Introduction to Analysis: Logic and Proof

Statements

First, we talk about how to talk about truth.

We use the term

statement

to refer to any declarative sentence that has a truth value.

By "truth value" we are referring to

bivalent logic

here: "true" and "false" are the *only* truth values we consider.

Conventions of Notation

Certain mathematical objects have “default” letters used in mathematical literature to represent them.

It is reasonable that ANY letter can be used to refer to ANY type of mathematical object.

These are merely conventions that many textbooks and papers use.

Conventions of Notation

- real numbers $\mathbb{R}$: variables, x, y, z; constants, a, b, c.
- rational numbers $\mathbb{Q}$: q, r
- integers $\mathbb{Z}$: n, m
- real numbers *representing time*: t, s
- *functions* of real numbers: f, g
- statements: P, Q, R, ϕ, ψ, p, q, r

Logical Connectives

There are several operators that allow you to combine statements into new (*compound*) statements.

The simplest ones are, with notation:

- NOT (**negation**) ($\sim P$, $\neg P$, $\overline{P}$)
- OR (inclusive or - **disjunction**) ($P \vee Q$)
- XOR (exclusive or - "either or") ($P \oplus Q$, $P \veebar Q$)
- AND (**conjunction**) ($P \wedge Q$)

Logical Connectives

- IMPLIES (**implication**, **conditional**)

$$\text{if } P, \text{ then } Q, \qquad P \implies Q$$

- converse implication

$$\text{if } Q, \text{ then } P, \qquad P \text{ only if } Q, \qquad Q \implies P, \qquad P \Leftarrow Q$$

- IFF (**logical equivalence**, **biconditional**) (if and only if)

$$P \iff Q, \qquad P \equiv Q$$

You may also see the conditional arrows in a single-bar format:

$$\rightarrow \qquad \leftarrow \qquad \longleftrightarrow$$

Order of Precedence

Precedence of logical operators is similar to elementary arithmetic:

$$\begin{array}{ccc} P, E & M, D & A, S \\ (), x^y & \times, \div & +, - \end{array}$$

becomes

$$\begin{array}{ccc} P, NOT & AND & OR \\ (), \neg & \wedge & \vee \end{array}$$

Truth Tables

A **truth table** gives the truth values of a compound statement.

It does so by checking every possible case of truth values for the simple statements in the compound statement.

If there are n elementary statements in a compound statement, the truth table must have 2^n rows.

Truth Tables

The truth tables for the basic logical connectives are:

P	Q	$\neg P$	$P \vee Q$	$P \wedge Q$	$P \implies Q$	$P \iff Q$
T	T	F	T	T	T	T
T	F	F	T	F	F	F
F	T	T	T	F	T	F
F	F	T	F	F	T	T

Note that every column here is different.

Truth Tables: Make them simpler to write

To easily write a truth table, add columns for substatements.

For example, the truth table for $(P \vee Q) \wedge \neg Q$ can be written

P	Q	$P \vee Q$	$\wedge$	$\neg Q$
T	T	T	F	F
T	F	T	T	T
F	T	T	F	F
F	F	F	F	T

Logical Equivalence

If two statements have the same exact column entries in a truth table, they are called

logically equivalent

and this fact is denoted by $\equiv$.

Using the previous example, we can deduce

$$((P \vee Q) \wedge \neg Q) \equiv \neg(P \implies Q).$$

Tautology (Always True)

A statement is called a

tautology

if its truth table column is all T.

The simplest tautology is the **law of excluded middle**:

$$P \vee \sim P$$

A tautology may be represented by the symbol $\top$ (*verum*).

Contradiction (Always False)

A statement is called a

contradiction

if its truth table column is all F.

The simplest contradiction is the **law of non-contradiction**:

$$P \wedge \sim P$$

A contradiction may be represented by the symbol $\perp$ (*falsum*).

Satisfiable (Not Always False)

A statement is called

satisfiable

if there exists a T in its truth table column.

A contradiction is the only **nonsatisfiable** type of statement.

DeMorgan's Laws

DeMorgan's Laws in logic give the negations of AND and OR.

Symbolically, for two statements P and Q, these laws are:

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

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

For proof, simply build truth tables.

We will see a set version of DeMorgan's Laws in the next section.

DeMorgan's Laws

Here is the truth table for DeMorgan's disjunction law.

