Module 1: Proofs

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Ichiro Hashimoto

University of Toronto

July 7, 2025

Outline

- Logic
- Review of Proof Techniques

Propositional logic

Propositions are statements that could be true or false. They have a corresponding **truth value**. T, F

ex. "n is odd" and "n is divisible by 2" are propositions . Let's call them P and Q. Whether they are true or not depends on what n is.

$P(n)$ $Q(n)$

We can negate statements: $\neg P$ is the statement "n is not odd"

We can combine statements:

- $P \wedge Q$ is the statement: P and Q = "n is odd and divisible by 2"
- $P \vee Q$ is the statement: P or Q = "n is odd or divisible by 2"
  We always assume the inclusive or unless specifically stated otherwise.

↳ $P \vee Q$ covers $P \wedge Q$

Examples

$P \Rightarrow Q$ "P implies Q" = "If P holds, then Q holds"

P = "It's raining"

Q = "I bring umbrella"

Symbol	Meaning
capital letters	propositions
$\Longrightarrow$	implies
$\wedge$	and
$\vee$	inclusive or
$\neg$	not

- If it's not raining, I won't bring my umbrella. $(\neg P) \Rightarrow (\neg Q)$
- I'm a banana or Toronto is in Canada.

  P ∨ Q
- If I pass this exam, I'll be both happy and surprised.

  P Q

  R

$$P \Rightarrow (Q \wedge R)$$

Truth values

Example

If it is snowing, then it is cold out.

It is snowing. → P

Therefore, it is cold out. → Q.

Write this using propositional logic:

$$P \Rightarrow Q$$

How do we know if this statement is true or not?

Truth table

$$P \implies Q$$

If it is snowing, then it is cold out.

When is this true or false?

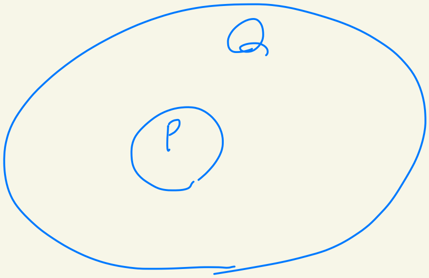
P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

When P is F, truth value of Q does not matter.

But why?

logic ⟷ Set theoretic understanding.

$P \Rightarrow Q$. ⟷ $P \subset Q$



P is F ⟷ $P = \phi$ empty set

empty set is a subset of any set.

$P \Rightarrow Q$ is true when P is F ⟷ $\phi \subset Q$.

Logical equivalence

Same!

logically equivalent!

$P \implies Q$

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

$\neg P \vee Q$

P	Q	$\neg P$	$\neg P \vee Q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

What is $\neg(P \implies Q)$?

$= \neg(\neg P \vee Q) = P \wedge \neg Q$

$P \Rightarrow Q \Longleftrightarrow P \subset Q$

$\Longleftrightarrow P^c \cup Q =$ Universal set.

$\Longleftrightarrow \neg P \vee Q.$

Quantifiers

For all

"for all" (also read "for any"), $\forall$, is also called the universal quantifier.

If $P(x)$ is some property that applies to x from some domain, then $\forall x P(x)$ means that the property P holds for every x in the domain.

"Every real number has a non-negative square." We write this as

$$\forall x,\ x^2 \geq 0$$

How do we prove a for all statement?

Quantifiers

There exists

"there exists", ∃, is also called the existential quantifier.
If $P(x)$ is some property that applies to x from some domain, then $\exists x P(x)$ means that the property P holds for some x in the domain.

