# Unit 4

## Proof Methods

# Outline of Unit 4

- 4.1 Why Proofs?
- 4.2 Validity of Arguments in Predicate Logic
- 4.3 Direct Proofs
- 4.4 Indirect Proofs

# Unit 4.1

Why Proofs?

# What is a Proof?

- A proof is a valid argument that establishes the truth of a statement.
  - If the statement is about mathematical objects (integers, triangles, sets, etc.), then it is a mathematical proof.
- In mathematical proofs,
  - more than one rule of inference are often used in a step,
  - steps may be skipped, and
  - the rules of inference may not be explicitly stated.

# The Pigeonhole Principle

- Suppose that you have $n$ pigeonholes.
- Suppose that you have $m$ pigeons, where $m > n$.
- If you put the $m$ pigeons into the $n$ pigeonholes, some pigeonhole will have more than one pigeon in it.

- $n = 9$ pigeonholes
- $m = 10$ pigeons
- Some pigeonhole has more than one pigeon.

How to prove it?

# Do We Need Proofs?

Mathematics consists in proving the most obvious thing in the least obvious way.

George Polya, a Hungarian mathematician

How about engineers?

**True love doesn't need proof. The eyes told what heart felt.**

Toba Beta, an Indonesian poet.

# Should EE Students Learn Proofs?

- My personal opinion:

  Engineering students should learn to discover, understand, and enjoy proofs.


- Why?
  - A way to convince oneself and others that a proposed engineering solution indeed works.
    - Network protocols, cryptographic protocols, database management, optimality of a (hardware/software) system, etc.
  - A sign of understanding.
    - Problem solving relies on deep understanding of a problem.
  - An intellectual challenge full of fun.
  - An art for appreciation.

# What is a Theorem?

- A theorem is a statement that can be proved to be true using
  - definitions,
  - other theorems,
  - axioms (statements which are given as true), and
  - rules of inference.

# Forms of Theorems

- Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, the triangles, the sets.
  - The universal quantifier is, however, often omitted.

- Example:

  "If $x > y$, where $x$ and $y$ are positive real numbers, then $x^2 > y^2$."

  can be written as the following universal statement:

  "$\forall x, y \in R_{++}$, if $x > y$, then $x^2 > y^2$."

# Unit 4.2

Validity of Arguments in Predicate Logic

# Proof of Validity in Predicate Logic

- To prove arguments consisting of quantified statements, we need to use
  - logical equivalence, and
    - (discussed in Units 2 and 3)
  - rules of inference for propositional logic, and
    - (discussed in Unit 3)
  - rules of inference for quantified statements
    - Universal Instantiation (UI)
    - Universal Generalization (UG)
    - Existential Instantiation (EI)
    - Existential Generalization (EG)

    } 4 basic rules

# Universal Instantiation (UI)

- If some property is true of *everything* in a set, then it is true of *any particular thing* in the set.

| | |
|---|---|
| All men are mortal. | $\forall x \in D, P(x)$ |
| Socrates was a man. | $s \in D$ |
| Socrates was mortal. | $P(s)$ |

# Universal Generalization (UG)

- If some property is true of *any arbitrary thing* in a set, then it is true of *everything* in the set.

$$\frac{P(s) \text{ for any arbitrary } s \in D}{\forall x \in D, P(x)}$$

- This rule allows you to move from a particular statement about an arbitrary object to a general statement using a quantified variable.
  - Used often implicitly in mathematical proofs.

# Existential Instantiation (EI)

$\exists x \in D, P(x)$.

---

$P(c)$ for some $c \in D$.

- Example

  There is someone who likes logic.

  ---

  Let's call her Jenny and say that Jenny likes logic.

# Existential Generalization (EG)

$P(c)$ for some specific $c \in D$.

---

$\exists x \in D, P(x)$.

- Example

  Newton is a scientist.

  ---

  There is a scientist.

# Classwork

- Show that the following argument is valid:

  Everyone is a logician.

  ---

  Someone is a logician.

Note: The domain is implicitly assumed to be the set of human beings, which is non-empty.

In this question, we may let it be {John, Bob, Eva, Sharon, …}.

- Solution:

# Universal Modus Ponens (UMP)

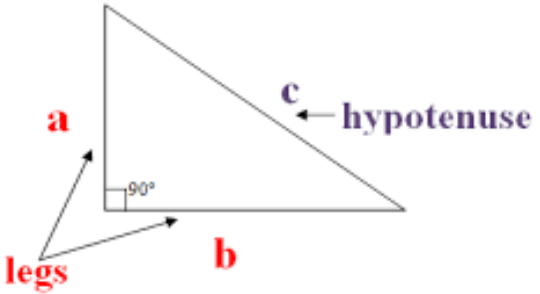
- Universal instantiation can be combined with modus ponens.