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

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

DeMorgan's Laws

Here is the truth table for DeMorgan's disjunction law.

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

P	Q	$\neg$	$(P \vee Q)$	$\neg P$	$\wedge$	$\neg Q$
T	T		T	F		F
T	F		T	F		T
F	T		T	T		F
F	F		F	T		T

DeMorgan's Laws

Here is the truth table for DeMorgan's disjunction law.

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

P	Q	$\neg$	$(P \vee Q)$	$\neg P$	$\wedge$	$\neg Q$
T	T	F	T	F	F	F
T	F	F	T	F	F	T
F	T	F	T	T	F	F
F	F	T	F	T	T	T

Predicates

Predicates are statements that contain variables.

Predicates are functions that take input, and output a truth value.

For a simple example predicate with integer input, define

$$e : \mathbb{Z} \to \{T, F\}$$

by

$$e(x) := \text{“}x \text{ is even.”}$$

Predicates

Predicates can be

always true, *sometimes true*, or *never true*,

depending on the domain of definition.

For the predicate $e(x)$ defined earlier, $e(2)$ is T and $e(-13)$ is F.

We could try to build a truth table for e with all values $x \in \mathbb{Z}$, ...
but it wouldn't go well.

Predicates

The predicate

$$p : \mathbb{Z} \to \{T, F\}$$

defined by

$$p(n) := \text{“}n^2 - 4 = 0\text{”}$$

is true for $n = \pm 2$, but false for all other $n \in \mathbb{Z}$.

In the usual situation, we will not write out the functional notation,

but we should specify what domain our statements are defined on.

Predicates

The predicate q defined by

$$q(x) := \text{“}x^2 - 5 = 0\text{”}$$

is never true for $x \in \mathbb{Z}$.

However, if q defined on $\mathbb{R}$, q is true for $x = \pm\sqrt{5}$.

Quantifiers

With predicates come two more logical connectives called

quantifiers.

These symbols declare the

quantity of *elements* of a *set*

that a statement is about.

Existential Quantifier

The **existential quantifier** $\exists$ means "there exists".

Computationally, $\exists$ means

"there is at least one of these"

elements in a given set satisfies a certain property.

Existential Quantifier

The existentially-quantified statement P defined by

$$P = \text{“}\exists x \in \mathbb{Z} : \; x^2 - 5 = 0\text{”}$$

is false, since no $x \in \mathbb{Z}$ satisfies $x^2 - 5 = 0$.

Existential Quantifier

Note that P defined by

$$P = \text{“}\exists x \in \mathbb{Z} : \ x^2 - 5 = 0\text{”}$$

is *not* a predicate, but if we rewrite P using ϕ as

$$\phi(x) = \text{“}x^2 - 5 = 0\text{”}$$

$$P = \text{“}\exists x \in \mathbb{Z} : \ \phi(x)\text{”}$$

then $\phi(x)$ *is* a predicate. (P is still a single false statement.)

Existential Quantifier

The statement

$$Q = \text{``}\exists x \in \mathbb{R} : \; x^2 - 5 = 0\text{''}$$

is true since there does exist such an $x \in \mathbb{R}$; namely, $x = \sqrt{5}$.

Note that the existence of just one such value x suffices for truth.

Universal Quantifier

The **universal quantifier** $\forall$ means "for all".

Computationally, $\forall$ means

"every one of these"

elements in a given set satisfies a certain property.

Universal Quantifier

The universally-quantified statement E defined by

$$E = \text{“}\forall n \in \mathbb{Z} : \; e(n)\text{”}$$

where $e(x) =$ “x is even” is false, since there exists an odd integer.

Note that existence of just one such value x suffices for falsehood.

Universal Quantifier

The statement Q defined by

$$Q = \text{“}\forall x \in \mathbb{Z}: \; x + y = 6 \text{ has a solution for } y \in \mathbb{Z}\text{”}$$

is true.

Can you *prove* this statement?

Speaking English With Quantifiers

Define the predicate

$$W(x) = \text{“I have watched episode } x \text{ of } \textit{The X-Files}\text{”}$$

over the domain

$$E = \{x : \ x \text{ is an episode of } \textit{The X-Files}\}.$$

Then the statement

$$\exists x \in E : \ W(x)$$

could be spoken as

“There exists an episode x of *The X-Files* such that I have watched episode x.”

