CMPUT 275

Topic 0: Proof Techniques

Rob Hackman and Xiao-Bo Li

Winter 2024

Credit

These slides are based on material from

- Dr. Steven Furino's notes "MATH 135: Algebra for Honours Mathematics" from the University of Waterloo and
- "How To Prove It" by D. J. Velleman.

Introduction

Writing and reading mathematical proofs is important for studying algorithms. We will review the main ways to write proofs.

Statement and Truth Tables

A **statement** is an expression that is either true or false.

- For example, "2 divides 6", also written as $2|6$, is a true statement.

A **compound statement** is composed of several statements.

- For example, "If $a|b$ and $b|c$, then $a|c$" has three compound statements.
  - $a|b$
  - $b|c$
  - $a|c$

A **truth table** is a table that defines or evaluates the truth value of a statement

Definition: Proposition, Theorem, Lemma, Corollary

A proposition is a true statement that has been proved by a valid argument.

A theorem is a significant proposition.

A lemma is a "helper" proposition used to help with proving a theorem.

A corollary is a proposition that follows immediately from a theorem.

Definition: Axiom

An axiom is a statement that is assumed to be true. No proof is given.

(aside: see Donald Hoffman's commentary on Godel's Incompleteness Theorem)

NOT Truth Table

The operation NOT has the following truth table. The symbol $\neg$ is also often used.

A	$\neg A$
T	F
F	T

AND and OR Truth Tables

AND ($\wedge$) and OR ($\vee$) have the following truth tables.

A	B	$A \wedge B$	$A \vee B$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

IMPLIES Truth Table

The symbol $\Longrightarrow$ is often used.

A	B	$A \Longrightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

A is the hypothesis and B is the conclusion. Note if the hypothesis is false, any conclusion can be true.

- "If the sun rises from the west, then human beings can fly" is true.

IF AND ONLY IF Truth Table

If and only if has the symbol $\iff$. It has the following truth table.

A	B	$A \iff B$
T	T	T
T	F	F
F	T	F
F	F	T

The statement $A \iff B$ is equivalent to $(A \implies B) \wedge (B \implies A)$. Use a truth table to verify this, and also verify $A \implies B$ is not the same as $B \implies A$.

Order of Operations

The order of operations for logic operators are as follows:

- brackets
- $\neg$ (NOT)
- $\wedge$ (AND)
- $\vee$ (OR)
- $\Longrightarrow$ (IMPLIES)
- $\Longleftrightarrow$ (IFF)
- $\equiv$ (truth value are equivalent)

Contrapositive vs Converse

Contrapositive and converse looks similar but do not mean the same thing.

They are both derived from $A \Longrightarrow B$.

Definition: Contrapositive

The **contrapositive** of $A \Longrightarrow B$ is

$$\neg B \Longrightarrow \neg A.$$

A statement and its contrapositive statement are equivalent.

$$A \Longrightarrow B \equiv \neg B \Longrightarrow \neg A.$$

If proving $A \Longrightarrow B$ is difficult, the try proving $\neg B \Longrightarrow \neg A$. One of these statements may be easier to proof than the other.

Definition: Converse

The **converse** of $A \Longrightarrow B$ is

$$B \Longrightarrow A.$$

A statement and its converse statement are *not* equivalent.

$$A \Longrightarrow B \not\equiv B \Longrightarrow A.$$

Quantifiers

The existential quantifier is the symbol $\exists$, it means "there exists a particular mathematical object".

The universal quantifier is the symbol $\forall$, it means "for all objects in a set".

A quantifer is used with some variable, such as x, the domain of x, and some open statement about x, denoted $P(x)$.

De Morgan's Law

De Morgan's Law states: if A and B are statements, then

- $\neg(A \vee B) = (\neg A) \wedge (\neg B)$
- $\neg(A \wedge B) = (\neg A) \vee (\neg B)$

Use a truth table to verify this.

Negation

The negation of the statement A is the statement NOT A.

- Use De Morgan's Law to negate statements with AND and OR.
- The negation of $\forall$ is $\exists$.

