

# Module 1: Proofs

## Operational math bootcamp



Statistical Sciences  
UNIVERSITY OF TORONTO

Huanlin Mao

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**.

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.

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

We can combine statements:

- $P \wedge Q$  is the statement:
- $P \vee Q$  is the statement:

We always assume the inclusive or unless specifically stated otherwise.

# Examples

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

- If it's not raining, I won't bring my umbrella.
- I'm a banana or Toronto is in Canada.
- If I pass this exam, I'll be both happy and surprised.

# Truth values

## Example

If it is snowing, then it is cold out.

It is snowing.

Therefore, it is cold out.

Write this using propositional logic:

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

# Truth table

If it is snowing, then it is cold out.

When is this true or false?

$$P \implies Q$$

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

# Logical equivalence

$$P \implies Q$$

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

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

# 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  $\forall xP(x)$  means that the property  $P$  holds for every  $x$  in the domain.

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

How do we prove a for all statement?

# Quantifiers

## There exists

“there exists”,  $\exists$ , is also called the existential quantifier.

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

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

How do we prove a there exists statement?

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

# Combining quantifiers

Often we will need to prove statements where we combine quantifiers.

Here are some examples:

Statement

Logical expression

---

Every non-zero rational number has a multiplicative inverse

Each integer has a unique additive inverse

$f: \mathbb{R} \rightarrow \mathbb{R}$  is continuous at  $x_0 \in \mathbb{R}$

# 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?

$$\forall x \in \mathbb{R} \forall y \in \mathbb{R} x + y = 2$$

$$\forall x \in \mathbb{R} \exists y \in \mathbb{R} x + y = 2$$

$$\exists x \in \mathbb{R} \forall y \in \mathbb{R} x + y = 2$$

$$\exists x \in \mathbb{R} \exists y \in \mathbb{R} x + y = 2$$

Negating quantifiers:

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

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

The negations of the statements above are:

(Note that we use De Morgan's laws, which are in your exercises:

$$\neg(P \wedge Q) = \neg P \vee \neg Q \text{ and } \neg(P \vee Q) = \neg P \wedge \neg Q.)$$

Logical expression	Negation
$\forall q \in \mathbb{Q} \setminus \{0\}, \exists s \in \mathbb{Q} \text{ such that } qs = 1$	
$\forall x \in \mathbb{Z}, \exists! y \in \mathbb{Z} \text{ such that } x + y = 0$	
$\forall \epsilon > 0 \exists \delta > 0 \text{ such that whenever }  x - x_0  < \delta,  f(x) - f(x_0)  < \epsilon$	

What do these mean in English?

# 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.*

## Definition

Let  $a, b \in \mathbb{Z}$ . We say that “ $a$  divides  $b$ ”, written  $a|b$ , 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  $a|b$  and  $b|c$ , then  $a|c$ .

*Proof.*

## Claim

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

How would you approach this proof?

# Proof by contrapositive

$$P \implies Q$$

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

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

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

# Proof by contrapositive

## Claim

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

*Proof.*

# Proof by contradiction

## Claim

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

*Proof.*

# 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  $n = n_0, \dots, k$ , then  $P(k+1)$  is true.

## Claim

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

*Proof.*

## 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:*

*Inductive hypothesis:*

*Inductive step:*

# 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.