Speaking English With Quantifiers

However, that's not usually how people speak.

"There exists an episode x of *The X-Files* such that I have watched episode x"

is more likely to be said

"I have watched an episode of *The X-Files*."

Speaking English With Quantifiers

Likewise, the statement

$$\forall x \in E,\ W(x)$$

could be spoken as

"For every episode x of *The X-Files*, I have watched episode x"

but would much more likely be said

"I have watched every episode of *The X-Files*".

Negating a Quantifier

To negate a quantified statement,

negate the predicate and switch the quantifier.

Notice in English: the negation of

"I have watched every episode of *The X-Files*"

is

"I have not watched every episode of *The X-Files*".

This negation is logically equivalent to the statement

"There is an episode of *The X-Files* that I have not watched".

Negating a Quantifier

A logical equivalent to a quantified statement with the other quantifier can be attained by

- negating the predicate
- and both switching and negating the quantifier.

Notice in English:

"I have watched every episode of *The X-Files*"

is logically equivalent to

"There is not an episode of *The X-Files* that I have not watched".

Why is that so?

Negating a Quantifier

Compare the following statements. Which are equivalent?

$\forall x \in E,\ W(x)$	"I have watched every episode of *The X-Files*"
$\neg(\forall x \in E,\ W(x))$	"I have not watched every episode of *The X-Files*"
$\exists x \in E : \neg W(x)$	"There is an episode of *The X-Files* that I have not watched"
$\neg(\exists x \in E : \neg W(x))$	"There is not an episode of *The X-Files* that I have not watched"

Axiomatic Proof

We establish mathematical truth via **mathematical proof**.

Definition

A **mathematical proof** of a proposition is a chain of logical deductions leading from a base set of **axioms** to the proposition.

Axiomatic Proof

... so what is an axiom?

Definition

Axioms are statements that are given as true and used, with logical connectives, as the basis of a mathematical proof system.

Propositions to Prove: Terminology

Some specialized terms for logical / mathematical statements:

A **proposition** is a logical statement (typically a *conditional* ("implication") or *biconditional* ("if and only if", or "iff")), that states **antecedents** (hypotheses) and yields a **consequent** (conclusion) as its result, which has a mathematical proof.

We use

$$\Longrightarrow$$

to denote *logical implication*, and

$$\therefore$$

as the word "therefore".

Propositions to Prove: Terminology

All of the following are special names for propositions.

- A **theorem** is an "important" proposition. A typical mathematical research paper will feature just a few theorems (sometimes only one) as its focal content.
- A **lemma** is a supporting proposition used to prove a theorem.
- A **corollary** is a proposition, interesting enough to state on its own, that follows quickly ("for free") from a lemma or theorem.

Types of Proof

Your antecedent is the statement P.
How can you reach the conclusion Q?

- direct proof #1:

$$\text{(modus ponens)} \quad P, (P \implies Q). \therefore Q$$

- direct proof #2: **contrapositive**:

$$\text{(modus tollens)} \quad \neg Q, (P \implies Q). \therefore \neg P$$

- indirect proof: **proof by contradiction**:

$$\text{(reductio ad absurdum)} \quad (\neg P \implies Q), (\neg P \implies \neg Q). \therefore P$$

In any case, when writing a proof, make sure you spell out the methods you are using for maximum clarity of comprehension.

Proof by Cases

Many propositions are complicated enough that they have several *cases* to cover.

By proving smaller pieces of a proposition, it becomes manageable to generate an overall proof.

Proof by Cases

For example, perhaps you discover different techniques to prove

$$P \implies Q$$

depending on whether a certain value a in P is even or odd.

Rewriting

$$P = (P \wedge \text{“}a \text{ is even”}) \vee (P \wedge \text{“}a \text{ is odd”}),$$

you can write two separate proofs, proving

$$(P \wedge \text{“}a \text{ is even”}) \implies Q, \quad (P \wedge \text{“}a \text{ is odd”}) \implies Q,$$

and, taken together, these prove $P \implies Q$.

Direct Proof #1

A **direct proof** of the implication

$$P \implies Q$$

is the most straightforward approach.

How this is done: First, assume P is true. Then, use logic and all the mathematics you can muster to show that Q logically follows from P being true.

(Simple, right?)

