Proofs

(Establishing the Truth of Propositions)

1 Rules of inference

1.1 What is a rule of inference?

In mathematical logic, an **argument** or **proof** is a sequence that starts from a list of statements called *premises*, *assumptions*, or *hypotheses* and returns a *conclusion*.

Such a proof is only valid when the sequence of rules needed to validate the conclusion (i.e. to show that it is true) is complete and sound.

Let us use an example. Assume that we are given the following hypotheses,

"If John is a poet, then he is poor"
"John is a poet"

and that we know that those premises are true. Can we conclude that *"John is poor"*? In other words, can we say that:

((If John is a poet then he is poor) and (John is a poet)) then John is poor.

Let us express the same phrase using the language of logic. We first define the two propositions

$$p : \text{John is a poet}$$
$$q : \text{John is poor}$$

The phrase becomes then

$$((p \to q) \land p) \to q$$

We want to know if this statement is a "valid", i.e. that it is always true,namely a tautology. We use a truth table to show that it is indeed the case:

p	q	$p \to q$	$(p \to q) \land p$	$((p \to q) \land p) \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

This "valid" statement ($((p \to q) \land p) \to q$) is called a **rule of inference**. It is usually written as

$$\begin{array}{l} p \to q \\ \underline{p \qquad\;} \\ \therefore q \end{array}$$

where the symbol $\therefore$ can be interpreted as *therefore*.

Do we have to build a truth table for all arguments that we try to validate? Thankfully no, as we can usually follow one of the rules of inference that have been established in logic. A list of such rule is provided in the next subsection.

1.2 Rules of inference

Rule	**Corresponding tautology**	**Name**
$\begin{array}{l} p \to q \\ \underline{p \qquad} \\ \therefore q \end{array}$	$((p \to q) \land p) \to q$	Modus Ponens
$\begin{array}{l} p \to q \\ \underline{\neg q \qquad} \\ \therefore \neg p \end{array}$	$((p \to q) \land \neg q) \to \neg p$	Modus Tollens
$\begin{array}{l} p \to q \\ \underline{q \to r} \\ \therefore p \to r \end{array}$	$((p \to q) \land (q \to r)) \to (p \neg r)$	Syllogism (transitivity)
$\begin{array}{l} p \lor q \\ \underline{\neg p \quad} \\ \therefore q \end{array}$	$((p \lor q) \land \neg p) \to q$	Disjunctive Syllogism
$\begin{array}{l} \underline{p \qquad} \\ \therefore p \lor q \end{array}$	$p \to (p \lor q)$	Addition
$\begin{array}{l} \underline{p \land q} \\ \therefore p \end{array}$	$(p \land q) \to p$	Simplification
$\begin{array}{l} p \\ \underline{q \qquad} \\ \therefore p \land q \end{array}$	$((p) \land (q)) \to (p \land q)$	Conjunction
$\begin{array}{l} p \lor q \\ \underline{\neg p \lor r} \\ \therefore q \lor r \end{array}$	$((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$	Resolution

> The rules of inference give us the tools to validate a conclusion from a set of hypotheses

1.3 Examples

Example 1

Let us consider the following assumptions:

a) *If it rains today, then we will go on a canoe trip*

b) *If we do not go on a canoe trip today, then we will go on a canoe trip tomorrow*

Can we conclude that

If it rains today, then we will go on a canoe trip tomorrow?

Proof:

Let us define the propositions:

$$\begin{aligned} p &: \text{It rains today} \\ q &: \text{We will not go on a canoe trip today} \\ r &: \text{We will go on a canoe trip tomorrow} \end{aligned}$$

Then

Step	**Reason**
$p \to q$	Hypothesis (a)
$q \to r$	Hypothesis (b)
$\therefore p \to r$	Transitivity (rule of inference)

Example 2

Let us consider a more complex set of assumptions:

a) *It is not sunny today and it is colder than yesterday*

b) *If we go swimming then it is sunny*

c) *If we do not go swimming, then we will have a barbecue*

d) *If we have a barbecue, then we will be home by sunset*

Can we conclude that

We will be home by sunset?

