Methods of Proof

Argument → statement
statement
Conclusion

} Assumptions

Arguments

Consider the sequence of statements.

> If x is a pig, then x is pink.
> Peppa is a pig.
> Therefore, Peppa is pink.

- **Argument:** a sequence of statements, all but the final of which are called assumptions/premises/ hypotheses, and final of which is called the conclusion.
- The word "therefore" is normally placed just before the conclusion.
- The logical form of the above argument is:

  If p, then q.
  p.
  Therefore, q.

- An argument is **valid** the conclusion is true whenever all the assumptions are true (no matter what particular statements are substituted for the variables).
- **Proof:** a valid argument used to establish a result.
- **Note:** The assumptions in an argument or a proof can be axioms, previously proved theorems, or may follow from previous statements by a mathematical or logical rule.

Exercise:

Prove that if $x \in \mathbb{R}$ and $n \in \mathbb{N}$ is even, then $x^n \geq 0$.

$n \in \mathbb{N}$ EVEN (given)

$n = 2m$ for some $m \in \mathbb{N}$ (def. of even numbers).

$x^n = x^{2m}$ (substitution)

$x^n = (x^m)^2$ (rule of exponents)

≥ 0 ($y^2 \geq 0 \ \forall y \in \mathbb{R}$) $\square$

- A proof should be complete (contain all necessary statements).
- A proof should be concise (not contain extra or unneeded statements).

Testing Validity

- To test an argument for validity, follow these steps:
  - Identify the assumptions and conclusion.
  - Construct a truth table of all the assumptions and the conclusion.
  - If the conclusion is true in every case where all the assumptions are true, the argument is valid.
  - If there is a row of all true assumptions and false conclusion, the argument is invalid.

Exercise:

Is the argument valid?

P => Q ∨ ~R,

Q => P ∧ R,

.:. P => R.

p	***q***	***r***	***p => q ∨ ~r***	***q => p ∧ r***	***p => r***
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	F	T	T
T	F	F	T	T	F
F	T	T	T	F	T
F	T	F	T	F	T
F	F	T	T	T	T
F	F	F	T	T	T

NOT VALID

All assumptions, true, conclusion MUST be true.

Exercise:

Test the validity:

a) $p \vee (q \vee r)$,
   $\sim r$,
   $\therefore p \vee q$

p	*q*	*r*	*~r*	*p ∨ (q ∨ r)*	*p ∨ q*	
T	T	T	F	T	T	
T	T	F	T	T	T	✓
T	F	T	F	T	T	
T	F	F	T	T	T	✓
F	T	T	F	T	T	
F	T	F	T	T	T	✓
F	F	T	F	T	F	
F	F	F	T	F	F	

This statement satisfies the validity test.

b) $p \Rightarrow q$,   (Modus Ponens)
   p,
   $\therefore q$.

p	*q*	*p => q*
T	T	T
T	F	F
F	T	T
F	F	T

This syllogism is valid.

- An argument consisting of 2 premises and a conclusion is called a **syllogism**.
- The most famous syllogism is the **modus ponens**, Latin for "method of affirming."

  If p, then q,
  p,
  Therefore, q.

Exercise:

a) Is the statement "n $\in \mathbb{N}$ is even => n^2 is even" true? Prove it.

b) Let n = 9866. Is it true or false to say n^2 is even?

a) $n = 2m$, $n \in \mathbb{N}$ (definition of even numbers)

$$n^2 = (2m)^2$$
$$= 4m^2$$
$$= 2(2m^2)$$
$$\therefore n^2 \text{ is even } \square$$

b) Let $n = 9866$,

$$n^2 = (9866)^2$$
$$= 97{,}337{,}956$$
$$\therefore n^2 \text{ is even}$$

Principles of Mathematical Induction

- If p(n) is a statement with $dom_p = \mathbb{N}$ such that
  a) p(1) is true, and
  b) p(k) true => p(k + 1) true,

  Then p(n) is true for all $n \in \mathbb{N}$.

Exercise:
Prove that $4^n - 1$ is a multiple of 3 $\forall\, n \in \mathbb{N}$.

