1 Mathematical logic and proof

Chapter contents

1.1 Propositional logic

A real variable x takes values in the set of real numbers $\mathbf{R}$.

A logical variable x takes values in the set $\{\mathsf{True}, \mathsf{False}\}$.

Definition 1.1. A *statement* is a sentence or expression that is either True or False.

A statement takes on the role of a logical variable. We generally use lower case letters p, q, r, ... to represent statements.

Example 1.2 (Which of these are statements?)**.**

- $1 + 1 = 3$
- f is continuous
- 6 is the largest integer
- potato
- if it is Saturday, there is no MAST20026 lecture
- $x > 2$
- for every $x \in \mathbf{Z}$, $x^2 \geqslant 0$
- every even number greater than 2 is the sum of two primes
- $\begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix}$ is invertible and $1 + 1 = 3$

Connectives Compound statements can be constructed by putting together simpler statements with the use of connectives and parentheses.

(This is similar to the formation of more complicated English sentences by putting together simpler sentences with the use of grammatical conjunctions and punctuation signs.)

The connectives we consider are:

- negation
- conjunction
- disjunction
- biconditional
- implication

Definition 1.3. Let p be a statement. The *negation* of p is the statement "not p" and is denoted $\neg p$:

p	$\neg p$
T	
F	

Example 1.4.

- Let p be the statement "$5 > 0$".
- Let r be the statement "this lecture is boring".

Definition 1.5. Let p, q be statements. The *conjunction* of p and q is the statement "p and q" and is denoted $p \wedge q$:

p	q	$p \wedge q$
T	T	
T	F	
F	T	
F	F	

Example 1.6. Let p be the statement "$\begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix}$ is invertible", and q the statement "$1 + 1 = 3$".

Definition 1.7. Let p, q be statements. The *disjunction* of p and q is the statement "p or q" and is denoted $p \vee q$:

p	q	$p \vee q$
T	T	
T	F	
F	T	
F	F	

Example 1.8. Let p be the statement "$\begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix}$ is invertible", and q the statement "$1 + 1 = 3$".

Mathematical usage of "or" is inclusive:

Typical English usage of "or" is exclusive:

Example 1.9. For which values of p and q are the following compound statements True?

(a) $(\neg p \wedge q) \wedge (p \vee q)$

p	q	$\neg p$	$\neg p \wedge q$	$p \vee q$	$(\neg p \wedge q) \wedge (p \vee q)$
T	T				
T	F				
F	T				
F	F				

(b) $(p \wedge \neg p) \wedge (q \vee \neg q)$

p	q	$\neg p$	$p \wedge \neg p$	$\neg q$	$(q \vee \neg q)$	$(p \wedge \neg p) \wedge (q \vee \neg q)$
T	T					
T	F					
F	T					
F	F					

Definition 1.10. Let p, q be statements. The *biconditional* "p if and only if q", denoted $p \Leftrightarrow q$, is given by:

p	q	$p \Leftrightarrow q$
T	T	
T	F	
F	T	
F	F	

Example 1.11. A square real matrix A is invertible if and only if $\det A \neq 0$.

Definition 1.12. Let p, q be statements. The *implication* "if p then q", denoted $p \Rightarrow q$, is given by:

p	q	$p \Rightarrow q$
T	T	
T	F	
F	T	
F	F	

Example 1.13. Let p be the statement "The temperature outside is colder than 0°C", and q the statement "Brian wears a beanie when he is outside".

Definition 1.14. Let p, q be statements. The *converse* of the implication $p \Rightarrow q$ is the implication $q \Rightarrow p$.

p	q	$p \Rightarrow q$	$q \Rightarrow p$
T	T	T	
T	F	F	
F	T	T	
F	F	T	

Definition 1.15. Let p, q be statements. The *contrapositive* of the implication $p \Rightarrow q$ is the implication $(\neg q) \Rightarrow (\neg p)$.

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$\neg q \Rightarrow \neg p$
T	T	T			
T	F	F			
F	T	T			
F	F	T			

Example 1.16. If it is Saturday, then there is no MAST20026 lecture.

Definition 1.17. Let A be a compound statement. We say that A is a ...

(a) ... *tautology* when A is always True ...

(b) ... *contradiction* when A is always False ...

... regardless of the truth values of the simpler statements used to build A.

Definition 1.18. Let r and s be statements. We say r and s are *logically equivalent*, denoted $r \equiv s$, when $r \Leftrightarrow s$ is a tautology.

