Introduction to mathematics

Part II: Basics of mathematical logic

Contents

1 Introduction

In this document we will present the basic elements of mathematical logic: propositions, logical operators and quantifiers. Then we will discuss the main methods of proof. No prerequisite is necessary: this is an intuitive introduction, hopefully well-suited for readers without prior knowledge of math. One exception is the concept of integers that will be used in some examples.

The goal of this document is to introduce the main vocabulary, notations and elementary notions of mathematical logic. The following questions will be answered in this document: What are propositions? How do we construct propositions? How do we know if a proposition holds true?

2 Propositions

Math, as most sciences do, tries to establish assertions, that is, statements that hold true in the context in which they are exposed. Here what we mean by statement is any kind of well-formed sentence formulated in some given language, let it be English, or any other natural or formal language. In classical mathematical logic, we work with a special kind of statements: **propositions**. By definition, a proposition is a statement with which exactly one *truth value* can be associated: either true or false. In other words, a proposition describes something that either holds true or is false and there is no third possible option.

Examples of propositions formulated in English could be "It is raining outside" or "Peter will not be there at the party". However, since a lot of nuances and ambiguities arise from natural languages such as English, we will most of the time use a specialised language in math, a so-called formal language, to express what we mean. For instance, one could argue that the first example we gave is not a proposition since "outside" is not expressly defined and we could make the argument that it is not raining in some other place that also qualifies as being "outside" and thus arrive at the conclusion that it is both raining and not raining outside which would *contradict* the definition of a proposition. To avoid this problem we will constraint ourselves to only use words we have explicitly defined in an unambiguous manner, with

the aid of a formal language for instance. Examples of propositions in a more mathematical language could be "$1 = 1$" or even "$1 = 2$". The language in of itself will not be formally defined comprehensively.

As it is the custom in math, in order to study this new concept, we are going to introduce "variables" that refer to propositions, abstracting out in that process the underlying nature of the studied propositions: we will call a **propositional variable** any symbol (such as P, Q, R...) that could be substituted for any proposition.

3 Truth tables

We are going to introduce a handy tool: **truth tables**. They describe the truth values of a proposition Q depending on the truth values of some fixed collection of n other propositions $P_1, \ldots, P_n$. On the left hand side, we will list all possible combinations of truth values among the n propositions $P_1, \ldots, P_n$ (one combination per row). On the right hand side, for each row, we indicate the truth value of the proposition Q when the propositions $P_1, \ldots, P_n$ are assumed to take truth values that are written on that same row.

Consider the following example:

"It is raining outside"	"I have an umbrella"	"I am wet"
$False$	$False$	$False$
$False$	$True$	$False$
$True$	$False$	$True$
$True$	$True$	$False$

Here, there are $n = 2$ propositions where P_1 is "It is raining outside" and P_2 is "I have an umbrella". The Q proposition is "I am wet".

Each row is meant to be read as follows (where V_1, V_2 and V are truth values): *if* P_1 is V_1 and P_2 is V_2, *then* Q is V. For instance, for the third row we read, *if* "It is raining outside" is true and "I have an umbrella" is false *then* "I am wet" is true.

Obviously, this example is not really satisfactory because there are numerous ways we could say this truth table does not reflect the reality. For example I could be taking a shower thus being wet without necessarily having it raining outside. In other words, it would mean the truth values of the proposition Q are dependent on some other propositions that are not among P_1 and P_2. However we trust the reader for understanding that this example was given solely as to provide some intuition behind truth tables. In practice we would use our mathematical language and our unambiguous definitions to overcome those obstacles.

It is easy to generalise the idea of truth tables to describe the truth values of any number m of propositions $Q_1, \ldots, Q_m$ depending on the n propositions $P_1, \ldots, P_n$. Indeed we just have to add columns to the right hand side of the table for each extra proposition Q_i and indicate the truth value for each of them depending on the truth values taken by the propositions $P_1, \ldots, P_n$ on the corresponding row.