Review this

A: $p(n)$: $4^n - 1$ is a multiple of 3

$$\frac{4^n - 1}{3} = m \text{ for some } m \in \mathbb{Z}$$

$$\Rightarrow 4^n - 1 = 3m$$

$$\Rightarrow 4^n = \underline{3m + 1}$$

very first case of $\mathbb{N}$

a) $p(1)$: $4^1 - 1 = 4 - 1 = 3$, a multiple of 3. (Proved first case)

let $4^k - 1$ be a multiple of 3,

b) $p(k+1)$: $\frac{4^{k+1} - 1}{3}$ is a whole number?

$$\Rightarrow \frac{4^{k+1} - 1}{3} = \frac{4 \cdot 4^k - 1}{3}$$

$$= \frac{4(3m+1) - 1}{3}$$

$$= \frac{12m + 4 - 1}{3}$$

$$= 4m + 1 \in \mathbb{Z} \quad \square$$

whole number in $\mathbb{Z}$

$\therefore 4^n - 1$ is a ~~multiple of~~ 3 for all $n \in \mathbb{N}$

p(k) - any general case

Induction b only applicable to $\mathbb{N}$

The Law of Syllogisms

- Is the following a tautology?

  [([p => q) ∧ (q => r)] => p => r

$\overline{F}$

$\underbrace{\underbrace{(p \Rightarrow q)}_{T} \wedge \underbrace{(q \Rightarrow r)}_{T}}_{T} \quad \underbrace{p \Rightarrow r}_{F}$ → p:T, r:F

T⇒T   T⇏F ⇏T   → q:T, r≠F

This is a tautology.

> **Law of Syllogism**
>
> If p => q and q => r, then p => r

Exercise:
Suppose these 2 statements are true.

a) If it rains today, then I'll drive to school.
b) If I drive to school today, then I'll go over my gas budget.

Then by the law of syllogism, we can infer another truth:

c) If it rains today, then I'll go over my gas budget.

Proving ∃ Statements

- How do we prove a statement of the form?

  ∃ x ∈ D ∋ p(x)

- We need to find at least one x ∈ D that makes p(x) true.

Exercise:
Prove that there exists an even number that can be written in two ways as the sum of two prime numbers.

Find one example that makes p(x) true.

2 = 1 + 1, 4 = 2 + 2, 8 = 5 + 3, 10 = 7 + 3, 5 + 5 ⇒ $\boxed{10}$

Exercise:

Prove $\exists\, x \in \mathbb{R} \ni x + 5 = 0$

If $x = -5$, $(-5) + 5 = 0$ $\square$

Exercise:

Prove there is a month of the year whose name has 3 letters.

May

Proving ∀ Statements

- How do we prove a statement of the form:

  $\forall\, x \in D, p(x)$

- There are two options:
  1) Method of Exhaustion
  2) Generalized Proof

- The method of exhaustion checks that p(x) is true for every $x \in D$.
- This is dine when D is small, but becomes a lot of work for D large.
- If D is infinite, this method fails to be of any use.

Exercise:

Prove that every even number between 4 and 16 can be written as the sum of 2 primes.

$4 = 3 + 1$ $\quad$ $10 = 5 + 5$ $\quad$ $16 = 11 + 5$

$6 = 3 + 3$ $\quad$ $12 = 7 + 5$

$8 = 3 + 5$ $\quad$ $14 = 7 + 7$ $\quad$ $\therefore$ As proven above $\square$

Exercise:

Prove that every even $n \in \mathbb{N}$ can be written as the sum of 2 primes.

$p(n)$: $\forall$ even $n \in \mathbb{N} \ni n = m + n$, $m, n \in \mathbb{P}$.

Let $k = 1$, $n = 2$,

$\Rightarrow 2 = 1 + 1$

$\therefore$ This statement is not true for $n \leq 2$

Trick Question

- The generalized proof is constructed so that it applies to every possible situation.

It takes as many nonspecific elements of D as needed and proves the statement, so that the proof is valid for all elements of D.