**Universal Modus Ponens**

| *Formal Version* | *Informal Version* |
|---|---|
| $\forall x$, if $P(x)$ then $Q(x)$. | If $x$ makes $P(x)$ true, then $x$ makes $Q(x)$ true. |
| $P(a)$ for a particular $a$. | $a$ makes $P(x)$ true. |
| $\therefore Q(a)$. | $\therefore a$ makes $Q(x)$ true. |

| | | |
|---|---|---|
| 1) | $\forall x \in D, P(x) \rightarrow Q(x)$ | (Premise) |
| 2) | $P(a) \rightarrow Q(a)$ | (UI 1) |
| 3) | $P(a)$ | (Premise) |
| 4) | $Q(a)$ | (MP 2,3) |

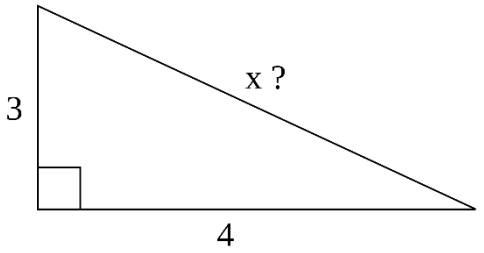
# Example: UMP




$a^2 + b^2 = c^2$

If a triangle is right-angled, then $c^2 = a^2 + b^2$.

The triangle shown at the right is a right-angled triangle.




---

$x^2 = 3^2 + 4^2$, (which implies $x = 5$).

# Universal Modus Tollens (UMT)

- Universal instantiation can be combined with modus tollens.

**Universal Modus Tollens**

| *Formal Version* | *Informal Version* |
| --- | --- |
| $\forall x$, if $P(x)$ then $Q(x)$. | If $x$ makes $P(x)$ true, then $x$ makes $Q(x)$ true. |
| $\sim Q(a)$, for a particular $a$. | $a$ does not make $Q(x)$ true. |
| $\therefore \sim P(a)$. | $\therefore a$ does not make $P(x)$ true. |

Validity can be shown in a similar way.

# Example: UMT

All muggles can't perform magic.

($\forall x$, if $x$ is a muggle, $x$ can't perform magic.)

Harry Potter can perform magic.

---

Harry Potter isn't a muggle.

Harry Potter, a fictional character.

"In the *Harry Potter* book series, a Muggle is a person who lacks any sort of magical ability and was not born in a magical family." – Wikipedia.

# Class Work

1) If you ***e***njoy watching a movie, you ***l***ove the lead actress of it.
2) You enjoy watching ***H****arry Potter*.
3) If you love the lead actress of *Harry Potter*, then you love the lead actress of ***B****eauty and the Beast*.

---

You must enjoy watching *Beauty and the Beast*.

Is it valid? Why or why not?

Hermione Granger, a fictional character in *Harry Potter*.

Belle, a fictional character in *Beauty and the Beast*.

# Analysis

| | | |
|---|---|---|
| 1) | $\forall x, e(x) \rightarrow l(x)$ | (Premise 1) |
| 2) | $e(H)$ | (Premise 2) |
| 3) | $l(H) \rightarrow l(B)$ | (Premise 3) |
| 4) | $l(H)$ | (UMP 1,2) |
| 5) | $l(B)$ | (MP 3,5) |
| 6) | $e(B) \rightarrow l(B)$ | (UI 1) |

The argument is invalid.

We can't conclude from lines 5 and 6 that $e(B)$ is true, since "affirming the consequent" is a fallacy.

# Unit 4.3

Direct Proofs

# Direct Proofs

- A way of showing the truth of a statement by using established facts (e.g. definition, lemmas, theorems), rules of inference, and logical equivalences.
- Proving Existential Statements
  - Proof by example
- Proving Universal Statements
  - Proof by exhaustion (a.k.a proof by cases)
  - Proof by UG

# Proving Existential Statements

- Consider an existential statement

$$\exists x \in D, Q(x).$$

> **Proof by example**
>
> Find an $x$ in $D$ that makes $Q(x)$ true.

- Validity follows from Existential Generalization (EG).

