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**.

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", $\forall$, 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

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

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

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	
$f : \mathbb{R} \to \mathbb{R}$ 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:
$\neg(P \wedge Q) = \neg P \vee \neg Q$ 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 $qs = 1$	
$\forall x \in \mathbb{Z}, \exists! y \in \mathbb{Z}$ such that $x + y = 0$	
$\forall \epsilon > 0\ \exists \delta > 0$ such that whenever $\lvert x - x_0 \rvert < \delta$, $\lvert f(x) - f(x_0) \rvert < \epsilon$	

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.

$\square$

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.

$\square$

Proof by contradiction

Claim

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

Proof.

$\square$

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

Claim

$n! > 2^n$ if $n \geq 4$.

Proof.

$\square$

Claim

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

Proof.

We prove this by induction on n.

Base case:

Inductive hypothesis:

Inductive step:

$\square$

Introduction to Set Theory

- We define a *set* to be a collection of mathematical objects.
- If S is a set and x is one of the objects in the set, we say x is an element of S and denote it by $x \in S$.
- The set of no elements is called empty set and is denoted by $\emptyset$.

Definition (Subsets, Union, Intersection)

Let S, T be sets.

- We say that S is a *subset* of T, denoted $S \subseteq T$, if $s \in S$ implies $s \in T$.
- We say that $S = T$ if $S \subseteq T$ and $T \subseteq S$.
- We define the *union* of S and T, denoted $S \cup T$, as all the elements that are in *either* S or T.
- We define the *intersection* of S and T, denoted $S \cap T$, as all the elements that are in *both* S and T.
- We say that S and T are *disjoint* if $S \cap T = \emptyset$.

Some examples

Example

$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Example

Let $a, b \in \mathbb{R}$ such that $a < b$.
Open interval: $(a, b) := \{x \in \mathbb{R} : a < x < b\}$ (a, b may be $-\infty$ or $+\infty$)
Closed interval: $[a, b] := \{x \in \mathbb{R} : a \leq x \leq b\}$
We can also define half-open intervals.

Example

Let $A = \{x \in \mathbb{N} : 3|x\}$ and $B = \{x \in \mathbb{N} : 6|x\}$ Show that $B \subseteq A$.

Proof.

$\square$

Difference of sets

Definition

Let $A, B \subseteq X$. We define the *set-theoretic difference* of A and B, denoted $A \setminus B$ (sometimes $A - B$) as the elements of X that are in A but *not* in B.
The complement of a set $A \subseteq X$ is the set $A^c := X \setminus A$.

Example

Let $X \subseteq \mathbb{R}$ be defined as $X = \{x \in \mathbb{R} : 0 < x \leq 40\} = (0, 40]$. Then
$X^c = \{x \in \mathbb{R} : x \leq 0 \text{ or } x > 40\} = (-\infty, 0] \cup (40, \infty)$.

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.

Runde, Volker (2005). *A Taste of Topology*. Universitext. url: https://link.springer.com/book/10.1007/0-387-28387-0