Exercise:

Prove that if a, b ∈ ℤ, then 10a + 8b is divisible by 2.

Let $a, b \in \mathbb{Z}$, then $10a + 8b = 2(5a + 4b)$.

Since $a, b \in \mathbb{Z}$, $5a + 4b \in \mathbb{Z}$

$\Rightarrow 2(5a + 4b)$ is even (given even number definition $n = 2m$)

$\therefore 10a + 8b$ is even $\square$

Disproving ∃ Statements

- To disprove a statement means to prove its negation.
- Recall the negation of an existential statement:

~(∃ x ∈ D ∋ p(x)) ≡ ∀ x ∈ D ∋ ~p(x)

- To disprove an ∃ statement, we must prove a ∀ statement, via method of exhaustion or generalized proof.

Exercise:

Disprove the statement "there exists an even prime number larger than 2."

A: $p(n)$: "there exists an even prime number larger than 2"

$\sim p(n)$: "for all prime numbers x larger than 2, x is odd"

Let $x > 2$ be prime.

Suppose x is even, then $x = 2n$ for some $n \in \mathbb{N}$

$$\Rightarrow \frac{x}{2} = \frac{2n}{2} = n,$$

So x is divisible by 2 and is not a prime.

- This is an example of proof by contradiction.

Disproving ∀ Statements

- To disprove a ∀ statement, we must prove an ∃ statement.

~(∀ x ∈ D, p(x)) ≡ ∃ x ∈ D ∋ ~p(x)

- We must find one x ∈ D such that p(x) is false (a counterexample).

Exercise:

Disprove the statement "$\forall x \in \mathbb{R}, x < 0 \vee x > 0$."

$p(n): \forall x \in \mathbb{R}, x < 0 \vee x > 0$

$\sim p(n): \exists x \in \mathbb{R} \ni x \geq 0 \wedge x \leq 0$

Let $x = 0$, then $x \geq 0 \wedge x \leq 0$ $\square$

Exercise:

Disprove the statement "$\forall$ a, b $\in \mathbb{R}$, if $a^2 = b^2$, then a = b.

$\sim p(n): \exists a, b \in \mathbb{R} \ni$ if $a^2 = b^2 \wedge a \neq b$

Let $a = 1$, $b = -1$, then

$\Rightarrow a^2 = b^2 \wedge a \neq b$

$1^2 = (-1)^2 \wedge 1 \neq -1$ $\square$

$\therefore$ The original statement is not true

Exercise:

Prove or disprove: "$\forall$ x $\in \mathbb{R}$, $\exists$ y $\in \mathbb{R}$ $\ni$ x + y = 0."

A: $x + y = 0, \forall x \in \mathbb{R}, \exists y \in \mathbb{R}$

Let $x \in \mathbb{R}$, $y = -x$, then $y \in \mathbb{R}$ and

$\Rightarrow x + y = x + (-x) = 0$ $\square$

Generalized Proof 1: Direct Proof

- A **direct proof** works in a straightforward manner from assumptions to solution.
- We often rewrite assumptions in logical notation.

Exercise:

Prove that if 3x – 9 = 15, then x = 8.

A: $3x - 1 = 15$

$3x = 15 + 1$

$x = \frac{16}{3}$

$x = 8$ $\square$

Exercise:
Prove that the sum of any two even numbers is even.

A: Let a, b be even, then $\exists\, c, d \in \mathbb{Z} \ni a = 2c, b = 2d$

$$a + b = 2c + 2d$$
$$= 2(c+d) \quad c, d \in \mathbb{Z} \Rightarrow c + d \in \mathbb{Z}.$$
$$\Rightarrow a + b = 2e, e \in \mathbb{Z}$$
$\therefore$ a + b is even.

Exercise:
Prove that if a, b are perfect squares, then ab is a perfect square.

