Module 1: Proofs

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Emma Kroell

University of Toronto

July 11, 2022

Outline

- Logic
- Review of Proof Techniques
- Introduction to Set Theory

Propositional logic

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

P Q

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:

and
- $P \wedge Q$ is the statement: n is odd & n is divisible by 2

or
- $P \vee Q$ 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

A : it's raining
B : I bring my umbrella

$\neg A \implies \neg B$

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

$C \vee D$

• $\underbrace{\text{I'm a banana}}_{C}$ or $\underbrace{\text{Toronto is in Canada}}_{D}$.

• If I pass this exam, I'll be both happy and surprised. $P \implies Q \wedge R$

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:

$$P \Rightarrow Q$$

$$P \quad \therefore \quad Q$$

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?

$$P \implies Q$$

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 $\neg(P \implies Q)$?

$P \wedge \neg Q$

Statistical Sciences
UNIVERSITY OF TORONTO

Quantifiers

For all

"for all", $\forall$, 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

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

How do we prove a for all statement?

Take x in the domain arbitrary.

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 one, i.e. find x in domain s.t. $P(x)$ is true

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

$$\exists!\, x \in \mathbb{N} \text{ s.t. } x^2 = 64$$

$$\mathbb{N} = \{1, 2, 3, \ldots\}. \quad \mathbb{N}_0 = \{0, 1, \ldots\}$$

Combining quantifiers

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

$\mathbb{Q}$: rationals

Statement	Logical expression
Every non-zero rational number has a multiplicative inverse	$\forall q \in \mathbb{Q} \setminus \{0\}\ \exists s \in \mathbb{Q}$ s.t. $qs = 1$
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. $\|x - x_0\| < \delta \Rightarrow \|f(x) - f(x_0)\| < \varepsilon$

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?

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

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

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 $n, m \in \mathbb{Z}$. Assume n is even. By definition, it means $\exists j \in \mathbb{Z}$ s.t. $n = 2j$.

Then $mn = m2j = 2\underbrace{(mj)}_{\in \mathbb{Z}}$ $\therefore$ mn is even

$\square$

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.

exercise

□

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

Proof by contrapositive

Claim

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

integer is odd $\Rightarrow$ integer squared is odd

Proof.

We prove the contrapositive.

Let $n \in \mathbb{Z}$ s.t. $n = 2k+1$ for some $k \in \mathbb{Z}$.

$$\Rightarrow n^2 = (2k+1)^2 = 4k^2 + 4k + 1$$
$$= 2\underbrace{(2k^2+2k)}_{\in \mathbb{Z}} + 1$$

$\therefore n^2$ is odd by definition. $\square$

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

$$q + r = s, \quad s \in \mathbb{Q}.$$

$\Rightarrow r = s - q$. We know that $s - q \in \mathbb{Q}$. $\square$

$\Rightarrow \Leftarrow$

$\therefore s \in \mathbb{R} \setminus \mathbb{Q}$

Statistical Sciences
UNIVERSITY OF TORONTO

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.

We prove this by induction on n.

Base case: $n = 4$ $\qquad n! = 24 > 16 = 2^4$ ✓

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

$$(k+1)! = (k+1)(k!) > \underbrace{(k+1)}_{>2} 2^k > 2 \cdot 2^k = 2^{k+1}$$

□

Thus the statement holds by induction.

Claim

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

Proof.

We prove this by induction on n.

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

Inductive hypothesis:

Suppose for $k \geq 2$, we can write an $n \in \mathbb{Z}$ with $2 \leq n \leq k$ as the product of primes.

Inductive step:

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

If $k+1$ is prime, we are done.

If $k+1$ is not prime, $k+1 = ab$ for some a, b with $1 < a, b < k+1$.

Using the inductive hyp, we are done. $\square$

(This is what it means to not be prime)

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.