For example, we have seen after Definition 1.15 that $p \Rightarrow q$ is logically equivalent to

Example 1.19. Check that $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	$[\neg(p \vee q)] \Leftrightarrow [(\neg p) \wedge (\neg q)]$
T	T	T		F	F		
T	F	T		F	T		
F	T	T		T	F		
F	F	F		T	T		

1.2 First-order logic

Definition 1.20. A *condition* is a mathematical sentence whose truth value depends on mathematical objects.

Here are some examples of conditions:

- $p(f)$:
- $q(x)$:
- $r(A)$:

Let q be a condition depending on a variable x in a domain D. Here are four scenarios:

notation	meaning
$(\forall x \in D)q(x)$	
$(\exists x \in D)q(x)$	
$(\forall x \in D)\neg q(x)$	
$(\exists x \in D)\neg q(x)$	

Definition 1.21.

- The symbol $\forall$ ("for all") is called the *universal quantifier*.
- The symbol $\exists$ ("there exists") is called the *existential quantifier*.

The negation of statements involving quantifiers follows the rules:

- $\neg[(\exists x \in D)p(x)] \equiv$

- $\neg[(\forall x \in D)p(x)] \equiv$

Example 1.22. Let $\mathcal{P}_1$ denote the set of all polynomial functions of degree one:

$$\mathcal{P}_1 = \{f : \ f(x) = ax + b, a \neq 0\}.$$

- For $f \in \mathcal{P}_1$, let $p(f)$ be the condition "the graph of f crosses the x-axis".

- On the other hand, for $f \in \mathcal{P}_1$, the condition $q(f)$: "$f'(x) > 0$"

Some concepts from elementary number theory

Definition 1.23. Let n be an integer.

- We say that n is *odd* if $(\exists k \in \mathbf{Z})n = 2k + 1$.
- We say that n is *even* if $(\exists k \in \mathbf{Z})n = 2k$.

Definition 1.24. Let n and d be integers. We say that d *divides* n, denoted $d \mid n$, if $(\exists k \in \mathbf{Z})n = dk$.
In this case, we say that d is a *divisor* of n, and n is a *multiple* of d.

Definition 1.25. Let p be a positive integer. We say that p is *prime* if it has exactly two positive divisors.

Definition 1.26. Let n be an integer, d a positive integer, and r an integer with $0 \leqslant r < d$. We say that r is the *remainder* of the division of n by d if $(\exists k \in \mathbf{Z})n = dk + r$.

Definition 1.27. Let x be a real number.

- We say that x is *rational* if $(\exists p \in \mathbf{Z})(\exists q \in \mathbf{Z}_{>0})x = \frac{p}{q}$.
- We say that x is *irrational* if

Translating statements into formal logic

Example 1.28. There exists a natural number n such that $2n$ is odd.

Example 1.29. Let U be a vector space over the real numbers. Every subspace of dimension 3 of U has a basis.

Example 1.30. Let U be a vector space over the real numbers. There exists a subspace of dimension 3 of U with no basis.

Example 1.31. For every $x \neq 0$ and every $y \neq 0$, the product of x and y is not zero.

Example 1.32. Let $p(f, g)$ be the condition "g is the first derivative of f".

- $p(x^2, 2x)$ is
- $p(x^3 + 1, 2x)$ is
- Let $f(x) = x^2 + 1$, let $\mathcal{P}$ be the set of polynomial functions $\mathbf{R} \longrightarrow \mathbf{R}$.

- "The derivative of any polynomial function is a polynomial function":

The order in which quantifiers appear in a condition makes an enormous difference.

Example 1.33. Consider the condition $q(x, y)$: "$x + 1 > y$".

- $(\forall x \in \mathbf{R})[(\exists y \in \mathbf{R})q(x, y)]$

- $(\exists y \in \mathbf{R})[(\forall x \in \mathbf{R})q(x, y)]$

1.3 Mathematical proofs

Most mathematical statements we encounter are of the form: "if p then q".

Example 1.34.

- Let $f : \mathbf{R} \longrightarrow \mathbf{R}$. If f is differentiable, then f is continuous.
- Let $f : \mathbf{R} \longrightarrow \mathbf{R}$. If f is a quadratic function, then the graph of f crosses the x-axis at most twice.
- Let V be a vector space. If V is finite-dimensional, then V has a basis.

All of these are conditions depending on a variable:

$$(\forall f \in \mathcal{F}) p(f) \Rightarrow q(f).$$

Definition 1.35. A *formal mathematical proof* of the statement $p \Rightarrow q$ is a finite sequence of statements

$$p_1, p_2, \ldots, p_n$$

such that $p_1 = p$, $p_n = q$, and each p_i is either

- known or assumed true, or
- can be inferred from a known or assumed true statement p_j with $j < i$.

The purpose of a formal mathematical proof is to verify the truth of a mathematical statement.