4 Logical operators

A logical operator (also known as logical connective) can be defined intuitively as a "process" to apply on one or more propositions that yields a new proposition whose truth value will be determine by the truth values of the original propositions. If it applies to only one proposition we call that operator a **unary** logical operator; if it applies to two propositions we call it **binary**. An example of such a binary operator in English is the word "and": given two propositions formulated in English, say "It is raining outside" and "Peter will not be there at the party", we can form a new statement "It is raining outside

and Peter will not be there at the party" that can be proven to be a proposition. However, we are not interested in presenting what are the logical operators in English so much as defining logical operators for our mathematical language.

Truth tables are a great way to describe the truth values of the newly created (by means of the logical operator) proposition in an unambiguous and straight-forward manner. This is because the truth value of the new proposition is completely determined by those of the preexisting propositions on which the logical operator acts.

Let P and Q be two propositional variables.

Definition 4.1 : Negation

The unary logical operator, called **negation**, written $\neg$, is defined as:

P	$\neg P$
F	T
T	F

The truth value of the new proposition $\neg P$ (read "not P") is the opposite truth value of the proposition P.

Definition 4.2 : Disjunction

The binary logical operator, called **disjunction** or **logical OR**, written $\vee$, is defined as:

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	T

The truth value of the new proposition $P \vee Q$ (read "P or Q") is false if and only if both P and Q are false.

Definition 4.3 : Conjunction

The binary logical operator, called **conjunction** or **logical AND**, written $\wedge$, is defined as:

P	Q	$P \wedge Q$
F	F	F
F	T	F
T	F	F
T	T	T

The truth value of the new proposition $P \wedge Q$ (read "P and Q") is true if and only if both P and Q are true.

Definition 4.4 : Implication

The binary logical operator, called **implication**, written $\Rightarrow$, is defined as:

P	Q	$P \Rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

The truth value of the new proposition $P \Rightarrow Q$ (read "P implies Q") is false if and only if P is true and Q is false.

It is worth noting that establishing the implication "$P \Rightarrow Q$" does not necessarily mean that there is a causal link between P and Q. Indeed consider the propositions "$1 = 2$" and "the sky is blue", the implication ["$1 = 2$" $\Rightarrow$ "the sky is blue"] is true (because $1 = 2$ is false) while there are no link between 1 being equal to 2 and the sky being blue. Similarly, the implication ["$1 = 1$" $\Rightarrow$ "the sky is blue"] is true (because both propositions are true) but there are no causality between 1 being equal to itself and the sky being blue.

Definition 4.5 : Equivalence

The binary logical operator, called **equivalence**, written $\Leftrightarrow$, is defined as:

P	Q	$P \Leftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

The truth value of the new proposition $P \Leftrightarrow Q$ (read "P equivalent to Q") is true if and only if P and Q have the same truth value.

In practice, if A and B are equivalent propositions then wherever A appears, we can substitute it by B: the logical equivalence assumes the role of the "equality" relation for logical propositions.

We have now the ability to combine preexisting propositions into new propositions. Now, how do we know whether a given proposition is true or false?

Before answering that question there is a significant difference we would like to emphasise: the difference between an 'atomic' and a 'compound' proposition. An atomic proposition is a proposition in which no logical operators appears (for example, "$1 = 2$") while a compound proposition is constructed from other propositions put in relation by means of logical operators (*e.g.* "$(1 = 1) \vee (1 = 2)$"). Here is the difference we want to point out: proving that an atomic proposition is true means showing that the *content* of the proposition holds true, while proving that a compound proposition is true means showing that the *relation* expressed by the logical operator holds true. For instance, let P and Q be propositional variables. Showing that Q is true means that the content of the proposition Q holds. However, showing that $P \Rightarrow Q$ is true consists in showing that *if* P is true *then* Q is true: the emphasis is on the relation between P and Q and not on the content of the propositions themselves. Thus, proving that the implication $P \Rightarrow Q$ does not require for us to know whether P is actually true but only that if it occurred that P would be true then it would follow that Q is also true. This means that we can establish the consequences of a proposition without knowing if that proposition is true. This is particularly useful when no proof for a proposition is known, as what we know as "open problems" in

math.

5 Tautologies and contradictions

A **tautology** is a proposition Q whose truth value is always true (T) and does not depend on any other proposition to be so. In other words, this means that the column for Q in the truth table is filled with T's no matter what are the $P_1, \ldots, P_n$ propositions we consider.

