

# Day 1: Proofs

## Operational math bootcamp



Statistical Sciences  
UNIVERSITY OF TORONTO

Emma Kroell

University of Toronto

May 6, 2022

# Outline

- Logic
- Review of Proof Techniques
- Examples



# 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 “ $n$  is odd and  $n$  is divisible by 2”.
- $P \vee Q$  is the statement “ $n$  is odd or  $n$  is divisible by 2”. 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:

$$\begin{array}{c} P \implies Q \\ P \end{array}$$

Conclusion:  $Q$

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

# Truth table

If it is snowing, then it is cold out.  
It is snowing.  
Therefore, it is cold out.

$$P \implies Q$$

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

# 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	F	T
T	F	F	F
F	T	T	T
F	F	T	T

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

# 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  $n, m \in \mathbb{Z}$ , with  $n$  even. By definition, there  $\exists j \in \mathbb{Z}$  such that  $n = 2j$ . Then

$$nm = (2j)m = 2(jm)$$

Therefore  $nm$  is even by definition. □

## 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

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

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

# Proof by contrapositive

$$P \implies Q$$

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

# Proof by contrapositive

## Claim

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

## Proof.

We prove the contrapositive. Let  $n$  be odd. Then there exists  $k \in \mathbb{Z}$  such that  $n = 2k + 1$ . We compute

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Thus  $n^2$  is odd.



# Proof by contradiction

## Claim

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

## Proof.

Let  $q \in \mathbb{Q}$  and  $r \in \mathbb{R} \setminus \mathbb{Q}$ . Suppose in order to derive a contradiction that their sum is rational, i.e.  $r + q = s$  where  $s \in \mathbb{Q}$ . But then  $r = s - q \in \mathbb{Q}$ . Contradiction.  $\square$

# 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  $n \geq 4$ .

## Proof.

We prove this by induction on  $n$ .

*Base case:* Let  $n = 4$ . Then  $n! = 4! = 24 > 16 = 2^4$ .

*Inductive hypothesis:* Suppose for some  $k \geq 4$ ,  $k! > 2^k$ .

Then

$$(k+1)! = (k+1)k! > (k+1)2^k > 2(2^k) = 2^{k+1}.$$



## Claim

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

## Proof.

We prove this by induction on  $n$ .

*Base case:*  $n = 2$  is prime.

*Inductive hypothesis:* Suppose for some  $k \geq 2$  that one can write every integer  $n$  such that  $2 \leq n \leq k$  as a product of primes.

We must show that we can write  $k + 1$  as a product of primes.

First, if  $k + 1$  is prime then we are done.

Otherwise, if  $k + 1$  is not prime, by definition it can be written as a product of some integers  $a, b$  such that  $1 < a, b < k + 1$ . By the induction hypothesis,  $a$  and  $b$  can both be written as products of primes, so we are done. □

# Exercises

- 1 Prove De Morgan's Laws:  $\neg(P \wedge Q) = \neg P \vee \neg Q$  and  $\neg(P \vee Q) = \neg P \wedge \neg Q$ .
- 2 Prove the Fundamental Theorem of Arithmetic, that every integer  $n \geq 2$  has a unique prime factorization (i.e. prove that the prime factorization from the last proof is unique).