Unit 1

Proof

Albert Sung

Tentative Teaching Plan for Part 2

- Instructor: Dr. Albert SUNG (replace Prof. Tommy Chow until further notice)
  - Office: G6354 (YEUNG)
  - Email: albert.sung@cityu.edu.hk
- One or two assignments
  - Due date for Assign 1: **Nov 2 (Tue) or later** (TBC)
- **Test: Nov 20** (Sat. of Week 12)
  - about one hour within the period **9:00 – 11:00 am**
  - Venues: **LT-5** and **LT-6**

Outline of Unit 1

- 1.1 Why Proofs?
- 1.2 Direct Proofs
- 1.3 Indirect Proofs
- 1.4 Mathematical Induction

Unit 1.1

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.

Is it true?

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.

Terminology

- **Definition**
  - a precise description of a mathematical term (e.g., odd number).
- **Axiom**
  - A statement assumed true without proof.
  - Axioms form a basic building block from which all theorems are proved.
- **Theorem**
  - a mathematical statement that is proved to be true using rigorous reasoning (i.e., rules of inference).
- **Lemma**
  - a minor result whose purpose is to help in proving a theorem.
    - Very occasionally, some lemmas are very important on their own.
- **Corollary**
  - a result whose (usually short) proof follows directly from a theorem.

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 1.2

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 (also called 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
  $$a^2 + b^2 = c^2.$$

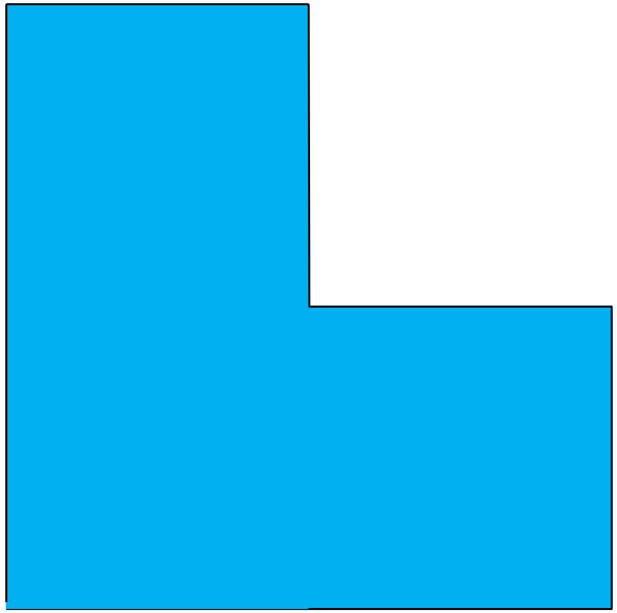
- Euler's conjecture (1769):

  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 $\min(x, y) \leq \max(x, y)$, where $x, y \in R$.

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 the 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

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

Therefore, $m + n$ is even.
Hence, the sum of any two even numbers is even.

Q.E.D.

Unit 1.3

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.

$$\boxed{p \to q \equiv \sim q \to \sim p}$$

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	$\sim p$	$\mathbf{c}$	$\sim p \to \mathbf{c}$	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

$$
\begin{aligned}
(\sim p \to \mathbf{c}) \to p &\equiv (p \vee \mathbf{c}) \to p \\
&\equiv p \to p \\
&\equiv \sim p \vee p \\
&\equiv \mathbf{t}
\end{aligned}
$$

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

$$\boxed{p \to q \equiv {\sim}q \to {\sim}p}$$

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

1. Assume ${\sim}q$ is true.
2. Show that ${\sim}p$ is true.
3. Conclude that $p \to q$.

This shows that ${\sim}q \to {\sim}p$ 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.*

If-and-Only-If Proof

- "P if and only if Q" (or simply P iff Q) can be split up into the two parts:

1) The "only if" part: $P \rightarrow Q$
2) The "if" part: $Q \rightarrow P$

- Each part is usually proved separately.

- Let $\boldsymbol{E}$ denote the equation $x^2 + px + q = 0$. Prove that $\boldsymbol{E}$ has two distinct real roots iff $p^2 - 4q > 0$.

Solution:

1) (if part) If $p^2 - 4q > 0$, by the quadratic formula, there are two distinct roots: $\frac{-p+\sqrt{p^2-4q}}{2}$ and $\frac{-p-\sqrt{p^2-4q}}{2}$.
2) (only if part) Suppose $\boldsymbol{E}$ has two distinct real roots. Denote them by α and β, where $\alpha \neq \beta$. Then,

$$x^2 + px + q = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta.$$

Comparing coefficients, $p = -(\alpha + \beta)$ and $q = \alpha\beta$.