Example

An example of such a tautology is "$A \Leftrightarrow A$". Indeed if we write the truth table with respect to the proposition A:

A	A	$A \Leftrightarrow A$
F	F	T
T	T	T

For such propositions, no proof (other than writing down its truth table and noting that it is indeed a tautology) is necessary to assert that they hold true, since they always do.

Naturally, there are what we call **contradictions** (or **antilogies**). These are always false (F).

Example

For instance $A \wedge \neg A$, where A is a propositional variable, is a contradiction since its truth table is given by:

A	$\neg A$	$A \wedge \neg A$
F	T	F
T	F	F

Again, no further proof is required to show that such propositions are false.

For propositions where the truth table yields neither only T's nor only F's a proof is required to show whether they are true or false. We will talk about the different ways to construct such proofs later in this document.

For now, let us list notable propositions that can be proven to be tautologies. The reader is invited to write down the truth tables to convince themselves they are indeed tautologies. We will use parentheses to avoid ambiguities (the operations are to be performed with respect to how deep in parentheses they are: the deepest in parentheses is the first to be performed and so on). Let A and B be propositional variables.

1. $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$: showing logical equivalence is the same as showing a double implication, one in each direction.

2. $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$: this proposition on the right hand side is called the **contrapositive** of the one on the left hand side. Showing one holds true (respectively false) is equivalent to showing the other also holds true (respectively false).

3. $A \Leftrightarrow \neg(\neg A)$: the negation of the negation of a proposition has the same truth value as that original proposition.

4. $A \vee \neg A$: given any proposition A, A or its negation is true.

5. $\neg(A \wedge \neg A)$: given any proposition A, A and its negation can never both be true or both false. Using the previous item, we arrive at the conclusion that, for any proposition A, exactly one of the

following is true: either A is true or $\neg A$ is true. Showing that A is true is equivalent to showing that $\neg A$ is false and vice versa.

6. $\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$ and $\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$: those are called the De Morgan laws. They express the duality between the operators $\wedge$ and $\vee$ when considering their negations.

Exercise 5.1

Show that the following propositions, expressing properties for $\vee$ and $\wedge$, are tautologies:

$$A \Leftrightarrow (A \wedge A) \qquad A \Leftrightarrow (A \vee A)$$
$$(A \wedge B) \Leftrightarrow (B \wedge A) \qquad (A \vee B) \Leftrightarrow (B \vee A)$$
$$((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C)) \qquad ((A \vee B) \vee C) \Leftrightarrow (A \vee (B \vee C))$$
$$(A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C)) \qquad (A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C))$$

The third of those tautologies in each column means that the order in which the logical operators are being applied does not impact the resulting truth values of the propositions. Therefore, we can define without ambiguities the disjunction and conjunction, for any arbitrary number n of propositional variables $A_1, A_2, \cdots, A_n$:

$$\bigvee_{k=1}^{n} A_k \overset{\text{def}}{\Leftrightarrow} A_1 \vee A_2 \vee \cdots \vee A_n \qquad \bigwedge_{k=1}^{n} A_k \overset{\text{def}}{\Leftrightarrow} A_1 \wedge A_2 \wedge \cdots \wedge A_n$$

(Here the symbol $\overset{\text{def}}{\Leftrightarrow}$ means that the left hand side of the equivalence is being defined as a shorthand for the right hand side of the equivalence.)

Exercise 5.2

Show that the following properties on the logical implication are tautologies:

$$A \Rightarrow A \qquad ((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$$
$$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B) \qquad \neg(A \Rightarrow B) \Leftrightarrow (A \wedge \neg B)$$
$$(A \Rightarrow B) \Rightarrow ((A \wedge C) \Rightarrow B) \qquad (A \Rightarrow B) \Rightarrow (A \Rightarrow (B \vee C))$$
$$(A \Rightarrow (B \Rightarrow C)) \Leftrightarrow ((A \wedge B) \Rightarrow C) \qquad (A \Rightarrow (B \Rightarrow C)) \Leftrightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$$

Exercise 5.3

Show that the following properties on the logical equivalence are tautologies:

$$(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A) \qquad ((A \Leftrightarrow B) \wedge (B \Leftrightarrow C)) \Rightarrow (A \Leftrightarrow C)$$
$$(A \Leftrightarrow B) \Leftrightarrow (\neg A \Leftrightarrow \neg B) \qquad \neg(A \Leftrightarrow B) \Leftrightarrow ((A \wedge \neg B) \vee (\neg A \wedge B))$$