Proof:

Let us define the propositions:

$$\begin{aligned} p &: \text{It is sunny today} \\ q &: \text{It is colder than yesterday} \\ r &: \text{We will go swimming} \\ s &: \text{We will have a barbecue} \\ t &: \text{We will be home before sunset} \end{aligned}$$

Then

Line #	**Step**	**Reason**
1	$\neg p \wedge q$	Hypothesis (a)
2	$\neg p$	Simplification rule applied to step 1
3	$r \rightarrow p$	Hypothesis (b)
4	$\neg r$	Modus Tollens rule applied to steps 2 and 3
5	$\neg r \rightarrow s$	Hypothesis (c)
6	s	Modus Ponens rule applied to steps 4 and 5
7	$s \rightarrow t$	Hypothesis (d)
8	$\therefore t$	Modus Ponens applied to steps 6 and 7

Example 3

Let p_1, p_2, and r be three propositions.
Show that

$$((p_1 \rightarrow q) \wedge (p_2 \rightarrow q)) \rightarrow ((p_1 \vee p_2) \rightarrow q)$$

is a tautology.

Proof:

Our hypothesis are that:

$$\begin{aligned} &\text{a) } p_1 \rightarrow q \\ &\text{b) } p_2 \rightarrow q \end{aligned}$$

are both true. Then

Line #	**Step**	**Reason**
1	$p_1 \rightarrow q$	Hypothesis (a)
2	$\neg p_1 \vee q$	Property of implications
3	$p_2 \rightarrow q$	Hypothesis (b)
4	$\neg p_2 \vee q$	Property of implications
5	$(\neg p_1 \vee q) \wedge (\neg p_2 \vee q)$	Conjunction rule applied to steps 2 and 4
6	$(\neg p_1 \wedge \neg p_2) \vee q$	Distributivity law
7	$(\neg(p_1 \vee p_2)) \vee q$	De Morgan's law
8	$(p_1 \vee p_2) \rightarrow q$	Property of implications

2 Methods of proof

Definition
A theorem is a statement that can be shown to be always true

We demonstrate that a theorem is true with a sequence of statements that forms an argument, or proof, as described in the previous section. Possible elements in such arguments / proofs include:

Statement	**Type**
Axioms, postulates Proved theorems	Underlying assumptions
Hypotheses / premises	
Body of the proof	Rules of inference
$\therefore$ Conclusion	

In many of the examples of proof shown below, we will use the concepts of odd and even for integers. Those concepts are defined here:

Definition 1
"An integer number n is even if and only if it is divisible by 2"
or
"An **integer number** n is even if and only if there exists an **integer number** k such that $n = 2k$".

Definition 2
"An integer number n is odd if and only if it is not divisible by 2"
or
"An **integer number** n is odd if and only if there exists an **integer number** k such that $n = 2k + 1$".

2.1 Proofs for implications

.

2.1.1 Methods of proof for implications

Let p and q be two propositions. Suppose that we wish to prove the implication $p \to q$. To understand the strategies that are available to us, it is useful the recall the truth table for an implication:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

The possible strategies are then:

1. Trivial proof of $P \to Q$:

If we know that Q is true, then $P \to Q$ is always true, independent of the truth value of Q

Prove $P \to Q$ is true:
We know Q is true
$\therefore P \to Q$ is true

2. Vacuous proof of $P \to Q$:

If P is false, then $P \to Q$ is always true, regardless of the truth value of Q

Prove $P \to Q$ is true:
We know P is false
$\therefore P \to Q$ is true

3. Direct proof of $P \to Q$:

We assume P (i.e. that P is true), and then we use the rules of inference, axioms, definitions, and logical equivalences to prove that Q is true.

Assume P
...
[Logical deductions]
...
Therefore Q.

4. Indirect proof of $P \to Q$ (*also called proof by contrapositive*):

Remember that an implication $p \to q$ is logically equivalent to its contrapositive, namely $\neg q \to \neg p$. We use then a direct proof of this contrapositive: we assume $\neg q$, and we use an argument to show that $\neg p$.

Assume Q is false
...
[Logical deductions]
...
Therefore P is false
Hence $\neg Q \to \neg P$.
By contraposition, this proves $P \to Q$

5. Proof by contradiction of $P \to Q$:

The implication $p \to q$ is false only when p is true and q is false. We assume that this is possible and we derive a contradiction F. In logic term, if S is the statement to prove and we have proved that $\neg S \to F$ is true, based on the truth table above this is only possible if $\neg S$ is false, namely if S is true.

Assume P is true, AND that Q is false
...
[Logical deductions]
...
Contradiction
Therefore our assumption that P is true and Q is false does not hold
By contradiction, this proves $P \to Q$

6. Proof by cases:

If the statement P can be separated into a set of cases $P_1 \vee P_2 \ldots \vee P_k$, we prove each of the propositions $P_1 \to Q$, $P_2 \to Q$, ..., $P_k \to Q$ separately. Note that this comes from the fact that

$$((p_1 \vee p_2 \ldots \vee p_k) \to q) \leftrightarrow (p_1 \to q) \wedge (p_2 \to q) \ldots \wedge (p_k \to q)$$

is a tautology.