Thus, $p^2 - 4q = (\alpha + \beta)^2 - 4\alpha\beta = (\alpha - \beta)^2 > 0$.

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 more than one object.

Theorem: Let m objects be distributed into n bins. If $m > n$, then some bin contains more than one object.

Proof:

Assume that every bin contains no more than one object. We want to prove $m \leq n$. (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.*

Unit 1.4

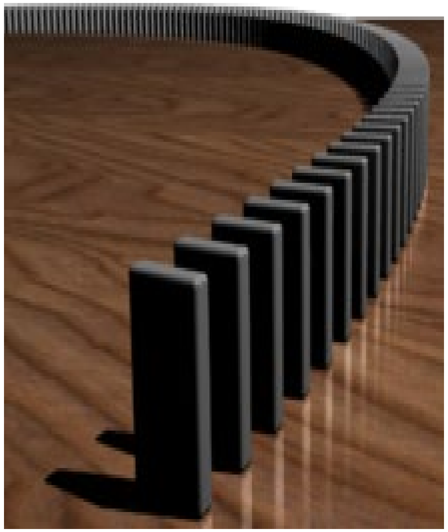
Mathematical Induction

Mathematical Induction

- Mathematical induction can be used to prove statements that assert that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function.
- A proof by induction contains two parts:

i. Base case: Show that $P(1)$ is true.

ii. Induction step: Show that for all positive integers k, if $P(k)$ is true, then $P(k+1)$ is also true.



Mathematical induction can be informally illustrated by reference to the sequential effect of falling dominoes (from Wikipedia)

Examples

- Prove that for all positive integers n,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Solution:

1) (Base case) Since $1 = \frac{1(1+1)}{2}$, the statement is true for $n = 1$.
2) (Induction step) Assume the statement is true for $n = k$ (where k is an arbitrary value), i.e.,

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Consider the case where $n = k + 1$.

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}.$$

Therefore, the statement is true for $n = k + 1$.

Hence, by induction, it is true for all positive integers.

- Prove that for all positive integers n,

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Solution:

1) (Base case) Since $1^2 = \frac{1(1+1)(2+1)}{6}$, the statement is true for $n = 1$.
2) (Induction step) Assume the statement is true for $n = k$, i.e.,

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Consider the case where $n = k + 1$.

$$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} = \frac{(k+1)[k(2k+1) + 6(k+1)]}{6}$$

$$= \frac{(k+1)[2k^2 + 7k + 6]}{6} = \frac{(k+1)(k+2)(2k+3)}{6}$$

Therefore, the statement is true for $n = k + 1$.

Hence, by induction, it is true for all positive integers.

Example: Summing a Geometric Series

- Let r be a fixed real number. Prove that for all integers n,

$$1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}.$$

Solution:

1) (Base case) Since $1 + r = \frac{1-r^2}{1-r}$, the statement is true for $n = 1$.
2) (Induction step) Assume the statement is true for $n = k$, i.e.,

$$1 + r + r^2 + \cdots + r^k = \frac{1 - r^{k+1}}{1 - r}.$$

Consider the case where $n = k + 1$.

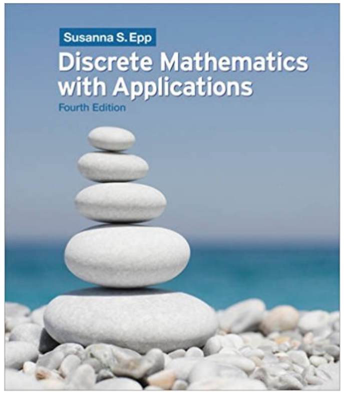
$$1 + r + r^2 + \cdots + r^k + r^{k+1} = \frac{1 - r^{k+1}}{1 - r} + r^{k+1}$$

$$= \frac{1 - r^{k+1} + (r^{k+1} - r^{k+2})}{1 - r} = \frac{1 - r^{k+2}}{1 - r}.$$

Therefore, the statement is true for $n = k + 1$.

Hence, by induction, it is true for all positive integers.

Recommended Reading



- Sections 4.1-4.7,5.2, Susanna S. Epp, *Discrete Mathematics with Applications*, 4th ed., Brooks Cole, 2010.

Appendix (optional)

Pythagoras Theorem

An Art for Appreciation

- An interesting demo:
  - https://www.youtube.com/watch?v=CAkMUdeB06o (<1 min.)

- How to prove it?
  - https://www.youtube.com/watch?v=BNCj-K2hd_k (~4 min.)