# Module 1: Proofs

## Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Ichiro Hashimoto

University of Toronto

July 8, 2024

# Outline

- Logic
- Review of Proof Techniques

# Propositional logic

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

If $n = 3$, $P$ is true and $Q$ is false.

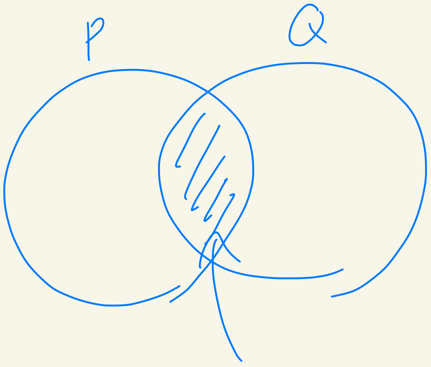
ex. "$n$ is odd" and "$n$ is divisible by 2" are propositions . Let's call them $P$ and $Q$. Whether they are true or not depends on what $n$ is.

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

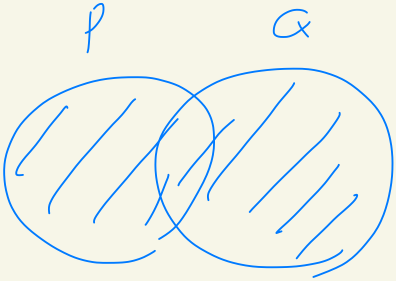
We can combine statements:

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

"either P or Q is true" + "Both P and Q is true"




$P \wedge Q$




$P \vee Q$

# Examples

$P \Rightarrow Q$ If $P$ holds, then $Q$ holds.

A: it's raining

B: I bring my 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. $\neg A \Rightarrow \neg B$
- I'm a banana or Toronto is in Canada. $= C$ ✓ $= D$
- If I pass this exam, I'll be both happy and surprised. $Q$ $R$ $S$

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

Statistical Sciences
UNIVERSITY OF TORONTO

# 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

$$P \implies Q$$

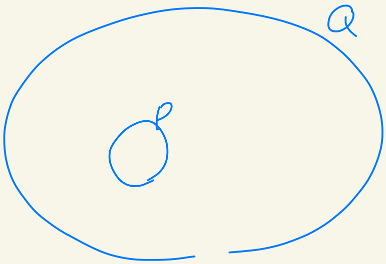
If it is snowing, then it is cold out.

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 logic $\qquad\qquad\qquad$ set

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




$P$ is F $\longleftrightarrow$ $P = \emptyset$ empty set

empty set is a subset of any set

$P \Rightarrow Q$ is True $\longleftrightarrow$ $\emptyset \subset Q$

when $P$ is F

# Logical equivalence

same. !

$p \Rightarrow Q$ and $\neg p \vee Q$ are 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 $\neg(P \implies Q)$?

# 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.

For any $x$, $P(x)$ holds.

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

$\forall x \in \mathbb{R},\ x^2 \geq 0$

How do we prove a for all statement?

Take arbitrary $x$ and show $P(x)$ is true.

Statistical Sciences
UNIVERSITY OF TORONTO

# 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.

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

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

How do we prove a there exists statement?

Find $x$ such that $P(x)$ is true.

"exists" and "unique"

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 | $\forall x \in \mathbb{Q}\setminus\{0\}, \exists y \in \mathbb{Q}\setminus\{0\}$ s.t. $xy=1$ |
| Each integer has a unique additive inverse | $\forall x \in \mathbb{Z}, \exists!\, y \in \mathbb{Z}$ s.t. $x+y=0$ |
| $f : \mathbb{R} \to \mathbb{R}$ is continuous at $x_0 \in \mathbb{R}$ | $\forall \varepsilon > 0, \exists \delta > 0$ s.t. $\lvert x - x_0 \rvert < \delta \Rightarrow \lvert f(x) - f(x_0) \rvert < \varepsilon$ |

# 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?

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

Negating quantifiers:

$$\neg \forall x P(x) = \exists x (\neg P(x)) \quad \text{exists } x \text{ s.t. } P(x) \text{ does not hold.}$$
$$\neg \exists x P(x) = \forall x (\neg P(x)) \quad \text{for any } x\text{, } P(x) \text{ is not true.}$$

Statistical Sciences
UNIVERSITY OF TORONTO

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

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

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

Then $nm = 2j \cdot m = 2(jm) =$ even by definition $\checkmark$

Statistical Sciences
UNIVERSITY OF TORONTO

## 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 $\exists\, j \in \mathbb{Z}$ s.t. $b = aj$ and $\exists\, k \in \mathbb{Z}$ s.t. $c = bk$.

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

Therefore, $a$ divides $c$.

Statistical Sciences
UNIVERSITY OF TORONTO

## Claim

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

How would you approach this proof?

$x^2 = 2n \qquad x = \sqrt{2n}$ ?

Direct proof does not work well

# Proof by contrapositive

Contrapositive of $P \Rightarrow Q$

logically equivalent

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

| $P$ | $Q$ | $P \implies Q$ |
|---|---|---|
| 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 an integer squared is even, then the integer is itself even.

$P$ $\qquad$ $Q$

*Proof.*

Instead of $P \Rightarrow Q$, we can show $\neg Q \Rightarrow \neg P$

We prove the contrapositive.

Let $n \in \mathbb{Z}$ is odd. $\exists j \in \mathbb{Z}$ s.t. $n = 2j+1$.

Then $n^2 = (2j+1)^2 = \underbrace{2(2j^2+2j)+1}_{\text{odd.}}$

Thus $n^2$ is 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 $x \in \mathbb{Q}$ and $y \in \mathbb{R} \setminus \mathbb{Q}$.

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

Then $\underbrace{y}_{\text{irrational}} = \underbrace{s}_{\text{rational}} - \underbrace{x}_{\text{rational}} = \text{rational}.$

Thus, irrational = rational which is a 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  starting point
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. Suppose $n = 4$.

$$\left.\begin{aligned} LHS &= 4! = 24 \\ RHS &= 2^4 = 16 \end{aligned}\right\} \therefore \; LHS > RHS.$$

Inductive hypothesis. Suppose $k! > 2^k$ for $k \geq 4$.

Then $2^{k+1} = \underbrace{2 \times 2^k < 2 \times k!}_{\text{by the inductive hypothesis}} < (k+1) \times k! = (k+1)!$

Therefore, the claim holds for any $n \geq 4$ by induction. //

## 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:*

$n=2$. 2 is prime. So the statement holds trivially.

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

*Inductive step:*

Consider $k+1$.

Case 1: If $k+1$ is prime, then the statement holds trivially.

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

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

Thus $k+1 = ab$ can be written by 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.