Here are some examples negations.

A	$\neg A$
$B \wedge C$	$(\neg B) \vee (\neg C)$
$a \mid b$ and $a \mid c$	$a \nmid b$ or $a \nmid c$
$B \vee C$	$(\neg B) \wedge (\neg C)$
$\exists x \in S$, $P(x)$ is true.	$\forall x \in S$, $P(x)$ is false
$\forall x \in S$, $P(x)$ is true.	$\exists x \in S$, $P(x)$ is false

In the statememnt "$\exists x \in S$, $P(x)$ is false", x is called a **counterexample**.

Proof Techniques

We are now ready to discuss proof techniques.

The Object Method

When proving $A \Longrightarrow B$, and A looks like:

- $\exists x \in S$ such that $P(x)$ is true.

The Object Method uses the following steps.

1. Assume $x \in S$ exists and $P(x)$ is true.
2. Generate the conclusion B.

Example Proof: The Object Method

Proposition

Let a, b, and c be integers. If $a|b$ and $b|c$, then $a|c$.

Proof.

The definition of $a|b$ implicitly uses an existential quantifier.

- Assume integer q_1 exists such that $q_1 a = b$. Assume integer q_2 exists such that $q_2 b = c$.
- Generate new statement $q_2 q_1 a = c$, so $a|c$.

The Construct Method

When proving $A \Longrightarrow B$, and B looks like:

- $\exists x \in S$ such that $P(x)$ is true.

The Construct Method uses the following steps.

1. Construct some x.
2. Show $x \in S$ and $P(x)$ is true.

Example Proof: The Construct Method

Proposition

If n is of the form $4a+1$ for some positive integer a, then $8|(n^2-1)$.

Proof.

A is "If n is of the form $4a+1$ for some positive integer a" and B is "$8|(n^2-1)$", where the meaning of $8|(n^2-1)$ uses an existential quantifier.

- Construct an integer q and show that $8q = (n^2-1)$.
- Use the information in A, $n = 4a+1$ so

$$n^2 - 1 = (4a+1)^2 - 1 = 16a^2 + 8a + 1 - 1 = 8(2a^2 + a)$$

- $(2a^2 + a)$ is an integer because a is an integer. So this is the q we wanted to construct.

The Select Method

The statement to prove looks like:

- "$\forall x \in S$, $P(x)$ is true", or "if $x \in S$, then $P(x)$ is true".

The Select method uses the following steps:

1. Select a representative object $x \in S$ which is not special in any way. If S is empty, the statement is vacuously true.
2. Show $P(x)$ is true.

Example Proof: The Select Method

Proposition

For all odd integers x, $4|(x^2 + 4x + 3)$.

Proof.

Select a representative odd integer x_0 and show $4|(x_0^2 + 4x_0 + 3)$.

Since x_0 is odd, $\exists q_0$ such that $x_0 = 2q_0 + 1$. Substitute this x_0 expression into $x_0^2 + 4x_0 + 3$

$$\begin{aligned} x_0^2 + 4x_0 + 3 =& (4q_0^2 + 4q_0 + 1) + (8q_0 + 4) + 3 \\ =& 4q_0^2 + 12q_0 + 8 \\ =& 4({q_0}^2 + 3q_0 + 2) \end{aligned}$$

Thus, we can conclude $4|(x_0^2 + 4x_0 + 3)$. □

Proof by Cases

To prove the statement $A \Longrightarrow B$, list out all possible cases of A, for each case shown B is true.

Using a truth table to prove a statement is an example of Proof by Case.

Proof by Contradiction

To prove the statement $A \Longrightarrow B$, assume A is true, assume B is false, use A and NOT B to reach a contradiction.

Contradiction is helpful if assuming NOT B simplifies the proof.

Example Proof: Contradiction

Proposition

The number of primes is infinite.

Proof.

There is no A, only B in this proposition.

