Module 1: Proofs

Operational math bootcamp

Statistical Sciences
UNIVERSITY OF TORONTO

Emma Kroell

University of Toronto

July 10, 2023

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.

P   Q

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

$\neg Q$: n is not divisible by 2

We can combine statements:

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

  We always assume the inclusive or unless specifically stated otherwise.

Statistical Sciences
UNIVERSITY OF TORONTO

Examples

A: it's raining
B: I bring my umbrella
$\neg A \implies \neg B$

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.

$C \vee D$

- I'm a $\underbrace{\text{banana}}_{C}$ or $\underbrace{\text{Toronto is in Canada}}_{D}$.
- If I pass this exam, I'll be both happy and surprised.

Q R S

$Q \implies (R \wedge S)$

Truth values

Example

If it is snowing, then it is cold out. $P \Rightarrow Q$
It is snowing. P
Therefore, it is cold out. $\therefore Q$ true

Write this using propositional logic:

P: it is snowing, Q: it is cold out

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

Logical equivalence

$\to$ implies
or If P, then Q

$P \implies Q$

$\neg P \vee Q$

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

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 $\neg(P \implies Q)$?

$\neg(\neg P \vee Q)$

$= P \wedge \neg Q$

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

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

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

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

How do we prove a for all statement?

Take x in the domain arbitrary, show $P(x)$ is true.

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 is domain such that 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

$$\exists! x \in \mathbb{Z}_+,\ x^2 = 64$$

Statistical Sciences
UNIVERSITY OF TORONTO

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	$\forall q \in \mathbb{Q} \setminus \{0\}\ \exists s \in \mathbb{Q}$ 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?

$$
\begin{aligned}
&(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x + y = 2) && F \\
&\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\ x + y = 2 && T \\
&\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\ x + y = 2 && F \\
&\exists x \in \mathbb{R}\, \exists y \in \mathbb{R}\ x + y = 2 && T
\end{aligned}
$$

Negating quantifiers:

$$
\begin{aligned}
\neg \forall x P(x) &= \exists x (\neg P(x)) \\
\neg \exists x P(x) &= \forall x (\neg P(x))
\end{aligned}
$$

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

$(\forall \varepsilon > 0)(\exists \delta > 0)(\lvert x - x_0\rvert < \delta) \Rightarrow (\lvert f(x) - f(x_0)\rvert < \varepsilon)$

What do these mean in English?

$(\exists \varepsilon > 0)(\forall \delta > 0)(\lvert x - x_0\rvert < \delta) \wedge (\lvert f(x) - f(x_0)\rvert \geq \varepsilon)$

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, i.e., $\exists j \in \mathbb{Z}$ s.t. $n = 2j$. (by definition).
Then $nm = 2jm = 2 \times (jm)$. Since $jm \in \mathbb{Z}$, mn 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. Let $a, b, c \in \mathbb{Z}$, $a \neq 0$.

$a|b \Rightarrow \exists j \in \mathbb{Z}$ s.t. $b = aj$

$b|c \Rightarrow \exists k \in \mathbb{Z}$ s.t. $c = bk$

Then $c = bk = ajk$. Since $jk \in \mathbb{Z}$, $a|c$ by definition.

Claim

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

How would you approach this proof?

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

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 $\underbrace{\text{an integer squared is even}}_{P}$, then $\underbrace{\text{the integer is itself even}}_{Q}$.

Proof.

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

Integer is odd $\Rightarrow$ integer squared is odd

We prove the contrapositive. Let $n \in \mathbb{Z}$ s.t. $\exists k \in \mathbb{Z}$ s.t. $n = 2k+1$.

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

Thus n^2 is odd by definition.

Proof by contradiction

Assume the statements aren't true and derive a 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

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

Then $r = s - q$. But $s - q \in \mathbb{Q}$. This is a contradiction.

Therefore $q + r$ must be irrational.

Summary

In sum, to prove $P \implies Q$:

$$\begin{aligned}
\text{Direct proof:} &\quad \text{assume } P \text{, prove } Q \\
\text{Proof by contrapositive:} &\quad \text{assume } \neg Q \text{, prove } \neg P \\
\text{Proof by contradiction:} &\quad \text{assume } P \wedge \neg Q \text{ and derive something that is impossible}
\end{aligned}$$

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 the claim by induction.

Base case: $n=4$ $\quad 4! = 4 \times 3 \times 2 \times 1 = 24$

$2^4 = 16$

Since $4! > 2^4$, the base case holds.

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

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 statement holds 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.

Inductive hypothesis: Suppose for $k \geq 2$, we can write any $n \in [2, k]$ as the product of primes, i.e., $\exists p_1, \ldots, p_m$ prime such that $n = p_1 \cdots p_m$.

Inductive step:

We want to show that $k+1$ can be written as the product of primes.

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

If $k+1$ is not prime, $k+1 = ab$ where $1 < a, b < k+1$.

Then by the inductive hypothesis, the conclusion holds.

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.