6 Sufficiency and necessity

Let us introduce some vocabulary. Suppose we have established that the proposition $P \Rightarrow Q$ is true, where P and Q are propositional variables. Then in English we would say that P is a **sufficient** condition for Q or, equivalently, that Q is a **necessary** condition for P. It is said be to sufficient because it *suffices* for P to be true to assert that Q is true. It is said to be necessary because for P to be true it *needs* for Q to be true or, in other words by contraposition, it suffices for Q to be false to assert that P is also false. If $P \Rightarrow Q$ is true, we also say that P is a **stronger** condition than Q or, equivalently, that Q is a **weaker** condition than P. We also call P the **hypothesis** and Q the **conclusion**.

Still assuming that the implication $P \Rightarrow Q$ is true, another way to express that in English words is saying: Q **if** P, or equivalently, P **only if** Q. Thus, as we have already establish that $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$ is a tautology, this means that $P \Leftrightarrow Q$ can be read as: P **if and only if** Q, often abbreviated as P **iff** Q. Another way of expressing that P and Q are **equivalent** is saying that P is **characterised** by Q (and vice versa) or that P is a **sufficient and necessary** condition for Q (and vice versa).

Finally, the proposition $Q \Rightarrow P$ is called the **converse** of the proposition $P \Rightarrow Q$. It is often that, when establishing that the proposition $P \Rightarrow Q$ is true, we ask ourselves if its converse $Q \Rightarrow P$ is also true. If that is indeed the case, we then conclude that P and Q are equivalent (which is a stronger statement).

7 Predicates and quantifiers

In general statements, **variables** can appear: they are placeholders in the form of a symbol where constant values from a certain collection of elements can be substituted in. For instance, in the statement "$x = 2$", the variable represented by the symbol x can be substituted by any actual number. We can distinguish between two types of variables: **bound variables** and **free variables**.

Bound variables are the result of an application of a **variable-binding operator**. In a sense, bound variables are "declared" by that operator and their entire meaning is bounded to that operator. Such operators include the quantifiers that we will introduce later in this document. One important property of this kind of variables is that if we were to swap *all* instances of the symbol representing a bound variable by another symbol (that does not already appear in the expression) then the meaning would remain unchanged. This is what differs from free variables: these are "declared" outside of the expression and thus the symbol by which it is represented cannot be replaced by another symbol without changing the meaning of the expression.

One important limitation to propositions is that no free variables within them is allowed. In other words, propositions describe constant statements that do not depend on any external entity. For instance "x is an even number" does not qualify as a proposition since x is not assigned a fixed value but is rather to be understood as a variable over the set of integers (as an example). Such statements, that comprise free variables and express a meaning that can be assigned either true or false if we were to substitute variables by some appropriate constant values, are called **predicates**. They can be viewed as "incomplete propositions" with placeholders for some variables.

The notation we are going to introduce in this paragraph is not conventional. Nevertheless it is useful because it removes some ambiguity with the notation from the next paragraph. If P is a predicate and $x_1, \ldots, x_n$ are variables then we write $P[x_1, \ldots, x_n]$ to denote that the free variables of the predicate P are among $x_1, \ldots, x_n$ (note that we say *among*, which means some, or even all, of the variables $x_1, \ldots, x_n$ may not be actual free variables in P. But a free variable in P will always be one of $x_1, \ldots, x_n$). For instance, consider the predicate P given by "$x^2 = 2$", we could write $P[x]$ because P has only one free variable, that is x. We could also write $P[x, y]$ because the free variables of P (so in our case here x) are among x and y. However, we could not write $P[y]$ because the free variable x of P is not y, nor could we write $P[y, z]$, etc. In the documents from this series, we will generally only use predicates depending on only at most a single free variable. This is to avoid cumbersome notation that makes the reading harder. Most of the results can be easily generalised to any number of free variables.