- Assume the number of primes is finite, NOT B. Label all primes $p_1, p_2, \ldots p_n$
- Reach a contradiction.
  Let $N = p_1 p_2 \ldots p_n + 1$. Since $N > p_i \ \forall i$, N is not prime. But no p_i is a factor of N, so N cannot be written as a product of primes, so N is prime, a contradiction.

Contrapositive

To prove the statement $A \Longrightarrow B$ is true, proof instead $\neg B \Longrightarrow \neg A$.

Example Proof: Contrapositive

Proposition

For some integer a, if $32 \nmid (a^2+3)(a^2+7)$, then a is even.

Proof.

The contrapositive of the statement to proof is:

- If a is odd, then "$32 \mid (a^2+3)(a^2+7)$"

Start with an arbitrary odd integer $a = 2q+1$, where q is another arbitrary integer. Substitute in a.

$$\begin{aligned}(a^2+3)(a^2+7) &= ((2q+1)^2+3)((2q+1)^2+7) \\ &= (4q^2+4q+4)(4q^2+4q+8) \\ &= 16(q^2+q+1)(q^2+q+2)\end{aligned}$$

Example Proof: Contrapositive (cont.)

Proof (cont.)

One of $(q^2 + q + 1)$ or $(q^2 + q + 2)$ must be even, assume $(q^2 + q + 1)$ is even so $(q^2 + q + 1) = 2p$ for another arbitrary integer p.

$$\begin{aligned}(a^2 + 3)(a^2 + 7) &= 16(q^2 + q + 1)(q^2 + q + 2) = 16(2p)(2p + 1) \\ &= 32p(2p + 1)\end{aligned}$$

Therefore, $32 \mid (a^2 + 3)(a^2 + 7)$. Since

$$\neg B \Longrightarrow \neg A \text{ is true}$$

it follows that

$$A \Longrightarrow B \text{ is also true}$$

by the method of Proof by Contrapositive.

Uniqueness

To prove a statements of the form:

- If . . . , then there is a unique object x in a set S such that $P(x)$ is true.

Use one of two approaches:

- Demonstrate there is at least one object in S such that $P(x)$ is true. Assume there are two objects x and y in S such that $P(x)$ and $P(y)$ are both true. Show $x = y$.
- Demonstrate there is at least one object in S such that $P(x)$ is true. Assume there are two distinct objects x and y in S such that $P(x)$ and $P(y)$ are both true. Derive a contradiction.

Example Proof 1: Uniqueness

Proposition

If $a \neq 0$ and b are integers and $a|b$, then there is a unique integer k such that $b = ka$.

Proof.

- Demonstrate there is at least one object: $a|b$ means $b = ka$.
- Assume there are two objects, let k_1 and k_2 be integers such that $b = k_1 a$ and $b = k_2 a$.
- This means $k_1 a = k_2 a$, so this shows $k_1 = k_2$.

Example Proof 2: Uniqueness

Proposition

Let

$$y = f_1(x) = m_1 x + b_1$$
$$y = f_2(x) = m_2 x + b_2$$

be a simultaneous equation where a solution exists. If $m_1 \neq m_2$, then there is a unique solution.

Proof.

Suppose there are two solutions $(x_1, y_1) \neq (x_2, y_2)$. Substitute these into $f_1(x)$

$$y_1 = m_1 x_1 + b_1$$
$$y_2 = m_1 x_2 + b_1$$

Example Proof 2: Uniqueness (cont.)

Proof (cont.)

then subtract

$$y_1 - y_2 = m_1(x_1 - x_2)$$

Substitute these into $f_2(x)$, then subtracting gives

$$y_1 - y_2 = m_2(x_1 - x_2)$$

Equate both expressions

$$\begin{aligned} m_1(x_1 - x_2) &= m_2(x_1 - x_2) \\ (m_1 - m_2)(x_1 - x_2) &= 0 \end{aligned}$$

But $m_1 \neq m_2$, so $x_1 - x_2 = 0$ must hold. But this means $y_1 = y_2$, so the two solutions are not distinct, a contradiction. □

The Elimination Method

To prove the statement

- "if A, then B or C".

prove the logically equivalent statement

- "if A and $\neg B$, then C".