4 has a square root in the reals. We write this as

$$\exists x, \ x^2 = 4$$

How do we prove a there exists statement?

you just need to provide one example

There is also a special way of writing when there exists a unique element: $\exists!$.
For example, we write the statement "there exists a unique positive integer square root of 64" as

$$\exists! x, \ x^2 = 64 \wedge x > 0$$

Combining quantifiers

Often we will need to prove statements where we combine quantifiers.
Here are some examples:

Statement	Logical expression
$\forall$ Every non-zero rational number has a multiplicative inverse $\hookrightarrow \exists$	$\forall x \in \mathbb{Q}\setminus\{0\}, \exists y \in \mathbb{Q}\setminus\{0\}, xy=1.$
$\forall$ Each integer has a unique additive inverse $\hookrightarrow \exists!$	$\forall x \in \mathbb{Z}, \exists! y \in \mathbb{Z}, x+y=0.$
$f : \mathbb{R} \to \mathbb{R}$ is continuous at $x_0 \in \mathbb{R}$	

$\forall \varepsilon>0, \exists \delta>0$ s.t. $|x-x_0|<\delta \implies |f(x)-f(x_0)|<\varepsilon.$

Quantifier order & negation

The order of quantifiers is important! Changing the order changes the meaning. Consider the following example. Which are true? Which are false?

$$\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\; x + y = 2 \qquad \text{F}$$
$$\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\; x + y = 2 \qquad \text{T (For any } x\text{, choose } y = 2 - x$$
$$\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\; x + y = 2 \qquad \text{F}$$
$$\exists x \in \mathbb{R}\, \exists y \in \mathbb{R}\; x + y = 2 \qquad \text{T}$$

Negating quantifiers: $\exists \xleftrightarrow{\text{negation}} \forall$

$$\neg \forall x P(x) = \exists x (\neg P(x))$$
$$\neg \exists x P(x) = \forall x (\neg P(x))$$

The negations of the statements above are:

(Note that we use De Morgan's laws, which are in your exercises:
$\neg(P \wedge Q) = \neg P \vee \neg Q$ and $\neg(P \vee Q) = \neg P \wedge \neg Q$.)

Logical expression	Negation
$\forall q \in \mathbb{Q} \setminus \{0\}, \exists s \in \mathbb{Q}$ such that $qs = 1$ $\downarrow$ $\downarrow$ $\exists$ $\forall$	$\exists q \in \mathbb{Q}\setminus\{0\}, \forall s \in \mathbb{Q}$ s.t. $qs \neq 1$
$\forall x \in \mathbb{Z}, \exists! y \in \mathbb{Z}$ such that $x + y = 0$ $\downarrow$ "exist" and "unique" $\exists$ $\downarrow$ or	$\exists x \in \mathbb{Z}$ s.t. $(\forall y \in \mathbb{Z}, x+y \neq 0) \vee (\exists y_1, y_2 \in \mathbb{Z}, y_1 \neq y_2, x+y_1 = x+y_2 = 0)$
$\forall \epsilon > 0\ \exists \delta > 0$ such that whenever $\lvert x - x_0 \rvert < \delta$, $\lvert f(x) - f(x_0) \rvert < \epsilon$	

What do these mean in English? $\exists \varepsilon > 0, \forall \delta > 0, \exists x$ s.t. $(\lvert x - x_0 \rvert < \delta) \wedge (\lvert f(x) - f(x_0) \rvert \geq \delta)$

Statistical Sciences
UNIVERSITY OF TORONTO

Types of proof

- Direct
- Contradiction
- Contrapositive
- Induction

Direct Proof

Approach: Use the definition and known results.

Example

Claim

The product of an even number with another integer is even.

Approach: use the definition of even.

Direct Proof

Claim

The product of an even number with another integer is even.

Definition

We say that an integer n is **even** if there exists another integer j such that $n = 2j$.
We say that an integer n is **odd** if there exists another integer j such that $n = 2j + 1$.

Proof. Let $m, n \in \mathbb{Z}$ and assume n is even.

Then $\exists\, j \in \mathbb{Z}$ s.t. $n = 2j$.

Then $mn = m \cdot (2j) = 2(mj) =$ even by definition

Definition

Let $a, b \in \mathbb{Z}$. We say that "a divides b", written $a \mid b$, if the remainder is zero when b is divided by a, i.e. $\exists j \in \mathbb{Z}$ such that $b = aj$.

Example

Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. By definition $\exists\, \underset{\underset{\mathbb{Z}}{\cap}}{j}$ s.t. $b = aj$, $\exists\, k \in \mathbb{Z}$ s.t. $c = bk$.