2.1.2 Examples

We will now look at examples for all strategies.

a) **Trivial proof of $P \to Q$**

Prove the statement: If there are 100 students in this class this quarter, then $5^2 = 25$

Proof: Let us define P : "there are 100 students in this class" and Q : "$5^2 = 25$". We want to show $P \to Q$. This assertion is *trivially* true, since Q is always true, independent of the truth value of P (which may, or may not be true, based on the actual enrollment in the class).

b) **Vacuous proof of $P \to Q$**

Prove the statement: If 9 is a prime number, then $1 = 2$

Proof: Let us define P : "9 is a prime number" and Q : "2=1". We want to show $P \to Q$. This assertion is *vacuously* true, since P is false. Note that when P is false, $P \to Q$ is always true, independent of the truth value of Q (in our example, Q is false).

c) **Direct proof of $P \to Q$**

Prove the statement: Let n be an integer. Show that if n is even, then n^2 is even.

Proof: Let n be an integer and let us define

$$\begin{aligned} P(n) &: n \text{ is even} \\ Q(n) &: n^2 \text{ is even.} \end{aligned}$$

We want to show $P(n) \to Q(n)$. In a direct proof, we start with the assumption that $P(n)$ is true. As n is an even number, we know (see above) that there exists an integer k such that

$$n = 2k$$

. We compute n^2:

$$\begin{aligned} n^2 &= n \times n \\ &= (2k) \times (2k) \\ &= 4k^2 \\ &= 2(2k^2) \end{aligned}$$

Let $k' = 2k^2$. As k is an integer, k' is an integer, and n^2 is written as $2k'$. Therefore n^2 is even, and the statement $P(n) \to Q(n)$ is true.

c) **Indirect proof of $P \to Q$**

Prove the statement: Let n be an integer. Show that if n^2 is even, then n is even.

Proof: Let n be an integer and let us define

$$\begin{aligned} P(n) &: n^2 \text{ is even} \\ Q(n) &: n \text{ is even.} \end{aligned}$$

We want to show $p \to q$. In the previous example, we started with n even and we were able to define a property for n^2. In this case, however, the situation is more complicated. Let us try a direct proof, and assume that p is true, namely that there exists an integer k (in fact, positive integer) such that

$$n^2 = 2k$$

. Can we compute n from this equation? This would involve taking a square root, but then we have no guarantee that the result, $\sqrt{2k}$ is an integer. We would then be stuck. We need a different approach and this is when an indirect proof becomes useful. Recall that the implication $P(n) \to Q(n)$ is logically equivalent to its contrapositive, $\neg Q(n) \to \neg P(n)$. Let us attempt a direct proof on the contrapositive. We assume that $\neg Q(n)$ is true, namely that n is not an even number, i.e. n is odd. There exists an integer k such that

$$n = 2k + 1$$

We compute n^2:

$$\begin{aligned} n^2 &= n \times n \\ &= (2k+1) \times (2k+1) \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

Let $k' = 2k^2 + 2k$. As k is an integer, k' is an integer, and n^2 is written as $2k' + 1$. Therefore n^2 is even. We have shown that $\neg Q(n) \to \neg P(n)$ is true, therefore $P(n) \to Q(n)$ is true.

d) **Proof by contradiction**

Prove the statement: Let x be a real number, $x \neq 0$. Show that if $x > 0$, then $x + \frac{1}{x} \geq 2$.

Proof: Let x be a non-zero real number and let us define:

$$P(x) : x > 0$$
$$Q(x) : a + \frac{1}{x} \geq 2$$

We want to show $P(x) \to Q(x)$. We use a proof by contradiction, namely we assume that $P(x)$ is true AND $\neg Q(x)$ is true.

Since $\neg Q(x)$ is true,

$$x + \frac{1}{x} < 2$$

. Since $P(x)$ is true, $x > 0$ and we can multiply the two sides of this inequality without changing its direction:

$$\begin{aligned} x \times x + \frac{x}{x} &< 2x \\ x^2 - 2x + 1 &< 0 \\ (x-1)^2 &< 0 \end{aligned}$$

. But $(x-1)^2$ is a square, and a square is always positive. We have reached a contradiction. This means that $P(x) \wedge \neg Q(x)$ is a contradiction, and therefore using one of the complement laws, $\neg P(x) \vee Q(x)$ is true, i.e. $P(x) \rightarrow Q(x)$ is true (property of implications).

d) **Proof by case**

Prove the statement: Let n be a real number. Show that if n is an integer, then $3n^2+n+1$ is an odd number.

