Module 1: Proofs

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Huanlin Mao hl.mao@mail.utoronto.ca

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

$P \vee Q$ includes / covers $P \wedge Q$

Examples

$P \Rightarrow Q$ "P implies Q" = "If raining, I will ..."

P = "It's raining"

Q = "I will bring my umbrella"

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

$(\neg P) \Rightarrow (\neg Q)$

- If it's not raining, I won't bring my umbrella.

P Q

- I'm a banana or Toronto is in Canada. ($P \vee Q$)
- 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

If it is snowing, then it is cold out.

When is this true or false?

$P \implies Q$ = "If P is true, then Q is true"

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

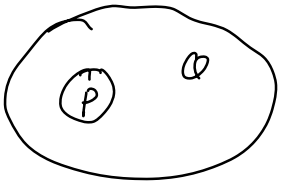
When P is F, truth value of Q does not matter

△. an implication "⇒" is just about what would happen when P holds / is true.

So if P is false, then this implication is not violated.

△ logic ⟷ set theory

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



P is F ⟷ $P = \phi$

when $P = \phi$, $P \subset$ any set

P is F. $P \Rightarrow Q$ is T ⟷ $P \subset Q$ for any Q / in any case in $P = \phi$

Logical equivalence

$\wedge$ and

$\vee$ or

Same!

$P \implies Q$

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 $\neg(P \implies Q)$?

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

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.

$\forall x,\ P(x)$

"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?

prove that for any / arbitrary x in the domain, $P(x)$ holds

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 $\exists x P(x)$ means that the property P holds for some x in the domain.

$\exists x, P(x)$

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

$\exists x, \; x^2 = 4$ ← If $x = 2, \in \mathbb{R}$ then $x^2 = 4$

How do we prove a "there exists" statement?

just need to find / 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 $\exists! \, x \in \mathbb{Z}, \; x^2 = 64$

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	$\forall x \in \mathbb{Q} \setminus \{0\}, \exists y \in \mathbb{Q} \setminus \{0\}, xy = 1$
∀	Each integer has a unique additive inverse	$\forall x \in \mathbb{Z}, \exists! y \in \mathbb{Z}$ (or $\exists! y \in \mathbb{R}$), $x + y = 0$

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

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

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?

$$\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\ x + y = 2 \qquad \text{F}$$
$$\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\ x + y = 2 \qquad \text{T}$$
$$\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\ x + y = 2 \qquad \text{F}$$
$$\exists x \in \mathbb{R}\, \exists y \in \mathbb{R}\ x + y = 2 \qquad \text{F}$$

$x=0$ and $y=0$, $x+y=0$

assume $y = 2 - x$

Negating quantifiers:

$$\begin{cases} \forall x,\ P(x) \\ \exists x,\ P(x) \end{cases}$$

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

$\exists$ $\Longleftrightarrow$ $\forall$ (negation)

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 $qs = 1$	$\exists\, q \in \mathbb{Q}\setminus\{0\},\ \forall\, s \in \mathbb{Q},\ \text{s.t.}\ qs \neq 1$
$\forall x \in \mathbb{Z}, \exists! y \in \mathbb{Z}$ such that $x + y = 0$	$\exists\, x \in \mathbb{Z},\ \text{s.t.}\ (\forall y \in \mathbb{Z},\ x+y \neq 0)$ or $(\exists y_1, y_2 \in \mathbb{Z},\ y_1 \neq y_2,\ x+y_1 = x+y_2 = 0)$
$\forall \epsilon > 0 \exists \delta > 0$ such that whenever $\lvert x - x_0\rvert < \delta$, $\lvert f(x) - f(x_0)\rvert \leq \epsilon$	$\exists\, \varepsilon > 0,\ \forall \delta > 0,\ \exists\, x$ s.t. $\lvert x - x_0\rvert < \delta,\ \lvert f(x) - f(x_0)\rvert \geq \varepsilon$

What do these mean in English?

Types of proof

- Direct
- Contradiction
- Contrapositive
- Induction

$P \Rightarrow Q$

"$P \Rightarrow Q$" $\equiv$ "$\neg P \vee Q$",

$\neg Q \Rightarrow \neg P$.

First assume $P \wedge \neg Q$.
Next, derive it's impossible

($\neg(P \Rightarrow Q)$ is impossible
$P \Rightarrow Q$ is true.)

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 $m, n \in \mathbb{Z}$, n is even

By definition of even, we know $\exists\, j \in \mathbb{Z}$, $n = 2j$

Then $m \cdot n = m \cdot 2j = 2 \cdot m \cdot j$, $m \cdot j$ is integer

So $m \cdot n = 2(m \cdot j)$ is even by definition

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. By definition, $a|b \rightarrow \exists j \in \mathbb{Z},\ b = aj$

$b|c \rightarrow \exists m \in \mathbb{Z},\ c = mb$

$c = m \cdot a \cdot j = (mj) \cdot a$

So $a|c$ by definition

Claim

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

How would you approach this proof?

$x^2 = 2n$, $x = \pm\sqrt{2n}$.

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

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
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

same

equivalent

Proof by contrapositive

Claim

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

Proof. $P \Rightarrow Q$

$\neg Q \Rightarrow \neg P$, $\neg P$ $x \in \mathbb{Z}$, x^2 is not even

$\neg Q$, x is not even

If x is odd, then x^2 is odd,

By definition, $x = 2j+1$, $x^2 = 4j^2+1+2j = (4j^2+2j)+1$

So x^2 is odd by definition. $= 2m+1$ with $m = 2j^2+j$

Proof by contradiction

$P \Rightarrow Q \quad \overset{\text{same}}{\Longleftrightarrow} \quad \neg P \vee Q$

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

{ First assume $P \wedge \neg Q$ ←
then find contradiction }

Claim

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

Proof. $P: x \in \mathbb{Q}, \; y \in \mathbb{R}/\mathbb{Q}$

$Q: x+y \in \mathbb{R}/\mathbb{Q}$

Assume $P \wedge \neg Q$. $x \in \mathbb{Q}, \; y \in \mathbb{R}/\mathbb{Q}, \; x+y \in \mathbb{Q}$

$\begin{cases} x+y \in \mathbb{Q} \\ x \in \mathbb{Q} \end{cases}$, assume $x+y = s, \; s \in \mathbb{Q}$

$y = \frac{s}{1} - \frac{x}{1}$ is rationale.

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

$\neg Q \Rightarrow \neg P \iff P \Rightarrow Q$

$\neg(P \wedge \neg Q) \iff P \Rightarrow Q$

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 $n=4$, $n! = 1\times2\times3\times4 = 24$, $2^n = 2^4 = 16$

$n! > 2^n$

Induction step : suppose $\exists k$, $k! > 2^k$

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

Conclude : $\forall\, n \geq 4$, $n! > 2^n$

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, it's trivial

Inductive hypothesis: Suppose $\exists\, k \geq 2$, $\forall\, n \in [2, k]$, n is $\mathbb{Z}$, n can be written as the product of primes

Inductive step: 1) If $k+1$ is prime, it's trivial

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

So $k+1$ is can 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.