Example Proof: Elimination

Proposition

If $x^2 - 7x + 12 \geq 0$, *then* $x \leq 3$ *or* $x \geq 4$.

Proof.

Statement A is "$x^2 - 7x + 12 \geq 0$", B is "$x \leq 3$" and C is "$x \geq 4$".

- Assume $A \wedge \neg B$, that is, $x^2 - 7x + 12 \geq 0$ and $x > 3$.
- Factoring $x^2 - 7x + 12 = (x - 3)(x - 4) \geq 0$
- Since $(x - 3) > 0$, $x - 4 \geq 0$.

Axiom: The Principle of Mathematical Induction (PoMI)

Let $P(n)$ be a statement that depends on $n \in \mathbb{N}$. If

- $P(1)$ is true, and
- $\forall k \in \mathbb{N}\ P(k) \Longrightarrow P(k+1)$

then, $P(n)$ is true $\forall n \in \mathbb{N}$.

POMI is used to prove statements of the form:

$$\forall n \geq 1\ P(n) \text{ is true.}$$

Proof by Induction

Let $P(n)$ be a statement that depends on $n \in \mathbb{N} = \{1, 2, 3, \dots\}$. The steps for proof by induction are:

- Base case: **verify** $P(1)$ is true.
- Inductive hypothesis: **assume** $\exists k \in \mathbb{N}$ such that $P(k)$ is true. Note this statement is saying there is *some* k, not for all k.
- Inductive conclusion: **show** $P(k+1)$ is true.

Then $P(n)$ is true $\forall n \in \mathbb{N}$.

Proof by Induction (cont.)

Induction works because the base cases establishes $P(1)$ is true. Then, $P(1)$ is used to show $P(2)$ is true, then $P(2)$ is used to show $P(3)$ is true.

$$P(1) \Longrightarrow P(2)$$
$$P(2) \Longrightarrow P(3)$$
$$\ldots$$
$$P(k) \Longrightarrow P(k+1)$$
$$\ldots$$

These pairs of implications continue indefinitely:and establishes

$$P(k) \Longrightarrow P(k+1)\ \forall k \in \mathbb{N}$$

is true. PoMI can then be applied.

Example Proof: Induction

Proposition

$\forall n \in \mathbb{N}$,

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

The inductive statement $P(n)$ is:

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

Example Proof: Induction (cont. 1)

Proof.

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

The left hand side (LHS) evaluates to:

$$\sum_{i=1}^{1} i^2 = 1^2 = 1$$

The right hand (RHS) evaluates to:

$$\frac{1(1+1)(2 \cdot 1 + 1)}{6} = 1.$$

Since LHS = RHS, the base case $P(1)$ is true.

Example Proof: Induction (cont. 2)

Proof (cont.)

Inductive hypothesis is to assume that

$$\exists k \in \mathbb{N}\ P(k) : \sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}.$$

is true.

Example Proof: Induction (cont. 3)

Proof (cont.)

Use the inductive hypothesis in the inductive conclusion.

$$\begin{aligned}\sum_{i=1}^{k+1} i^2 &= \sum_{i=1}^{k} i^2 + (k+1)^2 \\ &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} = \frac{(k+1)(2k^2+7k+6)}{6} \\ &= \frac{(k+1)(k+2)(2(k+1)+1)}{6}\end{aligned}$$

This shows $P(k+1)$ is true. □

Axiom: Principle of Strong Induction (PoSI)

Let $P(n)$ be a statement that depends on $n \in \mathbb{N}$. (same as PoMI)

If

- $\exists b > 0$ $P(1), P(2), \ldots, P(b)$ are true, and
- $\forall k \in \mathbb{N}$ $P(1) \wedge P(2) \wedge \cdots \wedge P(k) \Longrightarrow P(k+1)$

then, $P(n)$ is true $\forall n \in \mathbb{N}$.