Proof: Let n be a real number and let us define:

$$\begin{aligned} P(n) &: n \text{ is an integer} \\ Q(n) &: 3n^2+n+1 \text{ is an even number.} \end{aligned}$$

We want to show $P(n) \rightarrow Q(n)$. Notice that $Q(n)$ refers to a number being odd, while $P(n)$ contains no information about n being even or odd. However, an integer is either even or odd. Let us define:

$$\begin{aligned} P_1(n) &: n \text{ is an even integer} \\ P_2(n) &: n \text{ is an odd number.} \end{aligned}$$

We have $P(n) = P_1(n) \vee P_2(n)$. We use then a proof by case, namely we show that $P_1(n) \rightarrow Q(n)$ and $P_2(n) \rightarrow Q(n)$ are both true.

i) We show $P_1(n) \rightarrow Q(n)$ is true

We use a direct proof. Let us assume that $P_1(n)$ is true, i.e. that n is an even number. There exists an integer number k such that

$$n = 2k$$

We compute $3n^2+n+1$:

$$\begin{aligned} 3n^2+n+1 &= 3(2k)(2k)+2k+1 \\ &= 12k^2+2k+1 \\ &= 2(6k^2+k)+1 \\ &= 2k'+1 \end{aligned}$$

where we have defined $k' = 7k^2+k$. As k is an integer, k' is an integer. Therefore $3n^2+n+1$ is odd. $P_1(n) \rightarrow Q(n)$ is true.

ii) We show $P_2(n) \rightarrow Q(n)$ is true

We use a direct proof. Let us assume that $P_2(n)$ is true, i.e. that n is an odd number. There exists an integer number k such that

$$n = 2k+1$$

We compute $3n^2 + n + 1$:

$$\begin{aligned} 3n^2 + n + 1 &= 3(2k+1)(2k+1) + 2k + 1 + 1 \\ &= 12k^2 + 12k + 3 + 2k + 2 \\ &= 2(6k^2 + 7k + 2) + 1 \\ &= 2k' + 1 \end{aligned}$$

where we have defined $k' = 6k^2 + 7k + 1$. As k is an integer, k' is an integer. Therefore $3n^2 + n + 1$ is odd. $P_2(n) \to Q(n)$ is true.

As $P_1(n) \to Q(n)$ is true and $P_2(n) \to Q(n)$ is true, $P(n) \to Q(n)$ is true.

2.1.3 Choosing a proof technique

- **Trivial / Vacuous proofs:** Those are rare, but it is worth checking first if the premise P is always false, or if the conclusion Q is always true. In those cases, the proof is trivial!
- **Direct proof:** In most cases, the best strategy is to try a direct proof first; this is the simplest and most natural proof technique. Only when it fails should you consider other methods of proof.
- **Indirect proof:** This is the same as a direct proof, but applied to the contrapositive statement. It is worth considering when the direct proof does not seem to work.
- **Proof by contradiction:** A proof by contradiction for an implication is logically more complicated and more prone to errors. It can be effective is some situations, especially if what we want to conclude *does not* have a certain property (such as "is not rational", "is not a natural number", "is not a perfect square"...).
- **Proof by case:** This is appropriate if the problem naturally breaks down into several cases.

A special note on proof by contradiction

Most proofs mentioned above are specific to implications. A notable exception is the proof by contradiction. Let us assume we need to prove that a certain statement P is true, where P does not have to be an implication. If we can find a contradiction Q such that $\neg P \to Q$, then $\neg \to F$ is true, which is only possible if $\neg P$ is false, namely if P is true.

Example: *Show that $P : \sqrt{2}$ is irrational.*

Proof. Let us assume that P is false, i.e. that $\sqrt{2}$ is rational. There exists a pair (a, b) of integers, with $b \neq 0$, such that

$$\sqrt{2} = \frac{a}{b}$$

We can safely assume that a and b do not have any common factor. If such a common factor were to exist, it can be factored out.