A *mathematical proof* is a human-readable version of a formal mathematical proof that does not sacrifice the rigour. While the main purpose of a mathematical proof is still to verify the truth value of a statement, it also has the important secondary role of communicating the argument to others in a manner that is as clear and understandable as possible.

Theorem 1.36. *Let x be an integer. If x is even, then x^2 is even.*

Discovery (scrap work)

Hypothesis $p(x)$:

Conclusion $q(x)$:

Argument:

A formal proof

Proof.

Fix $x \in \mathbf{Z}$.

$p_1(x)$:

$p_2(x)$:

$p_3(x)$:

$p_4(x)$:

$p_5(x)$:

$p_6(x)$:

We conclude that □

An (informal) proof

Note that "informal" does not mean unrigorous! This should still be a sequence of statements that follow logically from previous ones, starting with the hypothesis and ending with the conclusion.

Theorem 1.37. *Let x and y be integers. If x and y are even, then $(x+y)^2$ is even.*

Scrap work:

Formal proof.

Fix $x, y \in \mathbf{Z}$.

$p_1(x, y)$:

$p_2(x, y)$:

$p_3(x, y)$:

$p_4(x, y)$:

$p_5(x, y)$:

$p_6(x, y)$:

$p_7(x, y)$:

We conclude that □

Fixing the gap

We realise that there is a gap in our proof in the justification of $p_6(x, y)$. We need:

Lemma 1.38. *If a, b, c are even integers, then $a + b + c$ is even.*

Another possibility is to simplify the approach altogether by proving

Lemma 1.39. *If a and b are even integers, then $a + b$ is even.*

Theorem 1.40. *Let x be an integer. If $x^2 - 6x + 5$ is even, then x is odd.*

(Attempted) formal proof. Let $x \in \mathbf{Z}$.

$p_1(x)$:

$p_2(x)$:

$p_3(x)$:

$\vdots$

$p_{n-1}(x)$:

$p_n(x)$: □

Proof by contraposition

A cleaner approach to Theorem 1.40 is to prove its contrapositive.

Recall that $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

The contrapositive of Theorem 1.40 is:

Formal proof of Theorem 1.40. We proceed by contraposition, that is, we prove that if x is an even integer, then $x^2 - 6x + 5$ is odd.

Fix $x \in \mathbf{Z}$.

$p_1(x)$:

$p_2(x)$:

$p_3(x)$:

$p_4(x)$:

$p_5(x)$:

This proves the contrapositive, hence also the statement of Theorem 1.40. □

Proof by contradiction

Proving that a statement s is True is equivalent to proving that its negation $\neg s$ is False.

In the case of a statement of the form $p \Rightarrow q$, this means

An essential point is that $\neg(p \Rightarrow q) \equiv (p \wedge \neg q)$:

p	q	$p \Rightarrow q$	$\neg(p \Rightarrow q)$	$\neg q$	$p \wedge \neg q$
T	T	T		F	
T	F	F		T	
F	T	T		F	
F	F	T		T	

Schematically, we then prove that $p \Rightarrow q$ as follows:

Proof.

We proceed by contradiction.

Suppose $p \wedge \neg q$ is True.

(. . . work to obtain a contradiction, that is something that we know is False . . .)

Therefore $p \wedge \neg q$ is False, hence its negation $p \Rightarrow q$ is True. □

Theorem 1.41. *Let a and b be real numbers. If a is rational and b is irrational, then $a+b$ is irrational.*

Let $p(a,b)$ be the statement

Let $q(a,b)$ be the statement

The theorem is then

The negation of the theorem is

Proof of Theorem 1.41.

We proceed by contradiction.

Suppose

Multiple cases

Theorem 1.42. *If an integer a divided by 8 gives a remainder of 1 or 7, then a^2 divided by 8 gives a remainder of 1.*

This is equivalent to conjunction of the two statements

(a) If an integer a divided by 8 gives a remainder of 1, then a^2 divided by 8 gives a remainder of 1.

(b) If an integer a divided by 8 gives a remainder of 7, then a^2 divided by 8 gives a remainder of 1.

It can therefore be proved as such (one statement at a time):

Proof.

(a) Suppose a divided by 8 gives a remainder of 1.

(b) Suppose a divided by 8 gives a remainder of 7.

□

Proof by example

A statement of the form $(\exists x \in D)p(x)$ is True precisely when $p(x)$ is True for at least one element of D.

Hence we can prove the statement by giving an example, that is finding one $a \in D$ for which $p(a)$ is True.

Theorem 1.43. *There exists a linear function* $\mathbf{R} \longrightarrow \mathbf{R}$ *whose graph passes through the origin.*

Let $D =$

Let $q(f)$:

Then the Theorem is:

Caveat: Proofs by example are only valid for statements of the form $(\exists x \in D)p(x)$.