For a predicate to be assigned a truth value, it needs to be "transformed" into a proposition: the free variables need to be substituted for some constant values. For instance "x is an even number" where x is indeterminate cannot be assigned a truth value while "2 is an even number" where we substituted x for the constant 2 is indeed a proposition. The collection of all the constants values that we are allowed to use for substitution is called the **domain of discourse** (or **universe**). It contains all the possible

values for our variables. Now suppose we have a predicate $P[x]$ with x as a free variable. To denote that we substitute the free variable x by a constant value, say a, we would write $P(a)$, which would thus be a proposition, as the free variable would have been replaced by a constant value.

Another way to "assign" a truth value to a predicate is by transforming the free variables into bound variables by means of a variable-binding operator such as quantifiers. There exist two quantifiers:

- the **universal quantifier**, written $\forall$, read "for all",
- the **existential quantifier**, written $\exists$, read "there exists".

If $P[x]$ denotes a predicate, then we can construct a proposition with each quantifier that transform the free variable into a bound variable:

- "$\forall x, P(x)$" is a proposition whose truth value is true, if and only if, the proposition $P(a)$ is true for any a being a constant value from our domain of discourse.
- "$\exists x, P(x)$" is a proposition whose truth value is true, if and only if, there exists a constant value a from our domain of discourse for which $P(a)$ is a true proposition.

The notation $P(x)$ here is to be understood as substituting the free variable x by all the constant values taken from the collection of values implied by the variable-binding operator. For quantifiers, this collection is the domain of discourse. For other variable-binding operators the collection is explicitly specified.

We can then construct more complex propositions by placing those quantifiers in succession, any number of times we wish. For instance we can build the proposition $\forall x, \exists y, x = 2y$.

It is of great importance to note that the order in which quantifiers appear affects significantly the meaning of the propositions. For example, consider the domain of discourse being the a subset of the rational numbers: numbers that can be expressed as a fraction of two integers.

- The proposition $\forall x, \exists y, x = 2y$ means that for any x in the domain of discourse we can find an element y from the domain of discourse such that $x = 2y$. If we suppose the domain of discourse contains a nonzero rational number x_0, it implies that the domain of discourse contains an infinite amount of numbers since x_0 being in the domain of discourse entails that so is $x_0/2$, and then $x_0/4$, and so on and so fourth.
- Now consider the proposition $\exists y, \forall x, x = 2y$. This means that there would exist a rational number y in our domain of discourse such that every rational number in the domain of discourse is equal to $2y$. That would imply that the domain of discourse either consists of only 0 or is empty. Indeed, suppose the nonzero rational number x_0 is in the domain discourse. Then $x_0 = 2y$, so y is nonzero. But y is in the domain of discourse, so $y = 2y$ which is impossible since $y \neq 0$.

We thus arrive at two radically different meanings just by switching the order of the quantifiers. The rule of thumb to follow is that when an existential quantifier $\exists y$ appears after a universal one $\forall x$, the element y can depend on each particular value x can take. While when an existential quantifier $\exists y$ precedes a universal one $\forall x$ the value of y cannot be dependent on the values of x.

Note that those concerns about quantifiers ordering arise only when we deal with a mix of existential and universal quantifiers: if we have only universal quantifiers (or only existential quantifiers) the order in which they appear does not matter.

Now, consider a predicate $P[x]$. Let us think about what it would mean to take the negation of the proposition "$\forall x, P(x)$". This proposition states that for any value a from the domain of discourse the proposition $P(a)$ is true. Saying that its negation is true is equivalent to saying that the proposition is false. Therefore, asserting that the negation of this proposition is true means that there exists some value a for which the proposition $P(a)$ is false. In other words, we have the equivalence:

$$\neg(\forall x, P(x)) \;\Leftrightarrow\; (\exists x, \neg P(x))$$

Conversely, by a similar reasoning, we can show that:

$$\neg(\exists x, P(x)) \;\Leftrightarrow\; (\forall x, \neg P(x))$$

What one must remember from those equivalences is that the quantifiers $\forall$ and $\exists$ are to be understood to be more or less the negation of one another. Furthermore, to show that the proposition $\forall x, P(x)$ is false it suffices to find a value a such that the proposition $P(a)$ is false: such a value a is called a **counterexample**.

Example

The negation of the proposition "$\forall x, \exists y, x = 2y$" is "$\exists x, \forall y, x \neq 2y$".