Then, $c = bk = (aj)k = a(jk)$.

That means $a \mid c$.

Claim

If an integer squared is even, then the integer is itself even.

How would you approach this proof?

$x^2 = 2n$ $\qquad$ $\underline{x = \pm\sqrt{2n}}$

How to remove $\sqrt{\ }$ and show x is even?

Direct proof doesn't work well.

Proof by contrapositive

logically equivalent

$$P \implies Q \longleftrightarrow \neg Q \implies \neg P$$

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$\neg P$	$\neg Q$	$\neg Q \implies \neg P$
T	T	F	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

same!

Proof by contrapositive

Claim

If $\overset{P}{\underline{\text{an integer squared is even}}}$, then $\overset{Q}{\underline{\text{the integer is itself even}}}$.

Proof. We'll prove this by contrapositive.

WTS: $\underset{\neg Q}{\underline{\text{if } x \text{ is odd}}}$, then $\underset{\neg P}{\underline{x^2 \text{ is odd.}}}$

$\Longrightarrow$

$\exists j \in \mathbb{Z}$ s.t. $x = 2j+1$.

Then $x^2 = (2j+1)^2 = 4j^2 + 4j + 1$ = odd. ✓

Proof by contradiction

Instead of $P \Rightarrow Q$, assume $P \wedge \neg Q$ and find contradiction.

Claim

The sum of a rational number and an irrational number is irrational.

Proof. Let $x \in \mathbb{Q}$, $y \in \mathbb{R} \setminus \mathbb{Q}$.

Suppose $x + y = s \in \mathbb{Q}$.

Then $y = \underset{\mathbb{Q}}{\underset{\cap}{s}} - \underset{\mathbb{Q}}{\underset{\cap}{x}} =$ rational, which is contradiction.

Therefore, $x+y$ must be irrational.

Summary

In sum, to prove $P \implies Q$:

Direct proof: assume P, prove Q

Proof by contrapositive: assume $\neg Q$, prove $\neg P$

Proof by contradiction: assume $P \wedge \neg Q$ and derive something that is impossible

Induction

Well-ordering principle for $\mathbb{N}$

Every nonempty set of natural numbers has a least element.

Principle of mathematical induction

Let n_0 be a non-negative integer. Suppose P is a property such that

1. (base case) $P(n_0)$ is true
2. (induction step) For every integer $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.

Then $P(n)$ is true for every integer $n \geq n_0$

Note: Principle of strong mathematical induction: For every integer $k \geq n_0$, if $P(n)$ is true for every $n = n_0, \ldots, k$, then $P(k+1)$ is true.

Claim

$n! > 2^n$ if $n \geq 4$ ($n \in \mathbb{N}$).

Proof.

(Base case)

If $n=4$, $n! = 24$

$2^n = 16$ $\therefore$ $n! > 2^n$.

(Induction step)

Suppose $k! > 2^k$.

Then $(k+1)! = (k+1) \times k! > (k+1) \times 2^k \geq 2 \times 2^k = 2^{k+1}$

Claim

Every integer $n \geq 2$ can be written as the product of primes.

Proof. We prove this by strong induction on n.

Base case:

If $n=2$, 2 is a prime, so the statement is trivially true.

Inductive hypothesis:

Suppose for $k \geq 2$, any $n \in [2, k]$ can be written as the product of primes.

Inductive step:

1) If $k+1$ is a prime, then the statement is trivially true.

2) If $k+1$ is not a prime, $\exists\ a, b \in [2, k]$ s.t.

$$k+1 = \underset{\uparrow}{a}\,\underset{\uparrow}{b}.$$

use the inductive hypothesis to both a and b.

Then, by the inductive hypothesis, both a and b can be written as the products of primes.

So, $k+1 = ab$ can also be written as the product of primes.

References

Gerstein, Larry J. (2012). *Introduction to Mathematical Structures and Proofs*. Undergraduate Texts in Mathematics. url: https://link.springer.com/book/10.1007/978-1-4614-4265-3

Lakins, Tamara J. (2016). *The Tools of Mathematical Reasoning*. Pure and Applied Undergraduate Texts.