Disproof by counterexample

A statement of the form $(\forall x \in D)p(x)$ is True precisely when $p(x)$ is True for every element of D.

Hence we can disprove the statement by giving a counterexample, that is finding one $a \in D$ for which $p(a)$ is False.

Example 1.44. "Every prime number is odd."

Proof by mathematical induction

For $n \in \mathbf{N}$, consider the sum

$$s(n) = \sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \cdots + 2^n.$$

For small values of n we have

$$\begin{aligned} s(0) &= & &= \\ s(1) &= & &= \\ s(2) &= & &= \\ s(3) &= & &= \end{aligned}$$

We conjecture that

This condition has two special properties: (a) the domain of the free variable n is the set of natural numbers $\mathbf{N}$; (b) there is a simple relation $s(n+1) = s(n) + 2^{n+1}$.

Theorem 1.45 (Principle of Mathematical Induction)**.** *Let $p(n)$ be a condition over $n \in \mathbf{N}$. If the following two statements are* True*, then $p(n)$ is* True *for every $n \in \mathbf{N}$.*

(a) (Base case) $p(0)$ is True*.*

(b) (Induction step) For each $k \in \mathbf{N}$, if $p(k)$ is True*, then $p(k+1)$ is* True*.*

In formal language:

We stated the Principle as a theorem (that we won't prove), but some take it as an axiom of the natural numbers $\mathbf{N}$. You should think of it as a fundamental property of $\mathbf{N}$.

We can now prove our conjecture:

Theorem 1.46. *For every $n \in \mathbf{N}$ we have*

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$$

You should now try your hand at the more general result:

Theorem 1.47 (Geometric Sum)**.** *Let* $r \in \mathbf{R}$*. For every* $n \in \mathbf{N}$ *we have*

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

Induction can start at other base cases than $n = 0$. In other words, the following slightly more general principle also holds:

Theorem 1.48 (Principle of Mathematical Induction)**.** *Let $p(n)$ be a condition over $n \in \mathbf{Z}$. Let $n_0 \in \mathbf{Z}$ be fixed. If the following two statements are* True*, then $p(n)$ is* True *for every $n \geqslant n_0$.*

(a) (Base case) $p(n_0)$ is True*.*

(b) (Induction step) For each $k \geqslant n_0$, if $p(k)$ is True*, then $p(k+1)$ is* True*.*

(In typical applications of this, the starting point n_0 is a non-negative integer.)

There is another formulation of the principle of induction:

Theorem 1.49 (Principle of Strong Mathematical Induction)**.** *Let $p(n)$ be a condition over $n \in \mathbf{Z}$. Let $n_0 \in \mathbf{Z}$ be fixed. If the following two statements are* True*, then $p(n)$ is* True *for every $n \geqslant n_0$.*

(a) (Base case) $p(n_0)$ is True*.*

(b) (Induction step) For each $k \geqslant n_0$, if $p(n_0), p(n_0+1), \ldots, p(k)$ are all True*, then $p(k+1)$ is* True*.*

"Strong" is an unfortunate misnomer: although it appears to require a stronger condition in the induction step (b) than Theorem 1.45, the two principles are logically equivalent.

Theorem 1.50. *Every integer $n \geqslant 2$ can be expressed as a product of prime numbers.*

More precisely: given any integer $n \geqslant 2$, there exists $r \in \mathbf{Z}_{\geqslant 1}$ and r prime numbers $p_1, \ldots, p_r$ (not necessarily distinct) such that

$$n = p_1 \ldots p_r.$$

In fact, more is true:

Theorem 1.51 (Fundamental Theorem of Arithmetic)**.** *Every integer $n \geqslant 2$ can be expressed uniquely (up to permutation of the factors) as a product of prime numbers.*

Balancing formality and readability

It is possible to overdo the use of formal language.

Here is some advice regarding your own proof writing in this subject:

- We generally prefer words to symbols, and we try to strike the right balance between conciseness and clarity (without sacrificing rigour).
- It is okay to use "and" instead of $\wedge$, "or" instead of $\vee$, "not" instead of $\neg$, "if... then..." instead of $\Rightarrow$, "if and only if" or "iff" instead of $\Leftrightarrow$. You should be familiar with the symbols however, as they may be used by others.
- The "three dots" symbols $\therefore$ and $\because$ are banned in this subject. Use appropriate words such as: so, hence, therefore, because, since.
- We generally prefer to give proofs in the informal style, rather than the formal enumeration of steps. However, as you refine your proof writing and reading skills, you may occasionally benefit from using the formal style to clarify an argument that you are trying to understand or to make. This is especially useful for figuring out the correct order in which to write the steps in the proof.