By default, in the expression $\exists x, P(x)$, the existential quantifier $\exists$ asserts the existence of *at least* one element satisfying the predicate $P[x]$. However, it is often the case that we want to know whether that element is *unique*, that is, it is the only one satisfying the predicate $P[x]$. To denote that it is indeed unique we use the special notation $\exists! x, P(x)$ and we say that y is **characterised** by P.

8 Methods of proof

A **formal proof** consists of a succession of propositions such that each proposition is one of the following:

- an *axiom* (that is, the propositions we take for granted as true in our theory),
- an *assumption* (that is, the hypotheses of the theorem to prove),
- a proposition that follows from the preceding propositions by means of a rule of inference.

The last proposition of a formal proof is called **theorem**.

In practice, a proof is written in English (or another natural language) and justify how the deduced propositions are consequences of the previous ones. The goal of a proof is to *convince* the reader that the deductions are indeed correct. Also, the word theorem is reserved for the most important true propositions. Other names for propositions proven to be true are:

- **lemma** for a proposition that will be used to prove a proposition but is not that important when considered outside of that context,
- **corollary** for a proposition that is a direct consequence or special case of a proposition,
- or even simply **proposition** for any other purposes

For our purposes we introduce only one rule of inference called "modus ponens". It states that, for P and Q any two propositions, if the implication $P \Rightarrow Q$ is true and if the proposition P is true, then we can infer that the proposition Q is true. Thus the role of the implication is central in order to establish new theorems. This is why we will focus on the ways we can prove that an implication is true. Let P and Q be propositions. Different methods of proof exist to prove that the implication $P \Rightarrow Q$ is true:

- **Direct proof**: we start by assuming that P is true, then, by using the content of the proposition P, we show that it necessarily follows that Q is true. The justification behind this method is that: firstly, the implication $P \Rightarrow Q$ is always true if P is false thus we do not need to worry about that case. Then, if P is true, that implication is true if and only if Q is true too. Thus if we show that the content of P, when assumed true, implies that the content of Q is true, then we would have shown that the case P true and Q false is impossible thus the implication $P \Rightarrow Q$ is necessarily true.

Example

Let us prove by a direct proof method that for all integers n, if n is divisible by 6, then it is an even number. If we set our domain of discourse to the integers we would then translate mathematically that sentence into the following implication:

$$\forall n, \quad (\exists m, n = 6m) \;\Rightarrow\; (\exists k, n = 2k)$$

Proof: Let n be an integer. Suppose that it is divisible by 6. Then there exists an integer m such that $n = 6m$. But since $6 = 2 \times 3$, then $n = 2 \times (3m)$. But since both m and 3 are integers, so is $3m$. If we let the integer k be $k = 3m$ we thus show that there indeed exists an integer such that $n = 2k$. In conclusion, n is an even number.

- **Proof by contrapositive**: We recall that the contrapositive of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$ and that they are logically equivalent. Thus showing that one is true (respectively false) is equivalent to showing the other one is true (respectively false). So to prove by contrapositive we start by assuming that $\neg Q$ is true (or, equivalently, that Q is false), then, by using the content of the proposition Q, we show that the proposition P is necessarily false (so $\neg P$ is true) thus showing (by a direct proof) that the implication $\neg Q \Rightarrow \neg P$ is true. Then, by modus ponens, it follows that $P \Rightarrow Q$ is also true.

  Example

  Let us show by contrapositive that if n is an integer and if $n \times n$ is even, then so is n. We translate it mathematically into the following, where the domain of discourse is the integers

  $$\forall n, \quad (n \times n \text{ is even}) \Rightarrow (n \text{ is even})$$

  Proof: Let n be an integer. Suppose that n is not even. It is then odd. But the product of two odd numbers is odd. Thus $n \times n$ cannot be even. We have thus shown that if n is not even, then $n \times n$ is not even either. By contrapositive, we have thus shown the given implication.