($x \in \mathbb{Z}$ is a perfect square if $x = y^2$ for some $y \in \mathbb{Z}$)

A: Let $a, b \in \mathbb{Z}$ be two perfect squares $\exists\, x, y \in \mathbb{Z} \ni a = x^2, b = y^2$

$$ab = x^2 \cdot y^2$$
$$= (xy)^2$$
$\therefore ab = k^2$ where $k \in \mathbb{Z}$ $\square$, ab is a perfect square

Exercise:
Prove that $\forall\, x \in \mathbb{R}, -x^2 + 2x + 1 \leq 2$.

A: $-x^2 + 2x + 1 \leq 2 \iff -x^2 + 2x - 1 \leq 0$
$$\iff x^2 + 2x + 1 \geq 0$$
$$\iff (x-1)^2 \geq 0 \text{ (Tautology)}$$
$\therefore -x^2 + 2x + 1 \leq 2 \ \forall\, x \in \mathbb{R}$

This is always positive

Generalised Proof 2: Proof by Contradiction

Exercise:
Prove that p => q ≡ ~q => ~p

Can do

p	***q***	***p => q***	***~q => ~p***
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

- To prove p => q, one may instead prove ~q => ~p.
- That is, assume that the negation of the conclusion is true, and show that one of the assumptions (or some other well-known truth) is false.

Exercise:

Prove "$\forall$ n $\in \mathbb{N}$, if n^2 is even, then n is even" by contradiction.

$p(n)$: n^2 is even, $n^2 = 2m$

$q(n)$: n is even, $n = 2m$

If $p \Rightarrow q$, we will prove $\sim q \Rightarrow \sim p$

Let n be odd, $\exists m \in \mathbb{Z} \ni n = 2m+1$

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

$\therefore n^2$ is odd

$\therefore n^2$ even $\Rightarrow n$ even $\square$

Exercise:

Prove by contradiction that y $\in \mathbb{R} \setminus \mathbb{Q}$ => y + 7 $\in \mathbb{R} \setminus \mathbb{Q}$. irrationals

A: To prove, assume $y+7 \in \mathbb{Q}$ and show that $y \in \mathbb{Q}$

Let $y+7 \in \mathbb{Q}$, then $\exists a, b \in \mathbb{Z}, b \neq 0 \ni y + 7 = \frac{a}{b}$

$$\begin{aligned} y &= \frac{a}{b} - 7 \\ &= \frac{a}{b} - \frac{7b}{b} \\ &= \frac{a-7b}{b} \in \mathbb{Q} \end{aligned}$$

$\therefore y + 7 \in \mathbb{R} \setminus \mathbb{Q}$

Set minus symbol "\"

{Real numbers} set minus {Rationals} $\therefore$ {irrationals}

Generalized Proof 3: Proof by Cases

- How do we prove "if $x \neq 0$ or $y \neq 0$, then $x^2 + y^2 > 0$"?
- We need to split the problem into cases, proving the conclusion first if $x \neq 0$, the if $y \neq 0$.
- Any statement of the form:

  $(p \vee q) \Rightarrow r$

  Can be done this way, because of the logical equivalence

  $(p \vee q) \Rightarrow r \equiv (p \Rightarrow r) \wedge (q \Rightarrow r)$

Exercise:

Prove "$x \neq 0$ or $y \neq 0 \Rightarrow x^2 + y^2 > 0$."

Case 1: Let $x \neq 0$, then $x^2 > 0$, and $y^2 \geq 0$

$\Rightarrow x^2 + y^2 > 0$

Case 2: Let $y \neq 0$, then $x^2 \geq 0$, and $y^2 > 0$

$\Rightarrow x^2 + y^2 > 0$

$\therefore$ If $x \neq 0$ or $y \neq 0$, then $x^2 + y^2 > 0$

Exercise:

Prove that $\forall m \in \mathbb{N}$, $m^2 + m + 1$ is odd.

Case 1: Let m be even, the m^2 is even.

$\Rightarrow m^2 + m$ is even

$\Rightarrow m^2 + m + 1$ is odd.

Case 2: Let m be odd, then m^2 is odd.

$\Rightarrow m^2 + m$ is even (odd + odd = even)

$\Rightarrow m^2 + m + 1$ is odd.

$\therefore \forall m \in \mathbb{N}$, $m^2 + m + 1$ is odd.