# Disproving Universal Statements

- Consider a universal statement

$$\forall x \in D, Q(x).$$

- That it is false is equivalent to that its negation is true.

$$\exists x \in D, \sim Q(x).$$

**Proof by counter-example**

Find an $x$ in $D$ that makes $Q(x)$ false.

# One Example is Enough

- It is easy to find an example to prove that

  There exists positive integers $a$, $b$, $c$ such that $a^2 + b^2 = c^2$.

- Euler's conjecture (1769):

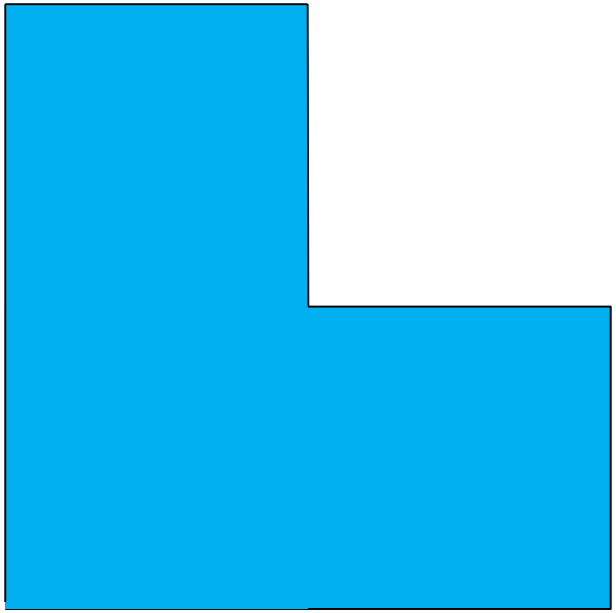
  There does not exist positive integers $a$, $b$, $c$, $d$ such that $a^4 + b^4 + c^4 = d^4$.

  - It is disproved in 1986 by a counter-example:

    $2862440^4 + 15365639^4 + 18796760^4 = 20615673^4$.

# Cutting Figures

- Congruent pieces: of the same shape and size, possibly rotated or flipped over.
- Prove that this figure can be cut into 2 congruent pieces.



*Too easy? How about cutting into 4 congruent pieces?*

# Proving Universal Statements

- Consider a universal statement

$$\forall x \in D, Q(x).$$

- Proof by Exhaustion (also called Proof by Cases)
  1) Split the domain $D$ into a finite number of cases (i.e. subsets).
  2) Check that the statement is true for each case (i.e. $Q(x)$ for all $x$ in each subset.)
- Proof by Universal Generalization (UG)
  1) Arbitrarily pick an element $x$ in $D$.
  2) Show that $x$ has the property $Q$.

# Two Examples (Proof by Exhaustion)

1. Prove that $x^2 \leq 16$ for $1 \leq x \leq 4$, $x$ is an integer.

Solution:

- $1^2 = 1 \leq 16, 2^2 = 4 \leq 16, 3^2 = 9 \leq 16, 4^2 = 16 \leq 16.$

Q.E.D.

2. Prove that $\min(x, y) \leq \max(x, y)$.

Solution:

- Case 1: $x \leq y$. Then $\min(x, y) = x \leq y = \max(x, y)$.
- Case 2: $x > y$. Then $\min(x, y) = y \leq x = \max(x, y)$.

Q.E.D.

# Even and Odd Integers

- Before we give an example to explain the proof method based on UG, we need the following:
- Definition
  - The integer $n$ is even if there exists an integer $k$ such that $n = 2k$, and
  - $n$ is odd if there exists an integer $k$, such that $n = 2k + 1$.

    - Note that every integer is either even or odd and no integer is both even and odd.

# Example (Proof by UG)

**Theorem:** *The sum of any two even numbers is even.*

**Proof:** Suppose $m$ and $n$ are (*arbitrarily chosen*) even numbers.
By definition of even numbers, $m = 2r$ and $n = 2s$ for some integers $r$ and $s$.

$$\begin{aligned} m + n &= 2r + 2s && \text{by substitution} \\ &= 2(r + s) && \text{by factoring out a 2.} \end{aligned}$$

Let $t = r + s$. Then

$$m + n = 2t \quad \text{where } t \text{ is an integer.}$$

By definition, $m + n$ is even.
Hence, (*by UG*), the sum of any two even numbers is even.

*Q.E.D.*

# Unit 4.4

Indirect Proofs

# Indirect Proofs (2 Major Types)

**Proof by Contradiction**

- Also called reductio ad absurdum
  - (i.e., Reduction to the Absurd)
- Classic: Used in Socratic method (~400 BC)
  - By asking questions, Socrates revealed contradictions in other people's belief, showing that the belief is false.