Note

If you assume P is false, then, by the implication truth table, $P \implies Q$ is true already. This doesn't tell us anything - the only logical case that matters is starting from P being true.

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

Direct Proof #1: Example

Proposition

For any $n \in \mathbb{Z}$, if n ends in 0, then n is even.

Proof Recall the definition of an even integer: n is called even if

$$\exists m \in \mathbb{Z} : \; n = 2m.$$

But if n ends in 0, then n is a multiple of 10; thus

$$\exists k \in \mathbb{Z} : \; n = 10k = 2(5k).$$

With $m = 5k$, we have that n is even. ∎

Direct Proof #1: Example

Proposition

For any even $n \in \mathbb{Z}$, $5n + 2$ is even.

Proof Since n is even, we know $\exists m \in \mathbb{Z} : n = 2m$. We derive:

$$\begin{aligned} n &= 2m \\ \implies 5n + 2 &= 5(2m) + 2 \\ &= 2(5m) + 2 \\ &= 2(5m + 1). \end{aligned}$$

Since $5m + 1 \in \mathbb{Z}$, we know $5n + 2$ is even. $\blacksquare$

Direct Proof #2: Contrapositive

The **contrapositive** of an implication is logically equivalent to the implication itself:

$$(P \implies Q) \equiv (\neg Q \implies \neg P)$$

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

Thus, you can do a direct proof of $P \implies Q$ by assuming that Q is false (i.e. $\neg Q$ is true) and showing that $\neg P$ logically follows.

(Contrapositive proofs *might* require a bit more cleverness.)

Direct Proof #2: Example

Proposition

For any even $n \in \mathbb{Z}$, $5n + 2$ is even.

Proof Assume $5n + 2$ is not even. Since we know every integer is either even or odd, then $5n + 2$ is odd.

We will prove that n is odd. Since $5n + 2$ is odd, we know $\exists m \in \mathbb{Z}$:

$$
\begin{aligned}
5n + 2 = 2m + 1 \implies \quad 5n &= 2m - 1 \\
\implies \quad n &= 2m - 1 - 4n \\
&= (2m - 4n - 2) + 1 = 2(m - 2n - 1) + 1.
\end{aligned}
$$

Since $m - 2n - 1 \in \mathbb{Z}$, we know n is odd. $\blacksquare$

Traps to Watch For (Logical Fallacies)

There are a number of logical mistakes that can be made in setting up a proof.

Be aware of basic implication structure, and know your logic.

Starting with the implication $P \implies Q$:

- The **logical converse** is not equivalent to the implication:

$$(Q \implies P) \not\equiv (P \implies Q)$$

Traps to Watch For (Logical Fallacies)

- The **contrapositive** is not equivalent to the negation of the implication, but is equivalent to the implication itself:

$$(\neg Q \implies \neg P) \not\equiv \neg(P \implies Q)$$

$$(\neg Q \implies \neg P) \equiv (P \implies Q)$$

- The contrapositive is not equivalent to the **logical inverse** of the implication (compare this to the first statement):

$$(\neg Q \implies \neg P) \not\equiv (\neg P \implies \neg Q)$$

Negation of the Implication

The negation of the implication has a non-implication form that can be useful in proof by contradiction.

P	Q	$P \implies Q$	$\neg(P \implies Q)$	$P \wedge \neg Q$
T	T	T	F	F
T	F	F	T	T
F	T	T	F	F
F	F	T	F	F

Therefore,

$$\neg(P \implies Q) \equiv (P \wedge \neg Q).$$

Indirect Proof, by Contradiction (reductio ad absurdum)

Proof by contradiction (*reductio ad absurdum*: "reduction to absurdity") is called an **indirect proof** because, instead of proving an implication, you show that some form of the negation of the implication leads to a contradiction.

$$(P \implies \perp) \equiv \neg P$$

$$((P \wedge \neg Q) \implies \perp) \equiv (P \implies Q)$$

$$((P \implies Q) \wedge (P \implies \neg Q)) \implies \neg P$$

We will often use a pair of facing arrows $\rightarrow\leftarrow$ to denote the deduction of a contradiction.

Know that **any** logical contradiction can be used to prove $0 = 1$.

Indirect Proof: Example

Proposition

For any even $n \in \mathbb{Z}$, $5n + 2$ is even.

Proof Assume, for a contradiction, that n is even and $5n + 2$ is not even[1]. Thus, $5n + 2$ is odd.

