inference for Predicate Logic
- **Basic Proof Technique**
  - Some Terminology
  - **Direct Proof**
  - Proof by Contraposition
  - Proof by Contradiction

Direct Proof

- A **direct proof** of a conditional statement $p \rightarrow q$

  The first step is the assumption that p is true.

  Subsequent steps are constructed using axioms, definitions, previously proved theorems, and rules of inference, with the final step showing that q must also be true.

Direct Proof

- **Example**

  Give a direct proof of the theorem "if n is an odd integer, then n^2 is odd". (An integer n is **odd** if there exists an integer k such that $n = 2k + 1$.)

- **Proof:**

  Assume that the hypothesis of this implication is true; namely, suppose that n is odd.

  Then $n = 2k + 1$, where k is an integer.

  It follows that $n^2 = (2k + 1)^2 = 2(2k^2+2k)+1$.

  Therefore, n^2 is odd.

Examples

- **Example**

  Give a direct proof that if m and n are both perfect squares, then mn is also a **perfect square**. (An integer a is a perfect square if there exists an integer b such that $a = b^2$.)

- **Example**

  Prove that the sum of two rational numbers is rational. (A real number r is **rational** if there exist integers p and q with $q \neq 0$ such that $r = p / q$. A real number that is not rational is called **irrational**.)

Limitation of Direct Proofs

- **Remark**

Direct proofs are useful but attempts at direct proofs sometimes lead to dead ends. There are other proof techniques.

Proofs that are not direct proofs, i.e., that do not start with the hypothesis and end with the conclusion, are called **indirect proofs**.

We will consider several types of indirect proofs.

Outline

- **Rules of Inference**
  - Rules of Inference for Propositional Logic
  - Rules of Inference for Predicate Logic
- **Basic Proof Technique**
  - Some Terminology
  - Direct Proof
  - **Proof by Contraposition**
  - Proof by Contradiction

Proof by contraposition

- A **proof by contraposition** makes use of the fact that the conditional statement $p \to q$ is equivalent to its contrapositive $\neg q \to \neg p$.

- This means that the conditional statement $p \to q$ can be proved by showing that its contrapositive $\neg q \to \neg p$ is true.

- To do so, we take $\neg q$ as a hypothesis, and using axioms, definitions, previously proved theorems, and rules of inference, we show that $\neg p$ must follow.

Examples

- **Example**

  Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

- **Proof**

  Assume that the conclusion of this implication is false;

  namely, assume that n is even.

  Then $n = 2k$ for some integer k.

  It follows that $3n + 2 = 3(2k)+2 = 2(3k+1)$

  Therefore, $3n + 2$ is even.

Examples

- **Example**

  Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Outline

- **Rules of Inference**
  - Rules of Inference for Propositional Logic
  - Rules of Inference for Predicate Logic
- **Basic Proof Technique**
  - Some Terminology
  - Direct Proof
  - Proof by Contraposition
  - **Proof by Contradiction**

Proof by Contradiction

- Suppose we want to prove that a statement p is true.

- Instead, we assume p is false, i.e., $\neg p$ is true. Then, using axioms, definitions, previously proved theorems, and rules of inference, we derive a contradiction **F.** This means that our assumption that $\neg p$ is true p is false. Consequently, p must be true.

- An example of contradiction is $r \wedge \neg r$, where r is a proposition.

Examples

- **Example**

  Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

- **Proof:**

  Suppose $\sqrt{2}$ is rational. We will show that this leads to a contradiction.

  There exists integers a and b with $\sqrt{2} = a/b$, where a and b have no common factors.

  ….

  We have shown that 2 divides a and b. We obtain a contradiction.

Proof by Contradiction for Conditional Statement

- Proofs by contradiction can be used to prove conditional statements $p \to q$.

We first assume that the negation of the conclusion is true. We then use the premises of the theorem and the negation of the conclusion to arrive at a contradiction.

That is, $(p \land \neg q) \to \mathbf{F}$.

The validity of such proofs is based on the logical equivalence of $p \to q$ and $(p \land \neg q) \to \mathbf{F}$.

Proof by Contradiction for Conditional Statement (cont'd)

- We can rewrite a proof by contraposition of a conditional statement $p \rightarrow q$ as a proof by contradiction.
- In a proof by contraposition, we assume that $\neg q$ is true and then show that $\neg p$ must also be true.
- To rewrite as a proof by contradiction, we suppose that both p and $\neg q$ are true. Then, we use the steps from the proof of $\neg q \rightarrow \neg p$ to show that $\neg p$ is true. This leads to the contradiction $p \wedge \neg p$, completing the proof.

Proof by Contradiction for Conditional Statement (cont'd)

- **Example** (compare with proof by contraposition)

  Give a proof by contradiction of the theorem "if $3n + 2$ is odd, then n is odd".

- **Proof:**

We assume $3n+2$ is odd and n is not odd, i.e., n is even.

Following the same steps as in the solution of proving this statement by contraposition:

> $n = 2k$ for some integer k.
>
> ……
>
> then $3n + 2$ is even.

This contradicts the assumption that $3n + 2$ is odd, completing the proof.

Proving Biconditional Statements

- To prove a theorem that is a biconditional statement of the form $p \leftrightarrow q$, we show that both $p \rightarrow q$ and $q \rightarrow p$ are true.

- **Example**

  Prove the theorem "if n is a positive integer, then n is odd if and only if n^2 is odd".

Example

- **Example**

  Show that these statements about the integer n are logically equivalent:

$$p_1 : n \text{ is even}$$

$$p_2 : n\text{-}1 \text{ is odd}$$

$$p_3 : n^2 \text{ is even}$$

- **Hint:** We will prove that the implications $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, and $p_3 \rightarrow p_1$ are true.

Some comments on proofs

- There are many other proof methods
  - We will over some later; many will not be covered in this course.
- Constructing proofs is an art that can be learned only by trying various lines of attack. There are no fixed procedures for proving theorems.
- Many statements that appear to be theorems have resisted the persistent efforts of mathematicians for hundreds of years.
- For instance, Goldbach’s conjecture: “every even positive integer greater than 4 is the sum of two primes” has not yet been proved, and no counterexample has been found.

Automated Theorem Proving

- Hilbert's program: A computer program that, starting from a finite number of axioms and using the rule of inference, automatically decides the truth of any mathematical statement.
- Gödel's incompleteness theorem: This is not possible.
- There are several automated theorem proving systems that can prove certain subsets of mathematics.
- Proofs require human insight!