**Proof by Contraposition**

- Based on the logical equivalence between a conditional and its contrapositive.
  - See Unit 2.

$$p \rightarrow q \equiv \sim q \rightarrow \sim p$$

# Proof by Contradiction

To prove that $p$ is true:

1. Assume that $p$ is false.
2. With the above assumption, show that there is a contradiction.
3. Conclude that $p$ is true.

**Contradiction rule:**

$$\frac{\sim p \rightarrow \mathbf{c}}{p}$$

where **c** is a contradiction.

Why does it work?

# Why is Contradiction Rule Valid?

- By truth table

| | | | premises | conclusion |
|---|---|---|---|---|
| $p$ | $\sim p$ | $\mathbf{c}$ | $\sim p \rightarrow \mathbf{c}$ | $p$ |
| T | F | F | T | T |
| F | T | F | F | |

There is only one critical row in which the premise is true, and in this row the conclusion is also true. Hence this form of argument is valid.

- By showing that it is a tautology

$$(\sim p \rightarrow \mathbf{c}) \rightarrow p \equiv (p \vee \mathbf{c}) \rightarrow p$$
$$\equiv p \rightarrow p$$
$$\equiv \sim p \vee p$$
$$\equiv \mathbf{t}$$

# Example (Proof by Contradiction)

**Theorem:** *There is no greatest integer.*

**Proof:** We prove by contradiction. Suppose there is a greatest integer $N$. Then $N \geq k$ for all integer $k$.

Let $M = N + 1$. Now $M$ is an integer and $M > N$.

Therefore, $N$ is not a greatest integer.

We have reached a contradiction.

Hence, the statement is true.

*Q.E.D.*

# Proof by Contraposition

- This method is based on

$$p \rightarrow q \equiv \sim q \rightarrow \sim p$$

To prove that $p \rightarrow q$ is true:

1. Assume $\sim q$ is true.
2. Show that $\sim p$ is true.
3. Conclude that $p \rightarrow q$.

This shows that $\sim q \rightarrow \sim p$ is true.

# Example (Proof by Contraposition)

**Theorem:** *For all integer n, if $n^2$ is even, then n is even.*

**Proof:** Suppose $n$ is not even. Then $n = 2k + 1$ for some integer $k$.

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Let $t = 2k^2 + 2k$, which is an integer.

Then $n^2 = 2t + 1$.

Therefore, $n^2$ is odd (i.e., not even).

Hence, the statement is proved. *Q.E.D.*

# The Pigeonhole Principle (revisited)

- There are $m$ pigeons and $n$ pigeonholes, where $m > n$.
- Some pigeonhole will have more than one pigeon.

**Theorem:** Let $m$ objects be distributed into $n$ bins. If $m > n$, then some bin contains at least two objects.

# A Textbook Proof

**Theorem:** Let $m$ objects be distributed into $n$ bins. If $m > n$, then some bin contains at least two objects.

**Proof:** Assume that every bin contains at most one object. We want to prove that $m \leq n$. (proof by contraposition)

Let $x_i$ be the number of objects in bin $i$.

By assumption, $x_i \leq 1$.

Since $m$ is the number of objects, we have

$$m = \sum_{i=1}^{n} x_i \leq \sum_{i=1}^{n} 1 = n.$$

Hence, $m \leq n$, as required.

*Q.E.D.*

# May be easier to understand in this way…

**Theorem:** There are $m$ pigeons and $n$ pigeonholes. If $m > n$, there exists a pigeonhole that has more than one pigeon.

**Proof:** Suppose for all pigeonholes, each of them has no more than one pigeon.

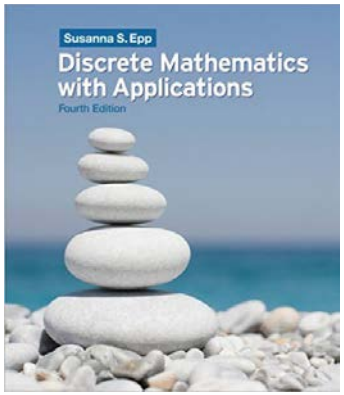
Since there are $n$ pigeonholes, there are at most $n$ pigeons in total.

By assumption, there are $m$ pigeons. So $m \leq n$.

The statement is proved by contraposition.

*Q.E.D.*

# Recommended Reading




- Sections 3.4, 4.1-4.7, Susanna S. Epp, *Discrete Mathematics with Applications*, 4th ed., Brooks Cole, 2010.