Note that:

$$P(1) \wedge P(2) \wedge \cdots \wedge P(k)$$

means $P(1), P(2), \ldots, P(b), \ldots, P(k)$ are *all* true.

Proof by Strong Induction

Let $P(n)$ be a statement that depends on $n \in \mathbb{N} = \{1, 2, 3, \dots\}$.

- Base case: **verify** $\exists b > 0$ $P(1), P(2), \dots, P(b)$ are all true.
- Inductive hypothesis: **assume**

$$\exists k \geq b \; P(1), P(2), \dots, P(k)$$

  are all true. Note this statement is saying there is *some* k, not for all k.
- **Show** $P(k+1)$ is true using the assumption.

Then $P(n)$ is true $\forall n \in \mathbb{N}$.

Proof by Strong Induction (cont.)

Proof by strong induction works because it establishes the following chain of proves starting with the base case:

$$
\begin{aligned}
&P(1) \wedge P(2) \wedge \cdots \wedge P(b) && \Longrightarrow P(b+1)\\
&P(1) \wedge P(2) \wedge \cdots \wedge P(b) \wedge P(b+1) && \Longrightarrow P(b+2)\\
&P(1) \wedge P(2) \wedge \cdots \wedge P(b) \wedge P(b+1) \wedge P(b+2) && \Longrightarrow P(b+3)\\
&\ldots
\end{aligned}
$$

Since this continues indefinitely, it establishes:

$$\forall k \in \mathbb{N}\ P(1) \wedge P(2) \wedge \cdots \wedge P(k) \Longrightarrow P(k+1)$$

PoSI can then be applied.

Example Proof: Strong Induction

Proposition

A sequence $\{x_n\}$, $n \geq 1$, *is defined by* $x_1 = 11$, $x_2 = 23$, *and when* $n \geq 3$,

$$x_n = x_{n-1} + 12x_{n-2}.$$

Prove that

$$x_n = 2 \cdot 4^n - (-3)^n,\ n \geq 1.$$

The inductive statement is:

$$P(n) : x_n = 2 \cdot 4^n - (-3)^n.$$

Example Proof: Strong Induction (cont. 1)

Proof .

Base case: verify $P(1)$ and $P(2)$ are true.

$$P(1) : x_1 = 2 \cdot 4^1 - (-3)^1 = 8 + 3 = 11$$
$$P(2) : x_2 = 2 \cdot 4^2 - (-3)^2 = 32 - 9 = 23.$$

Example Proof: Strong Induction (cont. 1)

Proof .

Inductive hypothesis: assume $\exists k \geq 2$ $P(1)$, $P(2)$, $\ldots$, $P(k)$ is true.

Example Proof: Strong Induction (cont. 2)

Proof (cont.)

Inductive conclusion: show $P(k+1)$ is true.

$$P(k+1) : x_{k+1} = 2 \cdot 4^{k+1} - (-3)^{k+1}$$

Start with the recurrence relation and use the inductive hypothesis:

$$\begin{aligned}
x_{k+1} &= x_k + 12x_{k-1} \\
&= (2 \cdot 4^k - (-3)^k) + 12 \cdot (2 \cdot 4^{k-1} - (-3)^{k-1}) \\
&= (2 \cdot 4^k + 12 \cdot 2 \cdot 4^{k-1}) - ((-3)^k + 12 \cdot (-3)^{k-1}) \\
&= (2 \cdot 4 + 12 \cdot 2)4^{k-1} - (-3)^{k-1}((-3) + 12) \\
&= 32 \cdot 4^{k-1} - (-3)^{k-1} \cdot 9 \\
&= 2 \cdot 4^{k+1} - (-3)^{k+1}
\end{aligned}$$

Summary

- The Object Method (assume the object exists)
- The Construct Method (construct the object required)
- The Select Method (select a representative object)
- Proof by Cases (list all possible cases)
- Proof by Contradiction
- Prove the Contrapositive
- Show Uniqueness
- The Elimination Method (eliminate one case)
- Proof by Induction (works because of the axiom PoMI)
- Proof by Strong Induction (works because of the axiom PoSI)