After multiplication by b and squaring:

$$\begin{aligned} a &= \sqrt{2}b \\ a^2 &= 2b \end{aligned}$$

Since b is an integer, a^2 is even. We have seen above (see example of indirect proof) that this implies that a **is even**. There exists an integer k such that

$$a = 2k$$

Replacing in the equation above that defines a^2, we get:

$$\begin{aligned} a^2 &= 2b \\ 4k^2 &= 2b \\ 2k^2 &= b \end{aligned}$$

Since k^2 is an integer, b **is even.** As both a and b are even, they have a common factor, 2. However, we stated that a and b do not have a common factor: we have reached a contradiction. Therefore the assumption that $\sqrt{2}$ is rational is false, and therefore $\sqrt{2}$ is irrational.

3 Proofs and quantifiers

3.1 Existence proofs

Many theorems are assertions that (at least) one object x of a particular type $\mathbb{D}$ satisfies a given predicate P :

$$\exists x \in \mathbb{D}, P(x)$$

To prove such theorems, we do not need to find all values of x that satisfy $P(x)$; we just needs to show the existence of one. There are two types of such existence proof:

a) **Constructive proofs:** We find the object x explicitly

b) **Non-constructive proofs:** We do not find x explicitly; we only show that there must exists one such x.

Examples:

a) **Constructive proofs:**

Prove that there exists a pair of consecutive integers such that one of them is a perfect square and the other is a perfect cube

Proof. Let us recall first what is a perfect square and what is a perfect cube:

- An integer a is a perfect square if there exists an integer n such that $a = n^2$
- An integer a is a perfect cube if there exists an integer n such that $a = n^3$

Let a be one (possible) integer that satisfies the property in the problem. Then we know that there exists an integer n such that $a = n^2$, and an integer p such that $a+1 = p^3$ or $a-1 = p^3$. We observe that if we set $n = 3$ and $p = 2$, then $n^2 = 9$ and $p^3 = 8$, i.e. the pair $(8, 9)$ satisfies the problem. As we only need to find one example, the assertion is true.

b) **Non-constructive proofs:**

Show that there exists a pair of irrational numbers a and b such that $c = a^b$ is rational

Proof. Let us recall first that an irrational number is a number that is not rational. We know one such number: $\sqrt{2}$. Let us define $c = \sqrt{2}^{\sqrt{2}}$. There are then two cases:

a) c is rational. We are done.

b) c is irrational. Let us define then $d = c^{\sqrt{2}}$. Note that $d = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2$, i.e. d is rational, and we are done.

In both cases, we have shown that a and b exists: in the first case, $a = b = \sqrt{2}$, while in the second case, $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. We know that one of these two cases is true, therefore the assertion is true. *(We do not know, however, which of the two cases is true, but it does not matter for the proof! This is why this is a non constructive proof.)*

3.2 Uniqueness proofs

Some theorems assert the existence of a unique object within a domain $\mathbb{D}$ with a particular property P. Proofs of such theorems require two steps:

- **Existence**: find $x \in \mathbb{D}$ such that $P(x)$ is true
- **Uniqueness**: Two options:
  - For $y \in \mathbb{D}$, show that if $y \neq x$, then $P(y)$ is false
  - For $(x, y) \in \mathbb{D}^2$, show that if $P(x)$ and $P(y)$ are both true, then $x = y$

Example:

Let a be a real number not equal to zero, and let x and b be two real numbers. Show that there is a unique solution x to the equation $ax + b = 0$.

Proof.

a) **Existence**

A solution x to the equation satisfies,

$$\begin{aligned} ax + b &= 0 \\ ax &= -b \\ x &= -\frac{b}{a} \end{aligned}$$

as $a \neq 0$. Therefore $x = -\frac{b}{a}$ is one solution to the equation. This proves the existence.

b) **Uniqueness**

Let x and y be two real numbers that are solutions to the equation. Then $ax + b = 0$ and $ay + b = 0$. Therefore,

$$\begin{aligned} ax + b &= ay + b \\ ax &= ay \\ x &= y \end{aligned}$$

again as $a \neq 0$. This proves the uniqueness.

3.3 Proof by counter example

To show that an expression of the form $[\forall x \in \mathbb{D}, P(x)]$ is false, it is enough to find one value of $x \in \mathbb{D}$ such that $P(x)$ is false. This value is called a counter-example.

Example:

Prove or disprove that

$$\forall n \in \mathbb{N}, 2^n + 1 \text{ is prime}$$

Proof.
We try different values of $n \in \mathbb{N}$:

$n = 1 :\ 2^n + 1 = 3$ which is prime

$n = 2 :\ 2^n + 1 = 5$ which is prime

$n = 3 :\ 2^n + 1 = 9$ which is not prime

Therefore the proposition is not true.