- **Proof by contradiction** (also known as, **reductio ad absurdum**): This method is more general in the sense that we can use it to show that any kind of proposition is true, not necessarily expressed in an implication form. Let us then set the goal as showing that the proposition P is true. For that, we start by assuming that $\neg P$ is true (or, equivalently, that P is false). Then, we try to show that the content of $\neg P$ when assumed true entails a certain contradiction (let us denote it R). We would have then proven that the implication $\neg P \Rightarrow R$ is true. By contrapositive and since $P \Leftrightarrow \neg(\neg P)$, we would then get that the implication $\neg R \Rightarrow P$ is true. But R is always false, by definition of a contradiction. So its negation $\neg R$ is a tautology: it is always true. Then, on one hand we have shown the implication $\neg R \Rightarrow P$ is true and on the other hand we know that $\neg R$ is true, it then follows from modus ponens that P is true. In practice the contradiction R we end up with is often in the form $Q \wedge \neg Q$ where Q is some proposition we prove to be both true and false.

  To use the method of proof by contradiction to prove that the implication $P \Rightarrow Q$ is true where P and Q are propositions, we start by assuming that P is true and that Q is false and show that it entails a contradiction. Then, in a similar way as above, we conclude that Q is true and thus that $P \Rightarrow Q$ is true.

Example

Let us prove that the product of two odd integers is odd. Let the domain of discourse be the integers. We want to prove that:

$$\forall n, \forall m, \quad ((n \text{ odd}) \wedge (m \text{ odd})) \Rightarrow (n \times m \text{ is odd})$$

Proof: Let n and m be integers. Suppose that n and m are odd. Thus there exists two integers a and b such that $n = 2a + 1$ and $m = 2b + 1$. Now suppose that $n \times m$ is not odd. It means that there exists an integer c such that $n \times m = 2c$. However, we compute $n \times m = (2a + 1) \times (2b + 1) = 4ab + 2(a + b) + 1 = 2(2ab + a + b) + 1$. But a and b being integers implies that $2ab + a + b$ is also an integer, let us denote it d. Thus we have shown that both $n \times m = 2c$ and $n \times m = 2d + 1$, which is a contradiction. Thus $n \times m$ is necessarily odd.

The examples given here are really simple so it is easy to find proofs for each one of them using different methods of proof. However, for more complex problems we sometimes know a proof using a specific method of proof, say proof by contradiction, while no direct proof or proof by contrapositive are known. Such examples require more knowledge in math so will be omitted in this document but it shows that the different methods of proof offer advantages and disadvantages depending on the situation.

In the examples of proofs given above, we started by using the linguistic expression "Let ... be ...". Every time we want to prove a proposition that comprises a universal quantifier we need to use that kind of expression. Translating $\forall x$ into "Let x be ..." transform the variable x into a constant value also denoted x. Yes that value is arbitrary but it is fixed for the rest of the proof and is not to be considered a variable anymore.

Similarly, considering a proposition in which intervenes an existential quantifier, say $\exists x, P(x)$ for instance, the proof will have to start by "Let us set $x = \ldots$. Now show that $P(x)$ is true.".

9 Recap

In this document, we have discussed the notions of propositions and truth values. We have introduced a tool called truth tables that help us explicitly state the truth values for any given proposition with respect to some other propositions.

We then used truth tables to define some logical operators: those syntactic elements that applies to other propositions to construct a new proposition whose truth value depends solely on the original propositions. We talked about the logical negation, disjunction, conjunction, implication and equivalence.

We have mentioned what are tautologies and contradictions: those kind of propositions that are either always true or always false. We then listed some note-worthy tautologies.

We have introduced some important vocabulary. If $P \Rightarrow Q$ is true, then we say that, from the perspective of the hypothesis P:

- P is a sufficient condition for Q,
- P is stronger than Q,
- P only if Q,

and from the perspective of the conclusion Q:

- Q is a necessary condition for P,
- Q is weaker than P,

- Q if P.

If $P \Leftrightarrow Q$ is true, we say that P and Q are equivalent, that one is characterised by the other, that one is a sufficient and necessary condition for the other, or that P if and only if Q.

Then, we have defined the concepts of free and bound variables, and, the notions of domain of discourse and predicates as "propositions with placeholders". Furthermore, we have discussed the two types of quantifiers: universal and existential.

Finally, we have described three important methods of proof: the direct proof, the proof by contrapositive and the proof by contradiction.

The reader is now hopefully equipped to understand elementary mathematical proofs and continue building their mathematical knowledge from here.