But if n is even, then $-5n$ is also even, and so by the familiar rule odd + even = odd,

$$5n + 2 + -5n = 2$$

is odd. $\rightarrow\leftarrow$ $\therefore$ if n is even, $5n + 2$ is even. ■

[1] We are using the second structure on the previous slide:

$$((P \wedge \neg Q) \implies \bot) \equiv (P \implies Q)$$

Reductio ad absurdum

We will see a proof by contradiction, labeling the statements along the way to show how to use logical connectives and inference rules in constructing the proof.

Theorem

There are infinitely many prime numbers. (Euclid, circa 300 BCE)

Euclid's proof of the infinitude of primes

Theorem

There are infinitely many prime numbers. (Euclid, circa 300 BCE)

Proof Label the set of primes A. We start by assuming there are only finitely many prime numbers, and will prove by contradiction.

$$\phi = \text{“}\exists n \in \mathbb{N}\colon\ |A| = n\text{”}$$

Write this set of primes as $A = \{p_1, p_2, ..., p_n\} \subset \mathbb{N}$.

Euclid's proof of the infinitude of primes

Let

$$q = 1 + \prod_{i=1}^{n} p_i = 1 + p_1 p_2 \cdots p_{n-1} p_n.$$

Since $p_1, p_2, ..., p_n$ are presumed to be all of the primes, then by the Fundamental Theorem of Arithmetic, q must be divisible by at least one of them.

Why? q must be composite (as $q > p_i$ for all $i = 1, 2, ..., n$).

$$\psi = \text{“}\exists i \in \{1, 2, ..., n\} : \tfrac{q}{p_i} \in \mathbb{N}\text{”}$$
$$\phi \implies \psi$$

Euclid's proof of the infinitude of primes

But q is not divisible by p_i for any $i = 1, 2, .., n$, since any division $q \div p_i$ results in a remainder of 1 – more precisely,

$$\frac{q}{p_i} = p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_{n-1} p_n + \frac{1}{p_i}.$$

$$\neg\psi = \text{“}\forall i \in \{1, 2, ..., n\}, \tfrac{q}{p_i} \notin \mathbb{N}\text{”}$$
$$\phi \implies \neg\psi$$

Since q is larger than all n primes that exist, it must also either be prime or a multiple of a prime we didn't consider. Thus, there is at least one more prime than the n primes we believed were the only ones. But n was arbitrarily chosen as the number of existing primes. Therefore, there must be an infinite number of primes.

$$\neg\phi = \text{“}\forall n \in \mathbb{N},\ |A| \neq n\text{ ”}$$
$$\phi \implies \psi,\ \phi \implies \neg\psi. \quad \therefore \quad \neg\phi. \qquad \blacksquare$$

Best Practices for Good Proof-writing

- State your plan.
- Keep the proof linear.
- *Write* and *explain*, don't merely symbolize.
- Spell things out: give clear definitions, and don't think things are "obvious".
- Finish the proof (don't leave details to the reader).

BONUS: ALL $2^4 = 16$ BINARY TRUTH COLUMNS

		0	1	2	3
P	Q	$\bot$	$\neg(P \wedge Q)$	$\neg(Q \implies P)$	$\neg P$
T	T	F	F	F	F
T	F	F	F	F	F
F	T	F	F	T	T
F	F	F	T	F	T

		4	5	6	7
P	Q	$\neg(P \implies Q)$	$\neg Q$	$\neg(P \iff Q)$	$\neg(P \vee Q)$
T	T	F	F	F	F
T	F	T	T	T	T
F	T	F	F	T	T
F	F	F	T	F	T

(If you are computer science-oriented, think of T as 1 and F as 0.)

BONUS: ALL $2^4 = 16$ BINARY TRUTH COLUMNS

		8	9	10	11
P	Q	$P \wedge Q$	$P \iff Q$	Q	$P \implies Q$
T	T	T	T	T	T
T	F	F	F	F	F
F	T	F	F	T	T
F	F	F	T	F	T

		12	13	14	15
P	Q	P	$Q \implies P$	$P \vee Q$	$\top$
T	T	T	T	T	T
T	F	T	T	T	T
F	T	F	F	T	T
F	F	F	T	F	T

(If you are computer science-oriented, think of T as 1 and F as 0.)